Guía del usuario de la versión 2

AWS Command Line Interface

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Command Line Interface: Guía del usuario de la versión 2

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

..... xv
Acerca del AWS CLI 1
Acerca de la versión 2 de AWS CLI 1
Mantenimiento y compatibilidad de las versiones principales del SDK 2
Acerca de Amazon Web Services 2
Acerca de los ejemplos 3
Documentación y recursos adicionales 4
Documentación y recursos de la AWS CLI 4
Otros AWS SDK y herramientas 5
Introducción 6
Requisitos previos 7
Crear una cuenta administrativa de IAM o del Centro de identidades de IAM 7
Siguientes pasos 8
Instalar o actualizar 9
Instrucciones de instalación y actualización de AWS CLI 9
Solución de errores de instalación y desinstalación de AWS CLI 29
Pasos a seguir a continuación 29
Versiones anteriores 29
Solución de errores de instalación y desinstalación de AWS CLI 45
Pasos a seguir a continuación 46
Compilar e instalar desde el origen 46
¿Por qué compilar desde el origen? 47
Pasos rápidos 47
Paso 1: configurar todos los requisitos 50
Paso 2: configurar la instalación de origen de la AWS CLI 55
Paso 3: compilar la AWS CLI 61
Paso 4: instalar la AWS CLI 62
Paso 5: verificar la instalación de AWS CLI 64
Ejemplos de flujo de trabajo 64
Solución de errores de instalación y desinstalación de AWS CLI 67
Pasos a seguir a continuación 67
Amazon ECR Public/Docker 68
Requisitos previos 68
Decisión entre Amazon ECR Public y Docker Hub 69

Ejecución de las imágenes oficiales ... 69
Notas sobre interfaces y compatibilidad con versiones anteriores de las imágenes oficiales ... 70
Uso de versiones y etiquetas específicas ... 71
Actualización a la imagen oficial más reciente ... 72
Comparta llos archivos anfitrión, credenciales, variables del entorno y configuración ... 72
Acortamiento del comando docker run ... 78
Configuración ... 81
Recopilar su información de credenciales para el acceso programático ... 82
Establecer una nueva configuración y credenciales ... 83
Uso de archivos de configuración y credenciales existentes ... 93
Configuración del AWS CLI ... 94
Prioridad de configuración y credenciales ... 94
Temas adicionales en esta sección ... 95
Opciones de configuración ... 96
Formato de los archivos de configuración y credenciales ... 96
¿Dónde se almacenan las opciones de configuración? ... 105
Uso de perfiles con nombre ... 106
Definir y ver las opciones de configuración mediante comandos ... 106
Establecimiento de una nueva configuración y ejemplos de comandos de credenciales ... 111
Configuraciones del archivo `config` admitidas ... 115
Variables de entorno ... 136
Cómo configurar las variables de entorno ... 137
AWS CLIVariables de entorno que admite la ... 138
Opciones de línea de comandos ... 151
Cómo utilizar las opciones de la línea de comandos ... 151
AWS CLIOpciones de la línea de comandos globales compatibles con ... 152
Usos comunes de las opciones de la línea de comandos ... 157
Finalización de comandos ... 158
Funcionamiento ... 158
Configuración de la finalización de comandos en Linux o macOS ... 159
Configuración de la finalización de comandos en Windows ... 163
Reintentos ... 164
Modos de reintento disponibles ... 164
Configuración de un modo de reintento ... 167
Visualización de registros de reintentos ... 168

Proxies HTTP ... 169
Uso de los ejemplos de la ... 170
Autenticación en un proxy ... 171
Uso de un proxy en instancias Amazon EC2 ... 171
Solución de problemas ... 172
puntos de conexión ... 172
Establecer punto de conexión para un solo comando ... 173
Establecer un punto de conexión global para todos los Servicios de AWS ... 173
Establecer para usar los puntos de conexión de FIPS para todos los Servicios de AWS ... 175
Establecer para utilizar los puntos de conexión de doble pila para todos los Servicios de AWS ... 176
Establecer puntos de conexión específicos del servicio ... 177
Puntos de conexión basados en cuentas ... 181
Prioridad de la configuración y los ajustes del punto de conexión ... 183
Credenciales de autenticación y acceso ... 184
Prioridad de configuración y credenciales ... 186
Temas adicionales en esta sección ... 187
Credenciales de consola ... 187
Requisitos previos ... 188
Inicie sesión en la AWS CLI con el comando `aws login`. ... 188
Ejecución de un comando con el perfil ... 190
Cierre de sesión con el comando de cierre de sesión de AWS ... 191
Solución de problemas ... 192
Recursos relacionados ... 194
Autenticación del Centro de identidades de IAM ... 194
Requisitos previos ... 195
Configurar el perfil con el asistente de `aws configure sso` ... 197
Configurar solo la sección `sso-session` con el asistente de `aws configure sso-session` ... 201
Configuración manual mediante el archivo `config` ... 201
Inicio de sesión en IAM Identity Center ... 204
Ejecución de un comando con el perfil de IAM Identity Center ... 206
Cierre de sesiones de IAM Identity Center ... 206
Solución de problemas ... 206
Recursos relacionados ... 206
Conceptos de IAM Identity Center ... 207

Tutorial: AWS IAM Identity Center y Amazon S3 212
Credenciales a corto plazo 218
Roles de IAM 219
Requisitos previos 220
Información general del uso de roles de IAM 220
Configuración y uso de un rol 221
Uso de MFA 224
Roles entre cuentas e ID externo 225
Especificación de un nombre de sesión de rol para simplificar las auditorías 226
Adopción de un rol con una identidad web 227
Borrado de las credenciales almacenadas en memoria caché 228
Usuarios de IAM 229
Paso 1: Crear el usuario de IAM 229
Paso 2: Obtener las claves de acceso 230
Paso 3: Configurar el AWS CLI 230
(Opcional) Uso de autenticación multifactor con las credenciales de usuario de IAM 232
Metadatos de Amazon EC2 234
Requisitos previos 234
Configuración de un perfil para metadatos de Amazon EC2 234
Credenciales externas 235
Uso de AWS CLI 238
Obtención de ayuda 239
El comando de ayuda de AWS CLI integrado 239
Guía de referencia de AWS CLI 244
Documentación de la API 244
Solución de errores 245
Ayuda adicional 245
Estructura de comandos 246
Estructura de comandos 246
Comandos de espera 247
Especificar valores de parámetros 248
Tipos de parámetros comunes 249
Comillas con cadenas 255
Parámetros de archivos 259
Generar una plantilla de esqueleto de la CLI 263
Sintaxis abreviada 277

Mensaje automático ... 280
Funcionamiento ... 281
Características del mensaje automático ... 281
Modos de mensaje automático ... 284
Configuración del mensaje automático ... 285
Salida del comando de control ... 285
Salida de información confidencial ... 286
Opciones de salida del servidor frente a las del cliente ... 286
Output Format (Formato de salida) ... 287
Paginación ... 297
Filtrar salida ... 303
Códigos de devolución ... 328
Asistentes ... 330
Funcionamiento ... 330
Alias ... 331
Requisitos previos ... 331
Paso 1: Creación del archivo de alias ... 332
Paso 2: Creación de un alias ... 333
Paso 3: Cómo llamar a un alias ... 336
Ejemplos de repositorio de alias ... 338
Recursos ... 339
Errores de solución de problemas ... 340
Solución de problemas generales para probar primero ... 340
Errores de comando no encontrado ... 349
El comando "`aws --version`" devuelve una versión diferente a la instalada ... 352
El comando "`aws --version`" devuelve una versión después de desinstalar la AWS CLI . 353
La AWS CLI ha procesado un comando con un nombre de parámetro incompleto ... 354
Errores de acceso denegado ... 355
Errores de credenciales y claves no válidas ... 356
Errores de firma que no coincide ... 358
Errores de certificado SSL ... 360
Errores de JSON no válido ... 361
Recursos adicionales ... 363
Ejemplos de AWS CLI ... 364
Ejemplos de comandos guiados ... 364
DynamoDB ... 365

Amazon EC2 369
Amazon Glacier 389
IAM 395
Amazon S3 400
Amazon SNS 421
Ejemplos de comando 423
ACM 430
API Gateway 442
API de WebSocket y HTTP de API Gateway 511
API de administración de puertas de enlace de API 565
App Mesh 567
App Runner 613
AWS AppConfig 649
Application Auto Scaling 685
Application Discovery Service 703
Application Signals 710
AppRegistry 732
Athena 744
escalado automático 779
Planes de Auto Scaling 852
AWS Backup 860
AWS Batch 866
AWS Budgets 881
Amazon Chime 892
API de control en la nube 939
AWS Cloud Map 946
AWS Cloud9 984
CloudFormation 993
CloudFront 1058
Amazon CloudSearch 1167
CloudTrail 1168
CloudWatch 1186
Registros de CloudWatch 1222
Monitor de red de CloudWatch 1229
CloudWatch Observability Access Monitor 1242
Administrador de observabilidad de CloudWatch 1254

CloudWatch Synthetics 1260
CodeArtifact 1279
CodeBuild 1309
CodeCommit 1375
CodeDeploy 1451
Revisor CodeGuru 1493
CodePipeline 1513
Notificaciones de AWS CodeStar 1546
CodeConnections 1557
Amazon Cognito Identity 1566
Amazon Cognito Identity Provider 1572
Amazon Comprehend 1723
Amazon Comprehend Medical 1864
AWS Config 1900
Amazon Connect 1925
AWS Cost and Usage Report 1943
Cost Explorer Service 1945
Firehose 1954
Administrador de vida útil de datos de Amazon 1957
AWS Data Pipeline 1963
DataSync 1973
DAX 1978
Detective 1997
Device Farm 2009
Direct Connect 2015
Directory Service 2068
Datos de Directory Service 2071
AWS DMS 2097
Amazon DocumentDB 2142
DynamoDB 2200
DynamoDB Streams 2298
Amazon EC2 2306
Conexión de la instancia Amazon EC2 3008
Amazon ECR 3009
Amazon ECR Public 3041
Amazon ECS 3071

Amazon EFS ... 3199
Amazon EKS ... 3208
Elastic Beanstalk ... 3309
ELB: versión 1 ... 3340
ELB: versión 2 ... 3369
ElastiCache ... 3424
MediaStore ... 3533
Amazon EMR ... 3551
Amazon EMR en EKS ... 3601
EventBridge ... 3603
Canalizaciones de EventBridge ... 3609
Firewall Manager ... 3618
AWS FIS ... 3628
Servidores de Amazon GameLift (Amazon GameLift Servers) ... 3648
Amazon Glacier ... 3682
Global Accelerator ... 3706
AWS Glue ... 3746
GuardDuty ... 3768
AWS Health ... 3789
HealthImaging ... 3797
HealthLake ... 3826
HealthOmics ... 3839
IAM ... 3911
Analizador de acceso de IAM ... 4060
Generador de imágenes ... 4098
Incident Manager ... 4140
Contactos de Incident Manager ... 4164
Amazon Inspector ... 4188
AWS IoT ... 4238
AWS IoT Analytics ... 4428
Asesor de dispositivos ... 4457
AWS IoT data ... 4473
AWS IoT Events ... 4476
AWS IoT Events-Data ... 4502
AWS IoT Greengrass ... 4529
AWS IoT Greengrass V2 ... 4618

Publicación de AWS IoT Jobs SDK 4645
AWS IoT SiteWise 4649
AWS IoT Things Graph 4701
AWS IoT Wireless 4729
Amazon IVS 4768
Chat de Amazon IVS 4814
Transmisión en tiempo real de Amazon IVS 4828
Amazon Kendra 4882
Kinesis 4892
AWS KMS 4912
Lake Formation 4988
Lambda 5041
License Manager 5085
Lightsail 5099
Macie 5227
Amazon Managed Grafana 5232
MediaConnect 5234
MediaConvert 5251
MediaLive 5277
MediaPackage 5283
VOD de MediaPackage 5299
Plano de datos de MediaStore 5311
MediaTailor 5317
MemoryDB 5322
Amazon MSK 5360
Monitor del flujo de red 5369
Administrador de red 5387
OpenSearch Service 5426
Organizations 5440
AWS Outposts 5480
AWS Payment Cryptography 5484
AWS Payment CryptographyPlano de datos de 5505
Amazon Pinpoint 5515
Amazon Polly 5539
Lista de precios de AWS 5546
AWS Private CA 5551

AWS Proton 5559
Amazon RDS 5571
Servicio de datos de Amazon RDS 5775
Información de rendimiento de Amazon RDS 5780
Amazon Redshift 5795
Amazon Rekognition 5878
AWS RAM 5955
Resource Explorer 5980
Resource Groups 6003
API de Resource Groups Tagging 6017
Route 53 6021
Registro de dominios de Route 53 6036
Perfiles de Route 53 6063
Route 53 Resolver 6075
Amazon S3 6121
Amazon S3 Control 6218
Secrets Manager 6235
CSPM de Security Hub 6264
Security Lake 6346
AWS Serverless Application Repository 6382
Service Catalog 6384
Service Quotas 6416
Amazon SES 6427
Escudo 6441
Signer 6458
Snowball Edge 6468
Amazon SNS 6470
Amazon SQS 6493
Storage Gateway 6514
AWS STS 6518
Soporte 6528
Amazon SWF 6542
Systems Manager 6558
Amazon Textract 6739
Amazon Transcribe 6750
Amazon Translate 6795

Trusted Advisor 6797
Verified Permissions 6817
VPC Lattice 6842
AWS WAF Classic 6880
AWS WAF Classic Regional 6886
AWS WAFV2 6892
WorkDocs 6938
Amazon WorkMail 6972
Flujo de mensajes de Amazon WorkMail 6997
WorkSpaces 6999
X-Ray 7015
Ejemplos de script Bash 7033
AWS Batch 7034
AWS Cloud Map 7045
CloudFront 7068
DynamoDB 7077
Amazon EC2 7176
HealthImaging 7334
IAM 7343
AWS KMS 7408
Lightsail 7410
Amazon S3 7418
AWS STS 7450
Seguridad 7454
Protección de los datos 7455
Cifrado de datos 7456
Gestión de identidad y acceso 7456
Público 7457
Autenticación con identidades 7457
Administración del acceso con políticas 7459
Cómo funcionan los Servicios de AWS con IAM 7461
Solución de problemas de identidades y accesos en AWS 7461
Validación de la conformidad 7463
Resiliencia 7464
Seguridad de infraestructuras 7464
Aplicación de una versión mínima de TLS 7465

Guía de migración 7466
Nuevas características y cambios 7466
Nuevas características de AWS CLI versión 2 7467
Cambios importantes entre la AWS CLI versión 1 y la AWS CLI versión 2 7469
Instrucciones de migración 7477
Reemplazo de la versión 1 por la versión 2 7477
Instalación en paralelo 7478
Uso del modo de actualización 7479
Funcionamiento 7479
Limitaciones 7483
Configuración del modo de depuración de actualizaciones 7485
Desinstalar 7486
Solución de errores de instalación y desinstalación de AWS CLI 7490
Historial de documentos 7491

¿Cuál es la de AWS Command Line Interface?

La AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante el uso de comandos en el intérprete de comandos de la línea de comandos. Con una configuración mínima, la AWS CLI le permite comenzar a utilizar comandos de ejecución que implementen una funcionalidad equivalente a la que ofrece la Consola de administración de AWS basada en navegador desde el símbolo del sistema del programa de terminal:

- Shells de Linux: utilice programas de shell comunes, tales como `bash`, `zsh` y `tcsh`, para ejecutar comandos en Linux o macOS.
- Línea de comandos de Windows: en Windows, ejecute comandos en símbolo del programa de Windows o en PowerShell.
- De forma remota: ejecute comandos en las instancias de Amazon Elastic Compute Cloud (Amazon EC2) a través de un programa de terminal remoto, como PuTTY o SSH, o con AWS Systems Manager.

Todas las funciones de administración, gestión y acceso de IaaS (infraestructura como servicio) de AWS de la Consola de administración de AWS están disponibles en la AWS API y la AWS CLI. Las nuevas funcionalidades y servicios de IaaS de AWS proporcionan la funcionalidad completa de la Consola de administración de AWS a través de la API y de la CLI en el momento del lanzamiento o en el plazo de 180 días del lanzamiento.

La AWS CLI proporciona acceso directo a las API públicas de los servicios de AWS. Puede explorar las capacidades de un servicio con la AWS CLI y desarrollar scripts de shell para administrar los recursos. Además de los comandos equivalentes de la API de bajo nivel, varios servicios de AWS ofrecen personalizaciones para la AWS CLI. Las personalizaciones pueden incluir comandos de un nivel superior que simplifican el uso de un servicio con una API compleja.

Acerca de la versión 2 de AWS CLI

La versión 2 de la AWS CLI es la versión principal y más reciente de la AWS CLI y es compatible con todas las características más recientes. Algunas características introducidas en la versión 2 no son compatibles con la versión 1 y debe realizar una actualización para acceder a esas características. Existen algunos cambios “notorios” de la versión 1 que pueden requerir que se modifiquen los

scripts. Para obtener una lista de los cambios notorios que se han producido en la versión 2, consulte Guía de migración para la versión 2 de la AWS CLI.

La versión 2 de la AWS CLI se puede instalar únicamente como un instalador empaquetado. Si bien es posible encontrarla en los administradores de paquetes, estos son paquetes no compatibles y no oficiales que no se generaron ni se administraron mediante AWS. Le recomendamos que solamente instale la AWS CLI desde los puntos de distribución oficiales de AWS, tal y como se indica en esta guía.

Para instalar la versión 2 de la AWS CLI, consulte the section called “Instalar o actualizar”.

Para comprobar la versión instalada actualmente, utilice el siguiente comando:

```
$ aws --version
aws-cli/2.27.41 Python/3.11.6 Linux/5.10.205-195.807.amzn2.x86_64 botocore/1.18.6
```

Para ver el historial de versiones, consulte el Registro de cambios de versión 2 de la AWS CLI en GitHub.

Mantenimiento y compatibilidad de las versiones principales del SDK

Para obtener información sobre el mantenimiento y la compatibilidad con las principales versiones del SDK y sus dependencias subyacentes, consulte lo siguiente en la Guía de Referencia de SDK y herramientas de AWS:

- Política de mantenimiento de SDK y herramientas de AWS
- Matriz de compatibilidad para versiones de SDK y herramientas de AWS

Acerca de Amazon Web Services

Amazon Web Services (AWS) es una colección de servicios de infraestructura digital que los desarrolladores pueden usar cuando desarrollan sus aplicaciones. Estos servicios incluyen recursos informáticos, almacenamiento, bases de datos y sincronización de aplicaciones (mensajería y colas). AWS usa un modelo de servicio de pago por uso. Solo se le cobrará por los servicios que usted, o sus aplicaciones, utilicen. Asimismo, para que AWS sea más accesible como plataforma para

prototipos y experimentos, AWS ofrece un nivel de uso gratuito. En esta capa, los servicios son gratuitos por debajo de determinado nivel de uso. Para obtener más información sobre los costes de AWS y la capa gratuita, consulte Uso de la capa gratuita de AWS. Para obtener una cuenta de AWS, consulte la página de inicio de AWS y elija Create an AWS Account (Crear una cuenta de AWS).

Acerca de los ejemplos de la Guía del usuario de la AWS CLI

Los ejemplos de la AWS Command Line Interface (AWS CLI) que aparecen en esta guía se formatean con las siguientes convenciones:

- Símbolo: el símbolo del sistema utiliza el símbolo de Linux y se muestra como ($). En los comandos específicos de Windows, `C:\>` se utiliza como símbolo del sistema. No incluya el símbolo al escribir comandos.
- Directorio: cuando los comandos se deben ejecutar desde un directorio específico, el nombre del directorio se muestra antes del símbolo de comando.
- Entrada del usuario: el texto del comando que se debe ingresar en la línea de comando se formatea como **`user input`**.
- Texto reemplazable: el texto variable, incluidos los nombres de los recursos que usted elija o los ID generados por los servicios de AWS que deba incluir en los comandos, se formatea como *`texto reemplazable`*. En comandos de varias líneas o comandos en los que se requiere una entrada específica desde el teclado, los comandos de teclado también se pueden mostrar como texto reemplazable.
- Salida: la salida devuelta por los servicios de AWS se muestra bajo la entrada del usuario, y se formatea como `computer output`.

El siguiente ejemplo de comando **`aws configure`** demuestra la entrada del usuario, el texto reemplazable, y la salida:

1. Escriba **`aws configure`** en la línea de comandos y luego presione INTRO.
2. La AWS CLI devuelve líneas de texto, solicitándole que introduzca información adicional.
3. Introduzca cada una de sus claves de acceso y después pulse Intro.
4. A continuación, especifique el nombre de una región de AWS en el formato que se muestra y pulse Intro. Después, vuelva a pulsar Intro para omitir la configuración del formato de salida.
5. El comando Intro final se muestra como texto reemplazable porque no hay entrada del usuario para esa línea.

```
$ aws configure
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
Default region name [None]: us-west-2
Default output format [None]: ENTER
```

El siguiente ejemplo muestra un comando simple con salida. Para usar este ejemplo, introduzca el texto completo del comando (el texto resaltado después del símbolo del sistema) y pulse Intro. El nombre del grupo de seguridad, *my-sg*, se puede sustituir por el nombre del grupo de seguridad deseado. El documento JSON, incluidas las llaves, produce una salida. Si configura la CLI para producir la salida en formado de texto o tabla, se aplicará un formato diferente a la misma. JSON es el formato de salida predeterminado.

```
$ aws ec2 create-security-group --group-name my-sg --description "My security group"
{
    "GroupId": "sg-903004f8"
}
```

Documentación y recursos adicionales para la AWS CLI

Documentación y recursos de la AWS CLI

Además de esta guía del usuario, estos son algunos otros recursos en línea útiles al utilizar la AWS CLI.

- Guía de referencia de la versión 2 de la AWS CLI
- Repositorio de ejemplos de código de scripting en bash de la AWS CLI. Abra los ejemplos de script bash de código abierto. Los ejemplos de script bash están alojados en el Repositorio de ejemplos de código de AWS en GitHub.
- Repositorio GitHub de la AWS CLI Puede ver y adaptar el código fuente de la AWS CLI en GitHub. Únase a la comunidad de usuarios de GitHub para hacernos llegar sus comentarios, solicitar características y realizar aportaciones. Esto también incluye ver y proporcionar ejemplos de comandos para la documentación de la AWS CLI.
- Repositorio de ejemplos de alias de la AWS CLI Puede ver y adaptar ejemplos de alias de la AWS CLI en GitHub.

- Registro de cambios de versión 2 de la AWS CLI

Otros AWS SDK y herramientas

En función de su caso de uso, es posible que desee elegir uno de los AWS SDK o herramientas según sus necesidades:

- Guía de referencia de herramientas y AWS SDK
- AWS SDK para C++
- AWS SDK para Go
- AWS SDK para Java
- AWS SDK para JavaScript
- AWS SDK para Kotlin
- AWS SDK para .NET
- AWS SDK para Python (Boto)
- AWS SDK para PHP
- Herramientas de AWS para PowerShell
- AWS SDK para Ruby
- AWS SDK para Rust
- AWS SDK para SAP ABAP
- AWS SDK para Swift
- AWS Amplify

Introducción al AWS CLI

En este capítulo se explican los primeros pasos para empezar a utilizar la versión 2 de la AWS Command Line Interface (AWS CLI), además de los enlaces a las instrucciones correspondientes.

1. Complete todos los requisitos previos: para acceder a los servicios de AWS con la AWS CLI, necesita como mínimo una Cuenta de AWS y las credenciales de IAM. Para aumentar la seguridad de la cuenta de AWS, le recomendamos que no utilice las credenciales de la cuenta raíz. Debe crear un usuario con privilegio mínimo para proporcionar credenciales de acceso a las tareas que ejecutará en AWS.
2. Para instalar o acceder a la AWS CLI, use uno de los siguientes métodos:
   - (Recomendado) the section called “Instalar o actualizar”.
   - the section called “Versiones anteriores”. La instalación de una versión específica se utiliza principalmente si su equipo alinea las herramientas con una versión específica.
   - the section called “Compilar e instalar desde el origen”. La compilación de la AWS CLI desde el código fuente de GitHub es un método más profundo que utilizan principalmente los clientes que trabajan en plataformas que no admiten directamente nuestros instaladores prediseñados.
   - the section called “Amazon ECR Public/Docker”.
   - Acceder a la versión 2 de AWS CLI en la consola de AWS desde el navegador con AWS CloudShell. Para obtener más información, consulte la Guía del usuario de AWS CloudShell.
3. Cuando tenga acceso a la AWS CLI, configure la AWS CLI con sus credenciales de IAM para usarlas por primera vez.

> **Solución de problemas de instalación o configuración**
>
> Si tiene problemas al instalar, desinstalar o configurar la AWS CLI, consulte the section called “Errores de solución de problemas” para ver los pasos de resolución de problemas.

Temas

- Requisitos previos para utilizar la versión 2 de AWS CLI
- Instalación o actualización de la versión más reciente de AWS CLI
- Instalación de versiones anteriores de la versión 2 de AWS CLI
- Compilación e instalación de la AWS CLI desde el origen

- Ejecución de las imágenes oficiales de Amazon ECR Public o Docker para la AWS CLI
- Configuración de AWS CLI

Requisitos previos para utilizar la versión 2 de AWS CLI

Para acceder a servicios de AWS con la AWS CLI, necesita una Cuenta de AWS con credenciales de IAM o de IAM Identity Center. Cuando se ejecutan comandos de AWS CLI, AWS CLI necesita tener acceso a esas credenciales de AWS. Para aumentar la seguridad de la cuenta de AWS, le recomendamos que utilice credenciales de corta duración cuando utilice usuarios raíz o de IAM. Debe crear un usuario con privilegio mínimo para proporcionar credenciales de acceso a las tareas que ejecutará en AWS. Para obtener información sobre las prácticas recomendadas, consulte Prácticas recomendadas de seguridad en la Guía del usuario de IAM.

Temas

- Crear una cuenta administrativa de IAM o del Centro de identidades de IAM
- Siguientes pasos

Crear una cuenta administrativa de IAM o del Centro de identidades de IAM

Para poder configurar la AWS CLI, debe crear una cuenta de IAM o IAM Identity Center.

Opciones de creación de cuentas

Elección de una forma de administrar las credenciales	Para	Cómo crear una cuenta	Cómo configurar el acceso mediante programación a la cuenta
Credenciales de la consola de administración de AWS	Use credenciales a corto plazo correspondientes al usuario raíz creadas durante la configuración inicial de la cuenta, un usuario de IAM o una identidad federada	Abra https://portal.aws.amazon.com/billing/signup y siga las instrucciones en línea.	No hace falta realizar ningún otro paso. Consulta de Inicio de sesión para el desarrollo local de AWS con credenciales de consola para iniciar sesión en

Elección de una forma de administrar las credenciales	Para	Cómo crear una cuenta	Cómo configurar el acceso mediante programación a la cuenta
	del proveedor de identidades.		la AWS CLI con la cuenta de AWS
IAM Identity Center	Use credencia les a corto plazo para acceder a los servicios de AWS.	Siga las instrucciones en Introducción de la Guía del usuario de AWS IAM Identity Center.	Configure el acceso mediante programac ión configurando el uso en la Guía del usuario de AWS IAM Identity Center.
AWS Identity and Access Management (No recomendado)	Use credencia les a largo plazo para acceder a los servicios de AWS.	Siga las instrucciones de Crear para acceso de emergencia de la Guía del usuario de IAM.	Configure el acceso mediante programac ión a través de Administrar las claves de acceso de los usuarios de IAM en la Guía del usuario de IAM.

Siguientes pasos

Después de crear una Cuenta de AWS y credenciales de IAM, para utilizar la AWS CLI puede realizar alguna de las operaciones siguientes:

- Instalar la versión más reciente de la versión 2 de AWS CLI en la computadora.
- Instalar una versión antigua de la versión 2 de AWS CLI en la computadora.
- Acceder a la versión 2 de AWS CLI desde la computadora mediante una imagen de Docker.
- Acceder a la versión 2 de AWS CLI en la consola de AWS desde el navegador con AWS CloudShell. Para obtener más información, consulte la Guía del usuario de AWS CloudShell.

Instalación o actualización de la versión más reciente de AWS CLI

En este tema se describe cómo instalar o actualizar la última versión de AWS Command Line Interface (AWS CLI) en sistemas operativos compatibles. Para obtener información sobre los lanzamientos más recientes de AWS CLI, consulte el registro de cambios de la versión 2 de la AWS CLI en GitHub.

Para instalar una versión anterior de la AWS CLI, consulte the section called “Versiones anteriores”. Para obtener instrucciones de desinstalación, consulte Desinstalar.

> **Important**
>
> Las versiones 1 y 2 de la AWS CLI utilizan el mismo nombre de comando de `aws`. Si ha instalado previamente la AWS CLI versión 1, consulte Guía de migración para la versión 2 de la AWS CLI.

Temas

- Instrucciones de instalación y actualización de AWS CLI
- Solución de errores de instalación y desinstalación de AWS CLI
- Pasos a seguir a continuación

Instrucciones de instalación y actualización de AWS CLI

Para obtener las instrucciones de instalación, amplíe la sección para el sistema operativo.

Linux

Requisitos de instalación y actualización

- Debe poder extraer o “descomprimir” el paquete descargado. Si el sistema operativo no tiene el comando `unzip` integrado, utiliza un equivalente.
- Los AWS CLI usa `glibc`, `groff` y `less`. Estos se incluyen de forma predeterminada en la mayoría de las distribuciones principales de Linux.
- Admitimos AWS CLI en las versiones de 64 bits de las distribuciones recientes de CentOS, Fedora, Ubuntu, Amazon Linux 1, Amazon Linux 2, Amazon Linux 2023 y Linux ARM.

- Debido a que AWS no mantiene los repositorios de terceros excepto `snap`, no podemos garantizar que contengan la versión más reciente de AWS CLI.

Instalación o actualización de AWS CLI

> **Warning**
>
> Si es la primera vez que actualiza en Amazon Linux, para instalar la versión más reciente de la AWS CLI, debe desinstalar la versión de `yum` instalada previamente mediante el siguiente comando:
>
> ```
> $ sudo yum remove awscli
> ```
>
> Después de que la instalación `yum` de la AWS CLI se haya eliminado, siga las instrucciones de instalación de Linux que se muestran a continuación.

Para instalar la AWS CLI, puede seguir uno de los siguientes métodos:

- El instalador de línea de comandos es una buena opción para el control de versiones, ya que puede especificar la versión que se va a instalar. Esta opción no se actualiza automáticamente y debe descargar un nuevo instalador cada vez que actualice para sobrescribir la versión anterior.
- El paquete **`snap`** compatible oficialmente es una buena opción para tener siempre la versión más reciente de la AWS CLI ya que los paquetes snap se actualizan automáticamente. No se ha integrado compatibilidad para seleccionar versiones secundarias de AWS CLI y, por lo tanto, no es un método de instalación óptimo si su equipo tiene que fijar versiones.

Command line installer - Linux x86 (64-bit)

Para actualizar la instalación actual de la AWS CLI en Windows, descargue un nuevo instalador cada vez que actualice para sobrescribir las versiones anteriores. Siga estos pasos desde la línea de comandos para instalar la AWS CLI en Linux.

A continuación, se presentan los pasos de instalación rápida en un solo grupo de copiar y pegar que proporcionan una instalación básica. Para obtener instrucciones guiadas, consulte los pasos a continuación.

> **Note**
>
> (Opcional) El siguiente bloque de comandos descarga e instala la AWS CLI sin verificar primero la integridad de la descarga. Para verificar la integridad de la descarga, siga las instrucciones paso a paso que se muestran a continuación.

Para instalar la AWS CLI, ejecute los siguientes comandos.

```
$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install
```

Para actualizar la instalación actual de la AWS CLI, agregue la información del enlace simbólico y del instalador existentes para construir el comando `install` con los parámetros `--bin-dir`, `--install-dir` y `--update`. El siguiente bloque de comandos utiliza un enlace simbólico de ejemplo de */usr/local/bin* y una ubicación de instalador de ejemplo de */usr/local/aws-cli* para instalar la AWS CLI localmente para el usuario actual.

```
$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install --bin-dir /usr/local/bin --install-dir /usr/local/aws-cli --
update
```

Pasos de la instalación guiada

1. Descargue el archivo de instalación de una de las siguientes maneras:

   - Use el comando **`curl`**: la opción `-o` especifica el nombre de archivo en el que se escribe el paquete descargado. Las opciones del comando de ejemplo siguiente escriben el archivo descargado en el directorio actual con el nombre local `awscliv2.zip`.

     ```
     $ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o
      "awscliv2.zip"
     ```

   - Descarga de la URL: para descargar el instalador con el navegador, utilice la URL siguiente: https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip

2. (Opcional) Verificación de la integridad del archivo zip descargado

Si eligió descargar manualmente el paquete del instalador de AWS CLI `.zip` en los pasos indicados anteriormente, puede usar los pasos siguientes para verificar las firmas mediante la herramienta GnuPG.

Los archivos `.zip` del paquete del instalador de la AWS CLI están firmados criptográficamente mediante firmas PGP. Si hay algún tipo de daño o alteración en los archivos, esta verificación produce un error, por lo que no debería continuar con la instalación.

a. Descargue e instale el comando gpg usando su administrador de paquetes. Para obtener más información acerca de GnuPG, consulte el sitio web de GnuPG.

b. Para crear el archivo de clave pública, cree un archivo de texto y pegue el siguiente texto en él:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBF2Cr7UBEADJZHcgusOJl7ENSyumXh85z0TRV0xJorM2B/JL0kHOyigQluUG
ZMLhENaG0bYatdrKP+3H91lvK050pXwnO/R7fB/FSTouki4ciIx5OuLlnJZIxSzx
PqGl0mkxImLNbGWoi6Lto0LYxqHN2iQtzlwTVmq9733zd3XfcXrZ3+LblHAgEt5G
TfNxEKJ8soPLyWmwDH6HWCnjZ/aIQRBTIQ05uVeEoYxSh6wOai7ss/KveoSNBbYz
gbdzoqI2Y8cgH2nbfgp3DSasaLZEdCSsIsK1u05CinE7k2qZ7KgKAUIcT/cR/grk
C6VwsnDU0OUCideXcQ8WeHutqvgZH1JgKDbznoIzeQHJD238GEu+eKhRHcz8/jeG
94zkcgJOz3KbZGYMiTh277Fvj9zzvZsbMBCedV1BTg3TqgvdX4bdkhf5cH+7NtWO
lrFj6UwAsGukBTAOxC0l/dnSmZhJ7Z1KmEWilro/gOrjtOxqRQutlIqG22TaqoPG
fYVN+en3Zwbt97kcgZDwqbuykNt64oZWc4XKCa3mprEGC3IbJTBFqglXmZ7l9ywG
EEUJYOlb2XrSuPWml39beWdKM8kzr1OjnlOm6+lpTRCBfo0wa9F8YZRhHPAkwKkX
XDeOGpWRj4ohOx0d2GWkyV5xyN14p2tQOCdOODmz80yUTgRpPVQUtOEhXQARAQAB
tCFBV1MgQ0xJIFRlYW0gPGF3cy1jbGlAYW1hem9uLmNvbT6JAlQEEwEIAD4CGwMF
CwkIBwIGFQoJCAsCBBYCAwECHgECF4AWIQT7Xbd/1cEYuAURraimMQrMRnJHXAUC
aGveYQUJDMpiLAAKCRCmMQrMRnJHXKBYD/9Ab0qQdGiO5hObchG8xh8Rpb4Mjyf6
0JrVo6m8GNjNj6BHkSc8fuTQJ/FaEhaQxj3pjZ3GXPrXjIIVChmICLlFuRXYzrXc
Pw0lniybypsZEVai5kO0tCNBCCFuMN9RsmmRG8mf7lC4FSTbUDmxG/QlYK+0IV/l
uJkzxWa+rySkdpm0JdqumjegNRgObdXHAQDWlubWQHWyZyIQ2B4U7AxqSpcdJp6I
S4Zds4wVLd1WE5pquYQ8vS2cNlDm4QNg8wTj58e3lKN47hXHMIb6CHxRnb947oJa
pg189LLPR5koh+EorNkA1wu5mAJtJvy5YMsppy2y/kIjp3lyY6AmPT1posgGk70Z
CmToEZ5rbd7AREXtlh76A0cabMDFlEHDIK8RNUOSRr7L64+KxOUegKBfQHb9dADY
qqiKqpCbKgvtWlds909Ms74JBgr2KwZCSY1HaOxnIr4CY43QRqAq5YHOay/mU+6w
hhmdF18vpyK0vfkvvGresWtSXbag7Hkt3XjaEw76BzxQH21EBDqU8WJVjHgU6ru+
DJTs+SxgJbaT3hb/vyjlw0lK+hFfhWKRwgOXH8vqducF95NRSUxtS4fpqxWVaw3Q
V2OWSjbne99A5EPEySzryFTKbMGwaTlAwMCwYevt4YT6eb7NmFhTx0Fis4TalUs+
j+c7Kg92pDx2uQ==
```

```
=OBAt
-----END PGP PUBLIC KEY BLOCK-----
```

Como referencia, a continuación se indican los detalles de la clave pública.

```
Key ID:           A6310ACC4672475C
Type:             RSA
Size:             4096/4096
Created:          2019-09-18
Expires:          2026-07-07
User ID:          AWS CLI Team <aws-cli@amazon.com>
Key fingerprint:  FB5D B77F D5C1 18B8 0511  ADA8 A631 0ACC 4672 475C
```

c. Importe la clave pública de la AWS CLI con el siguiente comando, sustituyendo *public-key-file-name* por el nombre del archivo de la clave pública que ha creado.

```
$ gpg --import public-key-file-name
gpg: /home/username/.gnupg/trustdb.gpg: trustdb created
gpg: key A6310ACC4672475C: public key "AWS CLI Team <aws-cli@amazon.com>"
 imported
gpg: Total number processed: 1
gpg:               imported: 1
```

d. Descargue el archivo de firma de la AWS CLI del paquete que descargó. Tiene la misma ruta y el mismo nombre que el archivo `.zip` al que corresponde, pero con la extensión `.sig`. En los siguientes ejemplos, lo guardaremos en el directorio actual como un archivo llamado `awscliv2.sig`.

   Para obtener la última versión de la AWS CLI, utilice el siguiente bloque de comandos.

```
$ curl -o awscliv2.sig https://awscli.amazonaws.com/awscli-exe-linux-
x86_64.zip.sig
```

e. Verifique la firma pasando los nombres de archivo `.sig` y `.zip` como parámetros al comando `gpg`.

```
$ gpg --verify awscliv2.sig awscliv2.zip
```

   El resultado de debería parecerse al siguiente.

```
gpg: Signature made Mon Nov  4 19:00:01 2019 PST
```

```
gpg:                using RSA key FB5D B77F D5C1 18B8 0511 ADA8 A631 0ACC
 4672 475C
gpg: Good signature from "AWS CLI Team <aws-cli@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
 owner.
Primary key fingerprint: FB5D B77F D5C1 18B8 0511  ADA8 A631 0ACC 4672 475C
```

> **Important**
>
> Se espera la advertencia en la salida y ello no indica un problema. Esto se produce porque no existe una cadena de confianza entre su clave PGP personal (si es su caso) y la clave PGP de la AWS CLI. Para obtener más información, consulta Red de confianza.

3. Descomprima el instalador. Si su distribución de Linux no tiene un comando `unzip` integrado, use un equivalente para descomprimirlo. El siguiente comando de ejemplo descomprime el paquete y crea un directorio denominado `aws` en el directorio actual.

```
$ unzip awscliv2.zip
```

> **Note**
>
> Al actualizar desde una versión anterior, el comando `unzip` solicita sobrescribir los archivos existentes. Para omitir estas instrucciones, por ejemplo, en el caso de la automatización de scripts, utilice la marca de actualización `-u` para `unzip`. Este indicador actualiza automáticamente los archivos existentes y crea otros nuevos según sea necesario.
>
> ```
> $ unzip -u awscliv2.zip
> ```

4. Ejecute el programa de instalación. El comando de instalación utiliza un archivo denominado `install` en el directorio `aws` recién descomprimido. De forma predeterminada, todos los archivos se instalan en `/usr/local/aws-cli` y se crea un enlace simbólico en `/usr/local/bin`. El comando incluye `sudo` para conceder permisos de escritura en esos directorios.

```
$ sudo ./aws/install
```

Puede realizar la instalación sin `sudo` si especifica directorios en los que ya tiene permisos de escritura. Utilice las siguientes instrucciones en el comando `install` para especificar la ubicación de instalación:

- Asegúrese de que las rutas que proporcione a los parámetros `-i` y `-b` no contengan nombres de volumen ni nombres de directorio que contengan caracteres de espacio u otros caracteres de espacio en blanco. Si hay un espacio, la instalación falla.
- `--install-dir` o `-i`: esta opción especifica el directorio en la que se copiarán todos los archivos.

  El valor predeterminado es `/usr/local/aws-cli`.
- `--bin-dir` o `-b`: esta opción especifica que el programa de `aws` principal del directorio de instalación está vinculado de forma simbólica al archivo `aws` en la ruta de acceso especificada. Debe tener permisos de escritura en el directorio especificado. Al crear un enlace simbólico a un directorio que ya está en su ruta, se elimina la necesidad de agregar el directorio de instalación a la variable $PATH del usuario.

  El valor predeterminado es `/usr/local/bin`.

```
$ ./aws/install -i /usr/local/aws-cli -b /usr/local/bin
```

> **Note**
>
> Para actualizar la instalación actual de AWS CLI, agregue la información del enlace simbólico y del instalador para construir el comando `install` con el parámetro `--update`.
>
> ```
> $ sudo ./aws/install --bin-dir /usr/local/bin --install-dir /usr/local/aws-cli --update
> ```
>
> Para localizar el enlace simbólico y el directorio de instalación existentes, siga los siguientes pasos:

1. Utilice el comando `which` para buscar el enlace simbólico. Esto le dará la ruta que puede utilizar con el parámetro `--bin-dir`.

```
$ which aws
/usr/local/bin/aws
```

2. Utilice el comando `ls` para buscar el directorio al que apunta el enlace simbólico. Esto le dará la ruta que puede utilizar con el parámetro `--install-dir`.

```
$ ls -l /usr/local/bin/aws
lrwxrwxrwx 1 ec2-user ec2-user 49 Oct 22 09:49 /usr/local/bin/aws -> /
usr/local/aws-cli/v2/current/bin/aws
```

5. Confirme la instalación con el siguiente comando.

```
$ aws --version
aws-cli/2.27.41 Python/3.11.6 Linux/5.10.205-195.807.amzn2.x86_64
```

Si no se encuentra el comando `aws`, es posible que deba reiniciar el terminal o seguir el proceso de solución de problemas en the section called “Errores de solución de problemas”.

Command line - Linux ARM

Para actualizar la instalación actual de la AWS CLI en Windows, descargue un nuevo instalador cada vez que actualice para sobrescribir las versiones anteriores. Siga estos pasos desde la línea de comandos para instalar la AWS CLI en Linux.

A continuación, se presentan los pasos de instalación rápida en un solo grupo de copiar y pegar que proporcionan una instalación básica. Para obtener instrucciones guiadas, consulte los pasos a continuación.

> **Note**
>
> (Opcional) El siguiente bloque de comandos descarga e instala la AWS CLI sin verificar primero la integridad de la descarga. Para verificar la integridad de la descarga, siga las instrucciones paso a paso que se muestran a continuación.

Para instalar la AWS CLI, ejecute los siguientes comandos.

```
$ curl "https://awscli.amazonaws.com/awscli-exe-linux-aarch64.zip" -o "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install
```

Para actualizar la instalación actual de la AWS CLI, agregue la información del enlace simbólico y del instalador existentes para construir el comando `install` con los parámetros `--bin-dir`, `--install-dir` y `--update`. El siguiente bloque de comandos utiliza un enlace simbólico de ejemplo de */usr/local/bin* y una ubicación de instalador de ejemplo de */usr/local/aws-cli*.

```
$ curl "https://awscli.amazonaws.com/awscli-exe-linux-aarch64.zip" -o "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install --bin-dir /usr/local/bin --install-dir /usr/local/aws-cli --
update
```

Pasos de la instalación guiada

1. Descargue el archivo de instalación de una de las siguientes maneras:

   - Use el comando **`curl`**: la opción `-o` especifica el nombre de archivo en el que se escribe el paquete descargado. Las opciones del comando de ejemplo siguiente escriben el archivo descargado en el directorio actual con el nombre local `awscliv2.zip`.

     ```
     $ curl "https://awscli.amazonaws.com/awscli-exe-linux-aarch64.zip" -o
      "awscliv2.zip"
     ```

   - Descarga de la URL: para descargar el instalador con el navegador, utilice la URL siguiente: https://awscli.amazonaws.com/awscli-exe-linux-aarch64.zip

2. (Opcional) Verificación de la integridad del archivo zip descargado

   Si eligió descargar manualmente el paquete del instalador de AWS CLI `.zip` en los pasos indicados anteriormente, puede usar los pasos siguientes para verificar las firmas mediante la herramienta `GnuPG`.

   Los archivos `.zip` del paquete del instalador de la AWS CLI están firmados criptográficamente mediante firmas PGP. Si hay algún tipo de daño o alteración en

los archivos, esta verificación produce un error, por lo que no debería continuar con la instalación.

a. Descargue e instale el comando gpg usando su administrador de paquetes. Para obtener más información acerca de GnuPG, consulte el sitio web de GnuPG.

b. Para crear el archivo de clave pública, cree un archivo de texto y pegue el siguiente texto en él:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBF2Cr7UBEADJZHcgusOJl7ENSyumXh85z0TRV0xJorM2B/JL0kHOyigQluUG
ZMLhENaG0bYatdrKP+3H91lvK050pXwnO/R7fB/FSTouki4ciIx5OuLlnJZIxSzx
PqGl0mkxImLNbGWoi6Lto0LYxqHN2iQtzlwTVmq9733zd3XfcXrZ3+LblHAgEt5G
TfNxEKJ8soPLyWmwDH6HWCnjZ/aIQRBTIQ05uVeEoYxSh6wOai7ss/KveoSNBbYz
gbdzoqI2Y8cgH2nbfgp3DSasaLZEdCSsIsK1u05CinE7k2qZ7KgKAUIcT/cR/grk
C6VwsnDU0OUCideXcQ8WeHutqvgZH1JgKDbznoIzeQHJD238GEu+eKhRHcz8/jeG
94zkcgJOz3KbZGYMiTh277Fvj9zzvZsbMBCedV1BTg3TqgvdX4bdkhf5cH+7NtWO
lrFj6UwAsGukBTAOxC0l/dnSmZhJ7Z1KmEWilro/gOrjtOxqRQutlIqG22TaqoPG
fYVN+en3Zwbt97kcgZDwqbuykNt64oZWc4XKCa3mprEGC3IbJTBFqglXmZ7l9ywG
EEUJYOlb2XrSuPWml39beWdKM8kzr1OjnlOm6+lpTRCBfo0wa9F8YZRhHPAkwKkX
XDeOGpWRj4ohOx0d2GWkyV5xyN14p2tQOCdOODmz80yUTgRpPVQUtOEhXQARAQAB
tCFBV1MgQ0xJIFRlYW0gPGF3cy1jbGlAYW1hem9uLmNvbT6JAlQEEwEIAD4CGwMF
CwkIBwIGFQoJCAsCBBYCAwECHgECF4AWIQT7Xbd/1cEYuAURraimMQrMRnJHXAUC
aGveYQUJDMpiLAAKCRCmMQrMRnJHXKBYD/9Ab0qQdGiO5hObchG8xh8Rpb4Mjyf6
0JrVo6m8GNjNj6BHkSc8fuTQJ/FaEhaQxj3pjZ3GXPrXjIIVChmICLlFuRXYzrXc
Pw0lniybypsZEVai5kO0tCNBCCFuMN9RsmmRG8mf7lC4FSTbUDmxG/QlYK+0IV/l
uJkzxWa+rySkdpm0JdqumjegNRgObdXHAQDWlubWQHWyZyIQ2B4U7AxqSpcdJp6I
S4Zds4wVLd1WE5pquYQ8vS2cNlDm4QNg8wTj58e3lKN47hXHMIb6CHxRnb947oJa
pg189LLPR5koh+EorNkA1wu5mAJtJvy5YMsppy2y/kIjp3lyY6AmPT1posgGk70Z
CmToEZ5rbd7AREXtlh76A0cabMDFlEHDIK8RNUOSRr7L64+KxOUegKBfQHb9dADY
qqiKqpCbKgvtWlds909Ms74JBgr2KwZCSY1HaOxnIr4CY43QRqAq5YHOay/mU+6w
hhmdF18vpyK0vfkvvGresWtSXbag7Hkt3XjaEw76BzxQH21EBDqU8WJVjHgU6ru+
DJTs+SxgJbaT3hb/vyjlw0lK+hFfhWKRwgOXH8vqducF95NRSUxtS4fpqxWVaw3Q
V2OWSjbne99A5EPEySzryFTKbMGwaTlAwMCwYevt4YT6eb7NmFhTx0Fis4TalUs+
j+c7Kg92pDx2uQ==
=OBAt
-----END PGP PUBLIC KEY BLOCK-----
```

Como referencia, a continuación se indican los detalles de la clave pública.

```
Key ID:          A6310ACC4672475C
Type:            RSA
```

```
Size:              4096/4096
Created:           2019-09-18
Expires:           2026-07-07
User ID:           AWS CLI Team <aws-cli@amazon.com>
Key fingerprint:  FB5D B77F D5C1 18B8 0511  ADA8 A631 0ACC 4672 475C
```

c. Importe la clave pública de la AWS CLI con el siguiente comando, sustituyendo *public-key-file-name* por el nombre del archivo de la clave pública que ha creado.

```
$ gpg --import public-key-file-name
gpg: /home/username/.gnupg/trustdb.gpg: trustdb created
gpg: key A6310ACC4672475C: public key "AWS CLI Team <aws-cli@amazon.com>"
 imported
gpg: Total number processed: 1
gpg:               imported: 1
```

d. Descargue el archivo de firma de la AWS CLI del paquete que descargó. Tiene la misma ruta y el mismo nombre que el archivo `.zip` al que corresponde, pero con la extensión `.sig`. En los siguientes ejemplos, lo guardaremos en el directorio actual como un archivo llamado `awscliv2.sig`.

Para obtener la última versión de la AWS CLI, utilice el siguiente bloque de comandos.

```
$ curl -o awscliv2.sig https://awscli.amazonaws.com/awscli-exe-linux-
aarch64.zip.sig
```

e. Verifique la firma pasando los nombres de archivo `.sig` y `.zip` como parámetros al comando gpg.

```
$ gpg --verify awscliv2.sig awscliv2.zip
```

El resultado de debería parecerse al siguiente.

```
gpg: Signature made Mon Nov  4 19:00:01 2019 PST
gpg:                using RSA key FB5D B77F D5C1 18B8 0511 ADA8 A631 0ACC
 4672 475C
gpg: Good signature from "AWS CLI Team <aws-cli@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
 owner.
Primary key fingerprint: FB5D B77F D5C1 18B8 0511  ADA8 A631 0ACC 4672 475C
```

> **Important**
>
> Se espera la advertencia en la salida y ello no indica un problema. Esto se produce porque no existe una cadena de confianza entre su clave PGP personal (si es su caso) y la clave PGP de la AWS CLI. Para obtener más información, consulta Red de confianza.

3. Descomprima el instalador. Si su distribución de Linux no tiene un comando `unzip` integrado, use un equivalente para descomprimirlo. El siguiente comando de ejemplo descomprime el paquete y crea un directorio denominado `aws` en el directorio actual.

```
$ unzip awscliv2.zip
```

> **Note**
>
> Al actualizar desde una versión anterior, el comando `unzip` solicita sobrescribir los archivos existentes. Para omitir estas instrucciones, por ejemplo, en el caso de la automatización de scripts, utilice la marca de actualización `-u` para `unzip`. Este indicador actualiza automáticamente los archivos existentes y crea otros nuevos según sea necesario.
>
> ```
> $ unzip -u awscliv2.zip
> ```

4. Ejecute el programa de instalación. El comando de instalación utiliza un archivo denominado `install` en el directorio `aws` recién descomprimido. De forma predeterminada, todos los archivos se instalan en `/usr/local/aws-cli` y se crea un enlace simbólico en `/usr/local/bin`. El comando incluye `sudo` para conceder permisos de escritura en esos directorios.

```
$ sudo ./aws/install
```

Puede realizar la instalación sin `sudo` si especifica directorios en los que ya tiene permisos de escritura. Utilice las siguientes instrucciones en el comando `install` para especificar la ubicación de instalación:

- Asegúrese de que las rutas que proporcione a los parámetros `-i` y `-b` no contengan nombres de volumen ni nombres de directorio que contengan caracteres de espacio u otros caracteres de espacio en blanco. Si hay un espacio, la instalación falla.
- `--install-dir` o `-i`: esta opción especifica el directorio en la que se copiarán todos los archivos.

  El valor predeterminado es `/usr/local/aws-cli`.
- `--bin-dir` o `-b`: esta opción especifica que el programa de `aws` principal del directorio de instalación está vinculado de forma simbólica al archivo `aws` en la ruta de acceso especificada. Debe tener permisos de escritura en el directorio especificado. Al crear un enlace simbólico a un directorio que ya está en su ruta, se elimina la necesidad de agregar el directorio de instalación a la variable $PATH del usuario.

  El valor predeterminado es `/usr/local/bin`.

```
$ ./aws/install -i /usr/local/aws-cli -b /usr/local/bin
```

> **Note**
>
> Para actualizar la instalación actual de AWS CLI, agregue la información del enlace simbólico y del instalador para construir el comando `install` con el parámetro `--update`.
>
> ```
> $ sudo ./aws/install --bin-dir /usr/local/bin --install-dir /usr/local/aws-cli --update
> ```
>
> Para localizar el enlace simbólico y el directorio de instalación existentes, siga los siguientes pasos:
>
> 1. Utilice el comando `which` para buscar el enlace simbólico. Esto le dará la ruta que puede utilizar con el parámetro `--bin-dir`.
>
>    ```
>    $ which aws
>    /usr/local/bin/aws
>    ```
> 2. Utilice el comando `ls` para buscar el directorio al que apunta el enlace simbólico. Esto le dará la ruta que puede utilizar con el parámetro `--install-dir`.

```
$ ls -l /usr/local/bin/aws
lrwxrwxrwx 1 ec2-user ec2-user 49 Oct 22 09:49 /usr/local/bin/aws -> /
usr/local/aws-cli/v2/current/bin/aws
```

5. Confirme la instalación con el siguiente comando.

```
$ aws --version
aws-cli/2.27.41 Python/3.11.6 Linux/5.10.205-195.807.amzn2.x86_64
```

Si no se encuentra el comando `aws`, es posible que deba reiniciar el terminal o seguir el proceso de solución de problemas en the section called “Errores de solución de problemas”.

Snap package

Proporcionamos una versión oficial de AWS compatible de la AWS CLI en `snap`. Si desea tener siempre instalada la versión más reciente de AWS CLI en su sistema, se la proporciona un paquete snap que se actualiza automáticamente. No se ha integrado compatibilidad para seleccionar versiones secundarias de AWS CLI y, por lo tanto, no es un método de instalación óptimo si su equipo tiene que fijar versiones. Si desea instalar una versión secundaria específica de la AWS CLI, le sugerimos que utilice el instalador de línea de comandos.

1. Si su plataforma Linux aún no tiene `snap` instalado, instale `snap` en su plataforma.

   a. Para obtener información sobre la instalación de `snap`, consulte Installing the daemon en la documentación de Snap.

   b. Puede que tenga que reiniciar el sistema para que las variables `PATH` se actualicen correctamente. Si tiene problemas durante la instalación, siga los pasos que se indican en la sección Fix common issues de la documentación de Snap.

   c. Para comprobar que `snap` se haya instalado correctamente, ejecute el siguiente comando.

   ```
   $ snap version
   ```

2. Ejecute el siguiente comando `snap install` para la AWS CLI.

```
$ snap install aws-cli --classic
```

En función de los permisos, es posible que tenga añadir `sudo` al comando.

```
$ sudo snap install aws-cli --classic
```

> **Note**
>
> Para ver el repositorio de snap de la AWS CLI, incluidas las instrucciones de `snap` adicionales, consulte la página `aws-cli` del sitio web de Canonical Snapcraft.

3. Compruebe que AWS CLI se ha instalado correctamente.

```
$ aws --version
aws-cli/2.27.41 Python/3.11.6 Linux/5.10.205-195.807.amzn2.x86_64
```

Si obtiene un error, consulte Solución de errores para la AWS CLI.

macOS

Requisitos de instalación y actualización

- Admitimos la AWS CLI en las versiones 11 y posteriores de macOS. Para obtener más información, consulte las actualizaciones de la política de compatibilidad de macOS para la versión 2 de AWS CLI en el blog de herramientas para desarrolladores de AWS.
- Debido a que AWS no mantiene repositorios de terceros, no podemos garantizar que contengan la última versión de AWS CLI.

Matriz de compatibilidad con versiones de macOS

Versión de AWS CLI	Versión de macOS compatible
2.21.0 - actual	11+
2.17.0 - 2.20.0	10.15+
2.0.0 - 2.16.12	10.14 y anteriores

Instalación o actualización de AWS CLI

Si va a actualizar a la versión más reciente, utilice el mismo método de instalación que utilizó en la versión actual. Puede instalar AWS CLI en macOS de las siguientes maneras.

GUI installer

En los pasos siguientes se muestra cómo instalar la versión más reciente de AWS CLI mediante la interfaz de usuario estándar de macOS y el navegador.

1. En el navegador, descargue el archivo `pkg` de macOS: https://awscli.amazonaws.com/AWSCLIV2.pkg
2. Ejecute el archivo descargado y siga las instrucciones que aparecen en pantalla. Puede elegir instalar la AWS CLI de las siguientes maneras:

   - Para todos los usuarios del equipo (requiere **sudo**)
     - Puede realizar la instalación en cualquier carpeta o elegir la carpeta predeterminada recomendada de `/usr/local/aws-cli`.
     - El instalador crea automáticamente un enlace simbólico en `/usr/local/bin/aws` que enlaza al programa principal en la carpeta de instalación elegida.
   - Solo para el usuario actual (no requiere **sudo**)
     - Puede realizar la instalación en cualquier carpeta en la que tenga permiso de escritura.
     - Debido a los permisos de usuario estándar, una vez finalizado el instalador, debe crear manualmente un archivo de enlace simbólico en `$PATH` que apunte a los programas `aws` y `aws_completer` mediante los siguientes comandos en el símbolo del sistema. La ubicación predeterminada de un enlace simbólico es `/usr/local/bin/`:

       ```
       $ ln -s /folder/installed/aws-cli/aws /usr/local/bin/aws
       $ ln -s /folder/installed/aws-cli/aws_completer /usr/local/bin/aws_completer
       ```

       Si no tiene permisos de escritura en la carpeta, puede que necesite usar `sudo` en el comando. En el siguiente ejemplo de `sudo`, se utiliza la ubicación predeterminada para un enlace simbólico en `/usr/local/bin/`:

       ```
       $ sudo ln -s /folder/installed/aws-cli/aws /usr/local/bin/aws
       $ sudo ln -s /folder/installed/aws-cli/aws_completer /usr/local/bin/
       aws_completer
       ```

> **Note**
>
> Puede ver los registros de depuración de la instalación si presiona Cmd+L en cualquier lugar del instalador. Esto abre un panel de registro que le permite filtrar y guardar el registro. El archivo de registro también se guarda automáticamente en `/var/log/install.log`.

3. Para comprobar que el shell puede encontrar y ejecutar el comando `aws` en `$PATH`, utilice los siguientes comandos.

```
$ which aws
/usr/local/bin/aws
$ aws --version
aws-cli/2.27.41 Python/3.11.6 Darwin/23.3.0
```

Si no se encuentra el comando `aws`, es posible que deba reiniciar el terminal o seguir el proceso de solución de problemas en the section called “Errores de solución de problemas”.

Command line installer - All users

Si tiene permisos `sudo`, puede instalar la AWS CLI para todos los usuarios del equipo. Proporcionamos los pasos agrupados para que resulte sencillo copiarlos y pegarlos. Consulte las descripciones de cada línea en los pasos siguientes.

```
$ curl "https://awscli.amazonaws.com/AWSCLIV2.pkg" -o "AWSCLIV2.pkg"
$ sudo installer -pkg AWSCLIV2.pkg -target /
```

Instrucciones de instalación guiada

1. Descargar el archivo con el comando `curl`. En este ejemplo, la opción `-o` especifica el nombre de archivo en el que se escribe el paquete descargado. En este ejemplo, el archivo se escribe `AWSCLIV2.pkg` en la carpeta actual.

```
$ curl "https://awscli.amazonaws.com/AWSCLIV2.pkg" -o "AWSCLIV2.pkg"
```

2. Ejecute el programa `installer` de macOS estándar, especificando el archivo `.pkg` descargado como fuente. Utilice el parámetro `-pkg` para especificar el nombre del paquete

que se va a instalar y el parámetro `-target /` para indicar la unidad en la que se instalará el paquete. Los archivos se instalan en `/usr/local/aws-cli` y se crea automáticamente un symlink en `/usr/local/bin`. Debe incluir `sudo` en el comando para conceder permisos de escritura a esas carpetas.

```
$ sudo installer -pkg ./AWSCLIV2.pkg -target /
```

Una vez completada la instalación, los registros de depuración se escriben en `/var/log/install.log`.

3. Para comprobar que el shell puede encontrar y ejecutar el comando `aws` en `$PATH`, utilice los siguientes comandos.

```
$ which aws
/usr/local/bin/aws
$ aws --version
aws-cli/2.27.41 Python/3.11.6 Darwin/23.3.0
```

Si no se encuentra el comando `aws`, es posible que deba reiniciar el terminal o seguir el proceso de solución de problemas en the section called “Errores de solución de problemas”.

Command line - Current user

1. Para especificar en qué carpeta se instala AWS CLI, debe crear un archivo XML con cualquier nombre de archivo. Es un archivo con formato XML que se parece al siguiente ejemplo. Deje todos los valores tal como se muestran. Es posible que deba reemplazar la ruta *`/Users/myusername`* de la línea 9 con la ruta de la carpeta en la que quiere instalar la AWS CLI. La carpeta ya debe existir o se producirá un error en el comando. El siguiente ejemplo XML, denominado *`choices.xml`*, especifica el instalador que va a instalar AWS CLI en la carpeta `/Users/myusername`, donde crea una carpeta denominada `aws-cli`.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
  <array>
    <dict>
      <key>choiceAttribute</key>
      <string>customLocation</string>
```

```
      <key>attributeSetting</key>
      <string>/Users/myusername</string>
      <key>choiceIdentifier</key>
      <string>default</string>
    </dict>
  </array>
</plist>
```

2. Descargue el instalador pkg con el comando `curl`. En este ejemplo, la opción `-o` especifica el nombre de archivo en el que se escribe el paquete descargado. En este ejemplo, el archivo se escribe `AWSCLIV2.pkg` en la carpeta actual.

```
$ curl "https://awscli.amazonaws.com/AWSCLIV2.pkg" -o "AWSCLIV2.pkg"
```

3. Ejecute el programa `installer` de macOS estándar con las siguientes opciones:

   - Especifique el nombre del paquete que desea instalar mediante el parámetro `-pkg`.
   - Para especificar una instalación solo para el usuario actual debe establecer el parámetro `-target` en `CurrentUserHomeDirectory`.
   - Especifique la ruta de acceso (relativa a la carpeta actual) y el nombre del archivo XML que creó en el parámetro `-applyChoiceChangesXML`.

   En el ejemplo siguiente se instala la AWS CLI en la carpeta `/Users/myusername/aws-cli`.

```
$ installer -pkg AWSCLIV2.pkg \
            -target CurrentUserHomeDirectory \
            -applyChoiceChangesXML choices.xml
```

4. Dado que los permisos de usuario estándar normalmente no permiten escribir en las carpetas de `$PATH`, el instalador en este modo no intenta agregar los enlaces simbólicos a los programas `aws` y `aws_completer`. Para que la AWS CLI se ejecute correctamente, debe crear manualmente los enlaces simbólicos una vez finalizado el instalador. Si su `$PATH` incluye una carpeta en la que puede escribir y especifica la carpeta como la ruta de destino, puede ejecutar el siguiente comando sin `sudo`. Si no tiene una carpeta en la que se pueda escribir en `$PATH`, debe usar `sudo` para obtener permisos para escribir en la carpeta de destino especificada. La ubicación predeterminada de un enlace simbólico es `/usr/local/bin/`. Reemplace `folder/installed` por la ruta de su instalación de la AWS CLI.

```
$ sudo ln -s /folder/installed/aws-cli/aws /usr/local/bin/aws
$ sudo ln -s /folder/installed/aws-cli/aws_completer /usr/local/bin/
aws_completer
```

Una vez completada la instalación, los registros de depuración se escriben en `/var/log/install.log`.

5. Para comprobar que el shell puede encontrar y ejecutar el comando `aws` en `$PATH`, utilice los siguientes comandos.

```
$ which aws
/usr/local/bin/aws
$ aws --version
aws-cli/2.27.41 Python/3.11.6 Darwin/23.3.0
```

Si no se encuentra el comando `aws`, es posible que deba reiniciar el terminal o seguir el proceso de solución de problemas en the section called “Errores de solución de problemas”.

Windows

Requisitos de instalación y actualización

- Admitimos AWS CLI en las versiones compatibles con Microsoft de Windows de 64 bits.
- Derechos de administrador para instalar software

Instalación o actualización de AWS CLI

Para actualizar la instalación actual de AWS CLI en Windows, descargue un nuevo instalador cada vez que actualice para sobrescribir las versiones anteriores. AWS CLI se actualiza periódicamente. Para ver si se ha lanzado la versión más reciente, consulte el registro de cambios de la versión 2 de la AWS CLI en GitHub.

1. Descargue y ejecute el instalador MSI de la AWS CLI para Windows (64 bits):

   https://awscli.amazonaws.com/AWSCLIV2.msi

   Si lo desea, también puede ejecutar el comando `msiexec` para ejecutar el instalador MSI.

```
C:\> msiexec.exe /i https://awscli.amazonaws.com/AWSCLIV2.msi
```

Para varios parámetros que se pueden usar con `msiexec`, consulte msiexec en el sitio web de Documentos de Microsoft. Por ejemplo, puede usar el indicador `/qn` para una instalación silenciosa.

```
C:\> msiexec.exe /i https://awscli.amazonaws.com/AWSCLIV2.msi /qn
```

2. Para confirmar la instalación, abra el menú Inicio, busque `cmd` para abrir una ventana del símbolo del sistema y, en el símbolo del sistema, use el comando `aws --version`.

```
C:\> aws --version
aws-cli/2.27.41 Python/3.11.6 Windows/10 exe/AMD64 prompt/off
```

Si Windows no puede encontrar el programa, es posible que tenga que cerrar y volver a abrir la ventana del símbolo del sistema para actualizar la ruta o siga el proceso de solución de problemas en the section called “Errores de solución de problemas”.

Solución de errores de instalación y desinstalación de AWS CLI

Si se encuentra con problemas después de instalar o desinstalar la AWS CLI, consulte en the section called “Errores de solución de problemas” los pasos para la solución de problemas. Para conocer los pasos más relevantes de la solución de problemas, consulte the section called “Errores de comando no encontrado”, the section called “El comando "`aws --version`" devuelve una versión diferente a la instalada” y the section called “El comando "`aws --version`" devuelve una versión después de desinstalar la AWS CLI”.

Pasos a seguir a continuación

Después de instalar de forma satisfactoria la AWS CLI, puede eliminar de forma segura los archivos del instalador descargados. Después de completar los pasos indicados en the section called “Requisitos previos” e instalar AWS CLI, debe realizar the section called “Configuración”.

Instalación de versiones anteriores de la versión 2 de AWS CLI

En este tema se describe cómo instalar las versiones anteriores de la versión 2 de AWS Command Line Interface (AWS CLI) en sistemas operativos compatibles. Para obtener información sobre las

publicaciones de la versión 2 de AWS CLI, consulte el registro de cambios de la versión 2 de AWS CLI en GitHub.

Instrucciones de instalación de la versión 2 de la AWS CLI:

Linux

Necesidades de instalación

- Sabe qué publicación de la versión 2 de AWS CLI le gustaría instalar. Para obtener una lista de las versiones, consulte el registro de cambios de la versión 2 de la AWS CLI en GitHub.
- Debe poder extraer o "descomprimir" el paquete descargado. Si el sistema operativo no tiene el comando `unzip` integrado, utiliza un equivalente.
- La versión 2 de la AWS CLI utiliza `glibc`, `groff` y `less`. Estos se incluyen de forma predeterminada en la mayoría de las distribuciones principales de Linux.
- Admitimos la versión 2 de AWS CLI en versiones de 64 bits de las distribuciones recientes de CentOS, Fedora, Ubuntu, Amazon Linux 1, Amazon Linux 2 y Linux ARM.
- Debido a que AWS no mantiene repositorios de terceros, no podemos garantizar que contengan la última versión de AWS CLI.

Instrucciones de instalación

Siga estos pasos desde la línea de comandos para instalar la AWS CLI en Linux.

Proporcionamos los pasos en un grupo fácil de copiar y pegar basado en si usa Linux de 64 bits o Linux ARM. Consulte las descripciones de cada línea en los pasos que se indican a continuación.

Linux x86 (64-bit)

> **Note**
>
> (Opcional) El siguiente bloque de comandos descarga e instala la AWS CLI sin verificar primero la integridad de la descarga. Para verificar la integridad de la descarga, siga las instrucciones paso a paso que se muestran a continuación.

Para obtener una lista de las versiones, consulte el registro de cambios de la versión 2 de la AWS CLI en GitHub.

Para instalar la AWS CLI, ejecute los siguientes comandos.

Para especificar un versión, agregue un guion y el número de versión al nombre del archivo. Para este ejemplo, el nombre de archivo de la versión *2.0.30* sería `awscli-exe-linux-x86_64-2.0.30.zip` lo que resultaría en el siguiente comando:

```
$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64-2.0.30.zip" -o
 "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install
```

Para actualizar la instalación actual de la AWS CLI, agregue la información del enlace simbólico y del instalador existentes para construir el comando `install` con los parámetros `--bin-dir`, `--install-dir` y `--update`. El siguiente bloque de comandos utiliza un enlace simbólico de ejemplo de */usr/local/bin* y una ubicación de instalador de ejemplo de */usr/local/aws-cli*.

```
$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64-2.0.30.zip" -o
 "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install --bin-dir /usr/local/bin --install-dir /usr/local/aws-cli --
update
```

Linux ARM

> **Note**
>
> (Opcional) El siguiente bloque de comandos descarga e instala la AWS CLI sin verificar primero la integridad de la descarga. Para verificar la integridad de la descarga, siga las instrucciones paso a paso que se muestran a continuación.

Para obtener una lista de las versiones, consulte el registro de cambios de la versión 2 de la AWS CLI en GitHub.

Para instalar la AWS CLI, ejecute los siguientes comandos.

Para especificar un versión, agregue un guion y el número de versión al nombre del archivo. Para este ejemplo, el nombre de archivo de la versión *2.0.30* sería `awscli-exe-linux-aarch64-2.0.30.zip` lo que resultaría en el siguiente comando:

```
$ curl "https://awscli.amazonaws.com/awscli-exe-linux-aarch64-2.0.30.zip" -o
 "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install
```

Para actualizar la instalación actual de la AWS CLI, agregue la información del enlace simbólico y del instalador existentes para construir el comando `install` con los parámetros `--bin-dir`, `--install-dir` y `--update`. El siguiente bloque de comandos utiliza un enlace simbólico de ejemplo de */usr/local/bin* y una ubicación de instalador de ejemplo de */usr/local/aws-cli*.

```
$ curl "https://awscli.amazonaws.com/awscli-exe-linux-aarch64-2.0.30.zip" -o
 "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install --bin-dir /usr/local/bin --install-dir /usr/local/aws-cli --
update
```

1. Descargue el archivo de instalación de una de las siguientes maneras:

   Linux x86 (64-bit)

   - Use el comando **`curl`**: la opción `-o` especifica el nombre de archivo en el que se escribe el paquete descargado. Las opciones del comando de ejemplo siguiente escriben el archivo descargado en el directorio actual con el nombre local `awscliv2.zip`.

     Para especificar un versión, agregue un guion y el número de versión al nombre del archivo. Para este ejemplo, el nombre de archivo de la versión *2.0.30* sería `awscli-exe-linux-x86_64-2.0.30.zip` lo que resultaría en el siguiente comando:

     ```
     $ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64-2.0.30.zip" -o
      "awscliv2.zip"
     ```

     Para obtener una lista de las versiones, consulte el registro de cambios de la versión 2 de la AWS CLI en GitHub.

   - Descarga de la URL:

     En el navegador, descargue la versión específica de AWS CLI, agregue un guión y el número de versión al nombre del archivo.

```
https://awscli.amazonaws.com/awscli-exe-linux-x86_64-version.number.zip
```

Para este ejemplo, el nombre de archivo de la versión *2.0.30* sería awscli-exe-linux-x86_64-2.0.30.zip lo que da como resultado el siguiente enlace: https://awscli.amazonaws.com/awscli-exe-linux-x86_64-2.0.30.zip

Linux ARM

- Use el comando **`curl`**: la opción `-o` especifica el nombre de archivo en el que se escribe el paquete descargado. Las opciones del comando de ejemplo siguiente escriben el archivo descargado en el directorio actual con el nombre local `awscliv2.zip`.

  Para especificar un versión, agregue un guion y el número de versión al nombre del archivo. Para este ejemplo, el nombre de archivo de la versión *2.0.30* sería `awscli-exe-linux-aarch64-2.0.30.zip` lo que resultaría en el siguiente comando:

  ```
  $ curl "https://awscli.amazonaws.com/awscli-exe-linux-aarch64-2.0.30.zip" -o
   "awscliv2.zip"
  unzip awscliv2.zip
  sudo ./aws/install
  ```

- Descarga de la URL:

  En el navegador, descargue la versión específica de AWS CLI, agregue un guión y el número de versión al nombre del archivo.

  ```
  https://awscli.amazonaws.com/awscli-exe-linux-aarch64-version.number.zip
  ```

  Para este ejemplo, el nombre de archivo de la versión *2.0.30* sería `awscli-exe-linux-aarch64-2.0.30.zip` lo que da como resultado el siguiente enlace: https://awscli.amazonaws.com/awscli-exe-linux-aarch64-2.0.30.zip

2. (Opcional) Verificación de la integridad del archivo zip descargado

   Si eligió descargar manualmente el paquete del instalador de AWS CLI `.zip` en los pasos indicados anteriormente, puede usar los pasos siguientes para verificar las firmas mediante la herramienta `GnuPG`.

Los archivos `.zip` del paquete del instalador de la AWS CLI están firmados criptográficamente mediante firmas PGP. Si hay algún tipo de daño o alteración en los archivos, esta verificación produce un error, por lo que no debería continuar con la instalación.

a. Descargue e instale el comando `gpg` usando su administrador de paquetes. Para obtener más información acerca de `GnuPG`, consulte el sitio web de GnuPG.

b. Para crear el archivo de clave pública, cree un archivo de texto y pegue el siguiente texto en él:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBF2Cr7UBEADJZHcgusOJl7ENSyumXh85z0TRV0xJorM2B/JL0kHOyigQluUG
ZMLhENaG0bYatdrKP+3H91lvK050pXwnO/R7fB/FSTouki4ciIx5OuLlnJZIxSzx
PqGl0mkxImLNbGWoi6Lto0LYxqHN2iQtzlwTVmq9733zd3XfcXrZ3+LblHAgEt5G
TfNxEKJ8soPLyWmwDH6HWCnjZ/aIQRBTIQ05uVeEoYxSh6wOai7ss/KveoSNBbYz
gbdzoqI2Y8cgH2nbfgp3DSasaLZEdCSsIsK1u05CinE7k2qZ7KgKAUIcT/cR/grk
C6VwsnDU0OUCideXcQ8WeHutqvgZH1JgKDbznoIzeQHJD238GEu+eKhRHcz8/jeG
94zkcgJOz3KbZGYMiTh277Fvj9zzvZsbMBCedV1BTg3TqgvdX4bdkhf5cH+7NtWO
lrFj6UwAsGukBTAOxC0l/dnSmZhJ7Z1KmEWilro/gOrjtOxqRQutlIqG22TaqoPG
fYVN+en3Zwbt97kcgZDwqbuykNt64oZWc4XKCa3mprEGC3IbJTBFqglXmZ7l9ywG
EEUJYOlb2XrSuPWml39beWdKM8kzr1OjnlOm6+lpTRCBfo0wa9F8YZRhHPAkwKkX
XDeOGpWRj4ohOx0d2GWkyV5xyN14p2tQOCdOODmz80yUTgRpPVQUtOEhXQARAQAB
tCFBV1MgQ0xJIFRlYW0gPGF3cy1jbGlAYW1hem9uLmNvbT6JAlQEEwEIAD4CGwMF
CwkIBwIGFQoJCAsCBBYCAwECHgECF4AWIQT7Xbd/1cEYuAURraimMQrMRnJHXAUC
aGveYQUJDMpiLAAKCRCmMQrMRnJHXKBYD/9Ab0qQdGiO5hObchG8xh8Rpb4Mjyf6
0JrVo6m8GNjNj6BHkSc8fuTQJ/FaEhaQxj3pjZ3GXPrXjIIVChmICLlFuRXYzrXc
Pw0lniybypsZEVai5kO0tCNBCCFuMN9RsmmRG8mf7lC4FSTbUDmxG/QlYK+0IV/l
uJkzxWa+rySkdpm0JdqumjegNRgObdXHAQDWlubWQHWyZyIQ2B4U7AxqSpcdJp6I
S4Zds4wVLd1WE5pquYQ8vS2cNlDm4QNg8wTj58e3lKN47hXHMIb6CHxRnb947oJa
pg189LLPR5koh+EorNkA1wu5mAJtJvy5YMsppy2y/kIjp3lyY6AmPT1posgGk70Z
CmToEZ5rbd7ARExtlh76A0cabMDFlEHDIK8RNUOSRr7L64+KxOUegKBfQHb9dADY
qqiKqpCbKgvtWlds909Ms74JBgr2KwZCSY1HaOxnIr4CY43QRqAq5YHOay/mU+6w
hhmdF18vpyK0vfkvvGresWtSXbag7Hkt3XjaEw76BzxQH21EBDqU8WJVjHgU6ru+
DJTs+SxgJbaT3hb/vyjlw0lK+hFfhWKRwgOXH8vqducF95NRSUxtS4fpqxWVaw3Q
V2OWSjbne99A5EPEySzryFTKbMGwaTlAwMCwYevt4YT6eb7NmFhTx0Fis4TalUs+
j+c7Kg92pDx2uQ==
=OBAt
-----END PGP PUBLIC KEY BLOCK-----
```

Como referencia, a continuación se indican los detalles de la clave pública.

```
Key ID:           A6310ACC4672
Type:             RSA
Size:             4096/4096
Created:          2019-09-18
Expires:          2026-07-07
User ID:          AWS CLI Team <aws-cli@amazon.com>
Key fingerprint:  FB5D B77F D5C1 18B8 0511  ADA8 A631 0ACC 4672 475C
```

c. Importe la clave pública de la AWS CLI con el siguiente comando, sustituyendo *public-key-file-name* por el nombre del archivo de la clave pública que ha creado.

```
$ gpg --import public-key-file-name
gpg: /home/username/.gnupg/trustdb.gpg: trustdb created
gpg: key A6310ACC4672475C: public key "AWS CLI Team <aws-cli@amazon.com>"
 imported
gpg: Total number processed: 1
gpg:               imported: 1
```

d. Descargue el archivo de firma de la AWS CLI del paquete que descargó. Tiene la misma ruta y el mismo nombre que el archivo `.zip` al que corresponde, pero con la extensión `.sig`. En los siguientes ejemplos, lo guardaremos en el directorio actual como un archivo llamado `awscliv2.sig`.

   Linux x86 (64-bit)

   Para obtener la última versión de la AWS CLI, utilice el siguiente bloque de comandos.

   ```
   $ curl -o awscliv2.sig https://awscli.amazonaws.com/awscli-exe-linux-
   x86_64.zip.sig
   ```

   Para una versión específica de la AWS CLI, agregue un guión y el número de versión al nombre del archivo. Para este ejemplo, el nombre de archivo de la versión *2.0.30* sería `awscli-exe-linux-x86_64-2.0.30.zip.sig` lo que resultaría en el siguiente comando:

   ```
   $ curl -o awscliv2.sig https://awscli.amazonaws.com/awscli-exe-linux-
   x86_64-2.0.30.zip.sig
   ```

Para obtener una lista de las versiones, consulte el registro de cambios de la versión 2 de la AWS CLI en GitHub.

Linux ARM

Para obtener la última versión de la AWS CLI, utilice el siguiente bloque de comandos:

```
$ curl -o awscliv2.sig https://awscli.amazonaws.com/awscli-exe-linux-aarch64.zip.sig
```

Para una versión específica de la AWS CLI, agregue un guión y el número de versión al nombre del archivo. Para este ejemplo, el nombre de archivo de la versión *2.0.30* sería `awscli-exe-linux-aarch64-2.0.30.zip.sig` lo que resultaría en el siguiente comando:

```
$ curl -o awscliv2.sig https://awscli.amazonaws.com/awscli-exe-linux-aarch64-2.0.30.zip.sig
```

Para obtener una lista de las versiones, consulte el registro de cambios de la versión 2 de la AWS CLI en GitHub.

e. Verifique la firma pasando los nombres de archivo `.sig` y `.zip` como parámetros al comando gpg.

```
$ gpg --verify awscliv2.sig awscliv2.zip
```

El resultado de debería parecerse al siguiente.

```
gpg: Signature made Mon Nov  4 19:00:01 2019 PST
gpg:                using RSA key FB5D B77F D5C1 18B8 0511 ADA8 A631 0ACC 4672
 475C
gpg: Good signature from "AWS CLI Team <aws-cli@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: FB5D B77F D5C1 18B8 0511  ADA8 A631 0ACC 4672 475C
```

> **Important**
>
> Se espera la advertencia en la salida y ello no indica un problema. Esto se produce porque no existe una cadena de confianza entre su clave PGP personal (si es su caso) y la clave PGP de la AWS CLI. Para obtener más información, consulta Red de confianza.

3. Descomprima el instalador. Si su distribución de Linux no tiene un comando `unzip` integrado, use un equivalente para descomprimirlo. El siguiente comando de ejemplo descomprime el paquete y crea un directorio denominado `aws` en el directorio actual.

```
$ unzip awscliv2.zip
```

4. Ejecute el programa de instalación. El comando de instalación utiliza un archivo denominado `install` en el directorio `aws` recién descomprimido. De forma predeterminada, todos los archivos se instalan en `/usr/local/aws-cli` y se crea un enlace simbólico en `/usr/local/bin`. El comando incluye `sudo` para conceder permisos de escritura en esos directorios.

```
$ sudo ./aws/install
```

   Puede realizar la instalación sin `sudo` si especifica directorios en los que ya tiene permisos de escritura. Utilice las siguientes instrucciones en el comando `install` para especificar la ubicación de instalación:

   - Asegúrese de que las rutas que proporcione a los parámetros `-i` y `-b` no contengan nombres de volumen ni nombres de directorio que contengan caracteres de espacio u otros caracteres de espacio en blanco. Si hay un espacio, la instalación falla.
   - `--install-dir` o `-i`: esta opción especifica el directorio en la que se copiarán todos los archivos.

     El valor predeterminado es `/usr/local/aws-cli`.
   - `--bin-dir` o `-b`: esta opción especifica que el programa de `aws` principal del directorio de instalación está vinculado de forma simbólica al archivo `aws` en la ruta de acceso especificada. Debe tener permisos de escritura en el directorio especificado. Al crear un enlace simbólico a un directorio que ya está en su ruta, se elimina la necesidad de agregar el directorio de instalación a la variable $PATH del usuario.

El valor predeterminado es `/usr/local/bin`.

```
$ ./aws/install -i /usr/local/aws-cli -b /usr/local/bin
```

> **Note**
>
> Para actualizar la instalación actual de la versión 2 de AWS CLI a una versión más reciente, agregue la información del enlace simbólico y del instalador existentes para construir el comando `install` con el parámetro `--update`.
>
> ```
> $ sudo ./aws/install --bin-dir /usr/local/bin --install-dir /usr/local/aws-cli --update
> ```
>
> Para localizar el enlace simbólico y el directorio de instalación existentes, siga los siguientes pasos:
>
> 1. Utilice el comando `which` para buscar el enlace simbólico. Esto le dará la ruta que puede utilizar con el parámetro `--bin-dir`.
>
>    ```
>    $ which aws
>    /usr/local/bin/aws
>    ```
>
> 2. Utilice el comando `ls` para buscar el directorio al que apunta el enlace simbólico. Esto le dará la ruta que puede utilizar con el parámetro `--install-dir`.
>
>    ```
>    $ ls -l /usr/local/bin/aws
>    lrwxrwxrwx 1 ec2-user ec2-user 49 Oct 22 09:49 /usr/local/bin/aws -> /usr/local/aws-cli/v2/current/bin/aws
>    ```

5. Confirme la instalación con el siguiente comando.

```
$ aws --version
aws-cli/2.27.41 Python/3.11.6 Linux/5.10.205-195.807.amzn2.x86_64
```

Si no se encuentra el comando `aws`, es posible que deba reiniciar el terminal o seguir el proceso de solución de problemas en the section called “Errores de solución de problemas”.

macOS

Necesidades de instalación

- Sabe qué publicación de la versión 2 de AWS CLI le gustaría instalar. Para obtener una lista de las versiones, consulte el registro de cambios de la versión 2 de la AWS CLI en GitHub.
- Admitimos la versión 2 de la AWS CLI en las versiones compatibles de Apple de macOS de 64 bits.
- Debido a que AWS no mantiene repositorios de terceros, no podemos garantizar que contengan la última versión de AWS CLI.

Instrucciones de instalación

Puede instalar la versión 2 de AWS CLI en macOS de una de las siguientes maneras.

GUI installer

En los pasos siguientes se muestra cómo instalar o actualizar a la versión más reciente de la versión 2 de la AWS CLI mediante la interfaz de usuario estándar de macOS y su navegador. Si va a actualizar a la versión más reciente, utilice el mismo método de instalación que utilizó para la versión actual.

1. En el navegador, descargue la versión específica de AWS CLI, agregue un guión y el número de versión al nombre del archivo.

   ```
   https://awscli.amazonaws.com/AWSCLIV2-version.number.pkg
   ```

   Para este ejemplo, el nombre de archivo de la versión *2.0.30* sería `AWSCLIV2-2.0.30.pkg` lo que da como resultado el siguiente enlace: https://awscli.amazonaws.com/AWSCLIV2-2.0.30.pkg.
2. Ejecute el archivo descargado y siga las instrucciones que aparecen en pantalla. Puede elegir instalar la versión 2 de la AWS CLI de las siguientes maneras:

   - Para todos los usuarios del equipo (requiere **sudo**)
     - Puede realizar la instalación en cualquier carpeta o elegir la carpeta predeterminada recomendada de `/usr/local/aws-cli`.
     - El instalador crea automáticamente un enlace simbólico en `/usr/local/bin/aws` que enlaza al programa principal en la carpeta de instalación elegida.

- Solo para el usuario actual (no requiere **sudo**)
  - Puede realizar la instalación en cualquier carpeta en la que tenga permiso de escritura.
  - Debido a los permisos de usuario estándar, una vez finalizado el instalador, debe crear manualmente un archivo de enlace simbólico en `$PATH` que apunte a los programas `aws` y `aws_completer` mediante los siguientes comandos en el símbolo del sistema. Si su `$PATH` incluye una carpeta en la que puede escribir, puede ejecutar el siguiente comando sin `sudo` si especifica esa carpeta como ruta de destino. Si no tiene una carpeta en la que se pueda escribir en `$PATH`, debe usar `sudo` en los comandos para obtener permisos para escribir en la carpeta de destino especificada. La ubicación predeterminada de un enlace simbólico es `/usr/local/bin/`.

```
$ sudo ln -s /folder/installed/aws-cli/aws /usr/local/bin/aws
$ sudo ln -s /folder/installed/aws-cli/aws_completer /usr/local/bin/
aws_completer
```

> **Note**
>
> Puede ver los registros de depuración de la instalación si presiona Cmd+L en cualquier lugar del instalador. Esto abre un panel de registro que le permite filtrar y guardar el registro. El archivo de registro también se guarda automáticamente en `/var/log/install.log`.

3. Para comprobar que el shell puede encontrar y ejecutar el comando `aws` en `$PATH`, utilice los siguientes comandos.

```
$ which aws
/usr/local/bin/aws
$ aws --version
aws-cli/2.27.41 Python/3.11.6 Darwin/23.3.0
```

Si no se encuentra el comando `aws`, es posible que deba reiniciar el terminal o seguir el proceso de solución de problemas en the section called “Errores de solución de problemas”.

Command line installer - All users

Si tiene permisos `sudo`, puede instalar la versión 2 de la AWS CLI para todos los usuarios del equipo. Proporcionamos los pasos agrupados para que resulte sencillo copiarlos y pegarlos. Consulte las descripciones de cada línea en los pasos siguientes.

En el caso de una versión específica de la AWS CLI, agregue un guion y el número de versión al nombre del archivo. Para este ejemplo, el nombre de archivo de la versión *`2.0.30`* sería `AWSCLIV2-2.0.30.pkg` lo que resultaría en el siguiente comando:

```
$ curl "https://awscli.amazonaws.com/AWSCLIV2-2.0.30.pkg" -o "AWSCLIV2.pkg"
$ sudo installer -pkg AWSCLIV2.pkg -target /
```

1. Descargar el archivo con el comando `curl`. En este ejemplo, la opción `-o` especifica el nombre de archivo en el que se escribe el paquete descargado. En este ejemplo, el archivo se escribe `AWSCLIV2.pkg` en la carpeta actual.

   En el caso de una versión específica de la AWS CLI, agregue un guion y el número de versión al nombre del archivo. Para este ejemplo, el nombre de archivo de la versión *`2.0.30`* sería `AWSCLIV2-2.0.30.pkg` lo que resultaría en el siguiente comando:

   ```
   $ curl "https://awscli.amazonaws.com/AWSCLIV2-2.0.30.pkg" -o "AWSCLIV2.pkg"
   ```

   Para obtener una lista de las versiones, consulte el registro de cambios de la versión 2 de la AWS CLI en GitHub.
2. Ejecute el programa `installer` de macOS estándar, especificando el archivo `.pkg` descargado como fuente. Utilice el parámetro `-pkg` para especificar el nombre del paquete que se va a instalar y el parámetro `-target /` para indicar la unidad en la que se instalará el paquete. Los archivos se instalan en `/usr/local/aws-cli` y se crea automáticamente un symlink en `/usr/local/bin`. Debe incluir `sudo` en el comando para conceder permisos de escritura a esas carpetas.

   ```
   $ sudo installer -pkg ./AWSCLIV2.pkg -target /
   ```

   Una vez completada la instalación, los registros de depuración se escriben en `/var/log/install.log`.
3. Para comprobar que el shell puede encontrar y ejecutar el comando `aws` en `$PATH`, utilice los siguientes comandos.

```
$ which aws
/usr/local/bin/aws
$ aws --version
aws-cli/2.27.41 Python/3.11.6 Darwin/23.3.0
```

Si no se encuentra el comando `aws`, es posible que deba reiniciar el terminal o seguir el proceso de solución de problemas en the section called “Errores de solución de problemas”.

Command line - Current user

1. Para especificar en qué carpeta se instala AWS CLI, debe crear un archivo XML. Es un archivo con formato XML que se parece al siguiente ejemplo. Deje todos los valores tal como se muestran, excepto que debe reemplazar la ruta */Users/myusername* de la línea 9 con la ruta de la carpeta en la que quiere instalar la versión 2 de AWS CLI. La carpeta ya debe existir o se producirá un error en el comando. En este ejemplo XML se especifica que el instalador realiza la instalación de la AWS CLI en la carpeta `/Users/myusername`, donde se crea una carpeta denominada `aws-cli`.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
  <array>
    <dict>
      <key>choiceAttribute</key>
      <string>customLocation</string>
      <key>attributeSetting</key>
      <string>/Users/myusername</string>
      <key>choiceIdentifier</key>
      <string>default</string>
    </dict>
  </array>
</plist>
```

2. Descargue el instalador `pkg` con el comando `curl`. En este ejemplo, la opción `-o` especifica el nombre de archivo en el que se escribe el paquete descargado. En este ejemplo, el archivo se escribe `AWSCLIV2.pkg` en la carpeta actual.

Para la versión específica de AWS CLI, agregue un guión y el número de versión al nombre del archivo. Para este ejemplo, el nombre de archivo de la versión *2.0.30* sería `AWSCLIV2-2.0.30.pkg` lo que resultaría en el siguiente comando:

```
$ curl "https://awscli.amazonaws.com/AWSCLIV2-2.0.30.pkg" -o "AWSCLIV2.pkg"
```

Para obtener una lista de las versiones, consulte el registro de cambios de la versión 2 de la AWS CLI en GitHub.

3. Ejecute el programa `installer` de macOS estándar con las siguientes opciones:

   - Especifique el nombre del paquete que desea instalar mediante el parámetro `-pkg`.
   - Para especificar una instalación solo para el usuario actual debe establecer el parámetro `-target` en `CurrentUserHomeDirectory`.
   - Especifique la ruta de acceso (relativa a la carpeta actual) y el nombre del archivo XML que creó en el parámetro `-applyChoiceChangesXML`.

   En el ejemplo siguiente se instala la AWS CLI en la carpeta `/Users/myusername/aws-cli`.

   ```
   $ installer -pkg AWSCLIV2.pkg \
               -target CurrentUserHomeDirectory \
               -applyChoiceChangesXML choices.xml
   ```

4. Dado que los permisos de usuario estándar normalmente no permiten escribir en las carpetas de `$PATH`, el instalador en este modo no intenta agregar los enlaces simbólicos a los programas `aws` y `aws_completer`. Para que la AWS CLI se ejecute correctamente, debe crear manualmente los enlaces simbólicos una vez finalizado el instalador. Si su `$PATH` incluye una carpeta en la que puede escribir y especifica la carpeta como la ruta de destino, puede ejecutar el siguiente comando sin `sudo`. Si no tiene una carpeta en la que se pueda escribir en `$PATH`, debe usar `sudo` para obtener permisos para escribir en la carpeta de destino especificada. La ubicación predeterminada de un enlace simbólico es `/usr/local/bin/`.

   ```
   $ sudo ln -s /folder/installed/aws-cli/aws /usr/local/bin/aws
   $ sudo ln -s /folder/installed/aws-cli/aws_completer /usr/local/bin/
   aws_completer
   ```

Una vez completada la instalación, los registros de depuración se escriben en `/var/log/install.log`.

5. Para comprobar que el shell puede encontrar y ejecutar el comando `aws` en `$PATH`, utilice los siguientes comandos.

```
$ which aws
/usr/local/bin/aws
$ aws --version
aws-cli/2.27.41 Python/3.11.6 Darwin/23.3.0
```

Si no se encuentra el comando `aws`, es posible que deba reiniciar el terminal o seguir el proceso de solución de problemas en the section called “Errores de solución de problemas”.

Windows

Necesidades de instalación

- Sabe qué publicación de la versión 2 de AWS CLI le gustaría instalar. Para obtener una lista de las versiones, consulte el registro de cambios de la versión 2 de la AWS CLI en GitHub.
- Admitimos AWS CLI en las versiones compatibles con Microsoft de Windows de 64 bits.
- Derechos de administrador para instalar software

Instrucciones de instalación

Para actualizar la instalación actual de la versión 2 de la AWS CLI en Windows, descargue un nuevo instalador cada vez que actualice para sobrescribir las versiones anteriores. La AWS CLI se actualiza periódicamente. Para ver si se ha lanzado la versión más reciente, consulte el registro de cambios de la versión 2 de la AWS CLI en GitHub.

1. Descargue y ejecute el instalador MSI de AWS CLI para Windows (64 bits) de una de las siguientes maneras:

   - Descargar y ejecutar el instalador de MSI: para crear el enlace de descarga para una versión específica de AWS CLI, agregue un guion y el número de versión al nombre del archivo.

```
https://awscli.amazonaws.com/AWSCLIV2-version.number.msi
```

Para este ejemplo, el nombre de archivo de la versión *2.0.30* sería `AWSCLIV2-2.0.30.msi` lo que da como resultado el siguiente enlace: https://awscli.amazonaws.com/AWSCLIV2-2.0.30.msi.

- Usar el comando msiexec: De forma opcional, puede utilizar el instalador de MSI agregando el enlace al comando `msiexec`. En el caso de una versión específica de la AWS CLI, agregue un guion y el número de versión al nombre del archivo.

```
C:\> msiexec.exe /i https://awscli.amazonaws.com/AWSCLIV2-version.number.msi
```

Para este ejemplo, el nombre de archivo de la versión *2.0.30* sería `AWSCLIV2-2.0.30.msi` lo que da como resultado el siguiente enlace https://awscli.amazonaws.com/AWSCLIV2-2.0.30.msi.

```
C:\> msiexec.exe /i https://awscli.amazonaws.com/AWSCLIV2-2.0.30.msi
```

Para varios parámetros que se pueden usar con `msiexec`, consulte msiexec en el sitio web de Documentos de Microsoft.

Para obtener una lista de las versiones, consulte el registro de cambios de la versión 2 de la AWS CLI en GitHub.

2. Para confirmar la instalación, abra el menú Inicio, busque `cmd` para abrir una ventana del símbolo del sistema y, en el símbolo del sistema, use el comando `aws --version`.

```
C:\> aws --version
aws-cli/2.27.41 Python/3.11.6 Windows/10 exe/AMD64 prompt/off
```

Si Windows no puede encontrar el programa, es posible que tenga que cerrar y volver a abrir la ventana del símbolo del sistema para actualizar la ruta o siga el proceso de solución de problemas en the section called “Errores de solución de problemas”.

Solución de errores de instalación y desinstalación de AWS CLI

Si se encuentra con problemas después de instalar o desinstalar la AWS CLI, consulte en the section called “Errores de solución de problemas” los pasos para la solución de problemas. Para conocer los pasos más relevantes de la solución de problemas, consulte the section called “Errores de comando

no encontrado”, the section called “El comando "`aws --version`" devuelve una versión diferente a la instalada” y the section called “El comando "`aws --version`" devuelve una versión después de desinstalar la AWS CLI”.

Pasos a seguir a continuación

Después de completar los pasos indicados en the section called “Requisitos previos” e instalar AWS CLI, debe realizar the section called “Configuración”.

Compilación e instalación de la AWS CLI desde el origen

En este tema, se describe cómo instalar o actualizar desde el origen la última versión de la AWS Command Line Interface (AWS CLI) en sistemas operativos compatibles.

Para obtener información sobre los lanzamientos más recientes de AWS CLI, consulte el registro de cambios de la versión 2 de la AWS CLI en GitHub.

> **Important**
>
> Las versiones 1 y 2 de la AWS CLI utilizan el mismo nombre de comando de `aws`. Si ha instalado previamente la AWS CLI versión 1, consulte Guía de migración para la versión 2 de la AWS CLI.

Temas

- ¿Por qué compilar desde el origen?
- Pasos rápidos
- Paso 1: configurar todos los requisitos
- Paso 2: configurar la instalación de origen de la AWS CLI
- Paso 3: compilar la AWS CLI
- Paso 4: instalar la AWS CLI
- Paso 5: verificar la instalación de AWS CLI
- Ejemplos de flujo de trabajo
- Solución de errores de instalación y desinstalación de AWS CLI
- Pasos a seguir a continuación

¿Por qué compilar desde el origen?

La AWS CLI está disponible como instaladores prediseñados para la mayoría de las plataformas y entornos, además de como una imagen de Docker.

Por lo general, estos instaladores ofrecen cobertura de la mayoría de los casos de uso. Las instrucciones de instalación desde el origen sirven para ayudar en los casos de uso que nuestros instaladores no cubren. A continuación, se indican algunos casos de uso:

- Los instaladores prediseñados no son compatibles con su entorno. Por ejemplo, los instaladores prediseñados no son compatibles con ARM de 32 bits.
- Los instaladores prediseñados tienen dependencias de las que carece su entorno. Por ejemplo, Alpine Linux usa `musl`, pero los instaladores actuales requieren `glibc`, por lo que los instaladores prediseñados no funcionan inmediatamente.
- Los instaladores prediseñados requieren recursos a los que su entorno restringe el acceso. Por ejemplo, es posible que los sistemas con seguridad reforzada no concedan permisos a la memoria compartida. Esto es necesario para el instalador de `aws` congelado.
- Los instaladores prediseñados suelen ser un obstáculo para los mantenedores en los administradores de paquetes, ya que es preferible tener un control total del proceso de compilación del código y los paquetes. Compilar desde el origen permite a los mantenedores de la distribución disponer de un proceso más ágil para mantener la AWS CLI actualizada. Capacitar a los mantenedores permite que los clientes tengan versiones más actualizadas de la AWS CLI cuando la instalan desde un administrador de paquetes de terceros como `brew`, `yum` y `apt`.
- Los clientes que aplican parches a la funcionalidad de la AWS CLI necesitan compilar e instalar la AWS CLI desde el origen. Esto es especialmente importante para los miembros de la comunidad que desean probar los cambios que han realizado en el origen antes de enviarlos al repositorio de GitHub de la AWS CLI.

Pasos rápidos

> **Note**
>
> Se asume que todo el código de ejemplo se ejecuta desde la raíz del directorio de origen.

Para compilar e instalar la AWS CLI desde el origen, siga los pasos de esta sección. La AWS CLI utiliza GNU Autotools para realizar la instalación desde el origen. En el caso más simple, la AWS CLI

se puede instalar desde el origen ejecutando los comandos de ejemplo predeterminados desde la raíz del repositorio de GitHub de la AWS CLI.

1. Configure todos los requisitos de su entorno. Esto incluye la posibilidad de ejecutar archivos generados por GNU Autotools y Python 3.8 o versiones posteriores si está instalado.
2. En su terminal, vaya al nivel superior de la carpeta de origen de la AWS CLI y ejecute el comando `./configure`. Este comando comprueba el sistema en busca de todas las dependencias necesarias y genera un`Makefile` para compilar e instalar la AWS CLI en función de las configuraciones detectadas y especificadas.

   Linux and macOS

   El siguiente comando `./configure` de ejemplo establece la configuración de compilación de la AWS CLI utilizando la configuración predeterminada.

   ```
   $ ./configure
   ```

   Windows PowerShell

   Antes de ejecutar cualquier comando que llame a MSYS2, debe conservar su directorio de trabajo actual:

   ```
   PS C:\> $env:CHERE_INVOKING = 'yes'
   ```

   A continuación, utilice el siguiente comando `./configure` de ejemplo para establecer la configuración de compilación de la AWS CLI. Para ello, se utiliza la ruta local al ejecutable de Python, se instala en C:\Program Files\AWSCLI y se descargan todas las dependencias.

   ```
   PS C:\> C:\msys64\usr\bin\bash  -lc " PYTHON='C:\path\to\python.exe' ./configure
    --prefix='C:\Program Files\AWSCLI' --with-download-deps "
   ```

   Para obtener más información, las opciones de configuración disponibles y la información de configuración predeterminada, consulte la sección the section called “Paso 2: configurar la instalación de origen de la AWS CLI”.
3. Ejecute el comando `make`. Este comando compila la AWS CLI acuerdo con los ajustes de configuración.

El siguiente comando `make` de ejemplo se compila con las opciones predeterminadas utilizando la configuración existente de `./configure`.

Linux and macOS

```
$ make
```

Windows PowerShell

```
PS C:\> C:\msys64\usr\bin\bash -lc "make"
```

Para obtener más información y las opciones de compilación disponibles, consulte la sección the section called “Paso 3: compilar la AWS CLI”.

4. Ejecute el comando `make install`. Este comando instala la AWS CLI compilada en la ubicación configurada del sistema.

   El siguiente comando `make install` de ejemplo instala la AWS CLI compilada y se crean los symlinks en las ubicaciones configuradas utilizando la configuración predeterminada del comando.

   Linux and macOS

   ```
   $ make install
   ```

   Windows PowerShell

   ```
   PS C:\> C:\msys64\usr\bin\bash -lc "make install"
   ```

   Tras la instalación, añada la ruta a la AWS CLI de la siguiente manera:

   ```
   PS C:\> $Env:PATH +=";C:\Program Files\AWSCLI\bin\"
   ```

   Para obtener más información y conocer las opciones de instalación disponibles, consulte la sección the section called “Paso 4: instalar la AWS CLI”.

5. Confirme que la AWS CLI se ha instalado correctamente utilizando el siguiente comando:

```
$ aws --version
aws-cli/2.27.41 Python/3.11.6 Windows/10 exe/AMD64 prompt/off
```

Para conocer los pasos de solución de problemas de los errores de instalación, consulte la sección the section called “Solución de errores de instalación y desinstalación de AWS CLI”.

Paso 1: configurar todos los requisitos

Para compilar la AWS CLI desde el origen, debe hacer lo siguiente de antemano:

> **Note**
>
> Se asume que todo el código de ejemplo se ejecuta desde la raíz del directorio de origen.

1. Descargue el origen de la AWS CLI bifurcando el repositorio de GitHub de la AWS CLI o descargando el archivo tar de origen. Las instrucciones son una de las siguientes:

   - Bifurque y clone el repositorio de la AWS CLI desde GitHub. Para obtener más información, consulte Fork a repo (Bifurcar un repositorio) en GitHub Docs (Documentación de GitHub).
   - Descargue el último tarball de origen en https://awscli.amazonaws.com/awscli.tar.gz y extraiga el contenido con los siguientes comandos:

     ```
     $ curl "https://awscli.amazonaws.com/awscli.tar.gz" -o "awscli.tar.gz"
     $ tar -xzf awscli.tar.gz
     ```

     > **Note**
     >
     > Para descargar una versión específica, utilice el siguiente formato de enlace: https://awscli.amazonaws.com/awscli-*versionnumber*.tar.gz
     > Por ejemplo, para la versión 2.10.0, el enlace es el siguiente: https://awscli.amazonaws.com/awscli-*2.10.0*.tar.gz
     > Las versiones de origen están disponibles a partir de la versión 2.10.0 de la AWS CLI.

(Opcional) Verificación de la integridad del archivo zip descargado mediante los siguientes pasos

1. Puede seguir los pasos indicados a continuación para verificar las firmas con la herramienta GnuPG.

   Los archivos `.zip` del paquete del instalador de la AWS CLI están firmados criptográficamente mediante firmas PGP. Si hay algún tipo de daño o alteración en los archivos, esta verificación produce un error, por lo que no debería continuar con la instalación.

2. Descargue e instale el comando gpg usando su administrador de paquetes. Para obtener más información acerca de GnuPG, consulte el sitio web de GnuPG.

3. Para crear el archivo de clave pública, cree un archivo de texto y pegue el siguiente texto en él:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBF2Cr7UBEADJZHcgusOJl7ENSyumXh85z0TRV0xJorM2B/JL0kHOyigQluUG
ZMLhENaG0bYatdrKP+3H91lvK050pXwnO/R7fB/FSTouki4ciIx5OuLlnJZIxSzx
PqGl0mkxImLNbGWoi6Lto0LYxqHN2iQtzlwTVmq9733zd3XfcXrZ3+LblHAgEt5G
TfNxEKJ8soPLyWmwDH6HWCnjZ/aIQRBTIQ05uVeEoYxSh6wOai7ss/KveoSNBbYz
gbdzoqI2Y8cgH2nbfgp3DSasaLZEdCSsIsK1u05CinE7k2qZ7KgKAUIcT/cR/grk
C6VwsnDU0OUCideXcQ8WeHutqvgZH1JgKDbznoIzeQHJD238GEu+eKhRHcz8/jeG
94zkcgJOz3KbZGYMiTh277Fvj9zzvZsbMBCedV1BTg3TqgvdX4bdkhf5cH+7NtWO
lrFj6UwAsGukBTAOxC0l/dnSmZhJ7Z1KmEWilro/gOrjtOxqRQutlIqG22TaqoPG
fYVN+en3Zwbt97kcgZDwqbuykNt64oZWc4XKCa3mprEGC3IbJTBFqglXmZ7l9ywG
EEUJYOlb2XrSuPWml39beWdKM8kzr1OjnlOm6+lpTRCBfo0wa9F8YZRhHPAkwKkX
XDeOGpWRj4ohOx0d2GWkyV5xyN14p2tQOCdOODmz80yUTgRpPVQUtOEhXQARAQAB
tCFBV1MgQ0xJIFRlYW0gPGF3cy1jbGlAYW1hem9uLmNvbT6JAlQEEwEIAD4CGwMF
CwkIBwIGFQoJCAsCBBYCAwECHgECF4AWIQT7Xbd/1cEYuAURraimMQrMRnJHXAUC
aGveYQUJDMpiLAAKCRCmMQrMRnJHXKBYD/9Ab0qQdGiO5hObchG8xh8Rpb4Mjyf6
0JrVo6m8GNjNj6BHkSc8fuTQJ/FaEhaQxj3pjZ3GXPrXjIIVChmICLlFuRXYzrXc
Pw0lniybypsZEVai5kO0tCNBCCFuMN9RsmmRG8mf7lC4FSTbUDmxG/QlYK+0IV/l
uJkzxWa+rySkdpm0JdqumjegNRgObdXHAQDWlubWQHWyZyIQ2B4U7AxqSpcdJp6I
S4Zds4wVLd1WE5pquYQ8vS2cNlDm4QNg8wTj58e3lKN47hXHMIb6CHxRnb947oJa
pg189LLPR5koh+EorNkA1wu5mAJtJvy5YMsppy2y/kIjp3lyY6AmPT1posgGk70Z
CmToEZ5rbd7AREXtlh76A0cabMDFlEHDIK8RNUOSRr7L64+KxOUegKBfQHb9dADY
qqiKqpCbKgvtWlds909Ms74JBgr2KwZCSY1HaOxnIr4CY43QRqAq5YHOay/mU+6w
hhmdF18vpyK0vfkvvGresWtSXbag7Hkt3XjaEw76BzxQH21EBDqU8WJVjHgU6ru+
DJTs+SxgJbaT3hb/vyjlw0lK+hFfhWKRwgOXH8vqducF95NRSUxtS4fpqxWVaw3Q
```

```
V2OWSjbne99A5EPEySzryFTKbMGwaTlAwMCwYevt4YT6eb7NmFhTx0Fis4TalUs+
j+c7Kg92pDx2uQ==
=OBAt
-----END PGP PUBLIC KEY BLOCK-----
```

Como referencia, a continuación se indican los detalles de la clave pública.

```
Key ID:          A6310ACC4672
Type:            RSA
Size:            4096/4096
Created:         2019-09-18
Expires:         2026-07-07
User ID:         AWS CLI Team <aws-cli@amazon.com>
Key fingerprint:  FB5D B77F D5C1 18B8 0511  ADA8 A631 0ACC 4672 475C
```

4. Importe la clave pública de la AWS CLI con el siguiente comando, sustituyendo *public-key-file-name* por el nombre del archivo de la clave pública que ha creado.

```
$ gpg --import public-key-file-name
gpg: /home/username/.gnupg/trustdb.gpg: trustdb created
gpg: key A6310ACC4672475C: public key "AWS CLI Team <aws-cli@amazon.com>"
 imported
gpg: Total number processed: 1
gpg:               imported: 1
```

5. Descargue el archivo de firma de la AWS CLI para el paquete que ha descargado en https://awscli.amazonaws.com/awscli.tar.gz.sig. Tiene la misma ruta y el mismo nombre que el archivo tarball al que corresponde, pero con la extensión `.sig`. Guárdelo en la misma ruta que el archivo tarball. O utilice el siguiente bloque de comandos:

```
$ curl awscliv2.sig https://awscli.amazonaws.com/ -o awscli.tar.gz.sig
```

6. Verifique la firma pasando los nombres de archivo `.sig` y `.zip` como parámetros al comando gpg.

```
$ gpg --verify awscliv2.sig awscli.tar.gz
```

El resultado de debería parecerse al siguiente.

```
gpg: Signature made Mon Nov  4 19:00:01 2019 PST
```

```
gpg:                using RSA key FB5D B77F D5C1 18B8 0511 ADA8 A631 0ACC 4672
 475C
gpg: Good signature from "AWS CLI Team <aws-cli@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: FB5D B77F D5C1 18B8 0511  ADA8 A631 0ACC 4672 475C
```

> **Important**
>
> Se espera la advertencia en la salida y ello no indica un problema. Esto se produce porque no existe una cadena de confianza entre su clave PGP personal (si es su caso) y la clave PGP de la AWS CLI. Para obtener más información, consulta Red de confianza.

2. Dispone de un entorno que puede ejecutar archivos generados por GNU Autotools, como `configure` y `Makefile`. Estos archivos suelen ser portables en las plataformas POSIX.

   Linux and macOS

   Si Autotools aún no está instalado en su entorno o necesita actualizarlo, siga las instrucciones de instalación que se encuentran en How do I install the Autotools (as user)? (¿Cómo instalo Autotools [como usuario]?) o Basic Installation (Instalación básica) en GNU Documentation (Documentación de GNU).

   Windows PowerShell

   > **Warning**
   >
   > Le sugerimos que si se encuentra en un entorno Windows, utilice los instaladores prediseñados. Para obtener las instrucciones de instalación de los instaladores prediseñados, consulte the section called “Instalar o actualizar”

   Dado que Windows no incluye un intérprete de comandos compatible con POSIX, debe instalar software adicional para instalar la AWS CLI desde el origen. MSYS2 incluye una colección de herramientas y bibliotecas para ayudar a compilar e instalar software de Windows, especialmente para los scripts basados en POSIX que utiliza Autotools.

1. Instale MSYS2. Para obtener información acerca de la instalación y el uso de MSYS2, consulte las instrucciones de instalación y uso en MSYS2 Documentation (Documentación de MSYS2).
2. Abra el terminal de MSYS2 e instale Autotools mediante el siguiente comando.

```
$ pacman -S autotools
```

> **Note**
>
> En los ejemplos de código de configuración, compilación e instalación de esta guía para Windows, se asume que se utiliza la ruta de instalación predeterminada de MSYS2 `C:\msys64\usr\bin\bash`. Al llamar a MSYS2 desde PowerShell, utilizará el siguiente formato, con el comando bash entre comillas:
>
> ```
> PS C:\> C:\msys64\usr\bin\bash  -lc "command example"
> ```
>
> El siguiente comando de ejemplo llama al comando `./configure`.
>
> ```
> PS C:\> C:\msys64\usr\bin\bash  -lc "./configure"
> ```

3. Se ha instalado un intérprete de Python 3.8 o una versión posterior. La versión mínima requerida de Python tiene los mismos plazos que se indican en la política de soporte oficial de Python para los SDK y las herramientas de AWS. Los intérpretes solo se admiten 6 meses después de la fecha de fin de soporte.
4. (Opcional) Instale todas las dependencias de compilación y ejecución de la biblioteca de Python de la AWS CLI. El comando `./configure` le informa si le falta alguna dependencia y cómo instalarla.

   Puede instalar y utilizar estas dependencias automáticamente mediante la configuración; consulte the section called “Descarga de dependencias” para obtener más información.

Paso 2: configurar la instalación de origen de la AWS CLI

La configuración para compilar e instalar la AWS CLI se especifica mediante el script `configure`. Para obtener la documentación de todas las opciones de configuración, ejecute el script `configure` con la opción `--help`:

Linux and macOS

```
$ ./configure --help
```

Windows PowerShell

```
PS C:\> C:\msys64\usr\bin\bash -lc "./configure --help"
```

Las opciones más importantes son las siguientes:

- Ubicación de instalación
- Intérprete de Python
- Descarga de dependencias
- Tipo de instalación

Ubicación de instalación

La instalación de origen de la AWS CLI utiliza dos directorios configurables para instalar la AWS CLI:

- `libdir`: directorio principal donde se instalará la AWS CLI. La ruta de acceso a la instalación de la AWS CLI es *<libdir-value>*`/aws-cli`. El valor predeterminado de `libdir` para Linux y macOS es `/usr/local/lib`, que crea el directorio de instalación predeterminado */usr/local/lib*`/aws-cli`.
- `bindir`: directorio donde están instalados los ejecutables de la AWS CLI. La ubicación predeterminada es `/usr/local/bin`.

Las siguientes opciones de `configure` controlan los directorios utilizados:

- `--prefix`: establece el prefijo del directorio que se utilizará para la instalación. El valor predeterminado para Linux y macOS es `/usr/local`.

- `--libdir`: establece el `libdir` que se utilizará para instalar la AWS CLI. El valor predeterminado es `<prefix-value>/lib`. Si no se especifican `--libdir` ni `--prefix`, el valor predeterminado para Linux y macOS es `/usr/local/lib/`.
- `--bindir`: establece el `bindir` que se utilizará para instalar los ejecutables AWS CLI, `aws` y `aws_completer`. El valor predeterminado es `<prefix-value>/bin`. Si no se especifican `bindir` ni `--prefix`, el valor predeterminado para Linux y macOS es `/usr/local/bin/`.

Linux and macOS

En el siguiente comando de ejemplo, se utiliza la opción `--prefix` para realizar una instalación de la AWS CLIpor parte del usuario local. Este comando instala la AWS CLI en `$HOME/.local/lib/aws-cli` y los ejecutables en `$HOME/.local/bin`:

```
$ ./configure --prefix=$HOME/.local
```

En el siguiente comando de ejemplo, se utiliza la opción `--libdir` para instalar la AWS CLI como aplicación complementaria en el directorio `/opt`. Este comando instala la AWS CLI en `/opt/aws-cli` y los ejecutables en su ubicación predeterminada de `/usr/local/bin`.

```
$ ./configure --libdir=/opt
```

Windows PowerShell

En el siguiente comando de ejemplo, se utiliza la opción `--prefix` para realizar una instalación de la AWS CLIpor parte del usuario local. Este comando instala la AWS CLI en `$HOME/.local/lib/aws-cli` y los ejecutables en `$HOME/.local/bin`:

```
$ C:\msys64\usr\bin\bash -lc "./configure --prefix='C:\Program Files\AWSCLI'"
```

En el siguiente comando de ejemplo, se utiliza la opción `--libdir` para instalar la AWS CLI como aplicación complementaria en el directorio `/opt`. Este comando instala la AWS CLI en `C:\Program Files\AWSCLI\opt\aws-cli`.

Intérprete de Python

> **Note**
>
> Se recomienda encarecidamente especificar el intérprete de Python al realizar la instalación para Windows.

El script `./configure` selecciona automáticamente un intérprete instalado de Python 3.8 o una versión posterior para usarlo para compilar y ejecutar la AWS CLI utilizando la macro de Autoconf `AM_PATH_PYTHON`.

El intérprete de Python que se utilice se puede configurar explícitamente mediante la variable de entorno PYTHON al ejecutar el script `configure`:

Linux and macOS

```
$ PYTHON=/path/to/python ./configure
```

Windows PowerShell

```
PS C:\> C:\msys64\usr\bin\bash -lc "PYTHON='C:\path\to\python' ./configure"
```

Descarga de dependencias

De forma predeterminada, se requiere que todas las dependencias de compilación y ejecución de la AWS CLI estén instaladas ya en el sistema. Esto incluye cualquier dependencia de la biblioteca de Python. Todas las dependencias se comprueban cuando se ejecuta el script `configure` y, si al sistema le falta alguna dependencia de Python, se produce un error en el script `configure`.

El siguiente ejemplo de código genera un error cuando faltan dependencias en el sistema:

Linux and macOS

```
$ ./configure
checking for a Python interpreter with version >= 3.8... python
checking for python... /Users/username/.envs/env3.11/bin/python
checking for python version... 3.11
checking for python platform... darwin
```

```
checking for GNU default python prefix... ${prefix}
checking for GNU default python exec_prefix... ${exec_prefix}
checking for python script directory (pythondir)... ${PYTHON_PREFIX}/lib/python3.11/
site-packages
checking for python extension module directory (pyexecdir)... ${PYTHON_EXEC_PREFIX}/
lib/python3.11/site-packages
checking for --with-install-type... system-sandbox
checking for --with-download-deps... Traceback (most recent call last):
  File "<frozen runpy>", line 198, in _run_module_as_main
  File "<frozen runpy>", line 88, in _run_code
  File "/Users/username/aws-code/aws-cli/./backends/build_system/__main__.py", line
 125, in <module>
    main()
  File "/Users/username/aws-code/aws-cli/./backends/build_system/__main__.py", line
 121, in main
    parsed_args.func(parsed_args)
  File "/Users/username/aws-code/aws-cli/./backends/build_system/__main__.py", line
 49, in validate
    validate_env(parsed_args.artifact)
  File "/Users/username/aws-code/aws-cli/./backends/build_system/validate_env.py",
 line 68, in validate_env
    raise UnmetDependenciesException(unmet_deps, in_venv)
validate_env.UnmetDependenciesException: Environment requires following Python
 dependencies:

awscrt (required: ('>=0.12.4', '<0.17.0')) (version installed: None)

We recommend using --with-download-deps flag to automatically create a virtualenv
 and download the dependencies.

If you want to manage the dependencies yourself instead, run the following pip
 command:
/Users/username/.envs/env3.11/bin/python -m pip install --prefer-binary
 'awscrt>=0.12.4,<0.17.0'

configure: error: "Python dependencies not met."
```

Windows PowerShell

```
PS C:\> C:\msys64\usr\bin\bash -lc "./configure"
checking for a Python interpreter with version >= 3.8... python
checking for python... /Users/username/.envs/env3.11/bin/python
checking for python version... 3.11
```

```
checking for python platform... darwin
checking for GNU default python prefix... ${prefix}
checking for GNU default python exec_prefix... ${exec_prefix}
checking for python script directory (pythondir)... ${PYTHON_PREFIX}/lib/python3.11/
site-packages
checking for python extension module directory (pyexecdir)... ${PYTHON_EXEC_PREFIX}/
lib/python3.11/site-packages
checking for --with-install-type... system-sandbox
checking for --with-download-deps... Traceback (most recent call last):
  File "<frozen runpy>", line 198, in _run_module_as_main
  File "<frozen runpy>", line 88, in _run_code
  File "/Users/username/aws-code/aws-cli/./backends/build_system/__main__.py", line
 125, in <module>
    main()
  File "/Users/username/aws-code/aws-cli/./backends/build_system/__main__.py", line
 121, in main
    parsed_args.func(parsed_args)
  File "/Users/username/aws-code/aws-cli/./backends/build_system/__main__.py", line
 49, in validate
    validate_env(parsed_args.artifact)
  File "/Users/username/aws-code/aws-cli/./backends/build_system/validate_env.py",
 line 68, in validate_env
    raise UnmetDependenciesException(unmet_deps, in_venv)
validate_env.UnmetDependenciesException: Environment requires following Python
 dependencies:

awscrt (required: ('>=0.12.4', '<0.17.0')) (version installed: None)

We recommend using --with-download-deps flag to automatically create a virtualenv
 and download the dependencies.

If you want to manage the dependencies yourself instead, run the following pip
 command:
/Users/username/.envs/env3.11/bin/python -m pip install --prefer-binary
 'awscrt>=0.12.4,<0.17.0'

configure: error: "Python dependencies not met."
```

Para instalar automáticamente las dependencias de Python necesarias, utilice la opción `--with-download-deps`. Al usar este indicador, el proceso de compilación hace lo siguiente:

- Omite la comprobación de dependencias de la biblioteca de Python.

- Configura los ajustes para descargar todas las dependencias de Python necesarias y usar solo las dependencias descargadas para compilar la AWS CLI durante la compilación `make`.

En el siguiente ejemplo del comando de configuración, se usa la opción `--with-download-deps` para descargar y usar las dependencias de Python:

Linux and macOS

```
$ ./configure --with-download-deps
```

Windows PowerShell

```
PS C:\> C:\msys64\usr\bin\bash -lc "./configure --with-download-deps"
```

Tipo de instalación

El proceso de instalación de origen admite los siguientes tipos de instalación:

- `system-sandbox`: (predeterminado) Crea un entorno virtual aislado de Python, instala la AWS CLI en el entorno virtual y utiliza symlinks al ejecutable `aws` y `aws_completer` en el entorno virtual. Esta instalación de la AWS CLI depende directamente del intérprete de Python seleccionado para su tiempo de ejecución.

  Se trata de un mecanismo de instalación ligero para instalar la AWS CLI en un sistema y sigue las prácticas recomendadas de Python al utilizar un entorno aislado en la instalación en un entorno virtual. Esta instalación está destinada a clientes que desean instalar la AWS CLI desde el origen de la forma más sencilla posible con la instalación acoplada a su instalación de Python.
- `portable-exe`: congela la AWS CLI en un ejecutable independiente que se puede distribuir a entornos de arquitecturas similares. Es el mismo proceso que se utiliza para generar los ejecutables oficiales prediseñados de la AWS CLI. La `portable-exe` se congela en una copia del intérprete de Python elegido en el paso `configure` para usarlo para el tiempo de ejecución de la AWS CLI. Esto permite moverlo a otras máquinas que es posible que no tengan un intérprete de Python.

  Este tipo de compilaciones son útiles porque puede asegurarse de que la instalación de la AWS CLI no esté acoplada a la versión de Python instalada en el entorno y puede distribuir una

compilación a otro sistema que tal vez no tenga instalado Python. Esto le permite controlar las dependencias y la seguridad de los ejecutables de la AWS CLI que utiliza.

Para configurar el tipo de instalación, utilice la opción `--with-install-type` y especifique un valor de `portable-exe` o `system-sandbox`.

En el siguiente comando `./configure` de ejemplo, se especifica un valor de `portable-exe`:

Linux and macOS

```
$ ./configure --with-install-type=portable-exe
```

Windows PowerShell

```
PS C:\> C:\msys64\usr\bin\bash -lc "./configure --with-install-type=portable-exe"
```

Paso 3: compilar la AWS CLI

Utilice el comando `make` para compilar la AWS CLI con sus ajustes de configuración:

Linux and macOS

```
$ make
```

Windows PowerShell

```
PS C:\> C:\msys64\usr\bin\bash -lc "make"
```

> **Note**
>
> Al utilizar el comando **`make`**, los siguientes pasos se realizan entre bastidores:
>
> 1. Se crea un entorno virtual en el directorio de compilación mediante el módulo `venv` de Python. El entorno virtual se inicia con una versión de pip que se suministra en la biblioteca estándar de Python.

2. Se copian las dependencias de la biblioteca de Python. Dependiendo de si el indicador `--with-download-deps` está especificado en el comando `configure`, este paso realiza una de las siguientes acciones:

   - Se especifica `--with-download-deps`. Las dependencias de Python se instalan con pip. Esto incluye `wheel`, `setuptools` y todas las dependencias en tiempo de ejecución de AWS CLI. Si está compilando el `portable-exe`, se instala `pyinstaller`. Todos estos requisitos se especifican en los archivos de bloqueo generados desde `pip-compile`.
   - No se especifica `--with-download-deps`. Las bibliotecas de Python del paquete del sitio del intérprete de Python más cualquier script (por ejemplo, `pyinstaller`) se copian en el entorno virtual que se utiliza para la compilación.

3. Se ejecuta `pip install` directamente en el código base de la AWS CLI para realizar una compilación e instalación sin conexión de la AWS CLI dentro del árbol en el entorno virtual de compilación. Esta instalación usa los indicadores pip --no-build-isolation, --use-feature=in-tree-build, --no-cache-dir y `--no-index`.
4. (Opcional) Si la `--install-type` se establece en `portable-exe` en el comando `configure`, compila un ejecutable independiente mediante `pyinstaller`.

Paso 4: instalar la AWS CLI

El comando `make install` instala la AWS CLI compilada en la ubicación configurada del sistema.

Linux and macOS

El siguiente comando de ejemplo instala la AWS CLI utilizando sus ajustes de configuración y compilación:

```
$ make install
```

Windows PowerShell

El siguiente comando de ejemplo instala la AWS CLI utilizando sus ajustes de configuración y compilación y, a continuación, añade una variable de entorno con la ruta de la AWS CLI:

```
PS C:\> C:\msys64\usr\bin\bash -lc " make install "
```

```
PS C:\> $Env:PATH +=";C:\Program Files\AWSCLI\bin\"
```

La regla `make install` admite la variable DESTDIR. Cuando se especifica, esta variable se usa como prefijo en la ruta especificada a la ruta de instalación ya configurada al instalar la AWS CLI. De forma predeterminada, no se establece ningún valor para esta variable.

Linux and macOS

En el siguiente código de ejemplo, se utiliza un indicador `--prefix=/usr/local` para configurar una ubicación de instalación y, a continuación, se modifica ese destino mediante `DESTDIR=/tmp/stage` para el comando `make install`. Estos comandos hacen que se instale la AWS CLI en `/tmp/stage/usr/local/lib/aws-cli` y sus ejecutables se colocan en `/tmp/stage/usr/local/bin`.

```
$ ./configure --prefix=/usr/local
$ make
$ make DESTDIR=/tmp/stage install
```

Windows PowerShell

En el siguiente código de ejemplo, se utiliza un indicador `--prefix=\awscli` para configurar una ubicación de instalación y, a continuación, se modifica ese destino mediante `DESTDIR=C:\Program Files` para el comando `make install`. Estos comandos hacen que la AWS CLI se instale en `C:\Program Files\awscli`.

```
$ ./configure --prefix=\awscli
$ make
$ make DESTDIR='C:\Program Files' install
```

> **Note**
>
> Cuando se ejecuta **`make install`**, se realizan los siguientes pasos entre bastidores
>
> 1. Se mueve uno de los siguientes elementos al directorio de instalación configurado:
>
>   - Si el tipo de instalación es `system-sandbox`, se mueve el entorno virtual compilado.
>   - Si el tipo de instalación es un `portable-exe`, se mueve el ejecutable independiente compilado.

2. Crea symlinks tanto para los ejecutables `aws` y `aws_completer` como para los ejecutables del directorio bin configurado.

Paso 5: verificar la instalación de AWS CLI

Confirme que la AWS CLI se ha instalado correctamente utilizando el siguiente comando:

```
$ aws --version
aws-cli/2.27.41 Python/3.11.6 Windows/10 exe/AMD64 prompt/off
```

Si no se reconoce el comando `aws`, es posible que deba reiniciar el terminal para que se actualicen los nuevos symlink. Si se encuentra con más problemas después de instalar o desinstalar la AWS CLI, consulte en the section called “Errores de solución de problemas” los pasos para la solución de problemas comunes.

Ejemplos de flujo de trabajo

En esta sección, se proporcionan algunos ejemplos básicos de flujos de trabajo básicos para la instalación desde el origen.

Instalación básica de Linux y macOS

A continuación, se ofrece un flujo de trabajo de instalación básico de ejemplo en el que la AWS CLI se instala en la ubicación predeterminada de `/usr/local/lib/aws-cli`.

```
$ cd path/to/cli/respository/
$ ./configure
$ make
$ make install
```

Instalación automatizada de Windows

> **Note**
>
> Debe ejecutar PowerShell como administrador para utilizar este flujo de trabajo.

MSYS2 se puede utilizar de forma automatizada en una configuración de CI; consulte Using MSYS2 in CI (Uso de MSYS2 en CI) en MSYS2 Documentation (Documentación de MSYS2).

Downloaded Tarball

Descargue el archivo `awscli.tar.gz`, extráigalo e instale la AWS CLI. Al utilizar los siguientes comandos, sustituya las siguientes rutas:

- `C:\msys64\usr\bin\bash` por la ubicación de su ruta de MSYS2.
- `.\awscli-2.x.x\` por el nombre de la carpeta `awscli.tar.gz` extraída.
- `PYTHON='C:\path\to\python.exe'` por su ruta local de Python.

En el siguiente código de ejemplo, se automatiza la compilación e instalación de la AWS CLI desde PowerShell mediante MSYS2 y se especifica qué instalación local de Python se debe utilizar:

```
PS C:\> curl "https://awscli.amazonaws.com/awscli.tar.gz" -o "awscliv2.zip"  #
 Download the awscli.tar.gz file in the current working directory
PS C:\> tar -xvzf .\awscli.tar.gz #  Extract awscli.tar.gz file
PS C:\> cd .\awscli-2.x.x\ #  Navigate to the root of the extracted files
PS C:\> $env:CHERE_INVOKING = 'yes' #  Preserve the current working directory
PS C:\> C:\msys64\usr\bin\bash  -lc " PYTHON='C:\path\to\python.exe' ./configure --
prefix='C:\Program Files\AWSCLI' --with-download-deps "
PS C:\> C:\msys64\usr\bin\bash  -lc "make"
PS C:\> C:\msys64\usr\bin\bash  -lc "make install"
PS C:\> $Env:PATH +=";C:\Program Files\AWSCLI\bin\"
PS C:\> aws --version
aws-cli/2.27.41 Python/3.11.6 Windows/10 source-sandbox/AMD64
```

GitHub Repository

Descargue el archivo `awscli.tar.gz`, extráigalo e instale la AWS CLI. Al utilizar los siguientes comandos, sustituya las siguientes rutas:

- `C:\msys64\usr\bin\bash` por la ubicación de su ruta de MSYS2.
- `C:path\to\cli\repository\` por la ruta a su repositorio de la AWS CLI clonado desde GitHub. Para obtener más información, consulte Fork a repo (Bifurcar un repositorio) en GitHub Docs (Documentación de GitHub).
- `PYTHON='C:\path\to\python.exe'` por su ruta local de Python.

En el siguiente código de ejemplo, se automatiza la compilación e instalación de la AWS CLI desde PowerShell mediante MSYS2 y se especifica qué instalación local de Python se debe utilizar:

```
PS C:\> cd C:path\to\cli\repository\
PS C:\> $env:CHERE_INVOKING = 'yes' #  Preserve the current working directory
PS C:\> C:\msys64\usr\bin\bash  -lc " PYTHON='C:\path\to\python.exe' ./configure --
prefix='C:\Program Files\AWSCLI' --with-download-deps "
PS C:\> C:\msys64\usr\bin\bash  -lc "make"
PS C:\> C:\msys64\usr\bin\bash  -lc "make install"
PS C:\> $Env:PATH +=";C:\Program Files\AWSCLI\bin\"
PS C:\> aws --version
```

Contenedor de Alpine Linux

A continuación, se muestra un Dockerfile de ejemplo que se puede utilizar para conseguir una instalación funcional de la AWS CLI en un contenedor de Alpine Linux como alternativa a los binarios prediseñados para Alpine. Al utilizar este ejemplo, sustituya *AWSCLI_VERSION* por el número de versión de la AWS CLI deseado:

```
FROM python:3.8-alpine AS builder

ENV AWSCLI_VERSION=2.10.1

RUN apk add --no-cache \
    curl \
    make \
    cmake \
    gcc \
    g++ \
    libc-dev \
    libffi-dev \
    openssl-dev \
    && curl https://awscli.amazonaws.com/awscli-${AWSCLI_VERSION}.tar.gz | tar -xz \
    && cd awscli-${AWSCLI_VERSION} \
    && ./configure --prefix=/opt/aws-cli/ --with-download-deps \
    && make \
    && make install

FROM python:3.8-alpine
```

```
RUN apk --no-cache add groff

COPY --from=builder /opt/aws-cli/ /opt/aws-cli/

ENTRYPOINT ["/opt/aws-cli/bin/aws"]
```

Se compila esta imagen y se invoca la AWS CLI desde un contenedor similar al que se compila en Amazon Linux 2:

```
$ docker build --tag awscli-alpine .
$ docker run --rm -it awscli-alpine --version
aws-cli/2.2.1 Python/3.8.11 Linux/5.10.25-linuxkit source-sandbox/x86_64.alpine.3
 prompt/off
```

El tamaño final de esta imagen es más pequeño que el tamaño de la imagen de Docker oficial de la AWS CLI. Para obtener información sobre la imagen de Docker oficial, consulte the section called “Amazon ECR Public/Docker”.

Solución de errores de instalación y desinstalación de AWS CLI

Para ver los pasos de solución de problemas relacionados con los errores de instalación, consulte the section called “Errores de solución de problemas” para conocer los pasos de solución de problemas comunes. Para conocer los pasos más relevantes de la solución de problemas, consulte the section called “Errores de comando no encontrado”, the section called “El comando "`aws --version`" devuelve una versión diferente a la instalada” y the section called “El comando "`aws --version`" devuelve una versión después de desinstalar la AWS CLI”.

Para cualquier problema que no esté incluido en las guías de solución de problemas, busque los problemas con la etiqueta `source-distribution` en el Repositorio de la AWS CLI de GitHub. Si no existe ningún problema que se refiera a sus errores, cree un nuevo problema para recibir ayuda de los mantenedores de la AWS CLI.

Pasos a seguir a continuación

Después de instalar la AWS CLI, debe realizar un the section called “Configuración”.

Ejecución de las imágenes oficiales de Amazon ECR Public o Docker para la AWS CLI

En este tema se describe cómo ejecutar, controlar la versión y configurar la AWS CLI versión 2 en Docker mediante la imagen oficial de Amazon Elastic Container Registry Public (Amazon ECR Public) o Docker Hub. Para obtener más información sobre cómo usar Docker, consulte la documentación de Docker.

Las imágenes oficiales proporcionan aislamiento, portabilidad y seguridad que AWS respalda y mantiene directamente. Esto le permite utilizar la versión 2 de la AWS CLI en un entorno basado en contenedores sin tener que administrar la instalación usted mismo.

Temas

- Requisitos previos
- Decisión entre Amazon ECR Public y Docker Hub
- Ejecución de las imágenes oficiales de AWS CLI versión 2
- Notas sobre interfaces y compatibilidad con versiones anteriores de las imágenes oficiales
- Uso de versiones y etiquetas específicas
- Actualización a la imagen oficial más reciente
- Comparta llos archivos anfitrión, credenciales, variables del entorno y configuración
- Acortamiento del comando docker run

Requisitos previos

Debe tener instalado Docker. Para obtener instrucciones de instalación, consulte el sitio web de Docker.

Para verificar la instalación de Docker, ejecute el siguiente comando y confirme que hay un resultado.

```
$ docker --version
Docker version 19.03.1
```

Decisión entre Amazon ECR Public y Docker Hub

Recomendamos utilizar Amazon ECR Public en lugar de Docker Hub para las imágenes de la AWS CLI. Docker Hub tiene una limitación de velocidad más estricta para los consumidores públicos, lo que puede causar problemas de limitación. Además, Amazon ECR Public replica imágenes en más de una región para proporcionar una disponibilidad sólida y controlar los problemas de interrupción de las regiones.

Para obtener más información sobre la limitación de velocidad de Docker Hub consulte Understanding Docker Hub Rate Limiting (Descripción de la limitación de velocidad de Docker Hub) en el sitio web de Docker.

Ejecución de las imágenes oficiales de AWS CLI versión 2

La primera vez que utilice el comando `docker run`, se descargará la última imagen en su equipo. Cada uso posterior del comando `docker run` se ejecuta desde la copia local.

Para ejecutar las imágenes Docker de la AWS CLI versión 2, utilice el comando `docker run`.

Amazon ECR Public

La imagen de Amazon ECR Public oficial de la AWS CLI versión 2 está alojada en Amazon ECR Public en el repositorio de `aws-cli/aws-cli`.

```
$ docker run --rm -it public.ecr.aws/aws-cli/aws-cli command
```

Docker Hub

La imagen de Docker oficial de la AWS CLI versión 2 está alojada en Docker Hub en el repositorio de `amazon/aws-cli`.

```
$ docker run --rm -it amazon/aws-cli command
```

El comando funciona de la siguiente manera:

- `docker run --rm -it` *`repository/name`*: el equivalente de la `aws` ejecutable. Cada vez que ejecuta este comando, Docker hace girar un contenedor de la imagen descargada y ejecuta el comando `aws`. De forma predeterminada, la imagen utiliza la versión más reciente de la AWS CLI versión 2.

Por ejemplo, para llamar al comando `aws --version` en Docker, ejecute lo siguiente.

Amazon ECR Public

```
$ docker run --rm -it public.ecr.aws/aws-cli/aws-cli --version
aws-cli/2.27.41 Python/3.7.3 Linux/4.9.184-linuxkit botocore/2.4.5dev10
```

Docker Hub

```
$ docker run --rm -it amazon/aws-cli --version
aws-cli/2.27.41 Python/3.7.3 Linux/4.9.184-linuxkit botocore/2.4.5dev10
```

- `--rm`: especifica que se limpie el contenedor después de que el comando salga.
- `-it`: especifica que se abra un pseudoTTY con `stdin`. Esto le permite proporcionar datos a la versión 2 de la AWS CLI mientras se está ejecutando en un contenedor, por ejemplo, mediante el uso de los comandos `aws configure` y `aws help`. Al elegir si se debe omitir `-it`, tenga en cuenta lo siguiente:
  - Si está ejecutando scripts, `-it` no es necesario.
  - Si experimenta errores con los scripts, omitir `-it` de la llamada Docker puede resolver el problema.
  - Si está intentando canalizar la salida, `-it` puede provocar errores y la omisión `-it` de la llamada Docker puede resolver este problema. Si desea conservar la marca `-it`, pero aún así quisiera canalizar la salida, desactivar la Paginación del lado del cliente que AWS CLI usa de forma predeterminada debería resolver el problema.

Para obtener más información sobre el comando `docker run`, consulte la guía de referencia de Docker.

Notas sobre interfaces y compatibilidad con versiones anteriores de las imágenes oficiales

- La única herramienta admitida en la imagen es AWS CLI. Solo el ejecutable `aws` se debe ejecutar directamente. Por ejemplo, aunque `less` y `groff` están instalados explícitamente en la imagen, no se deben ejecutar directamente fuera de un comando AWS CLI.
- El directorio de trabajo de `/aws` está controlado por el usuario. La imagen no se escribirá en este directorio, a menos que el usuario le indique que ejecute un comando de AWS CLI.

- No hay garantías de compatibilidad con versiones anteriores para confiar en la última etiqueta. Para garantizar la compatibilidad con versiones anteriores, debe anclar una etiqueta `<major.minor.patch>` específica, ya que esas etiquetas son inmutables; solo se enviarán una vez.

Uso de versiones y etiquetas específicas

La imagen oficial de la AWS CLI versión 2 tiene varias versiones que puede usar, comenzando con la versión `2.0.6`. Para ejecutar una versión específica de la versión 2 de la AWS CLI, agregue la etiqueta adecuada al comando `docker run`. La primera vez que utiliza el comando `docker run` con una etiqueta, la imagen más reciente para esa etiqueta se descarga en el equipo. Cada uso posterior del comando `docker run` con esa etiqueta se ejecuta desde la copia local.

Puede utilizar dos tipos de etiquetas:

- `latest`: define la última versión de la de la AWS CLI versión 2 para la imagen. Le recomendamos que utilice la etiqueta `latest` cuando desee la versión más reciente de la versión 2 de la AWS CLI. Sin embargo, no hay garantías de compatibilidad con versiones anteriores al usar esta etiqueta. La etiqueta `latest` se utiliza de forma predeterminada en el comando `docker run`. Para utilizar explícitamente la etiqueta `latest`, agregue la etiqueta al nombre de la imagen del contenedor.

  Amazon ECR Public

  ```
  $ docker run --rm -it public.ecr.aws/aws-cli/aws-cli:latest command
  ```

  Docker Hub

  ```
  $ docker run --rm -it amazon/aws-cli:latest command
  ```

- `<major.minor.patch>`: define una versión específica de la AWS CLI versión 2 para la imagen Docker. Si piensa utilizar una imagen oficial en producción, le recomendamos que use una versión específica de la AWS CLI versión 2 para garantizar la compatibilidad con versiones anteriores. Por ejemplo, para ejecutar la versión `2.0.6`, agregue la versión al nombre de la imagen del contenedor.

  Amazon ECR Public

  ```
  $ docker run --rm -it public.ecr.aws/aws-cli/aws-cli:2.0.6 command
  ```

Docker Hub

```
$ docker run --rm -it amazon/aws-cli:2.0.6 command
```

Actualización a la imagen oficial más reciente

Dado que la imagen más reciente se descarga en el equipo solo la primera vez que utiliza el comando `docker run`, debe extraer manualmente una imagen actualizada. Para actualizar manualmente a la versión más reciente, le recomendamos que extraiga la imagen etiquetada `latest`. Al extraer la imagen, se descarga la versión más reciente en el equipo.

Amazon ECR Public

```
$ docker pull public.ecr.aws/aws-cli/aws-cli:latest
```

Docker Hub

```
$ docker pull amazon/aws-cli:latest
```

Comparta llos archivos anfitrión, credenciales, variables del entorno y configuración

Dado que la versión 2 de la AWS CLI se ejecuta en un contenedor, la CLI no puede acceder de forma predeterminada al sistema de archivos anfitrión, que incluye la configuración y las credenciales. Para compartir el sistema de archivos anfitrión, las credenciales y la configuración en el contenedor, monte el directorio `~/.aws` del sistema host en el contenedor en `/root/.aws` con la etiqueta `-v` del comando `docker run`. Esto permite que la versión 2 de la AWS CLI, que se está ejecutando en el contenedor, localice la información del archivo anfitrión.

Amazon ECR Public

Linux y macOS

```
$ docker run --rm -it -v ~/.aws:/root/.aws public.ecr.aws/aws-cli/aws-cli command
```

Símbolo del sistema de Windows

```
$ docker run --rm -it -v %userprofile%\.aws:/root/.aws public.ecr.aws/aws-cli/aws-cli command
```

Windows PowerShell

```
C:\> docker run --rm -it -v $env:userprofile\.aws:/root/.aws  public.ecr.aws/aws-cli/aws-cli command
```

Docker Hub

Linux y macOS

```
$ docker run --rm -it -v ~/.aws:/root/.aws amazon/aws-cli command
```

Símbolo del sistema de Windows

```
$ docker run --rm -it -v %userprofile%\.aws:/root/.aws amazon/aws-cli command
```

Windows PowerShell

```
C:\> docker run --rm -it -v $env:userprofile\.aws:/root/.aws  amazon/aws-cli command
```

Para obtener más información acerca la etiqueta `-v` y el montaje, consulte la guía de referencia de Docker.

> **Note**
>
> Para obtener información sobre los archivos de `config` y `credentials`, consulte the section called “Opciones de configuración”.

Ejemplo 1: proporcionar credenciales y configuración

En este ejemplo, proporcionamos las credenciales de anfitrión y la configuración al ejecutar el comando `s3 ls` para mostrar los buckets en Amazon Simple Storage Service (Amazon S3). Los siguientes ejemplos utilizan la ubicación predeterminada para los archivos de credenciales y de configuración de la AWS CLI, para utilizar una ubicación diferente, cambie la ruta del archivo.

Amazon ECR Public

Linux y macOS

```
$ docker run --rm -it -v ~/.aws:/root/.aws public.ecr.aws/aws-cli/aws-cli s3 ls
2020-03-25 00:30:48 aws-cli-docker-demo
```

Símbolo del sistema de Windows

```
$ docker run --rm -it -v %userprofile%\.aws:/root/.aws public.ecr.aws/aws-cli/aws-
cli s3 ls
2020-03-25 00:30:48 aws-cli-docker-demo
```

Windows PowerShell

```
C:\> docker run --rm -it -v $env:userprofile\.aws:/root/.aws public.ecr.aws/aws-cli/
aws-cli s3 ls
```

Docker Hub

Linux y macOS

```
$ docker run --rm -it -v ~/.aws:/root/.aws amazon/aws-cli s3 ls
2020-03-25 00:30:48 aws-cli-docker-demo
```

Símbolo del sistema de Windows

```
$ docker run --rm -it -v %userprofile%\.aws:/root/.aws amazon/aws-cli s3 ls
2020-03-25 00:30:48 aws-cli-docker-demo
```

Windows PowerShell

```
C:\> docker run --rm -it -v $env:userprofile\.aws:/root/.aws amazon/aws-cli s3 ls
```

Puede llamar a variables de entorno específicas del sistema utilizando el marcador `-e`. Para utilizar una variable de entorno, llámelo por su nombre.

Amazon ECR Public

Linux y macOS

```
$ docker run --rm -it -v ~/.aws:/root/.aws -e ENVVAR_NAME public.ecr.aws/aws-cli/
aws-cli s3 ls
2020-03-25 00:30:48 aws-cli-docker-demo
```

Símbolo del sistema de Windows

```
$ docker run --rm -it -v %userprofile%\.aws:/root/.aws -e ENVVAR_NAME
 public.ecr.aws/aws-cli/aws-cli s3 ls
2020-03-25 00:30:48 aws-cli-docker-demo
```

Windows PowerShell

```
C:\> docker run --rm -it -v $env:userprofile\.aws:/root/.aws -e ENVVAR_NAME
 public.ecr.aws/aws-cli/aws-cli s3 ls
```

Docker Hub

Linux y macOS

```
$ docker run --rm -it -v ~/.aws:/root/.aws -e ENVVAR_NAME amazon/aws-cli s3 ls
2020-03-25 00:30:48 aws-cli-docker-demo
```

Símbolo del sistema de Windows

```
$ docker run --rm -it -v %userprofile%\.aws:/root/.aws -e ENVVAR_NAME amazon/aws-cli
 s3 ls
2020-03-25 00:30:48 aws-cli-docker-demo
```

Windows PowerShell

```
C:\> docker run --rm -it -v $env:userprofile\.aws:/root/.aws -e ENVVAR_NAME amazon/
aws-cli s3 ls
```

Ejemplo 2: Descarga de un archivo Amazon S3 en el sistema de anfitrión

Para algunos comandos de la AWS CLI versión 2, puede leer archivos del sistema de host en el contenedor o escribir archivos desde el contenedor en el sistema de host.

En este ejemplo, descargamos el objeto S3 `s3://aws-cli-docker-demo/hello` a su sistema de archivos local montando el directorio de trabajo actual en el directorio `/aws` del contenedor. Al descargar el objeto `hello` en el directorio `/aws` del contenedor, el archivo también se guarda en el directorio de trabajo actual del sistema de host.

Amazon ECR Public

Linux y macOS

```
$ docker run --rm -it -v ~/.aws:/root/.aws -v $(pwd):/aws public.ecr.aws/aws-cli/
aws-cli s3 cp s3://aws-cli-docker-demo/hello .
download: s3://aws-cli-docker-demo/hello to ./hello
```

Símbolo del sistema de Windows

```
$ docker run --rm -it -v %userprofile%\.aws:/root/.aws -v %cd%:/aws public.ecr.aws/
aws-cli/aws-cli s3 cp s3://aws-cli-docker-demo/hello .
download: s3://aws-cli-docker-demo/hello to ./hello
```

Windows PowerShell

```
C:\> docker run --rm -it -v $env:userprofile\.aws:/root/.aws -v $pwd\aws:/aws
 public.ecr.aws/aws-cli/aws-cli s3 cp s3://aws-cli-docker-demo/hello .
```

Docker Hub

Linux y macOS

```
$ docker run --rm -it -v ~/.aws:/root/.aws -v $(pwd):/aws amazon/aws-cli s3 cp s3://
aws-cli-docker-demo/hello .
download: s3://aws-cli-docker-demo/hello to ./hello
```

Símbolo del sistema de Windows

```
$ docker run --rm -it -v %userprofile%\.aws:/root/.aws -v %cd%:/aws amazon/aws-cli
 s3 cp s3://aws-cli-docker-demo/hello .
download: s3://aws-cli-docker-demo/hello to ./hello
```

Windows PowerShell

```
C:\> docker run --rm -it -v $env:userprofile\.aws:/root/.aws -v $pwd\aws:/aws
 amazon/aws-cli s3 cp s3://aws-cli-docker-demo/hello .
```

Para confirmar que el archivo descargado existe en el sistema de archivos local, ejecute lo siguiente.

Linux y macOS

```
$ cat hello
Hello from Docker!
```

Windows PowerShell

```
$ type hello
Hello from Docker!
```

Ejemplo 3: uso de la variable de entorno AWS_PROFILE

Puede llamar a variables de entorno específicas del sistema utilizando el marcador `-e`. Llame a cada variable de entorno que desee utilizar. En este ejemplo, proporcionamos las credenciales de anfitrión, la configuración y la variable de entorno *`AWS_PROFILE`* cuando se ejecuta el comando `s3 ls` para mostrar los buckets en Amazon Simple Storage Service (Amazon S3).

Amazon ECR Public

Linux y macOS

```
$ docker run --rm -it -v ~/.aws:/root/.aws -e AWS_PROFILE public.ecr.aws/aws-cli/
aws-cli s3 ls
2020-03-25 00:30:48 aws-cli-docker-demo
```

Símbolo del sistema de Windows

```
$ docker run --rm -it -v %userprofile%\.aws:/root/.aws -e AWS_PROFILE
 public.ecr.aws/aws-cli/aws-cli s3 ls
2020-03-25 00:30:48 aws-cli-docker-demo
```

Windows PowerShell

```
C:\> docker run --rm -it -v $env:userprofile\.aws:/root/.aws -e AWS_PROFILE
 public.ecr.aws/aws-cli/aws-cli s3 ls
```

Docker Hub

Linux y macOS

```
$ docker run --rm -it -v ~/.aws:/root/.aws -e AWS_PROFILE amazon/aws-cli s3 ls
2020-03-25 00:30:48 aws-cli-docker-demo
```

Símbolo del sistema de Windows

```
$ docker run --rm -it -v %userprofile%\.aws:/root/.aws -e AWS_PROFILE amazon/aws-cli
 s3 ls
2020-03-25 00:30:48 aws-cli-docker-demo
```

Windows PowerShell

```
C:\> docker run --rm -it -v $env:userprofile\.aws:/root/.aws -e AWS_PROFILE amazon/
aws-cli s3 ls
```

Acortamiento del comando docker run

Para acortar el comando `docker run`, le sugerimos que utilice la capacidad del sistema operativo para crear un `symbolic link` (enlace simbólico) o `alias` en Linux y macOS o `doskey` en Windows. Para establecer el alias de `aws`, puede ejecutar uno de los siguientes comandos:

- Para obtener acceso básico a los comandos de `aws`, ejecute lo siguiente.

  Amazon ECR Public

  Linux y macOS

  ```
  $ alias aws='docker run --rm -it public.ecr.aws/aws-cli/aws-cli'
  ```

  Símbolo del sistema de Windows

  ```
  C:\> doskey aws=docker run --rm -it public.ecr.aws/aws-cli/aws-cli $*
  ```

Windows PowerShell

```
C:\> Function AWSCLI {docker run --rm -it public.ecr.aws/aws-cli/aws-cli $args}
Set-Alias -Name aws -Value AWSCLI
```

Docker Hub

Linux y macOS

```
$ alias aws='docker run --rm -it amazon/aws-cli'
```

Símbolo del sistema de Windows

```
C:\> doskey aws=docker run --rm -it amazon/aws-cli $*
```

Windows PowerShell

```
C:\> Function AWSCLI {docker run --rm -it amazon/aws-cli $args}
Set-Alias -Name aws -Value AWSCLI
```

- Para acceder al sistema de archivos anfitrión y a las opciones de configuración cuando se utilizan comandos de `aws`, ejecute lo siguiente.

  Amazon ECR Public

  Linux y macOS

  ```
  $ alias aws='docker run --rm -it -v ~/.aws:/root/.aws -v $(pwd):/aws
   public.ecr.aws/aws-cli/aws-cli'
  ```

  Símbolo del sistema de Windows

  ```
  C:\> doskey aws=docker run --rm -it -v %userprofile%\.aws:/root/.aws -v %cd%:/aws
   public.ecr.aws/aws-cli/aws-cli $*
  ```

  Windows PowerShell

  ```
  C:\> Function AWSCLI {docker run --rm -it -v $env:userprofile\.aws:/root/.aws -v
   $pwd\aws:/aws public.ecr.aws/aws-cli/aws-cli $args}
  ```

```
Set-Alias -Name aws -Value AWSCLI
```

Docker Hub

Linux y macOS

```
$ alias aws='docker run --rm -it -v ~/.aws:/root/.aws -v $(pwd):/aws amazon/aws-
cli'
```

Símbolo del sistema de Windows

```
C:\> doskey aws=docker run --rm -it -v %userprofile%\.aws:/root/.aws -v %cd%:/aws
 amazon/aws-cli $*
```

Windows PowerShell

```
C:\> Function AWSCLI {docker run --rm -it -v $env:userprofile\.aws:/root/.aws -v
 $pwd\aws:/aws amazon/aws-cli $args}
Set-Alias -Name aws -Value AWSCLI
```

- Para asignar una versión específica para usarla en su alias de aws, agregue la etiqueta de versión.

  Amazon ECR Public

  Linux y macOS

```
$ alias aws='docker run --rm -it -v ~/.aws:/root/.aws -v $(pwd):/aws
 public.ecr.aws/aws-cli/aws-cli:2.0.6'
```

  Símbolo del sistema de Windows

```
C:\> doskey aws=docker run --rm -it -v %userprofile%\.aws:/root/.aws -v %cd%:/aws
 public.ecr.aws/aws-cli/aws-cli:2.0.6 $*
```

  Windows PowerShell

```
C:\> Function AWSCLI {docker run --rm -it -v $env:userprofile\.aws:/root/.aws -v
 $pwd\aws:/aws public.ecr.aws/aws-cli/aws-cli:2.0.6 $args}
Set-Alias -Name aws -Value AWSCLI
```

Docker Hub

Linux y macOS

```
$ alias aws='docker run --rm -it -v ~/.aws:/root/.aws -v $(pwd):/aws amazon/aws-cli:2.0.6'
```

Símbolo del sistema de Windows

```
C:\> doskey aws=docker run --rm -it -v %userprofile%\.aws:/root/.aws -v %cd%:/aws
 amazon/aws-cli:2.0.6 $*
```

Windows PowerShell

```
C:\> Function AWSCLI {docker run --rm -it -v $env:userprofile\.aws:/root/.aws -v
 $pwd\aws:/aws amazon/aws-cli:2.0.6 $args}
Set-Alias -Name aws -Value AWSCLI
```

Después de configurar el alias, puede ejecutar la AWS CLI versión 2 desde un contenedor como si estuviera instalado en su sistema host.

```
$ aws --version
aws-cli/2.27.41 Python/3.7.3 Linux/4.9.184-linuxkit botocore/2.4.5dev10
```

Configuración de AWS CLI

En este tema, se explica cómo se configuran las opciones básicas que utiliza AWS Command Line Interface (AWS CLI) para interactuar con AWS. Entre ellos, se incluyen las credenciales de seguridad, el formato de salida predeterminado y la región de AWS predeterminada.

Temas

- Recopilar su información de credenciales para el acceso programático
- Establecer una nueva configuración y credenciales
- Uso de archivos de configuración y credenciales existentes

Recopilar su información de credenciales para el acceso programático

Necesitará acceso programático si desea interactuar con AWS fuera de la Consola de administración de AWS. Para obtener instrucciones sobre autenticación y credenciales, elija una de las siguientes opciones:

Tipo de autenticación	Finalidad	Instrucciones
Credenciales de la consola de administración de AWS	(Recomendado) Use credenciales de corto plazo iniciando sesión en la AWS CLI con las credenciales de la consola. Se recomienda utilizar usuarios raíz, usuarios de IAM o federación con IAM para el acceso a la cuenta de AWS	the section called “Credenciales de consola”
Credenciales a corto plazo de los usuarios del personal de IAM Identity Center	Use credenciales a corto plazo para un usuario del personal de IAM Identity Center. La práctica recomendada de seguridad es utilizar AWS Organizations con IAM Identity Center. Aquí se combinan las credenciales de corta duración con un directorio de usuarios, como el directorio integrado de IAM Identity Center o Active Directory.	the section called “Autenticación del Centro de identidades de IAM”
Credenciales a corto plazo de usuarios de IAM	Utilice las credenciales a corto plazo de los usuarios de IAM, que son más seguras que las credenciales a largo plazo. Si sus credenciales están comprometidas, tiene un	the section called “Credenciales a corto plazo”

Tipo de autenticación	Finalidad	Instrucciones
	tiempo limitado para usarlas antes de que caduquen.	
Los usuarios de IAM o IAM Identity Center en una instancia de Amazon EC2	Usar metadatos de la instancia de Amazon EC2 para consultar credenciales temporales mediante el rol asignado a la instancia de Amazon EC2.	the section called “Metadatos de Amazon EC2”
Asumir roles para los permisos	Emparejar otro método de credenciales y asumir un rol para el acceso temporal a los Servicios de AWS a los que su usuario podría no tener acceso.	the section called “Roles de IAM”
Credenciales a largo plazo de usuarios de IAM	(No recomendado) Usar credenciales a largo plazo, que no tienen fecha de caducidad.	the section called “Usuarios de IAM”
Almacenamiento externo de los usuarios del personal de IAM o IAM Identity Center	(No recomendado) Emparejar otro método de credenciales pero almacenar los valores de credenciales en una ubicación fuera de la AWS CLI. Este método es tan seguro como la ubicación externa en la que se almacenan las credenciales.	the section called “Credenciales externas”

Establecer una nueva configuración y credenciales

La AWS CLI almacena su información de configuración y credenciales en un perfil (una colección de configuraciones) en los archivos `credentials` y `config`.

Hay principalmente dos métodos para instalarse rápidamente:

- Configuración mediante comandos de la AWS CLI
- Edición manual de las credenciales y los archivos de configuración

Los siguientes ejemplos utilizan valores de muestra para cada uno de los métodos de autenticación. Reemplace los valores de muestra por los suyos propios.

Configuración mediante comandos de la AWS CLI

Para uso general, los comandos `aws configure` o `aws configure sso` en su terminal preferido son la forma más rápida de configurar su instalación de la AWS CLI. Según el método de credenciales que prefiera, la AWS CLI le solicitará la información pertinente. De forma predeterminada, la información de este perfil se utiliza cuando se ejecuta un comando de la AWS CLI que no especifica explícitamente un perfil que se va a utilizar.

Para obtener más información sobre los archivos de `credentials` y `config`, consulte Opciones de los archivos de configuración y credenciales en la AWS CLI.

Console sessions as short-term credentials

Este ejemplo le permite usar sus credenciales de consola existentes con el comando `aws login`. Este método de inicio de sesión se puede utilizar con las credenciales raíz creadas durante la configuración inicial de la cuenta, con un usuario de IAM o con una identidad federada del proveedor de identidades. Para obtener más información, consulte Iniciar sesión para el desarrollo local de AWS con credenciales de consola.

```
$ aws login
No AWS region has been configured. The AWS region is the geographic location of your
 AWS resources.

If you've used AWS before and already have resources in your account, tell us which
 region they were
created in. If you haven't created resources in your account before, you can pick
 the region closest to you:
https://docs.aws.amazon.com/global-infrastructure/latest/regions/aws-regions.html.
 You are able to change
the region in the CLI at any time with the command `aws configure set region
 NEW_REGION`.
```

```
AWS Region [us-east-1]: us-east-1
Attempting to open the login page for `us-east-1` in your default browser. If the
 browser does not open,
use the following URL to complete your login:

https://us-east-1.signin.aws.amazon.com/v1/authorize<abbreviated>

If you cannot connect to this URL, make sure that you have specified a valid region.

Waiting for login...

Logged in with role `arn:aws:sts::012345678910:user/iam-user`, and configured
 profile
`default` to use `us-east-1`. This session will expire on October 14, 2025 at 2:04
 PST. After this time, you
can renew your session with `aws login`.
```

IAM Identity Center (SSO)

Este ejemplo corresponde a AWS IAM Identity Center con el asistente de `aws configure sso`. Para obtener más información, consulte the section called “Autenticación del Centro de identidades de IAM”.

```
$ aws configure sso
SSO session name (Recommended): my-sso
SSO start URL [None]: https://my-sso-portal.awsapps.com/start
SSO region [None]:us-east-1

Attempting to automatically open the SSO authorization page in your default browser.

There are 2 AWS accounts available to you.
> DeveloperAccount, developer-account-admin@example.com (111122223333)
  ProductionAccount, production-account-admin@example.com (444455556666)

Using the account ID 111122223333

There are 2 roles available to you.
> ReadOnly
  FullAccess

Using the role name "ReadOnly"

CLI default client Region [None]: us-west-2
```

```
CLI default output format [None]: json
CLI profile name [123456789011_ReadOnly]: user1
```

IAM Identity Center (Legacy SSO)

Este ejemplo corresponde al método heredado de AWS IAM Identity Center con el asistente `aws configure sso`. Para usar el SSO heredado, deje el nombre de la sesión en blanco. Para obtener más información, consulte the section called “Autenticación del Centro de identidades de IAM”.

```
$ aws configure sso
SSO session name (Recommended):
SSO start URL [None]: https://my-sso-portal.awsapps.com/start
SSO region [None]:us-east-1

SSO authorization page has automatically been opened in your default browser.
Follow the instructions in the browser to complete this authorization request.

There are 2 AWS accounts available to you.
> DeveloperAccount, developer-account-admin@example.com (111122223333)
  ProductionAccount, production-account-admin@example.com (444455556666)

Using the account ID 111122223333

There are 2 roles available to you.
> ReadOnly
  FullAccess

Using the role name "ReadOnly"

CLI default client Region [None]: us-west-2
CLI default output format [None]: json
CLI profile name [123456789011_ReadOnly]: user1
```

Short-term credentials

Este ejemplo corresponde a las credenciales de corta duración de AWS Identity and Access Management. El asistente aws configure se utiliza para establecer los valores iniciales y, a continuación, el comando `aws configure set` asigna el último valor necesario. Para obtener más información, consulte the section called “Credenciales a corto plazo”.

```
$ aws configure
```

```
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
Default region name [None]: us-west-2
Default output format [None]: json
$ aws configure set
 aws_session_token fcZib3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZVERYLONG
```

IAM role

Este ejemplo se usa para asumir un rol de IAM. Los perfiles que utilizan roles de IAM extraen las credenciales de otro perfil y, a continuación, aplican los permisos de rol de IAM. En los siguientes ejemplos, `default` es el perfil de origen de las credenciales y `user1` toma prestadas las mismas credenciales y, a continuación, asume un nuevo rol. No existe ningún asistente para este proceso, por lo que cada valor se establece con el comando `aws configure set`. Para obtener más información, consulte the section called “Roles de IAM”.

```
$ aws configure set role_arn arn:aws:iam::123456789012:role/defaultrole
$ aws configure set source_profile default
$ aws configure set role_session_name session_user1
$ aws configure set region us-west-2
$ aws configure set output json
```

Amazon EC2 instance metadata credentials

Este ejemplo corresponde a las credenciales obtenidas de los metadatos de la instancia de Amazon EC2 de alojamiento. No existe ningún asistente para este proceso, por lo que cada valor se establece con el comando `aws configure set`. Para obtener más información, consulte the section called “Metadatos de Amazon EC2”.

```
$ aws configure set role_arn arn:aws:iam::123456789012:role/defaultrole
$ aws configure set credential_source Ec2InstanceMetadata
$ aws configure set region us-west-2
$ aws configure set output json
```

Long-term credentials

> **Warning**
>
> Para evitar riesgos de seguridad, no utilice a los usuarios de IAM para la autenticación cuando desarrolle software especialmente diseñado o trabaje con datos reales. En

cambio, utilice la federación con un proveedor de identidades como AWS IAM Identity Center.

Este ejemplo corresponde a las credenciales de larga duración de AWS Identity and Access Management. Para obtener más información, consulte the section called “Usuarios de IAM”.

```
$ aws configure
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
Default region name [None]: us-west-2
Default output format [None]: json
```

Para información más detallada sobre los métodos de autenticación y credenciales, consulte Credenciales de autenticación y acceso.

Edición manual de las credenciales y los archivos de configuración

Cuando copie y pegue información, le sugerimos que edite manualmente el archivo `config` y `credentials`. Según el método de credenciales que prefiera, los archivos se configuran de forma diferente.

Los archivos se almacenan en el directorio principal, en la carpeta `.aws`. La ubicación del directorio principal varía en función del sistema operativo, pero se hace referencia a él mediante las variables de entorno `%UserProfile%` en Windows y `$HOME` o ~ (tilde) en los sistemas basados en Unix. Para obtener más información sobre dónde se almacenan estos ajustes, consulte the section called “¿Dónde se almacenan las opciones de configuración?”.

En los siguientes ejemplos se muestra un perfil de `default` y un perfil denominado `user1`, y se utilizan valores de muestra. Reemplace los valores de muestra por los suyos propios. Para obtener más información sobre los archivos de `credentials` y `config`, consulte Opciones de los archivos de configuración y credenciales en la AWS CLI.

IAM Identity Center (SSO)

Este es un ejemplo de AWS IAM Identity Center. Para obtener más información, consulte the section called “Autenticación del Centro de identidades de IAM”.

Archivo de credenciales

El archivo `credentials` no se utiliza para este método de autenticación.

Archivo de configuración

```
[default]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = readOnly
region = us-west-2
output = text

[profile user1]
sso_session = my-sso
sso_account_id = 444455556666
sso_role_name = readOnly
region = us-east-1
output = json

[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_registration_scopes = sso:account:access
```

IAM Identity Center (Legacy SSO)

Este ejemplo corresponde al método heredado de AWS IAM Identity Center. Para obtener más información, consulte the section called “Autenticación del Centro de identidades de IAM”.

Archivo de credenciales

El archivo `credentials` no se utiliza para este método de autenticación.

Archivo de configuración

```
[default]
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_region = us-east-1
sso_account_id = 111122223333
sso_role_name = readOnly
region = us-west-2
output = text

[profile user1]
```

```
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_region = us-east-1
sso_account_id = 444455556666
sso_role_name = readOnly
region = us-east-1
output = json
```

Short-term credentials

Este ejemplo corresponde a las credenciales de corta duración de AWS Identity and Access Management. Para obtener más información, consulte the section called “Credenciales a corto plazo”.

Archivo de credenciales

```
[default]
aws_access_key_id=ASIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
aws_session_token
 = IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZVERYLONGSTRINGEXAMPLE

[user1]
aws_access_key_id=ASIAI44QH8DHBEXAMPLE
aws_secret_access_key=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
aws_session_token
 = fcZib3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZVERYLONGSTRINGEXAMPLE
```

Archivo de configuración

```
[default]
region=us-west-2
output=json

[profile user1]
region=us-east-1
output=text
```

IAM role

Este ejemplo se usa para asumir un rol de IAM. Los perfiles que utilizan roles de IAM extraen las credenciales de otro perfil y, a continuación, aplican los permisos de rol de IAM. En los siguientes ejemplos, `default` es el perfil de origen de las credenciales y `user1` toma prestadas las mismas

credenciales y, a continuación, asume un nuevo rol. Para obtener más información, consulte the section called “Roles de IAM”.

Archivo de credenciales

El archivo `credentials` depende de la autenticación que utilice su perfil de origen. En el siguiente ejemplo, el perfil de origen utiliza credenciales de corta duración.

```
[default]
aws_access_key_id=ASIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
aws_session_token
 = IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZVERYLONGSTRINGEXAMPLE
```

Archivo de configuración

```
[default]
region=us-west-2
output=json

[profile user1]
role_arn=arn:aws:iam::777788889999:role/user1role
source_profile=default
role_session_name=session_user1
region=us-east-1
output=text
```

Amazon EC2 instance metadata credentials

Este ejemplo corresponde a las credenciales obtenidas de los metadatos de la instancia de Amazon EC2 de alojamiento. Para obtener más información, consulte the section called “Metadatos de Amazon EC2”.

Archivo de credenciales

El archivo `credentials` no se utiliza para este método de autenticación.

Archivo de configuración

```
[default]
role_arn=arn:aws:iam::123456789012:role/defaultrole
credential_source=Ec2InstanceMetadata
```

```
region=us-west-2
output=json

[profile user1]
role_arn=arn:aws:iam::777788889999:role/user1role
credential_source=Ec2InstanceMetadata
region=us-east-1
output=text
```

Long-term credentials

> **Warning**
>
> Para evitar riesgos de seguridad, no utilice a los usuarios de IAM para la autenticación cuando desarrolle software especialmente diseñado o trabaje con datos reales. En cambio, utilice la federación con un proveedor de identidades como AWS IAM Identity Center.

Este ejemplo corresponde a las credenciales de larga duración de AWS Identity and Access Management. Para obtener más información, consulte the section called “Usuarios de IAM”.

Archivo de credenciales

```
[default]
aws_access_key_id=AKIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

[user1]
aws_access_key_id=AKIAI44QH8DHBEXAMPLE
aws_secret_access_key=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
```

Archivo de configuración

```
[default]
region=us-west-2
output=json

[profile user1]
region=us-east-1
output=text
```

Para información más detallada sobre los métodos de autenticación y credenciales, consulte Credenciales de autenticación y acceso.

Uso de archivos de configuración y credenciales existentes

Si tiene archivos de configuración y credenciales existentes, se pueden utilizar para AWS CLI.

Para utilizar los archivos de `config` y `credentials`, muévalos a la carpeta denominada `.aws` en el directorio principal. La ubicación del directorio principal varía en función del sistema operativo, pero se hace referencia a él mediante las variables de entorno `%UserProfile%` en Windows y `$HOME` o ~ (tilde) en los sistemas basados en Unix.

Puede especificar una ubicación no predeterminada para los archivos de `config` y `credentials`configurando las variables de entorno `AWS_CONFIG_FILE` y `AWS_SHARED_CREDENTIALS_FILE` en otra ruta local. Para obtener más información, consulte Configuración de variables de entorno para la AWS CLI.

Para obtener más información sobre archivos de configuración y credenciales, consulte the section called “Opciones de configuración”.

Configuración de los ajustes de AWS CLI

En esta sección, se explica cómo se configuran los parámetros que AWS Command Line Interface (AWS CLI) utiliza para interactuar con AWS. Estos incluyen los siguientes:

- Las credenciales identifican quién llama a la API. Las credenciales de acceso se utilizan para cifrar la solicitud a los servidores de AWS a fin de confirmar su identidad y recuperar las políticas de permisos asociadas. Estos permisos determinan las acciones que puede realizar. Para obtener información sobre cómo configurar las credenciales, consulte Credenciales de autenticación y acceso.
- Otros detalles de configuración para indicar a la AWS CLI cómo procesar las solicitudes, como el formato de salida predeterminado y la región de AWS predeterminada.

> **Note**
>
> AWS requiere que todas las solicitudes entrantes estén firmadas criptográficamente. El AWS CLI lo hace automáticamente. La "firma" incluye una marca temporal de fecha/hora. Por lo tanto, debe asegurarse de que la fecha y la hora de su equipo se haya establecido correctamente. De lo contrario, si la fecha y la hora de la firma difieren en gran medida de la fecha y la hora reconocidas por el servicio de AWS, AWS rechazará la solicitud.

Prioridad de configuración y credenciales

Las credenciales y las opciones de configuración se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. Ciertas ubicaciones tienen prioridad sobre otras. Las credenciales de la AWS CLI y las opciones de configuración tienen prioridad en el siguiente orden:

1. Opciones de línea de comandos: anula la configuración en cualquier otra ubicación, como los parámetros `--region`, `--output` y `--profile`.
2. Variables de entorno: puede almacenar valores en las variables de entorno de su sistema.
3. Asumir rol: asuma los permisos de un rol de IAM mediante la configuración o el comando `assume-role`.

4. Asumir rol con identidad web: asuma los permisos de un rol de IAM con identidad web mediante la configuración o el comando `assume-role-with-web-identity`.
5. AWS IAM Identity Center: los ajustes de configuración de IAM Identity Center guardados en el archivo `config` se actualizan al ejecutar el comando `aws configure sso`. A continuación, las credenciales se autentican al ejecutar el comando `aws sso login`. El archivo `config` se encuentra en `~/.aws/config` en Linux o macOS, o en `C:\Users\`*`USERNAME`*`\.aws\config` en Windows.
6. Archivo de credenciales: los archivos `credentials` y `config` se actualizan al ejecutar el comando `aws configure`. El archivo `credentials` se encuentra en `~/.aws/credentials` en Linux o macOS, o en `C:\Users\`*`USERNAME`*`\.aws\credentials` en Windows.
7. Proceso personalizado: obtenga sus credenciales de un origen externo.
8. Archivo de configuración: los archivos `credentials` y `config` se actualizan al ejecutar el comando `aws configure`. El archivo `config` se encuentra en `~/.aws/config` en Linux o macOS, o en `C:\Users\`*`USERNAME`*`\.aws\config` en Windows.
9. Credenciales contenedor: puede asociar un rol de IAM con cada una de las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS). Las credenciales temporales de ese rol estarán disponibles para los contenedores de esa tarea. Para obtener más información, consulte Roles de IAM para tareas en la Guía para desarrolladores de Amazon Elastic Container Service.
10. Credenciales de perfil de instancia de Amazon EC2: puede asociar un rol de IAM con cada una de las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las credenciales temporales de ese rol estarán disponibles para el código que se ejecute en la instancia. Las credenciales se entregan a través del servicio de metadatos de Amazon EC2. Para obtener más información, consulte Roles de IAM para Amazon EC2 en la Guía del usuario de Amazon EC2 y Uso de perfiles de instancia en la Guía del usuario de IAM.

Temas adicionales en esta sección

- the section called “Opciones de configuración”
- the section called “Variables de entorno”
- the section called “Opciones de línea de comandos”
- the section called “ Finalización de comandos”
- the section called “Reintentos”
- the section called “Proxies HTTP”

Opciones de los archivos de configuración y credenciales en la AWS CLI

Puede guardar las opciones de configuración y las credenciales que utiliza con frecuencia en archivos que son mantenidos por la AWS CLI.

Los archivos se dividen en `profiles`. De forma predeterminada, la AWS CLI utiliza las opciones que se encuentran en el perfil denominado `default`. Para utilizar una configuración diferente, puede crear y hacer referencia a perfiles adicionales.

También es posible anular una opción individual estableciendo una de las variables de entorno compatibles o utilizando un parámetro de la línea de comandos. Para obtener más información sobre la prioridad de opciones de configuración, consulte Configuración de los ajustes de AWS CLI.

> **Note**
>
> Para obtener información sobre cómo configurar las credenciales, consulte Credenciales de autenticación y acceso.

Temas

- Formato de los archivos de configuración y credenciales
- ¿Dónde se almacenan las opciones de configuración?
- Uso de perfiles con nombre
- Definir y ver las opciones de configuración mediante comandos
- Establecimiento de una nueva configuración y ejemplos de comandos de credenciales
- Configuraciones del archivo config admitidas

Formato de los archivos de configuración y credenciales

Los archivos `config` y `credentials` están organizados en secciones. Las secciones incluyen perfiles, sso-sessions y servicios. Una sección es una colección con nombre de configuraciones y continúa hasta que se encuentra otra línea de definición de sección. Se pueden almacenar varios perfiles y secciones en los archivos `config` y `credentials`.

Son archivos de texto sin formato que utilizan el formato siguiente:

- Los nombres de las secciones aparecen entre corchetes [] como `[default]`, `[profile user1]` y `[sso-session]`.
- Todas las entradas de una sección adoptan el formato general de `setting_name=value`.
- Las líneas se pueden comentar si se inician con un carácter de almohadilla (#).

Los archivos config y credentials contienen los siguientes tipos de secciones:

- Tipo de sección: profile
- Tipo de sección: sso-session
- Tipo de sección: services

Tipo de sección: **`profile`**

En función del archivo, los nombres de la sección del perfil utilizan el formato siguiente:

- Archivo de configuración: `[default]` `[profile user1]`
- Archivo de credenciales: `[default]` `[user1]`

  no utilice la palabra `profile` cuando cree una entrada en el archivo `credentials`.

Cada perfil puede usar credenciales diferentes y también puede especificar diferentes formatos de salida y regiones de AWS. Al asignar un nombre al perfil en un archivo `config`, incluya la palabra de prefijo “`profile`”, pero no la incluya en el archivo `credentials`.

En los siguientes ejemplos se muestra un archivo `credentials` y `config` con dos perfiles, región y salida especificados. El primero [predeterminado] se utiliza cuando se ejecuta un comando de la AWS CLI sin un perfil especificado. El segundo se utiliza cuando se ejecuta un comando de la AWS CLI con el parámetro `--profile user1`.

IAM Identity Center (SSO)

Este es un ejemplo de AWS IAM Identity Center. Para obtener más información, consulte the section called “Autenticación del Centro de identidades de IAM”.

Archivo de credenciales

El archivo `credentials` no se utiliza para este método de autenticación.

Archivo de configuración

```
[default]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = readOnly
region = us-west-2
output = text

[profile user1]
sso_session = my-sso
sso_account_id = 444455556666
sso_role_name = readOnly
region = us-east-1
output = json

[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_registration_scopes = sso:account:access
```

IAM Identity Center (Legacy SSO)

Este ejemplo corresponde al método heredado de AWS IAM Identity Center. Para obtener más información, consulte the section called “Autenticación del Centro de identidades de IAM”.

Archivo de credenciales

El archivo `credentials` no se utiliza para este método de autenticación.

Archivo de configuración

```
[default]
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_region = us-east-1
sso_account_id = 111122223333
sso_role_name = readOnly
region = us-west-2
output = text

[profile user1]
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_region = us-east-1
sso_account_id = 444455556666
sso_role_name = readOnly
```

```
region = us-east-1
output = json
```

Short-term credentials

Este ejemplo corresponde a las credenciales de corta duración de AWS Identity and Access Management. Para obtener más información, consulte the section called “Credenciales a corto plazo”.

Archivo de credenciales

```
[default]
aws_access_key_id=ASIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
aws_session_token
 = IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZVERYLONGSTRINGEXAMPLE

[user1]
aws_access_key_id=ASIAI44QH8DHBEXAMPLE
aws_secret_access_key=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
aws_session_token
 = fcZib3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZVERYLONGSTRINGEXAMPLE
```

Archivo de configuración

```
[default]
region=us-west-2
output=json

[profile user1]
region=us-east-1
output=text
```

IAM role

Este ejemplo se usa para asumir un rol de IAM. Los perfiles que utilizan roles de IAM extraen las credenciales de otro perfil y, a continuación, aplican los permisos de rol de IAM. En los siguientes ejemplos, `default` es el perfil de origen de las credenciales y `user1` toma prestadas las mismas credenciales y, a continuación, asume un nuevo rol. Para obtener más información, consulte the section called “Roles de IAM”.

Archivo de credenciales

El archivo `credentials` depende de la autenticación que utilice su perfil de origen. En el siguiente ejemplo, el perfil de origen utiliza credenciales de corta duración.

```
[default]
aws_access_key_id=ASIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
aws_session_token
 = IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZVERYLONGSTRINGEXAMPLE
```

Archivo de configuración

```
[default]
region=us-west-2
output=json

[profile user1]
role_arn=arn:aws:iam::777788889999:role/user1role
source_profile=default
role_session_name=session_user1
region=us-east-1
output=text
```

Amazon EC2 instance metadata credentials

Este ejemplo corresponde a las credenciales obtenidas de los metadatos de la instancia de Amazon EC2 de alojamiento. Para obtener más información, consulte the section called “Metadatos de Amazon EC2”.

Archivo de credenciales

El archivo `credentials` no se utiliza para este método de autenticación.

Archivo de configuración

```
[default]
role_arn=arn:aws:iam::123456789012:role/defaultrole
credential_source=Ec2InstanceMetadata
region=us-west-2
output=json

[profile user1]
role_arn=arn:aws:iam::777788889999:role/user1role
```

```
credential_source=Ec2InstanceMetadata
region=us-east-1
output=text
```

Long-term credentials

> **Warning**
>
> Para evitar riesgos de seguridad, no utilice a los usuarios de IAM para la autenticación cuando desarrolle software especialmente diseñado o trabaje con datos reales. En cambio, utilice la federación con un proveedor de identidades como AWS IAM Identity Center.

Este ejemplo corresponde a las credenciales de larga duración de AWS Identity and Access Management. Para obtener más información, consulte the section called “Usuarios de IAM”.

Archivo de credenciales

```
[default]
aws_access_key_id=AKIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

[user1]
aws_access_key_id=AKIAI44QH8DHBEXAMPLE
aws_secret_access_key=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
```

Archivo de configuración

```
[default]
region=us-west-2
output=json

[profile user1]
region=us-east-1
output=text
```

Para obtener más información y métodos adicionales de autorización y credenciales, consulte the section called “Usuarios de IAM”.

Tipo de sección: **`sso-session`**

La sección `sso-session` del archivo `config` se usa para agrupar las variables de configuración para adquirir los tokens de acceso SSO, que luego se pueden usar para adquirir credenciales de AWS. Se utilizan las siguientes configuraciones:

- (Obligatorio) `sso_start_url`
- (Obligatorio) `sso_region`
- `sso_account_id`
- `sso_role_name`
- `sso_registration_scopes`

Defina una sección `sso-session` y asóciela a un perfil. `sso_region` y`sso_start_url` deben establecerse en la sección `sso-session`. Normalmente, `sso_account_id` y `sso_role_name` deben establecerse en la sección `profile` para que el SDK pueda solicitar las credenciales de SSO.

En el siguiente ejemplo se configura el SDK para que solicite credenciales de SSO y admita la actualización automática de tokens:

```
[profile dev]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = SampleRole

[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
```

Esto también permite reutilizar las configuraciones de `sso-session` en varios perfiles:

```
[profile dev]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = SampleRole

[profile prod]
sso_session = my-sso
sso_account_id = 111122223333
```

```
sso_role_name = SampleRole2

[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
```

No obstante, `sso_account_id` y `sso_role_name` no son necesarios para todos los escenarios de configuración de token de SSO. Si su aplicación solo utiliza servicios de AWS que admiten la autenticación de portador, no son necesarias las credenciales de AWS tradicionales. La autenticación de portador es un esquema de autenticación HTTP que utiliza tokens de seguridad denominados tokens de portador. En este escenario, no se necesitan `sso_account_id` ni `sso_role_name`. Consulte la guía individual de su servicio de AWS para determinar si admite la autorización de token de portador.

Además, los ámbitos de registro pueden configurarse como parte de `sso-session`. El alcance es un mecanismo de OAuth 2.0 para limitar el acceso de una aplicación a la cuenta de un usuario. Una solicitud puede pedir uno o varios ámbitos y el token de acceso emitido a la solicitud se limitará a los ámbitos concedidos. Estos ámbitos definen los permisos cuya autorización se solicita para el cliente OIDC registrado y los tokens de acceso recuperados por el cliente. El siguiente ejemplo establece `sso_registration_scopes` para proporcionar acceso para enumerar cuentas/roles:

```
[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_registration_scopes = sso:account:access
```

El token de autenticación se almacena en caché en el disco en el directorio `~/.aws/sso/cache` con un nombre de archivo basado en el nombre de la sesión.

Para obtener más información sobre este tipo de configuración, consulte the section called “Autenticación del Centro de identidades de IAM”.

Tipo de sección: **`services`**

La sección de `services` es un grupo de ajustes que configura puntos de conexión personalizados para las solicitudes de Servicio de AWS. A continuación, se vincula un perfil a una sección de `services`.

```
[profile dev]
services = my-services
```

La sección de `services` se separa en subsecciones por líneas `<SERVICE> = `, donde `<SERVICE>` es la clave del identificador de Servicio de AWS. El identificador de Servicio de AWS se basa en `serviceId` del modelo de la API, sustituyendo todos los espacios por guiones bajos y poniendo en minúsculas todas las letras. Para obtener una lista de todas las claves de identificación de servicio que se van a utilizar en la sección de `services`, consulte Uso de puntos de conexión en la AWS CLI. La clave del identificador del servicio va seguida de configuraciones anidadas, cada una en su propia línea y marcada con dos espacios.

En el siguiente ejemplo, se configura el punto de conexión que se utilizará en las solicitudes realizadas al servicio de Amazon DynamoDB en la sección *`my-services`* que se utiliza en el perfil de *`desarrollo`*. Todas las líneas inmediatamente siguientes que estén sangradas se incluyen en esa subsección y se aplican a ese servicio.

```
[profile dev]
services = my-services

[services my-services]
dynamodb =
  endpoint_url = http://localhost:8000
```

Para obtener más información sobre puntos de conexión específicos del servicio, consulte Uso de puntos de conexión en la AWS CLI.

Si el perfil tiene credenciales basadas en roles configuradas mediante un parámetro `source_profile` para la funcionalidad de asumir roles de IAM, el SDK solo usa configuraciones de servicio para el perfil especificado. No utiliza perfiles que estén vinculados a él por roles. Por ejemplo, mediante el siguiente archivo `config` compartido:

```
[profile A]
credential_source = Ec2InstanceMetadata
endpoint_url = https://profile-a-endpoint.aws/

[profile B]
source_profile = A
role_arn = arn:aws:iam::123456789012:role/roleB
services = profileB

[services profileB]
ec2 =
  endpoint_url = https://profile-b-ec2-endpoint.aws
```

Si usa el perfil `B` y realiza una llamada en el código a Amazon EC2, el punto de conexión se resuelve como `https://profile-b-ec2-endpoint.aws`. Si el código realiza una solicitud a cualquier otro servicio, la resolución del punto de conexión no seguirá ninguna lógica personalizada. El punto de conexión no se convierte en el punto de conexión global definido en el perfil `A`. Para que un punto de conexión global surta efecto en el perfil `B`, tendrá que configurar `endpoint_url` directamente dentro del perfil `B`.

¿Dónde se almacenan las opciones de configuración?

La AWS CLI almacena la información confidencial de las credenciales especificadas con `aws configure` en un archivo local denominado `credentials` en una carpeta denominada `.aws` del directorio principal. Las opciones de configuración menos confidenciales especificadas con `aws configure` se guardan en un archivo local denominado `config`, que también se almacena en la carpeta `.aws` del directorio principal.

> **Almacenamiento de credenciales en el archivo de configuración**
>
> Puede mantener todas las opciones de perfil en un solo archivo, ya que la AWS CLI puede leer las credenciales del archivo `config`. Si hay credenciales en ambos archivos para un perfil que comparte el mismo nombre, las claves del archivo de credenciales tienen prioridad. Sugerimos guardar las credenciales en los archivos `credentials`. Los kits de desarrollo de software (SDK) de varios lenguajes también utilizan estos archivos. Si utiliza uno de los SDK además de la AWS CLI, confirme si las credenciales deben almacenarse en su propio archivo.

La ubicación del directorio principal varía en función del sistema operativo, pero se hace referencia a él mediante las variables de entorno `%UserProfile%` en Windows y `$HOME` o ~ (tilde) en los sistemas basados en Unix. Puede especificar una ubicación no predeterminada para los archivos configurando las variables de entorno `AWS_CONFIG_FILE` y `AWS_SHARED_CREDENTIALS_FILE` en otra ruta local. Para obtener más información, consulte Configuración de variables de entorno para la AWS CLI.

Cuando se utiliza un perfil compartido que especifica un rol de AWS Identity and Access Management (IAM), la AWS CLI llama a la operación AWS STS de `AssumeRole` para recuperar las credenciales temporales. A continuación, se almacenan estas credenciales (en `~/.aws/cli/cache`). Los comandos de la AWS CLI posteriores utilizan las credenciales temporales almacenadas en caché hasta que caducan, momento en el cual la AWS CLI las actualiza automáticamente.

Uso de perfiles con nombre

Si no se define explícitamente ningún perfil, se utilizará el perfil `default`.

Para usar un perfil con nombre, añada la opción `--profile` *`profile-name`* a su comando. En el siguiente ejemplo se muestran todas las instancias de Amazon EC2 con las credenciales y la configuración definidas en el perfil `user1`.

```
$ aws ec2 describe-instances --profile user1
```

Si desea utilizar un perfil con nombre para varios comandos, puede evitar especificarlo en cada comando mediante el establecimiento de la variable de entorno `AWS_PROFILE` como el perfil predeterminado. Puede invalidar esta configuración con el parámetro `--profile`.

Linux or macOS

```
$ export AWS_PROFILE=user1
```

Windows

```
C:\> setx AWS_PROFILE user1
```

El uso de `set` para configurar una variable de entorno cambia el valor usado hasta que finalice la sesión de símbolo de sistema actual o hasta que otorgue a la variable un valor diferente.

El uso de `setx` para establecer una variable de entorno cambia el valor de todos los shells de comandos que cree después de ejecutar el comando. No afecta a ningún shell de comandos que ya se esté ejecutando en el momento en que ejecuta el comando. Cierre y reinicie el shell de comandos para ver los efectos del cambio.

La configuración de la variable de entorno cambia el perfil predeterminado hasta que finalice la sesión del shell, o hasta que otorgue a la variable a un valor diferente. Puede hacer que las variables de entorno persistan en sesiones futuras poniéndolas en el script de inicio del shell. Para obtener más información, consulte Configuración de variables de entorno para la AWS CLI.

Definir y ver las opciones de configuración mediante comandos

Hay varias formas de ver y establecer las opciones de configuración mediante comandos.

aws configure

Ejecute este comando para establecer y ver rápidamente las credenciales, la región y el formato de salida. En el ejemplo siguiente se muestran los valores de ejemplo.

```
$ aws configure
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
Default region name [None]: us-west-2
Default output format [None]: json
```

aws configure set

Puede establecer las credenciales o las opciones de configuración mediante `aws configure set`. Especifique el perfil que desea ver o modificar con la opción `--profile`.

Por ejemplo, el siguiente comando configura `region` en el perfil denominado `integ`.

```
$ aws configure set region us-west-2 --profile integ
```

Para quitar una opción, elimine manualmente el ajuste en los archivos `config` y `credentials` en un editor de texto.

aws configure get

Puede recuperar las credenciales o las opciones de configuración que haya establecido utilizando `aws configure get`. Especifique el perfil que desea ver o modificar con la opción `--profile`.

Por ejemplo, el siguiente comando recupera la opción `region` en el perfil denominado `integ`.

```
$ aws configure get region --profile integ
us-west-2
```

Si la salida está vacía, significa que la configuración no está establecida de forma explícita y se utiliza el valor predeterminado.

aws configure import

Importe las credenciales de CSV generadas desde la consola web de IAM. No es para las credenciales generadas desde Centro de identidades de IAM; los clientes que usen Centro de identidades de IAM deben usar aws configure sso. Se importa un archivo CSV con el nombre de perfil correspondiente al nombre de usuario. El archivo CSV debe contener los siguientes encabezados.

- User Name
- ID de clave de acceso
- Clave de acceso secreta

> **Note**
>
> Durante la creación del par de claves inicial, una vez que cierre el cuadro de diálogo Download .csv file (Descargar archivo .csv), no puede acceder a la clave de acceso secreta después de cerrar el cuadro de diálogo. Si necesita un archivo `.csv`, tendrá que crear uno usted mismo con los encabezados necesarios y la información del par de claves almacenada. Si no tiene acceso a la información del par de claves, debe crear un nuevo par de claves.

```
$ aws configure import --csv file://credentials.csv
```

aws configure list

Para mostrar los datos de configuración, utilice el comando `aws configure list`. Este comando muestra el perfil, la clave de acceso, la clave secreta y la información de configuración de la región utilizada para el perfil especificado. Para cada elemento de configuración, muestra el valor, dónde se recuperó el valor de configuración y el nombre de la variable de configuración.

Por ejemplo, si proporciona el valor Región de AWS en una variable de entorno, este comando le mostrará el nombre de la región que ha configurado, que este valor proviene de una variable de entorno y el nombre de la variable de entorno.

En el caso de los métodos de credenciales temporales, como los roles y el Centro de identidades de IAM, este comando muestra la clave de acceso almacenada temporalmente en caché y se muestra la clave de acceso secreta.

```
$ aws configure list
NAME       : VALUE                : TYPE                     : LOCATION
profile    : <not set>            : None                     : None
access_key : ****************ABCD : shared-credentials-file :
secret_key : ****************ABCD : shared-credentials-file :
region     : us-west-2            : env                      : AWS_DEFAULT_REGION
```

aws configure list-profiles

Para enumerar todos los nombres de perfil, utilice el comando `aws configure list-profiles`.

```
$ aws configure list-profiles
default
test
```

aws configure mfa-login

Ejecute este comando para configurar un nuevo perfil para usarlo con la autenticación multifactor (MFA) y las credenciales del usuario de IAM en el perfil especificado. Si no se especifica ningún perfil, la MFA se basa en el perfil `default`. Si no hay ningún perfil predeterminado configurado, el comando `mfa-login` le solicitará las credenciales de AWS antes de solicitar su información de MFA. En el ejemplo de comando siguiente, se usa la configuración predeterminada y se crea un perfil de MFA.

```
$ aws configure mfa-login
MFA serial number or ARN: arn:aws:iam::123456789012:mfa/MFADeviceName
MFA token code: 123456
Profile to update [session-MFADeviceName]:
Temporary credentials written to profile 'session-MFADeviceName'
Credentials will expire at 2023-05-19 18:06:10 UTC
To use these credentials, specify --profile session-MFADeviceName when running AWS
 CLI commands
```

Para actualizar un perfil existente, utilice el parámetro `--update-profile`.

```
$ aws configure mfa-login --profile myprofile --update-profile mfaprofile
MFA token code: 123456
Temporary credentials written to profile 'mfaprofile'
Credentials will expire at 2023-05-19 18:06:10 UTC
To use these credentials, specify --profile mfaprofile when running AWS CLI commands
```

Este comando actualmente solo admite hardware o software basado en autenticadores de contraseña de un solo uso (OTP). Actualmente, este comando no admite claves de acceso ni dispositivos U2F.

Para obtener más información sobre el uso de MFA con IAM, consulte Autenticación multifactor de AWS en IAM en la Guía del usuario de AWS Identity and Access Management.

aws configure sso

Ejecute este comando para establecer y ver rápidamente las credenciales de AWS IAM Identity Center, la región y el formato de salida. En el ejemplo siguiente se muestran los valores de ejemplo.

```
$ aws configure sso
SSO session name (Recommended): my-sso
SSO start URL [None]: https://my-sso-portal.awsapps.com/start
SSO region [None]: us-east-1
SSO registration scopes [None]: sso:account:access
```

aws configure sso-session

Ejecute este comando para establecer y ver rápidamente las credenciales de AWS IAM Identity Center, la región y el formato de salida en la sección `sso-session` de los archivos `credentials` y `config`. En el ejemplo siguiente se muestran los valores de ejemplo.

```
$ aws configure sso-session
SSO session name: my-sso
SSO start URL [None]: https://my-sso-portal.awsapps.com/start
SSO region [None]: us-east-1
SSO registration scopes [None]: sso:account:access
```

aws configure export-credentials

Ejecute este comando para exportar las credenciales establecidas actualmente en el formato especificado. De forma predeterminada, el comando exporta las credenciales predeterminadas en el formato `process`, que es un formato JSON compatible con el formato de credenciales de los SDK y las herramientas de AWS.

```
$ aws configure export-credentials
{
  "Version": 1,
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
}
```

Para exportar un perfil y un formato específicos, utilice las opciones `--profile` y `--format`. Las opciones de formato son las siguientes:

- (predeterminado)**`process`**: el formato JSON admitido en la configuración de `credential_process` de los SDK y las herramientas de AWS.
- **`env`** - variables de entorno en formato de intérprete de comandos exportado.
- **`env-no-export`** - variables de entorno no exportadas en formato de intérprete de comandos.
- **`powershell`** - variables de entorno en formato de PowerShell.
- **`windows-cmd`** - variables de entorno en formato de línea de comandos de Windows.

En el siguiente ejemplo, se exporta el perfil `user1` a un formato de intérprete de comandos exportado.

```
$ aws configure export-credentials --profile user1 --format env
export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

Establecimiento de una nueva configuración y ejemplos de comandos de credenciales

En los siguientes ejemplos se muestra la configuración de un perfil predeterminado con credenciales, región y salida especificados para diferentes métodos de autenticación.

Console sessions as short-term credentials

Este ejemplo le permite usar sus credenciales de consola existentes con el comando `aws login`. Este método de inicio de sesión se puede utilizar con las credenciales raíz creadas durante la configuración inicial de la cuenta, con un usuario de IAM o con una identidad federada del proveedor de identidades. Para obtener más información, consulte Iniciar sesión para el desarrollo local de AWS con credenciales de consola.

```
$ aws login
No AWS region has been configured. The AWS region is the geographic location of your
 AWS resources.

If you've used AWS before and already have resources in your account, tell us which
 region they were
created in. If you haven't created resources in your account before, you can pick
 the region closest to you:
https://docs.aws.amazon.com/global-infrastructure/latest/regions/aws-regions.html.
 You are able to change
```

```
the region in the CLI at any time with the command `aws configure set region
 NEW_REGION`.

AWS Region [us-east-1]: us-east-1
Attempting to open the login page for `us-east-1` in your default browser. If the
 browser does not open,
use the following URL to complete your login:

https://us-east-1.signin.aws.amazon.com/v1/authorize<abbreviated>

If you cannot connect to this URL, make sure that you have specified a valid region.

Waiting for login...

Logged in with role `arn:aws:sts::012345678910:user/iam-user`, and configured
 profile
`default` to use `us-east-1`. This session will expire on October 14, 2025 at 2:04
 PST. After this time, you
can renew your session with `aws login`.
```

IAM Identity Center (SSO)

Este ejemplo corresponde a AWS IAM Identity Center con el asistente de `aws configure sso`. Para obtener más información, consulte the section called “Autenticación del Centro de identidades de IAM”.

```
$ aws configure sso
SSO session name (Recommended): my-sso
SSO start URL [None]: https://my-sso-portal.awsapps.com/start
SSO region [None]:us-east-1

Attempting to automatically open the SSO authorization page in your default browser.

There are 2 AWS accounts available to you.
> DeveloperAccount, developer-account-admin@example.com (111122223333)
  ProductionAccount, production-account-admin@example.com (444455556666)

Using the account ID 111122223333

There are 2 roles available to you.
> ReadOnly
  FullAccess
```

```
Using the role name "ReadOnly"

CLI default client Region [None]: us-west-2
CLI default output format [None]: json
CLI profile name [123456789011_ReadOnly]: user1
```

IAM Identity Center (Legacy SSO)

Este ejemplo corresponde al método heredado de AWS IAM Identity Center con el asistente `aws configure sso`. Para usar el SSO heredado, deje el nombre de la sesión en blanco. Para obtener más información, consulte the section called “Autenticación del Centro de identidades de IAM”.

```
$ aws configure sso
SSO session name (Recommended):
SSO start URL [None]: https://my-sso-portal.awsapps.com/start
SSO region [None]:us-east-1

SSO authorization page has automatically been opened in your default browser.
Follow the instructions in the browser to complete this authorization request.

There are 2 AWS accounts available to you.
> DeveloperAccount, developer-account-admin@example.com (111122223333)
  ProductionAccount, production-account-admin@example.com (444455556666)

Using the account ID 111122223333

There are 2 roles available to you.
> ReadOnly
  FullAccess

Using the role name "ReadOnly"

CLI default client Region [None]: us-west-2
CLI default output format [None]: json
CLI profile name [123456789011_ReadOnly]: user1
```

Short-term credentials

Este ejemplo corresponde a las credenciales de corta duración de AWS Identity and Access Management. El asistente aws configure se utiliza para establecer los valores iniciales y, a

continuación, el comando `aws configure set` asigna el último valor necesario. Para obtener más información, consulte the section called “Credenciales a corto plazo”.

```
$ aws configure
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
Default region name [None]: us-west-2
Default output format [None]: json
$ aws configure set
 aws_session_token fcZib3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZVERYLONG
```

IAM role

Este ejemplo se usa para asumir un rol de IAM. Los perfiles que utilizan roles de IAM extraen las credenciales de otro perfil y, a continuación, aplican los permisos de rol de IAM. En los siguientes ejemplos, `default` es el perfil de origen de las credenciales y `user1` toma prestadas las mismas credenciales y, a continuación, asume un nuevo rol. No existe ningún asistente para este proceso, por lo que cada valor se establece con el comando `aws configure set`. Para obtener más información, consulte the section called “Roles de IAM”.

```
$ aws configure set role_arn arn:aws:iam::123456789012:role/defaultrole
$ aws configure set source_profile default
$ aws configure set role_session_name session_user1
$ aws configure set region us-west-2
$ aws configure set output json
```

Amazon EC2 instance metadata credentials

Este ejemplo corresponde a las credenciales obtenidas de los metadatos de la instancia de Amazon EC2 de alojamiento. No existe ningún asistente para este proceso, por lo que cada valor se establece con el comando `aws configure set`. Para obtener más información, consulte the section called “Metadatos de Amazon EC2”.

```
$ aws configure set role_arn arn:aws:iam::123456789012:role/defaultrole
$ aws configure set credential_source Ec2InstanceMetadata
$ aws configure set region us-west-2
$ aws configure set output json
```

Long-term credentials

> **Warning**
>
> Para evitar riesgos de seguridad, no utilice a los usuarios de IAM para la autenticación cuando desarrolle software especialmente diseñado o trabaje con datos reales. En cambio, utilice la federación con un proveedor de identidades como AWS IAM Identity Center.

Este ejemplo corresponde a las credenciales de larga duración de AWS Identity and Access Management. Para obtener más información, consulte the section called “Usuarios de IAM”.

```
$ aws configure
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
Default region name [None]: us-west-2
Default output format [None]: json
```

Configuraciones del archivo `config` admitidas

Temas

- Configuración global
- Configuración de comandos personalizados de S3

Se admiten las siguientes opciones en el archivo `config`. Se utilizan los valores enumerados en el perfil especificado (o predeterminado) a menos que queden anulados por la presencia de una variable de entorno con el mismo nombre o una opción de línea de comandos con el mismo nombre. Para obtener más información sobre las opciones que tienen prioridad, consulte Configuración de los ajustes de AWS CLI

Configuración global

`account_id_endpoint_mode`

Especifica si se deben utilizar los ID de punto de conexión basados en cuentas de AWS para las llamadas a los Servicios de AWS compatibles. Para obtener más información sobre los puntos

de conexión basados en cuentas, consulte the section called “Puntos de conexión basados en cuentas”.

Esta configuración puede establecerse en lo siguiente:

- (predeterminado) **`preferred`**: el punto de conexión debe incluir el ID de cuenta si está disponible.
- **`disabled`** – un punto de conexión resuelto no incluye el ID de cuenta.
- **`required`** – el punto de conexión debe incluir el ID de cuenta. Si el ID de la cuenta no está disponible, el SDK lanza un error.

Se puede anular mediante la variable de entorno `AWS_ACCOUNT_ID_ENDPOINT_MODE`. Para utilizar puntos de conexión basados en cuentas, el ID debe estar establecido en la variable de entorno `AWS_ACCOUNT_ID` o en la configuración de `aws_account_id`.

```
account_id_endpoint_mode = preferred
```

> **Prioridad de los puntos de conexión**
>
> Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. La AWS CLI comprueba estas configuraciones de punto de conexión en un orden determinado y utiliza la configuración de punto de conexión con la prioridad más alta. Para ver la lista de prioridad de los puntos de conexión, consulte the section called “Prioridad de la configuración y los ajustes del punto de conexión”.

`aws_access_key_id`

Especifica la clave de acceso de AWS que se utiliza como parte de las credenciales para autenticar la solicitud del comando. Aunque puede estar almacenada en el archivo `config`, recomendamos almacenar esta información en el archivo `credentials`.

Se puede anular mediante la variable de entorno `AWS_ACCESS_KEY_ID`. No se puede especificar el ID de clave de acceso como una opción de línea de comandos.

```
aws_access_key_id = AKIAIOSFODNN7EXAMPLE
```

`aws_account_id`

Especifica el ID de punto de conexión basado en la cuenta de AWS que se utilizará para las llamadas a los Servicios de AWS compatibles. Para obtener más información sobre los puntos de conexión basados en cuentas, consulte the section called “Puntos de conexión basados en cuentas”.

Se puede anular mediante la variable de entorno `AWS_ACCOUNT_ID`. La variable de entorno `AWS_ACCOUNT_ID_ENDPOINT_MODE` o la configuración de `account_id_endpoint_mode` deben estar configuradas en `preferred` o `required` para poder utilizar esta configuración.

```
aws_account_id = 123456789EXAMPLE
```

> **Prioridad de los puntos de conexión**
>
> Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. La AWS CLI comprueba estas configuraciones de punto de conexión en un orden determinado y utiliza la configuración de punto de conexión con la prioridad más alta. Para ver la lista de prioridad de los puntos de conexión, consulte the section called “Prioridad de la configuración y los ajustes del punto de conexión”.

`aws_secret_access_key`

Especifica la clave secreta de AWS que se utiliza como parte de las credenciales para autenticar la solicitud del comando. Aunque puede estar almacenada en el archivo `config`, recomendamos almacenar esta información en el archivo `credentials`.

Se puede anular mediante la variable de entorno `AWS_SECRET_ACCESS_KEY`. No se puede especificar la clave de acceso secreta como una opción de línea de comandos.

```
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

`aws_session_token`

Especifica un token de sesión de AWS. Un token de sesión solo es necesario si especifica manualmente credenciales de seguridad temporales. Aunque puede estar almacenada en el archivo `config`, recomendamos almacenar esta información en el archivo `credentials`.

Se puede anular mediante la variable de entorno `AWS_SESSION_TOKEN`. No se puede especificar un token de sesión como una opción de línea de comandos.

```
aws_session_token = AQoEXAMPLEH4aoAH0gNCAPyJxz4BlCFFxWNE1OPTgk5TthT
+FvwqnKwRcOIfrRh3c/LTo6UDdyJwOOvEVPvLXCrrrUtdnniCEXAMPLE/
IvU1dYUg2RVAJBanLiHb4IgRmpRV3zrkuWJOgQs8IZZaIv2BXIa2R4Olgk
```

`ca_bundle`

Especifica un paquete de certificados de CA (un archivo con la extensión `.pem`) que se utiliza para verificar certificados SSL.

Se puede anular mediante la variable de entorno `AWS_CA_BUNDLE` o la opción de línea de comandos `--ca-bundle`.

```
ca_bundle = dev/apps/ca-certs/cabundle-2019mar05.pem
```

`cli_auto_prompt`

Habilita la petición automática para la versión 2 de AWS CLI. Hay dos configuraciones que se pueden usar:

- **`on`** utiliza el modo de petición automática completa cada vez que intenta ejecutar un comando de `aws`. Esto incluye presionar ENTER (INTRO) después de un comando completo o un comando incompleto.

  ```
  cli_auto_prompt = on
  ```

- **`on-partial`** utiliza el modo de petición automática parcial. Si un comando está incompleto o no se puede ejecutar debido a errores de validación del lado del cliente, se utiliza la petición automática. Este modo es especialmente útil si tiene scripts preexistentes, runbooks, o solo desea que se le pregunte automáticamente sobre los comandos con los que no está familiarizado en lugar de preguntarle sobre cada comando.

  ```
  cli_auto_prompt = on-partial
  ```

Puede anular esta configuración mediante la variable de entorno de `aws_cli_auto_prompt` o los parámetros de la línea de comandos `--cli-auto-prompt` y `--no-cli-auto-prompt`.

Para obtener información sobre la características de petición automática de la versión 2 de AWS CLI, consulte Activación y uso de los símbolos del sistema en la AWS CLI.

`cli_binary_format`

Especifica cómo la versión 2 de AWS CLI interpreta los parámetros de entrada binarios. Puede ser uno de los siguientes valores:

- base64: este es el valor predeterminado. Un parámetro de entrada escrito como un objeto binario grande (BLOB) acepta una cadena codificada en base64. Para pasar verdadero contenido binario, coloque el contenido en un archivo y proporcione la ruta y el nombre del archivo con el prefijo `fileb://` como valor del parámetro. Para pasar el texto codificado en base64 incluido en un archivo, proporcione la ruta y el nombre del archivo con el prefijo `file://` como valor del parámetro.
- raw-in-base64-out: valor predeterminado para la AWS CLI versión 1. Si el valor de la configuración es `raw-in-base64-out`, los archivos a los que se hace referencia mediante el prefijo `file://` se leen como texto y, a continuación, la AWS CLI intenta codificarlo en binario.

Esta entrada no tiene una variable de entorno equivalente. Puede especificar el valor en un solo comando mediante el parámetro `--cli-binary-format raw-in-base64-out`.

```
cli_binary_format = raw-in-base64-out
```

Si hace referencia a un valor binario en un archivo mediante la notación del prefijo `fileb://`, la AWS CLI siempre espera que el archivo incluya contenido binario sin codificar y no intenta convertir el valor.

Si hace referencia a un valor binario en un archivo mediante la notación del prefijo `file://`, la AWS CLI tratará el archivo de acuerdo con el valor de `cli_binary_format` actual. Si el valor de esa configuración es `base64` (el valor predeterminado cuando no se establece explícitamente), la AWS CLI espera que el archivo contenga texto codificado en base64. Si el valor de esa configuración es `raw-in-base64-out`, la AWS CLI espera que el archivo incluya contenido binario sin codificar.

`cli_help_output`

A partir de la versión `2.31.0` La visualización del comando `help` se configura mediante el ajuste `cli_help_output` y tiene los siguientes valores:

- (predeterminado) `terminal`: abra la página principal en el terminal.
- `browser`: abra la página principal como un archivo HTML local en el navegador predeterminado. Se imprime un aviso en el terminal cuando se abre el navegador predeterminado y un mensaje de error si la AWS CLI no puede abrir el navegador.
- `url`: imprima la URL de la guía de referencia de AWS CLI en línea de la versión de la AWS CLI que ha instalado. Se respetan los ajustes de la paginación del cliente, como la variable de entorno `AWS_PAGER`.

```
cli_help_output = browser
```

Para obtener más información acerca del comando `help`, consulte the section called “Obtención de ayuda”.

`cli_history`

Está deshabilitado de forma predeterminada. Esta configuración habilita el historial de comandos para la AWS CLI. Después de habilitar esta configuración, la AWS CLI registra el historial de comandos `aws`.

```
cli_history = enabled
```

Puede hacer una lista de su historial con el comando `aws history list` y utilizar los `command_ids` resultantes en el comando `aws history show` para obtener más información. Para obtener más información, consulte `aws history` en la Guía de referencia de la AWS CLI.

`cli_pager`

Especifica el programa de paginación utilizado para la salida. De forma predeterminada, la versión 2 de AWS CLI devuelve todas las salidas a través del paginador predeterminado de su sistema operativo.

Puede ser anulado por la variable de entorno AWS_PAGER.

```
cli_pager=less
```

`cli_timestamp_format`

Especifica el formato de los valores de la marca temporal de la salida. Puede especificar cualquiera de los siguientes valores:

- iso8601: el valor predeterminado para la versión 2 de AWS CLI. Si se especifica, la AWS CLI cambia el formato de todas las marcas temporales en la salida conforme a ISO 8601. Las marcas temporales con formato ISO 8601 se parecen a los siguientes ejemplos. En el ejemplo siguiente, se muestra cómo se formatea la hora separando la fecha y la hora con una T e incluyendo una Z después de la hora.

  ```
  YYYY-MM-DDThh:mm:ssZ
  ```

  En los ejemplos siguientes, se muestra una marca temporal utilizando el formato anterior.

  ```
  2024-05-08T15:16:43Z
  ```

- wire: el valor predeterminado para la versión 1 de AWS CLI. Si se especifica, la AWS CLI muestra todos los valores de las marcas temporales exactamente como se recibieron en la respuesta de la consulta HTTP.

Esta configuración no tiene una variable de entorno equivalente ni una opción de línea de comandos. Esta configuración no modifica las entradas de la marca temporal, solo el formato de salida.

```
cli_timestamp_format = iso8601
```

credential_process

Especifica un comando externo que la AWS CLI ejecuta para generar o recuperar las credenciales de autenticación que se van a utilizar para este comando. El comando debe devolver las credenciales en un formato específico. Para obtener más información sobre el uso de esta configuración, consulte Obtención de credenciales con un proceso externo en la AWS CLI.

Esta entrada no tiene una variable de entorno equivalente ni una opción de línea de comandos.

```
credential_process = /opt/bin/awscreds-retriever --username susan
```

credential_source

Se utiliza en instancias o en contenedores de Amazon EC2 para especificar dónde la AWS CLI puede encontrar credenciales para usar a fin de asumir el rol que usted especificó con el parámetro `role_arn`. No puede especificar `source_profile` y `credential_source` en el mismo perfil.

Este parámetro puede tener uno de tres valores:

- Environment (entorno): especifica que la AWS CLI va a recuperar las credenciales fuente a partir de las variables de entorno.
- Ec2InstanceMetadata: especifica que la AWS CLI va a utilizar el rol de IAM asociado al perfil de instancia EC2 para obtener las credenciales fuente.
- EcsContainer: especifica que la AWS CLI va a utilizar el rol de IAM asociado al contenedor de ECS como credenciales fuente.

```
credential_source = Ec2InstanceMetadata
```

`duration_seconds`

Especifica la duración máxima de la sesión de rol, en segundos. Este valor puede oscilar entre 900 segundos (15 minutos) y el valor de la duración máxima de la sesión para el rol (que puede ser 43200 como máximo). Se trata de un parámetro opcional y, de forma predeterminada, el valor se establece en 3600 segundos.

`endpoint_url`

Especifica el punto de conexión que se utiliza para todas las solicitudes de servicio. Si esta configuración se usa en la sección de `services` del archivo `config`, el punto de conexión se usa solo para el servicio especificado. Para obtener más información, consulte the section called "Establecer un punto de conexión global para todos los Servicios de AWS".

En el siguiente ejemplo, se utiliza el punto de conexión global `http://localhost:1234` y un punto de conexión específico del servicio de `http://localhost:4567` para Amazon S3.

```
[profile dev]
endpoint_url = http://localhost:1234
services = s3-specific

[services s3-specific]
s3 =
  endpoint_url = http://localhost:4567
```

> **Prioridad de los puntos de conexión**
>
> Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de

AWS locales o declarados explícitamente en la línea de comandos como un parámetro. La AWS CLI comprueba estas configuraciones de punto de conexión en un orden determinado y utiliza la configuración de punto de conexión con la prioridad más alta. Para ver la lista de prioridad de los puntos de conexión, consulte the section called "Prioridad de la configuración y los ajustes del punto de conexión".

`ignore_configure_endpoint_urls`

Si está habilitada, la AWS CLI ignora todas las configuraciones de punto de conexión personalizadas especificadas en el archivo `config`. Los valores válidos son **`true`** y **`false`**.

```
ignore_configure_endpoint_urls = true
```

> **Prioridad de los puntos de conexión**
>
> Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. La AWS CLI comprueba estas configuraciones de punto de conexión en un orden determinado y utiliza la configuración de punto de conexión con la prioridad más alta. Para ver la lista de prioridad de los puntos de conexión, consulte the section called "Prioridad de la configuración y los ajustes del punto de conexión".

`external_id`

Especifica un identificador único utilizado por terceros para adoptar un rol en las cuentas de los clientes. Se asigna al parámetro `ExternalId` en la operación `AssumeRole`. Este parámetro solo es necesario si la política de confianza del rol especifica un valor para `ExternalId`. Para obtener más información, consulte Cómo utilizar un ID externo al conceder acceso a los recursos de AWS a terceros en la Guía del usuario de IAM.

`max_attempts`

Especifica un valor de los intentos de reintento máximos que utiliza el controlador de reintentos de AWS CLI, donde la llamada inicial cuenta hasta el valor `max_attempts` que usted le proporciona.

Puede invalidar este valor mediante la variable de entorno de `AWS_MAX_ATTEMPTS`.

```
max_attempts = 3
```

`mfa_serial`

El número de identificación del dispositivo MFA que se debe utilizar al asumir un rol. Este valor solo es obligatorio si la política de confianza del rol que se ha asumido incluye una condición que requiere autenticación MFA. El valor puede ser un número de serie de un dispositivo de hardware (como `GAHT12345678`) o un nombre de recurso de Amazon (ARN) de un dispositivo MFA virtual (como `arn:aws:iam::123456789012:mfa/user`).

`output`

Especifica el formato de la salida predeterminado para los comandos solicitados con este perfil. Puede especificar cualquiera de los siguientes valores:

- **`json`**: la salida se formatea como una cadena JSON.
- **`yaml`**: la salida se formatea como una cadena YAML.
- **`yaml-stream`**: la salida se transmite y se formatea como una cadena YAML. La transmisión permite gestionar tipos de datos de gran tamaño de forma más rápida.
- **`text`** – la salida tiene el formato de varias líneas de valores de cadena separados por tabuladores. Esto puede ser útil para pasar la salida a un procesador de texto, como `grep`, `sed` o `awk`.
- **`table`** – el resultado tiene el formato de una tabla en la que se usan los caracteres +|- para los bordes de celda. Normalmente, la información se presenta en un formato que es más fácil de leer que los demás formatos, pero que no es útil para programar.

Se puede anular mediante la variable de entorno `AWS_DEFAULT_OUTPUT` o la opción de línea de comandos `--output`.

```
output = table
```

`parameter_validation`

Especifica si el cliente de la AWS CLI intenta validar parámetros antes de enviarlos al punto de enlace de servicio de AWS.

- true (verdadero): es el valor predeterminado. Si se especifica, la AWS CLI realiza la validación local de los parámetros de la línea de comandos.

- false (falso): si se especifica, la AWS CLI no valida los parámetros de la línea de comandos antes de enviarlos al punto de enlace de servicio de AWS.

Esta entrada no tiene una variable de entorno equivalente ni una opción de línea de comandos.

```
parameter_validation = false
```

`region`

Especifica la Región de AWS a la que se envían solicitudes para los comandos solicitados con este perfil.

- Puede especificar cualquiera de los códigos de región disponibles para el servicio elegido que se muestran en Regiones y puntos de conexión de AWS en la Referencia general de Amazon Web Services.
- `aws_global` le permite especificar el punto de conexión global para los servicios que admiten un punto de conexión global además de puntos de conexión regionales, como AWS Security Token Service (AWS STS) y Amazon Simple Storage Service (Amazon S3).

Puede invalidar este valor mediante la variable de entorno `AWS_REGION`, variable de entorno `AWS_DEFAULT_REGION` o la opción de línea de comandos `--region`.

```
region = us-west-2
```

`request_checksum_calculation`

Especifica cuándo se calcula una suma de comprobación para las cargas útiles de solicitud y tiene las siguientes opciones:

- `when_supported`: (predeterminado) la suma de comprobación de la carga útil de la solicitud se calcula cuando una operación especifica un algoritmo de suma de comprobación en su modelo de servicio o requiere sumas de comprobación de la solicitud.
- `when_required`: la suma de comprobación de la carga útil de la solicitud se calcula cuando una operación requiere sumas de control de la solicitud o cuando un usuario proporciona un `requestAlgorithmMember` que está modelado por el Servicio de AWS.

```
request_checksum_calculation = when_supported
```

La variable de entorno AWS_REQUEST_CHECKSUM_CALCULATION anula esta configuración.

response_checksum_validation

Especifica cuándo se realiza una validación de suma de comprobación para las cargas útiles de respuesta y tiene las siguientes opciones:

- `when_supported`: (predeterminado) la validación de la suma de comprobación de la carga útil de respuesta se realiza cuando una operación especifica un algoritmo de respuesta en su modelo de servicio que admite AWS CLI.
- `when_required`: la validación de la suma de comprobación de la carga útil de respuesta se realiza cuando una operación especifica un algoritmo de respuesta en su modelo de servicio que admite la AWS CLI, y establece el `requestValidationModeMember` modelado en `ENABLED` en la entrada de la operación.

```
response_checksum_validation = when_supported
```

La variable de entorno AWS_RESPONSE_CHECKSUM_VALIDATION anula esta configuración.

retry_mode

Especifica qué modo de reintento utiliza AWS CLI. Hay tres modos de reintento disponibles: `standard` (predeterminado), `legacy` (predeterminado) y `adaptive`. Para obtener más información acerca de los reintentos, consulte Reintentos de AWS CLI en la AWS CLI.

Puede invalidar este valor mediante la variable de entorno de `AWS_RETRY_MODE`.

```
retry_mode = standard
```

role_arn

Especifica el nombre de recurso de Amazon (ARN) del rol de IAM que desea utilizar para ejecutar los comandos de la AWS CLI. También debe especificar uno de los siguientes parámetros para identificar las credenciales que tienen permiso para asumir este rol:

- source_profile
- credential_source

```
role_arn = arn:aws:iam::123456789012:role/role-name
```

La variable de entorno AWS_ROLE_ARN anula esta configuración.

Para obtener más información sobre el uso de las identidades web, consulte the section called “Adopción de un rol con una identidad web”.

role_session_name

Especifica el nombre que se va a asociar a la sesión de rol. Este valor se proporciona al parámetro `RoleSessionName` cuando la AWS CLI llama a la operación `AssumeRole` y pasa a formar parte del ARN del usuario del rol asumido: `arn:aws:sts::123456789012:assumed-role/role_name/role_session_name`. Se trata de un parámetro opcional. Si no proporciona este valor, se genera automáticamente un nombre de sesión. Este nombre aparece en los registros de AWS CloudTrail correspondientes a las entradas asociadas a esta sesión.

```
role_session_name = maria_garcia_role
```

La variable de entorno AWS_ROLE_SESSION_NAME anula esta configuración.

Para obtener más información sobre el uso de las identidades web, consulte the section called "Adopción de un rol con una identidad web".

services

Especifica la configuración del servicio que se utilizará en el perfil.

```
[profile dev-s3-specific-and-global]
endpoint_url = http://localhost:1234
services = s3-specific

[services s3-specific]
s3 =
  endpoint_url = http://localhost:4567
```

Para obtener más información sobre la sección de `services`, consulte the section called "`services`".

La variable de entorno AWS_ROLE_SESSION_NAME anula esta configuración.

Para obtener más información sobre el uso de las identidades web, consulte the section called "Adopción de un rol con una identidad web".

sdk_ua_app_id

Varias aplicaciones de los clientes pueden utilizar una sola Cuenta de AWS para realizar llamadas a los Servicios de AWS. El ID de aplicación identifica qué aplicación de origen ha realizado un conjunto de llamadas mediante un Servicio de AWS. AWS Los SDK y los servicios solo utilizan e interpretan este valor para mostrarlo de nuevo en las comunicaciones con los

clientes. Por ejemplo, este valor se puede incluir en los correos electrónicos operativos para identificar de forma exclusiva qué aplicaciones están asociadas a la notificación.

El ID de la aplicación es una cadena con una longitud máxima de 50 caracteres. Los valores permitidos incluyen letras, números y los siguientes caracteres especiales: `! $ % & * + - . , ^ _ ` | ~`. De forma predeterminada, no se establece ningún valor.

```
sdk_ua_app_id = prod1
```

Esta configuración se puede sobrescribir utilizando la variable de entorno AWS_SDK_UA_APP_ID. No se puede establecer este valor como parámetro de la línea de comandos.

sigv4a_signing_region_set

Especifica las regiones que se van a utilizar al firmar con SigV4a mediante una lista delimitada por comas. Si esta variable no está establecida, la AWS CLI utiliza la variable predeterminada utilizada por Servicio de AWS. Si el Servicio de AWS no tiene un valor predeterminado, la firma de la solicitud pasa a ser válida en todas las regiones con un valor de `*`.

```
sigv4a_signing_region_set = us-west-2, us-east-1
```

Para obtener más información sobre SigV4a, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM

Esta configuración se puede sobrescribir utilizando la variable de entorno AWS_SIGV4A_SIGNING_REGION_SET. No se puede establecer este valor como parámetro de la línea de comandos.

source_profile

Especifica un perfil con nombre con credenciales duraderas que la AWS CLI puede utilizar para asumir el rol que ha especificado con el parámetro `role_arn`. No puede especificar `source_profile` y `credential_source` en el mismo perfil.

```
source_profile = production-profile
```

sso_account_id

Especifica el ID de la cuenta de AWS que contiene el rol de IAM con el permiso que desea conceder al usuario de IAM Identity Center asociado.

Esta configuración no tiene ninguna variable de entorno ni ninguna opción de línea de comandos.

```
sso_account_id = 123456789012
```

sso_region

Especifica la región de AWS que contiene el host del portal de acceso de AWS. Esto es independiente (y puede ser una región diferente) del parámetro `region` predeterminado de la CLI.

Esta configuración no tiene ninguna variable de entorno ni ninguna opción de línea de comandos.

```
sso_region = us_west-2
```

sso_registration_scopes

Una lista delimitada por comas de los ámbitos que deben autorizarse para la `sso-session`. Los ámbitos autorizan el acceso a los puntos de conexión autorizados por el token de portador del Centro de identidades de IAM. Un ámbito válido es una cadena, por ejemplo, `sso:account:access`. Esta configuración no es aplicable a la configuración heredada no actualizable.

```
sso_registration_scopes = sso:account:access
```

sso_role_name

Especifica el nombre descriptivo del rol de IAM que define los permisos que tiene el usuario cuando utiliza este perfil.

Esta configuración no tiene ninguna variable de entorno ni ninguna opción de línea de comandos.

```
sso_role_name = ReadAccess
```

sso_start_url

Especifica la URL que apunta al portal de acceso de AWS de la organización. La AWS CLI utiliza esta dirección URL para establecer una sesión con el servicio IAM Identity Center para autenticar a sus usuarios. Para encontrar la URL del portal de acceso de AWS, puede usar una de las opciones siguientes:

- Abra el correo electrónico de invitación, aparece la URL del portal de acceso de AWS.
- Abra la consola de AWS IAM Identity Center en https://console.aws.amazon.com/singlesignon/. La URL del portal de acceso de AWS aparece en la configuración.

Esta configuración no tiene ninguna variable de entorno ni ninguna opción de línea de comandos.

```
sso_start_url = https://my-sso-portal.awsapps.com/start
```

`use_dualstack_endpoint`

Permite el uso de puntos de conexión de doble pila para enviar solicitudes de AWS. Para obtener más información sobre los puntos de conexión de doble pila, que admiten tráfico de IPv4 e IPv6, consulte Uso de puntos de conexión de doble pila de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service. Los puntos de conexión de doble pila están disponibles para algunos servicios en algunas regiones. Si no existe un punto de conexión de doble pila para el servicio o Región de AWS, la solicitud produce un error. Los parámetros válidos son `true` y `false`. Esta opción está deshabilitada de forma predeterminada. Para obtener más información, consulte the section called “Establecer para utilizar los puntos de conexión de doble pila para todos los Servicios de AWS”.

Es mutuamente excluyente con la configuración `use_accelerate_endpoint`.

> **Prioridad de los puntos de conexión**
>
> Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. La AWS CLI comprueba estas configuraciones de punto de conexión en un orden determinado y utiliza la configuración de punto de conexión con la prioridad más alta. Para ver la lista de prioridad de los puntos de conexión, consulte the section called “Prioridad de la configuración y los ajustes del punto de conexión”.

`use_fips_endpoint`

Algunos servicios de AWS ofrecen puntos de conexión compatibles que admiten el Estándar de procesamiento de la información federal (FIPS) 140-2 en algunas Regiones de AWS. Cuando el servicio de AWS es compatible con FIPS, esta configuración establece qué punto de conexión FIPS debe utilizar la AWS CLI. A diferencia de los puntos de conexión de AWS estándar, los

puntos de conexión FIPS utilizan una biblioteca de software TLS que cumple con FIPS 140-2. Las empresas que trabajan con el gobierno de los Estados Unidos pueden requerir estos puntos de conexión. Para obtener más información, consulte the section called “Establecer para usar los puntos de conexión de FIPS para todos los Servicios de AWS”.

Si esta configuración está habilitada pero no existe un punto de conexión FIPS para el servicio en la Región de AWS, es posible que el comando AWS produzca un error. En este caso, especifique manualmente el punto de conexión que se va a utilizar en el comando mediante la opción `--endpoint-url` o utilice los puntos de conexión específicos del servicio.

> **Prioridad de los puntos de conexión**
>
> Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. La AWS CLI comprueba estas configuraciones de punto de conexión en un orden determinado y utiliza la configuración de punto de conexión con la prioridad más alta. Para ver la lista de prioridad de los puntos de conexión, consulte the section called “Prioridad de la configuración y los ajustes del punto de conexión”.

`web_identity_token_file`

Especifica la ruta de un archivo que contiene un token de acceso de OAuth 2.0 o un token de ID de OpenID Connect proporcionado por un proveedor de identidades. La AWS CLI carga el contenido de este archivo y lo pasa como argumento `WebIdentityToken` a la operación `AssumeRoleWithWebIdentity`.

La variable de entorno `AWS_WEB_IDENTITY_TOKEN_FILE` anula esta configuración.

Para obtener más información sobre el uso de las identidades web, consulte the section called “Adopción de un rol con una identidad web”.

`tcp_keepalive`

Especifica si el cliente de la AWS CLI utiliza paquetes keep-alive de TCP.

Esta entrada no tiene una variable de entorno equivalente ni una opción de línea de comandos.

```
tcp_keepalive = false
```

Configuración de comandos personalizados de S3

Amazon S3 admite varios ajustes que configuran la forma en que la AWS CLI realiza operaciones de Amazon S3. Algunos se aplican a todos los comandos de S3 tanto en los espacios de nombres `s3api` como `s3`. Otros son específicos de los comandos "personalizados" de S3 que abstraen operaciones comunes y hacen más que un mapeo uno a uno en una operación de la API. Los comandos de `aws s3` de transferencia `cp`, `sync`, `mv` y `rm` tienen opciones adicionales que puede utilizar para controlar las transferencias de S3.

Para configurar todas estas opciones, especifique la configuración `s3` anidada en su archivo `config`. A continuación, se introduce con sangría cada configuración en su propia línea.

> **Note**
>
> Estos ajustes son completamente opcionales. Debe poder utilizar los comandos de transferencia de `aws s3` sin configurar ninguno de estos ajustes. Estas opciones se ofrecen para afinar el rendimiento o para tener en cuenta el entorno específico en el que se ejecutan estos comandos de `aws s3`.

Estos ajustes se establecen con una clave de `s3` de alto nivel en el archivo `config`, tal y como se muestra en el siguiente ejemplo del perfil `development`.

```
[profile development]
s3 =
  max_concurrent_requests = 20
  max_queue_size = 10000
  multipart_threshold = 64MB
  multipart_chunksize = 16MB
  max_bandwidth = 50MB/s
  use_accelerate_endpoint = true
  addressing_style = path
```

Los siguientes ajustes se aplican a cualquier comando de S3 en el espacio de nombres `s3` o `s3api`.

`addressing_style`

Especifica qué estilo de direccionamiento debe usarse. Esto controla si el nombre del bucket está en el hostname o es parte de la URL. Los valores válidos son `path`, `virtual` y `auto`. El valor predeterminado es `auto`.

Hay dos estilos para crear un punto enlace de Amazon S3. El primero se llama `virtual` e incluye el nombre del bucket como parte del nombre de host. Por ejemplo: `https://`*`bucketname`*`.s3.amazonaws.com`. Si lo desea, también puede utilizar el estilo `path`, que tratará el nombre del bucket como si fuera una ruta del URI; por ejemplo, `https://s3.amazonaws.com/`*`bucketname`*. El valor predeterminado en la CLI es utilizar `auto`, que intenta utilizar el estilo `virtual` siempre que puede, pero usará el estilo `path` cuando sea necesario. Por ejemplo, si el nombre del bucket no es compatible con DNS, el nombre del bucket no puede formar parte del nombre de host y debe estar en la ruta. Con `auto`, la CLI detectará esta condición y cambiará automáticamente al estilo `path`. Si establece el estilo de direccionamiento en `path`, debe asegurarse de que la región de AWS que ha configurado en la AWS CLI coincida con la región del bucket.

`payload_signing_enabled`

Especifica si firma con SHA256 cargas de sigv4. De forma predeterminada, esta opción está deshabilitada para cargas de streaming (`UploadPart` y `PutObject`) cuando se utiliza https. De forma predeterminada, la opción está configurada en `false` para cargas de streaming (`UploadPart` y `PutObject`), pero solo si está presente un `ContentMD5` (se genera de forma predeterminada) y el punto de enlace utiliza HTTPS.

Si se establece en verdadero, las solicitudes de S3 reciben validación de contenido adicional en forma de suma de comprobación SHA256 que se calcula automáticamente y se incluye en la firma de la solicitud. Si se establece en falso, la suma de comprobación no se calcula. Deshabilitar esta opción puede ser útil para reducir la sobrecarga de rendimiento creada por el cálculo de la suma de comprobación.

`use_accelerate_endpoint`

Utilice el punto de enlace de aceleración de Amazon S3 para todos los comandos `s3` y `s3api`. El valor predeterminado es false. Es mutuamente excluyente con la configuración `use_dualstack_endpoint`.

Si se establece en true (verdadero), la AWS CLI dirige todas las solicitudes de Amazon S3 al punto de enlace de `S3 Accelerate` en `s3-accelerate.amazonaws.com`. Para utilizar este punto de enlace, debe habilitar el bucket para que use `S3 Accelerate`. Todas las solicitudes se envían mediante el direccionamiento al bucket de estilo virtual: .: *`my-bucket`*`.s3-accelerate.amazonaws.com`. Las solicitudes `ListBuckets`, `CreateBucket` y `DeleteBucket` no se envían al punto de enlace de S3 Accelerate, ya que este punto de enlace no admite estas operaciones. Este comportamiento también se puede establecer si el

parámetro `--endpoint-url` está establecido en `https://s3-accelerate.amazonaws.com` o `http://s3-accelerate.amazonaws.com` para cualquier comando `s3` o `s3api`.

`use_dualstack_endpoint`

Permite el uso de puntos de conexión de doble pila para enviar solicitudes de `s3` y `s3api`. Para obtener más información sobre los puntos de conexión de doble pila, que admiten tráfico de IPv4 e IPv6, consulte Uso de puntos de conexión de doble pila de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service. Los puntos de conexión de doble pila están disponibles para algunos servicios en algunas regiones. Si no existe un punto de conexión de doble pila para el servicio o Región de AWS, la solicitud produce un error. Los parámetros válidos son `true` y `false`. Esta opción está deshabilitada de forma predeterminada. Para obtener más información, consulte the section called “Establecer para utilizar los puntos de conexión de doble pila para todos los Servicios de AWS”.

Es mutuamente excluyente con la configuración `use_accelerate_endpoint`.

Estos ajustes de configuración solo se aplican a los comandos del conjunto de comandos del espacio de nombres de `s3`:

`max_bandwidth`

Especifica el ancho de banda máximo que puede ser consumido para cargar y descargar datos desde y hacia Amazon S3. El valor predeterminado es sin límite.

Esto limita el ancho de banda máximo que los comandos de S3 pueden utilizar para transferir datos desde y hacia Amazon S3. Este valor se aplica únicamente a cargas y descargas; no se aplica a copias o eliminaciones. El valor se expresa como bytes por segundo. El valor puede especificarse como:

- Un número entero. Por ejemplo, `1048576` establece el uso de ancho de banda máximo en 1 megabyte por segundo.
- Un número entero seguido de un sufijo de velocidad. Puede especificar sufijos de velocidad mediante: `KB/s`, `MB/s` o `GB/s`. Por ejemplo, `300KB/s`, `10MB/s`.

En general, se recomienda intenta reducir primero el consumo de ancho de banda, disminuyendo las `max_concurrent_requests`. Si así no se reduce el consumo de ancho de banda lo suficiente para conseguir la velocidad deseada, puede utilizar la opción `max_bandwidth` para limitar más el consumo de ancho de banda. Esto se debe a que `max_concurrent_requests` controla la cantidad de subprocesos se están ejecutando en este momento. Si en su lugar reduce

primero `max_bandwidth` pero deja `max_concurrent_requests` en un valor alto, puede provocar que los subprocesos tengan que esperar innecesariamente. Esto puede provocar un consumo excesivo de recursos y que se agoten los tiempos de espera de conexión.

`max_concurrent_requests`

Especifica el número máximo de solicitudes concurrentes. El valor predeterminado es 10.

Los comandos de transferencia de `aws s3` tienen varios subprocesos. En un momento dado, es posible que se estén ejecutando varias solicitudes de Amazon S3. Por ejemplo, cuando utiliza el comando `aws s3 cp localdir s3://bucket/ --recursive` para cargar archivos en un bucket de S3, la AWS CLI puede cargar los archivos `localdir/file1`, `localdir/file2` y `localdir/file3` en paralelo. La configuración `max_concurrent_requests` especifica el número máximo de operaciones de transferencia que se pueden ejecutar al mismo tiempo.

Es posible que tenga que cambiar este valor por varios motivos:

- Reducir el valor: en algunos entornos, el valor predeterminado de 10 solicitudes simultáneas puede ser demasiado para un sistema. Esto puede provocar tiempos de espera de conexión o ralentizar la capacidad de respuesta del sistema. Al reducir este valor, los comandos de transferencia de S3 consumen menos recursos. La desventaja es que las transferencias de S3 puede tardar más en completarse. Puede ser necesario reducir este valor si utiliza una herramienta para limitar el ancho de banda.
- Aumentar el valor: en algunos casos, puede ser conveniente que las transferencias de Amazon S3 se completen lo más rápido posible, con el mayor ancho de banda de red según sea necesario. En este caso, el número predeterminado de solicitudes simultáneas podría no ser suficiente para utilizar todo el ancho de banda de red disponible. Al aumentar este valor puede mejorar el tiempo que se tarda en completar una transferencia de Amazon S3.

`max_queue_size`

Especifica el número máximo de tareas en la cola. El valor predeterminado es 1000.

La AWS CLI utiliza internamente un modelo que pone en cola las tareas de Amazon S3 que luego ejecutan los consumidores, cuyo número está limitado por `max_concurrent_requests`. Una tarea, por lo general, se asigna a una sola operación de Amazon S3. Por ejemplo, una tarea puede ser `PutObjectTask`, `GetObjectTask` o `UploadPartTask`. La velocidad a la que se añaden tareas a la cola puede ser mucho más rápida que la velocidad en la que los consumidores finalizan las tareas. Para evitar el crecimiento ilimitado, el tamaño de la cola de tareas se limita a un tamaño específico. Esta configuración cambia el valor de ese número máximo.

Por lo general, no tendrá que cambiar este ajuste. Esta configuración también se corresponde con el número de tareas que la AWS CLI sabe que tienen que ejecutarse. Esto significa que, de forma predeterminada, la AWS CLI solo puede ver 1000 tareas. Aumentar este valor significa que la AWS CLI puede saber con mayor rapidez el número total de tareas necesario, suponiendo que la velocidad de la cola sea más rápida que la velocidad de finalización de la tarea. La desventaja es que un valor mayor en max_queue_size, exige también más memoria.

`multipart_chunksize`

Especifica el tamaño del fragmento que la AWS CLI utiliza en las transferencias multiparte de archivos individuales. El valor predeterminado es 8 MB, con un mínimo de 5 MB.

Cuando la transferencia de un archivo supera el `multipart_threshold`, la AWS CLI divide el archivo en fragmentos de este tamaño. Este valor puede especificarse utilizando la misma sintaxis que en `multipart_threshold`, ya sea especificando el número de bytes como un número entero o especificando un tamaño y un sufijo.

`multipart_threshold`

Especifica el umbral de tamaño que la AWS CLI utiliza en las transferencias multiparte de archivos individuales. El valor predeterminado es 8 MB.

Al cargar, descargar o copiar un archivo, los comandos de Amazon S3 cambian a operaciones multiparte si el archivo supera este tamaño. Puede especificar este valor de una de las dos formas siguientes:

- El tamaño del archivo en bytes. Por ejemplo, `1048576`.
- El tamaño del archivo con un sufijo de tamaño. Puede utilizar `KB`, `MB`, `GB` o `TB`. Por ejemplo: `10MB`, `1GB`.

> **Note**
>
> S3 puede imponer restricciones en los valores válidos que se pueden utilizar para las operaciones multiparte. Para obtener más información, consulte la documentación Carga multiparte de S3 en la Guía de del usuario de Amazon Simple Storage Service.

Configuración de variables de entorno para la AWS CLI

Las variables de entorno constituyen otro mecanismo para especificar opciones de configuración y credenciales, y pueden ser útiles para crear script.

Prioridad de las opciones

- Si especifica una opción mediante una de las variables de entorno que se describen en este tema, se invalidará cualquier valor carga desde un perfil en el archivo de configuración.
- Si especifica una opción mediante un parámetro en la línea de comando de la AWS CLI, se invalidará cualquier valor de la variable de entorno correspondiente o un perfil en el archivo de configuración.

Para obtener más información acerca de la prioridad y de cómo la AWS CLI determina la credenciales que debe utilizar, consulte Configuración de los ajustes de AWS CLI.

Temas

- Cómo configurar las variables de entorno
- AWS CLIVariables de entorno que admite la

Cómo configurar las variables de entorno

En los siguientes ejemplos se muestra cómo se pueden configurar las variables de entorno para el usuario predeterminado.

Linux or macOS

```
$ export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
$ export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
$ export AWS_DEFAULT_REGION=us-west-2
```

La configuración de la variable de entorno cambia el valor usado hasta el final de su sesión del intérprete de comandos o hasta que otorgue a la variable un valor diferente. Puede hacer que las variables persistan en sesiones futuras configurándolas en el script de startup del intérprete de comandos.

Windows Command Prompt

Para configurar todas las sesiones

```
C:\> setx AWS_ACCESS_KEY_ID AKIAIOSFODNN7EXAMPLE
C:\> setx AWS_SECRET_ACCESS_KEY wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
C:\> setx AWS_DEFAULT_REGION us-west-2
```

El uso de `setx` para establecer una variable de entorno cambia el valor usado en la sesión de símbolo del sistema actual y en todas las sesiones de símbolo del sistema que cree después de ejecutar el comando. La operación no afecta a otros comandos del shell que ya se están ejecutando en el momento de ejecutar el comando. Puede que tenga que reiniciar el terminal para que se cargue la configuración.

Para configurar solo para la sesión actual

El uso de `set` para configurar una variable de entorno cambia el valor usado hasta que finalice la sesión de símbolo de sistema actual o hasta que otorgue a la variable un valor diferente.

```
C:\> set AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
C:\> set AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
C:\> set AWS_DEFAULT_REGION=us-west-2
```

PowerShell

```
PS C:\> $Env:AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
PS C:\> $Env:AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
PS C:\> $Env:AWS_DEFAULT_REGION="us-west-2"
```

Si establece una variable de entorno en el símbolo del sistema de PowerShell, tal y como se muestra en los ejemplos anteriores, el valor se guarda únicamente durante la sesión actual. Para que el valor de la variable de entorno persista en todas las sesiones de PowerShell y del símbolo del sistema, guárdelo mediante la aplicación Sistema en el Panel de control. También puede definir la variable para todas las sesiones de PowerShell futuras añadiéndolo a su perfil de PowerShell. Consulte la documentación de PowerShell para obtener más información sobre el almacenamiento de variables de entorno o su persistencia entre sesiones.

AWS CLIVariables de entorno que admite la

La AWS CLI admite las siguientes variables de entorno.

`AWS_ACCESS_KEY_ID`

Especifica una clave de acceso de AWS asociada a una cuenta de IAM.

Si se define, esta variable de entorno anula el valor de la configuración del perfil `aws_access_key_id`. No se puede especificar el ID de clave de acceso mediante una opción de línea de comandos.

AWS_ACCOUNT_ID

Especifica el ID de punto de conexión basado en la cuenta de AWS que se utilizará para las llamadas a los Servicios de AWS compatibles. Para obtener más información sobre los puntos de conexión basados en cuentas, consulte the section called “Puntos de conexión basados en cuentas”.

Esta configuración invalida la configuración de `aws_account_id`. La variable de entorno `AWS_ACCOUNT_ID_ENDPOINT_MODE` o la configuración de `account_id_endpoint_mode` deben estar configuradas en `preferred` o `required` para poder utilizar esta configuración.

> **Prioridad de los puntos de conexión**
>
> Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. La AWS CLI comprueba estas configuraciones de punto de conexión en un orden determinado y utiliza la configuración de punto de conexión con la prioridad más alta. Para ver la lista de prioridad de los puntos de conexión, consulte the section called “Prioridad de la configuración y los ajustes del punto de conexión”.

AWS_ACCOUNT_ID_ENDPOINT_MODE

Especifica si se deben utilizar los ID de punto de conexión basados en cuentas de AWS para las llamadas a los Servicios de AWS compatibles. Para obtener más información sobre los puntos de conexión basados en cuentas, consulte the section called “Puntos de conexión basados en cuentas”.

Esta configuración puede establecerse en lo siguiente:

- (predeterminado) **`preferred`**: el punto de conexión debe incluir el ID de cuenta si está disponible.
- **`disabled`** – un punto de conexión resuelto no incluye el ID de cuenta.
- **`required`** – el punto de conexión debe incluir el ID de cuenta. Si el ID de la cuenta no está disponible, el SDK lanza un error.

Esta configuración invalida la configuración de `account_id_endpoint_mode`. Para utilizar puntos de conexión basados en cuentas, el ID debe estar establecido en la variable de entorno `AWS_ACCOUNT_ID` o en la configuración de `aws_account_id`.

> **Prioridad de los puntos de conexión**
>
> Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. La AWS CLI comprueba estas configuraciones de punto de conexión en un orden determinado y utiliza la configuración de punto de conexión con la prioridad más alta. Para ver la lista de prioridad de los puntos de conexión, consulte the section called "Prioridad de la configuración y los ajustes del punto de conexión".

`AWS_CA_BUNDLE`

Especifica la ruta a un paquete de certificados que desea utilizar para la validación de certificados HTTPS.

Si se define, esta variable de entorno anula el valor de la configuración del perfil `ca_bundle`. Puede anular esta variable de entorno mediante el parámetro de la línea de comandos `--ca-bundle`.

`AWS_CLI_AUTO_PROMPT`

Habilita la petición automática para la versión 2 de AWS CLI. Hay dos configuraciones que se pueden usar:

- **`on`** utiliza el modo de petición automática completa cada vez que intenta ejecutar un comando de `aws`. Esto incluye presionar ENTER (INTRO) después de un comando completo o un comando incompleto.
- **`on-partial`** utiliza el modo de petición automática parcial. Si un comando está incompleto o no se puede ejecutar debido a errores de validación del cliente, se utiliza la petición automática. Este modo es útil si tiene scripts preexistentes, manuales de procedimientos o solo desea que se le pregunte automáticamente sobre los comandos con los que no está familiarizado en lugar de preguntarle sobre cada comando.

Si se define, esta variable de entorno anula el valor de la configuración del perfil `cli_auto_prompt`. Puede anular esta variable de entorno mediante los parámetros de la línea de comandos `--cli-auto-prompt` y `--no-cli-auto-prompt`.

Para obtener más información sobre la característica de petición automática de la versión 2 de AWS CLI, consulte Activación y uso de los símbolos del sistema en la AWS CLI.

AWS_CLI_FILE_ENCODING

Especifica la codificación utilizada para los archivos de texto. De forma predeterminada, la codificación coincide con su configuración regional. Para establecer que una codificación distinta de la configuración regional, utilice la variable de entorno `aws_cli_file_encoding`. Por ejemplo, si utiliza Windows con codificación predeterminada `CP1252`, la configuración de `aws_cli_file_encoding=UTF-8` establece la CLI para que abra archivos de texto mediante `UTF-8`.

AWS_CLI_S3_MV_VALIDATE_SAME_S3_PATHS

Si los buckets de origen y destino son los mismos al utilizar el comando `s3 mv`, el archivo u objeto de origen se puede mover sobre sí mismo, lo que puede provocar la eliminación accidental del archivo u objeto de origen. La variable de entorno `AWS_CLI_S3_MV_VALIDATE_SAME_S3_PATHS` y la opción `--validate-same-s3-paths` especifican si se deben validar los ARN de punto de acceso o los alias de puntos de acceso en las URI de origen o destino de Amazon S3.

> **Note**
>
> La validación de rutas de `s3 mv` requiere llamadas a la API adicionales.

AWS_CLI_UPGRADE_DEBUG_MODE

Habilita el modo de depuración de actualizaciones para guiar las actualizaciones de la AWS CLI v1 a la AWS CLI v2. Los valores válidos son `true` y `false`.

Si se configura en `true`, la AWS CLI detectará el uso de características que se actualizaron con cambios importantes en AWS CLI v2 y mostrará advertencias por cada uso detectado que pueda verse afectado. Puede utilizar este modo para preparar el entorno y el uso de AWS CLI para la actualización a v2.

Puede anular esta variable de entorno mediante el parámetro de la línea de comandos `--v2-debug`.

Para obtener información sobre el modo de depuración de actualizaciones de la AWS CLI v1 a v2, consulte Uso del modo de depuración de actualizaciones para actualizar la AWS CLI versión 1 a AWS CLI versión 2.

`AWS_CONFIG_FILE`

Especifica la ubicación del archivo que la AWS CLI utiliza para almacenar perfiles de configuración. La ruta predeterminada es . `~/.aws/config`.

No puede especificar este valor en una configuración de perfil con nombre o mediante un parámetro de la línea de comandos.

`AWS_DATA_PATH`

Una lista de directorios adicionales para comprobar fuera de la ruta de búsqueda integrada de `~/.aws/models` al cargar datos de AWS CLI. La configuración de esta variable de entorno indica los directorios adicionales que hay que comprobar primero antes de recurrir a las rutas de búsqueda integradas. Varias entradas se deben separar con el carácter `os.pathsep` que es `:` en Linux o macOS y `;` en Windows.

`AWS_DEFAULT_OUTPUT`

Especifica el formato de salida que se va a utilizar.

Si se define, esta variable de entorno anula el valor de la configuración del perfil `output`. Puede anular esta variable de entorno mediante el parámetro de la línea de comandos `--output`.

`AWS_DEFAULT_REGION`

`Default region name` identifica la región de AWS a cuyos servidores desea enviar las solicitudes de forma predeterminada. Suele ser la región más cercana a usted, pero puede ser cualquier región. Por ejemplo, puede escribir `us-west-2` para utilizar EE.UU. Oeste (Oregón). Esta es la región a la que se envían todas las solicitudes posteriores, a menos que especifique lo contrario en un comando concreto.

> **Note**
>
> Cuanto utilice la AWS, debe especificar una región de AWS CLI, ya sea de forma explícita o estableciendo una región predeterminada. Para obtener una lista de las regiones disponibles, consulte Regiones y puntos de enlace. Los designadores de región que la AWS CLI utiliza son los mismos nombres que aparecen en las URL y los puntos de enlace de servicio de Consola de administración de AWS.

Si se define, esta variable de entorno anula el valor de la configuración del perfil `region`. Puede invalidar esta variable de entorno mediante el parámetro de la línea de comandos `--region` y la variable de entorno `AWS_REGION` compatible con el AWS SDK.

`AWS_EC2_METADATA_DISABLED`

Desactiva el uso del servicio de metadatos de la instancia de Amazon EC2 (IMDS).

Si se establece en true (verdadero), las credenciales de usuario o la configuración (como la región) no se solicitan desde IMDS.

`AWS_ENDPOINT_URL`

Especifica el punto de conexión que se utiliza para todas las solicitudes de servicio. Para obtener más información, consulte the section called “Establecer un punto de conexión global para todos los Servicios de AWS”.

> **Prioridad de los puntos de conexión**
>
> Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. La AWS CLI comprueba estas configuraciones de punto de conexión en un orden determinado y utiliza la configuración de punto de conexión con la prioridad más alta. Para ver la lista de prioridad de los puntos de conexión, consulte the section called “Prioridad de la configuración y los ajustes del punto de conexión”.

`AWS_ENDPOINT_URL_<SERVICE>`

Especifica un punto de conexión personalizado que se utiliza para un servicio específico, donde `<SERVICE>` se sustituye por el identificador de Servicio de AWS. Por ejemplo, Amazon DynamoDB tiene un `serviceId` de `DynamoDB`. Para este servicio, la variable de entorno de la URL del punto de conexión es `AWS_ENDPOINT_URL_DYNAMODB`.

Para obtener una lista de todas las variables de entorno específicas del servicio, consulte Lista de identificadores específicos del servicio.

> **Prioridad de los puntos de conexión**
>
> Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. La AWS CLI comprueba estas configuraciones de punto de conexión en un orden determinado y utiliza la configuración de punto de conexión con la prioridad más alta. Para ver la lista de prioridad de los puntos de conexión, consulte the section called "Prioridad de la configuración y los ajustes del punto de conexión".

`AWS_IGNORE_CONFIGURED_ENDPOINT_URLS`

Si está habilitada, AWS CLI ignora todas las configuraciones de punto de conexión personalizadas. Los valores válidos son **`true`** y **`false`**. Para obtener más información, consulte the section called "Establecer un punto de conexión global para todos los Servicios de AWS".

Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. Para conocer la prioridad de los puntos de conexión, consulte the section called "Prioridad de la configuración y los ajustes del punto de conexión".

> **Prioridad de los puntos de conexión**
>
> Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. La AWS CLI comprueba estas configuraciones de punto de conexión en un orden determinado y utiliza la configuración de punto de conexión con la prioridad más alta. Para ver la lista de prioridad de los puntos de conexión, consulte the section called "Prioridad de la configuración y los ajustes del punto de conexión".

`AWS_MAX_ATTEMPTS`

Especifica un valor de los intentos de reintento máximos que utiliza el controlador de reintentos de AWS CLI, donde la llamada inicial cuenta para el valor que proporciona. Para obtener más información acerca de los reintentos, consulte Reintentos de AWS CLI en la AWS CLI.

Si se define, esta variable de entorno anula el valor de la configuración de los perfiles `max_attempts`.

`AWS_METADATA_SERVICE_NUM_ATTEMPTS`

Al intentar recuperar las credenciales en una instancia de Amazon EC2 que se haya configurado con un rol de IAM, AWS CLI intenta recuperar las credenciales una vez del servicio de metadatos de la instancia antes de detenerse. Si sabe que los comandos se ejecutarán en una instancia de Amazon EC2, puede aumentar este valor para que AWS CLI realice varios intentos antes de desistir.

`AWS_METADATA_SERVICE_TIMEOUT`

El número de segundos antes de que una conexión al servicio de metadatos de la instancia agote el tiempo de espera. Al intentar recuperar las credenciales en una instancia de Amazon EC2 que se ha configurado con un rol de IAM, una conexión al servicio de metadatos de instancia agotará el tiempo de espera después de 1 segundo de forma predeterminada. Si sabe que está ejecutando en una instancia de Amazon EC2 con un rol de IAM configurado, puede aumentar este valor si es necesario.

`AWS_PAGER`

Especifica el programa de paginación utilizado para la salida. De forma predeterminada, la versión 2 de AWS CLI devuelve todas las salidas a través del paginador predeterminado de su sistema operativo.

Para deshabilitar todo el uso de un programa de paginación externo, establezca la variable en una cadena vacía.

Si se define, esta variable de entorno anula el valor de la configuración del perfil `cli_pager`.

`AWS_PROFILE`

Especifica el nombre del perfil de la AWS CLI con las credenciales y las opciones que se van a utilizar. Puede ser el nombre de un perfil almacenado en un archivo `credentials` o `config`, o el valor `default` para utilizar el perfil predeterminado.

Si se define, esta variable de entorno anula el comportamiento de utilizar el perfil llamado `[default]` en el archivo de configuración. Puede anular esta variable de entorno mediante el parámetro de la línea de comandos `--profile`.

AWS_REGION

La variable de entorno compatible con el SDK de AWS que especifica la región de AWS a la que se va a enviar la solicitud.

Si se define, esta variable de entorno invalida los valores de la variable de entorno `AWS_DEFAULT_REGION` y la configuración del perfil de `region`. Puede anular esta variable de entorno mediante el parámetro de la línea de comandos `--region`.

AWS_REQUEST_CHECKSUM_CALCULATION

Especifica cuándo se calcula una suma de comprobación para las cargas útiles de solicitud y tiene las siguientes opciones:

- `when_supported`: (predeterminado) la suma de comprobación de la carga útil de la solicitud se calcula cuando una operación especifica un algoritmo de suma de comprobación en su modelo de servicio o requiere sumas de comprobación de la solicitud.
- `when_required`: la suma de comprobación de la carga útil de la solicitud se calcula cuando una operación requiere sumas de control de la solicitud o cuando un usuario proporciona un `requestAlgorithmMember` que está modelado por el Servicio de AWS.

Si se define, esta variable de entorno anula el valor de la configuración de los perfiles `request_checksum_calculation`.

AWS_RESPONSE_CHECKSUM_VALIDATION

Especifica cuándo se realiza una validación de suma de comprobación para las cargas útiles de respuesta y tiene las siguientes opciones:

- `when_supported`: (predeterminado) la validación de la suma de comprobación de la carga útil de respuesta se realiza cuando una operación especifica un algoritmo de respuesta en su modelo de servicio que admite AWS CLI.
- `when_required`: la validación de la suma de comprobación de la carga útil de respuesta se realiza cuando una operación especifica un algoritmo de respuesta en su modelo de servicio que admite la AWS CLI, y establece el `requestValidationModeMember` modelado en `ENABLED` en la entrada de la operación.

Si se define, esta variable de entorno anula el valor de la configuración de los perfiles `response_checksum_validation`.

AWS_RETRY_MODE

Especifica qué modo de reintento utiliza AWS CLI. Hay tres modos de reintento disponibles: heredado (predeterminado), estándar y adaptativo. Para obtener más información acerca de los reintentos, consulte Reintentos de AWS CLI en la AWS CLI.

Si se define, esta variable de entorno anula el valor de la configuración de los perfiles `retry_mode`.

AWS_ROLE_ARN

Especifica el nombre de recurso de Amazon (ARN) de un rol de IAM con un proveedor de identidades web que desea utilizar para ejecutar los comandos de AWS CLI.

Se utiliza con las variables de entorno `AWS_WEB_IDENTITY_TOKEN_FILE` y `AWS_ROLE_SESSION_NAME`.

Si se define, esta variable de entorno anula el valor de la configuración del perfil `role_arn`. No se puede especificar un nombre de sesión de rol como parámetro de línea de comandos.

> **Note**
>
> Esta variable de entorno solo se aplica a un rol asumido con proveedor de identidad web y no se aplican a la configuración general del proveedor de roles asumidos.

Para obtener más información sobre el uso de identidades web, consulte the section called "Adopción de un rol con una identidad web".

AWS_ROLE_SESSION_NAME

Especifica el nombre que se va a asociar a la sesión de rol. Este valor se proporciona al parámetro `RoleSessionName` cuando la AWS CLI llama a la operación `AssumeRole` y pasa a formar parte del ARN del usuario del rol asumido: `arn:aws:sts::123456789012:assumed-role/role_name/role_session_name`. Se trata de un parámetro opcional. Si no proporciona este valor, se genera automáticamente un nombre de sesión. Este nombre aparece en los registros de AWS CloudTrail correspondientes a las entradas asociadas a esta sesión.

Si se define, esta variable de entorno anula el valor de la configuración del perfil `role_session_name`.

Se utiliza con las variables de entorno `AWS_ROLE_ARN` y `AWS_WEB_IDENTITY_TOKEN_FILE`.

Para obtener más información sobre el uso de identidades web, consulte the section called "Adopción de un rol con una identidad web".

> **Note**
>
> Esta variable de entorno solo se aplica a un rol asumido con proveedor de identidad web y no se aplican a la configuración general del proveedor de roles asumidos.

`AWS_SDK_UA_APP_ID`

Varias aplicaciones de los clientes pueden utilizar una sola Cuenta de AWS para realizar llamadas a los Servicios de AWS. El ID de aplicación identifica qué aplicación de origen ha realizado un conjunto de llamadas mediante un Servicio de AWS. AWS Los SDK y los servicios solo utilizan e interpretan este valor para mostrarlo de nuevo en las comunicaciones con los clientes. Por ejemplo, este valor se puede incluir en los correos electrónicos operativos para identificar de forma exclusiva qué aplicaciones están asociadas a la notificación.

De manera predeterminada, no hay ningún valor.

El ID de la aplicación es una cadena con una longitud máxima de 50 caracteres. Los valores permitidos incluyen letras, números y los siguientes caracteres especiales:

```
! $ % & * + - . , ^ _ ` | ~
```

Si se define, esta variable de entorno anula el valor de la configuración del perfil `sdk_ua_app_id`. No se puede especificar el ID de aplicación como una opción de línea de comandos.

`AWS_SECRET_ACCESS_KEY`

Especifica la clave secreta asociada a la clave de acceso. Se trata básicamente de la contraseña de la clave de acceso.

Si se define, esta variable de entorno anula el valor de la configuración del perfil `aws_secret_access_key`. No se puede especificar la ID de clave de acceso secreta como una opción de línea de comandos.

`AWS_SESSION_TOKEN`

Especifica el valor del token de sesión que se requiere si utiliza credenciales de seguridad temporales que ha recuperado directamente de las operaciones de AWS STS. Para obtener

más información, consulte la sección Output del comando de rol asumido en la Referencia de comando de AWS CLI.

Si se define, esta variable de entorno anula el valor de la configuración del perfil `aws_session_token`.

`AWS_SHARED_CREDENTIALS_FILE`

Especifica la ubicación del archivo que la AWS CLI utiliza para almacenar claves de acceso. La ruta predeterminada es . `~/.aws/credentials`.

No puede especificar este valor en una configuración de perfil con nombre o mediante un parámetro de la línea de comandos.

`AWS_SIGV4A_SIGNING_REGION_SET`

Especifica las regiones que se van a utilizar al firmar con SigV4a mediante una lista delimitada por comas. Si esta variable no está establecida, la AWS CLI utiliza la variable predeterminada utilizada por Servicio de AWS. Si el Servicio de AWS no tiene un valor predeterminado, la firma de la solicitud pasa a ser válida en todas las regiones con un valor de `*`.

Para obtener más información sobre SigV4a, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM

Si se define, esta variable de entorno anula el valor de la configuración del perfil `sigv4a_signing_region_set`.

`AWS_USE_DUALSTACK_ENDPOINT`

Permite el uso de puntos de conexión de doble pila para enviar solicitudes de AWS. Para obtener más información sobre los puntos de conexión de doble pila, que admiten tráfico de IPv4 e IPv6, consulte Uso de puntos de conexión de doble pila de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service. Los puntos de conexión de doble pila están disponibles para algunos servicios en algunas regiones. Si no existe un punto de conexión de doble pila para el servicio o Región de AWS, la solicitud produce un error. Esta opción está deshabilitada de forma predeterminada. Para obtener más información, consulte the section called “Establecer para utilizar los puntos de conexión de doble pila para todos los Servicios de AWS”.

> **Prioridad de los puntos de conexión**
>
> Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de

AWS locales o declarados explícitamente en la línea de comandos como un parámetro. La AWS CLI comprueba estas configuraciones de punto de conexión en un orden determinado y utiliza la configuración de punto de conexión con la prioridad más alta. Para ver la lista de prioridad de los puntos de conexión, consulte the section called "Prioridad de la configuración y los ajustes del punto de conexión".

`AWS_USE_FIPS_ENDPOINT`

Algunos servicios de AWS ofrecen puntos de conexión compatibles que admiten el Estándar de procesamiento de la información federal (FIPS) 140-2 en algunas Regiones de AWS. Cuando el servicio de AWS es compatible con FIPS, esta configuración establece qué punto de conexión FIPS debe utilizar la AWS CLI. A diferencia de los puntos de conexión de AWS estándar, los puntos de conexión FIPS utilizan una biblioteca de software TLS que cumple con FIPS 140-2. Las empresas que trabajan con el gobierno de los Estados Unidos pueden requerir estos puntos de conexión. Para obtener más información, consulte the section called "Establecer para usar los puntos de conexión de FIPS para todos los Servicios de AWS".

Si esta configuración está habilitada pero no existe un punto de conexión FIPS para el servicio en la Región de AWS, es posible que el comando AWS produzca un error. En este caso, especifique manualmente el punto de conexión que se va a utilizar en el comando mediante la opción `--endpoint-url` o utilice los puntos de conexión específicos del servicio.

> **Prioridad de los puntos de conexión**
>
> Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. La AWS CLI comprueba estas configuraciones de punto de conexión en un orden determinado y utiliza la configuración de punto de conexión con la prioridad más alta. Para ver la lista de prioridad de los puntos de conexión, consulte the section called "Prioridad de la configuración y los ajustes del punto de conexión".

`AWS_WEB_IDENTITY_TOKEN_FILE`

Especifica la ruta de un archivo que contiene un token de acceso de OAuth 2.0 o un token de ID de OpenID Connect proporcionado por un proveedor de identidades. La AWS CLI carga

el contenido de este archivo y lo pasa como argumento `WebIdentityToken` a la operación `AssumeRoleWithWebIdentity`.

Se utiliza con las variables de entorno `AWS_ROLE_ARN` y `AWS_ROLE_SESSION_NAME`.

Si se define, esta variable de entorno anula el valor de la configuración del perfil `web_identity_token_file`.

Para obtener más información sobre el uso de identidades web, consulte the section called "Adopción de un rol con una identidad web".

> **Note**
>
> Esta variable de entorno solo se aplica a un rol asumido con proveedor de identidad web y no se aplican a la configuración general del proveedor de roles asumidos.

Opciones de línea de comandos en la AWS CLI

En AWS CLI, las opciones de línea de comandos son parámetros globales que puede utilizar para invalidar los ajustes de configuración predeterminados, cualquier configuración de perfil correspondiente o la configuración de variable de entorno de ese comando concreto. No se pueden utilizar las opciones de línea de comandos para especificar credenciales directamente, aunque es posible especificar qué perfil se debe utilizar.

Temas

- Cómo utilizar las opciones de la línea de comandos
- AWS CLIOpciones de la línea de comandos globales compatibles con
- Usos comunes de las opciones de la línea de comandos

Cómo utilizar las opciones de la línea de comandos

La mayoría de las opciones de la línea de comandos son cadenas simples, como el nombre del perfil `profile1` en el siguiente ejemplo:

```
$ aws s3 ls --profile profile1
amzn-s3-demo-bucket1
amzn-s3-demo-bucket2
```

```
...
```

Cada opción toma un argumento que requiere un espacio o un signo igual (=) que separa el argumento del nombre de la opción. Si el valor del argumento es una cadena que contiene un espacio, debe utilizar comillas en torno al argumento. Para obtener más información sobre los tipos de argumentos y el formato de los parámetros, consulte Especificación de valores de parámetros en la AWS CLI.

AWS CLIOpciones de la línea de comandos globales compatibles con

En la AWS CLI puede utilizar las siguientes opciones de línea de comandos para anular los ajustes de configuración predeterminados, cualquier configuración de perfil correspondiente o la variable de entorno de ese comando concreto.

--ca-bundle ***<string>***

Especifica el paquete de certificados de la entidad emisora de certificados (CA) que se va a utilizar para verificar los certificados SSL.

Si se define, esta opción anula el valor de la configuración del perfil `ca_bundle` y la variable del entorno de `AWS_CA_BUNDLE`.

--cli-auto-prompt

Habilita el modo de solicitud automática para un solo comando. Como muestran los siguientes ejemplos, se puede especificar en cualquier momento.

```
$ aws --cli-auto-prompt
$ aws dynamodb --cli-auto-prompt
$ aws dynamodb describe-table --cli-auto-prompt
```

Esta opción anula la variable de entorno de `aws_cli_auto_prompt` y la configuración del perfil `cli_auto_prompt`.

Para obtener información sobre la característica de solicitud automática de la versión 2 de AWS CLI, consulte Activación y uso de los símbolos del sistema en la AWS CLI.

--cli-binary-format

Especifica cómo la versión 2 de AWS CLI interpreta los parámetros de entrada binarios. Puede ser uno de los siguientes valores:

- base64: este es el valor predeterminado. Un parámetro de entrada escrito como un objeto binario grande (BLOB) acepta una cadena codificada en base64. Para pasar verdadero contenido binario, coloque el contenido en un archivo y proporcione la ruta y el nombre del archivo con el prefijo `fileb://` como valor del parámetro. Para pasar el texto codificado en base64 incluido en un archivo, proporcione la ruta y el nombre del archivo con el prefijo `file://` como valor del parámetro.
- raw-in-base64-out: valor predeterminado para la AWS CLI versión 1. Si el valor de la configuración es `raw-in-base64-out`, los archivos a los que se hace referencia mediante el prefijo `file://` se leen como texto y, a continuación, la AWS CLI intenta codificarlo en binario.

Esto anula la opción de configuración de archivo `cli_binary_format`.

```
$ aws lambda invoke \
    --cli-binary-format raw-in-base64-out \
    --function-name my-function \
    --invocation-type Event \
    --payload '{ "name": "Bob" }' \
    response.json
```

Si hace referencia a un valor binario en un archivo mediante la notación del prefijo `fileb://`, la AWS CLI siempre espera que el archivo incluya contenido binario sin codificar y no intenta convertir el valor.

Si hace referencia a un valor binario en un archivo mediante la notación del prefijo `file://`, la AWS CLI tratará el archivo de acuerdo con el valor de `cli_binary_format` actual. Si el valor de esa configuración es `base64` (el valor predeterminado cuando no se establece explícitamente), la AWS CLI espera que el archivo contenga texto codificado en base64. Si el valor de esa configuración es `raw-in-base64-out`, la AWS CLI espera que el archivo incluya contenido binario sin codificar.

--cli-connect-timeout ***<número entero>***

Especifica el máximo tiempo de conexión del conector en segundos. Si el valor se establece en cero (0), la conexión del socket espera de forma indefinida (bloqueo) y no se agota el tiempo de espera. El valor de predeterminado es de 60 segundos.

--cli-read-timeout ***<número entero>***

Especifica el máximo tiempo de lectura del conector en segundos. Si el valor se establece en cero (0), la lectura del socket espera de forma indefinida (bloqueo) y no se agota el tiempo de espera. El valor de predeterminado es de 60 segundos.

--color *<cadena>*

Especifica la compatibilidad con el color de salida. Los valores válidos son on, `off` y `auto`. El valor predeterminado es `auto`.

--debug

Modificador booleano que permite registrar la depuración. De manera predeterminada, la AWS CLI proporciona información limpia con respecto a los éxitos o errores en relación con los resultados de los comandos en la salida del comando. La `--debug` proporciona los registros completos de Python. Esto incluye información de diagnóstico adicional de `stderr` sobre la operación del comando que puede ser útil para resolver problemas si un comando proporciona resultados inesperados. Para ver fácilmente los registros de depuración, sugerimos enviar los registros a un archivo para buscar la información más fácilmente. Puede hacer esto utilizando de los siguientes métodos.

Para enviar solo la información de diagnóstico de `stderr`, agregue `2> debug.txt` donde `debug.txt` es el nombre que desea usar para su archivo de depuración:

```
$ aws servicename commandname options --debug 2> debug.txt
```

Para enviar ambos la salida y la información de diagnóstico de `stderr`, agregue `&> debug.txt` donde `debug.txt` es el nombre que desea usar para su archivo de depuración:

```
$ aws servicename commandname options --debug &> debug.txt
```

--endpoint-url *<cadena>*

Especifica la URL a la que se va a enviar la solicitud. En la mayoría de comandos, la AWS CLI determina automáticamente la URL en función del servicio seleccionado y la región de AWS especificada. Sin embargo, algunos comandos requieren que especifique una dirección URL específica de la cuenta. También puede configurar algunos servicios de AWS para alojar un punto de enlace directamente dentro de la VPC privada, que entonces debería especificarse.

El siguiente ejemplo de comando usa una URL de punto de conexión de Amazon S3 personalizada.

```
$ aws s3 ls --endpoint-url http://localhost:4567
```

> **Prioridad de los puntos de conexión**
>
> Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. La AWS CLI comprueba estas configuraciones de punto de conexión en un orden determinado y utiliza la configuración de punto de conexión con la prioridad más alta. Para ver la lista de prioridad de los puntos de conexión, consulte the section called "Prioridad de la configuración y los ajustes del punto de conexión".

--no-cli-auto-prompt

Deshabilita el modo de solicitud automática para un solo comando.

```
$ aws dynamodb describe-table --table-name Table1 --no-cli-auto-prompt
```

Esta opción anula la variable de entorno de `aws_cli_auto_prompt` y la configuración del perfil `cli_auto_prompt`.

Para obtener información sobre la característica de solicitud automática de la versión 2 de AWS CLI, consulte Activación y uso de los símbolos del sistema en la AWS CLI.

—no-cli-pager

Modificador booleano que desactiva el uso de un buscapersonas para la salida del comando.

--no-paginate

Un conmutador booleano que desactiva las llamadas múltiples que AWS CLIrealiza en forma automática para recibir todos los resultados de comandos que crean la paginación de la salida. Esto significa que solo se muestra la primera página de su salida.

--no-sign-request

Modificador booleano que deshabilita la firma de las solicitudes HTTP para el punto de enlace de servicio de AWS. Impide que se carguen las credenciales.

--no-verify-ssl

De forma predeterminada, la AWS CLI utiliza SSL cuando se comunica con los servicios de AWS. Para cada conexión y llamada SSL, la AWS CLI verifica los certificados SSL. El uso de esta opción invalida el comportamiento predeterminado de la verificación de los certificados SSL.

> **Warning**
>
> Esta opción no es una práctica recomendada. Si usa `--no-verify-ssl`, el tráfico entre el cliente y los servicios de AWS ya no está protegido. Esto significa que el tráfico representa un riesgo para la seguridad y es vulnerable a los ataques de intermediarios. Si tiene problemas con los certificados, es mejor que los resuelva. Para conocer los pasos para solucionar problemas de certificados, consulte the section called "Errores de certificado SSL".

--output *<cadena>*

Especifica el formato de salida que se va a utilizar con este comando. Puede especificar cualquiera de los siguientes valores:

- **`json`**: la salida se formatea como una cadena JSON.
- **`yaml`**: la salida se formatea como una cadena YAML.
- **`yaml-stream`**: la salida se transmite y se formatea como una cadena YAML. La transmisión permite gestionar tipos de datos de gran tamaño de forma más rápida.
- **`text`** – la salida tiene el formato de varias líneas de valores de cadena separados por tabuladores. Esto puede ser útil para pasar la salida a un procesador de texto, como `grep`, `sed` o `awk`.
- **`table`** – el resultado tiene el formato de una tabla en la que se usan los caracteres +|- para los bordes de celda. Normalmente, la información se presenta en un formato que es más fácil de leer que los demás formatos, pero que no es útil para programar.

--profile *<cadena>*

Especifica el perfil con nombre que se va a utilizar con este comando. Para configurar perfiles con nombre adicionales, puede utilizar el comando `aws configure` con la opción `--profile`.

```
$ aws configure --profile <profilename>
```

--query *<cadena>*

Especifica una consulta de JMESPath que se usa para filtrar los datos de la respuesta. Para obtener más información, consulte Filtrado de la salida en la AWS CLI.

--region *<cadena>*

Especifica a qué región de AWS se va a enviar la solicitud de AWS de este comando. Para obtener una lista de todas las regiones que se pueden especificar, consulte Regiones y puntos de enlace de AWS en la Referencia general de Amazon Web Services.

--v2-debug

Habilita el modo de depuración de actualizaciones de v1 a v2. Cuando está en este modo, la AWS CLI detectará el uso de características que se actualizaron con cambios importantes en AWS CLI v2 y mostrará advertencias por cada uso detectado que pueda verse afectado. Puede utilizar este modo para preparar el entorno y el uso de AWS CLI para la actualización a v2.

Esta opción invalida la variable de entorno `AWS_CLI_UPGRADE_DEBUG_MODE`.

Para obtener información sobre el modo de depuración de actualizaciones de la AWS CLI v1 a v2, consulte Uso del modo de depuración de actualizaciones para actualizar la AWS CLI versión 1 a AWS CLI versión 2.

--version

Modificador booleano que muestra la versión actual del programa de la AWS CLI que se está ejecutando.

Usos comunes de las opciones de la línea de comandos

Entre los usos habituales de las opciones de la línea de comandos se incluyen la comprobación de sus recursos en varias regiones de AWS y el cambio del formato de salida para obtener una mayor legibilidad o facilidad de uso al generar scripts. En los siguientes ejemplos, ejecutamos el comando describe-instances en cada región hasta que encontremos en qué región se encuentra la instancia.

```
$ aws ec2 describe-instances --output table --region us-west-1
------------------
|DescribeInstances|
+-----------------+
$ aws ec2 describe-instances --output table --region us-west-2
-------------------------------------------------------------------------------
|                            DescribeInstances                                |
+-----------------------------------------------------------------------------+
||                              Reservations                                 ||
|+-----------------------------------+-----------------------------------+|
```

```
||  OwnerId                          |  012345678901                        ||
||  ReservationId                    |  r-abcdefgh                          ||
|+-----------------------------------+--------------------------------------+|
|||                              Instances                                  |||
||+-------------------------+-----------------------------------------------+||
|||  AmiLaunchIndex         |  0                                            |||
|||  Architecture           |  x86_64                                       |||
...
```

Configuración de la finalización de comandos en la AWS CLI

El AWS Command Line Interface (AWS CLI) incluye una característica de finalización de comandos compatibles con bash que le permite utilizar la tecla Tab (Tabulador) para completar un comando introducido parcialmente. En la mayoría de los sistemas, debe configurarlo manualmente.

Para obtener información sobre la característica de petición automática de la versión 2 de AWS CLI, consulte Activación y uso de los símbolos del sistema en la AWS CLI.

Temas

- Funcionamiento
- Configuración de la finalización de comandos en Linux o macOS
- Configuración de la finalización de comandos en Windows

Funcionamiento

Cuando se introduce parcialmente un comando, parámetro u opción, la función de finalización de comandos completa automáticamente el comando o muestra una lista sugerida de comandos. Para solicitar que se complete el comando, ingrese parcialmente un comando y pulse la tecla de finalización, que normalmente es *Tab* (Tabulador) en la mayoría de los shells.

En los ejemplos siguientes se muestran diferentes formas de utilizar la finalización de comandos:

- Introduzca parcialmente un comando y pulse *Tab (Tabulador)* para mostrar una lista sugerida de comandos.

```
$ aws dynamodb dTAB
delete-backup                       describe-global-table
delete-item                         describe-global-table-settings
```

```
delete-table                        describe-limits
describe-backup                     describe-table
describe-continuous-backups         describe-table-replica-auto-scaling
describe-contributor-insights       describe-time-to-live
describe-endpoints
```

- Introduzca parcialmente un parámetro y pulse *Tab (Tabulador)* para mostrar una lista sugerida de parámetros.

```
$ aws dynamodb delete-table --TAB
--ca-bundle              --endpoint-url           --profile
--cli-connect-timeout    --generate-cli-skeleton  --query
--cli-input-json         --no-paginate            --region
--cli-read-timeout       --no-sign-request        --table-name
--color                  --no-verify-ssl          --version
--debug                  --output
```

- Introduzca un parámetro y pulse *Tab (Tabulador)* para mostrar una lista sugerida de valores de recursos. Esta función solo está disponible en la versión 2 de la AWS CLI.

```
$ aws dynamodb delete-table --table-name TAB
Table 1                  Table 2                  Table 3
```

Configuración de la finalización de comandos en Linux o macOS

Para configurar la finalización de comandos en Linux o macOS, debe conocer el nombre del shell que se está utilizando y la ubicación del script `aws_completer`.

> **Note**
>
> La finalización de comandos se configura y habilita automáticamente de forma predeterminada en las instancias de Amazon EC2 que ejecutan Amazon Linux.

Temas

- Confirme que la carpeta del Completer está en su ruta
- Habilitar la finalización de comandos
- Verifique la finalización de comandos

Confirme que la carpeta del Completer está en su ruta

Para que el Completer de AWS funcione con éxito, `aws_completer` debe estar en a ruta de su shell. El comando `which` puede verificar si el Completer está en su ruta.

```
$ which aws_completer
/usr/local/bin/aws_completer
```

Si el comando qué no puede encontrar el completador, siga los pasos siguientes para agregar la carpeta del completer a su ruta.

Paso 1: Ubique el Completer de AWS

La ubicación del Completer de AWS puede variar en función del método de instalación utilizado.

- Administrador de paquetes: los programas como `pip`, `yum`, `brew` y `apt-get` suelen instalar el Completer de AWS (o un symlink al mismo) en una ubicación de ruta estándar.
  - Si utilizó `pip` sin el parámetro `--user`, la ruta predeterminada es `/usr/local/bin/aws_completer`.
  - Si utilizó `pip` con el parámetro `--user`, la ruta predeterminada es /home/*username*/`.local/bin/aws_completer`.
- Instalador agrupado: si utilizó el instalador agrupado, la ruta predeterminada es `/usr/local/bin/aws_completer`.

Si no funciona ninguna de las opciones anteriores, puede utilizar el comando `find` para buscar su sistema de archivos para el completer de AWS.

```
$ find / -name aws_completer
/usr/local/bin/aws_completer
```

Paso 2: Identificación de su shell

Para identificar qué shell está utilizando, puede usar uno de los siguientes comandos.

- echo $SHELL: muestra el nombre de archivo de programa del shell. Normalmente coincide con el nombre del shell en uso, a menos que haya iniciado otro shell tras iniciar sesión.

  ```
  $ echo $SHELL
  ```

```
/bin/bash
```

- ps: muestra los procesos en ejecución para el usuario actual. Uno de ellos es el shell.

```
$ ps
  PID TTY          TIME CMD
 2148 pts/1    00:00:00 bash
 8756 pts/1    00:00:00 ps
```

Paso 3: agregar la carpeta del completer a la ruta

1. Busque el script de perfil de su shell en su carpeta de usuario.

```
$ ls -a ~/
.  ..  .bash_logout  .bash_profile  .bashrc  Desktop  Documents  Downloads
```

   - Bash: `.bash_profile`, `.profile` o `.bash_login`
   - Zsh: `.zshrc`
   - Tcsh: `.tcshrc`, `.cshrc` o `.login`

2. Añada un comando de exportación al final del script de su perfil igual que en el siguiente ejemplo. Reemplace *`/usr/local/bin/`* por el nombre de la carpeta que ha creado en la sección anterior.

```
export PATH=/usr/local/bin/:$PATH
```

3. Vuelva a cargar el perfil en la sesión actual para que esos cambios surtan efecto. Reemplace *`.bash_profile`* por el nombre del script de shell que ha creado en la primera sección.

```
$ source ~/.bash_profile
```

Habilitar la finalización de comandos

Después de confirmar que el completer está en su ruta, habilite la finalización de comandos ejecutando el comando apropiado para el shell que está utilizando. Puede agregar el comando a su perfil del shell para que se ejecute cada vez que abra un nuevo shell. En cada comando, reemplace la ruta *`/usr/local/bin/`* por la de su sistema en Confirme que la carpeta del Completer está en su ruta.

- **bash**: use el comando `complete` integrado.

```
$ complete -C '/usr/local/bin/aws_completer' aws
```

  Agregue el comando anterior a `~/.bashrc` para que se ejecute cada vez que abra un nuevo shell. Su `~/.bash_profile` debe obtener `~/.bashrc` para asegurarse de que el comando también se ejecuta en los shells de inicio de sesión.

- **zsh**: ejecutar la finalización de comandos, debe ejecutar `bashcompinit` añadiendo la siguiente línea de carga automática al final del script de perfil de `~/.zshrc`.

```
$ autoload bashcompinit && bashcompinit
$ autoload -Uz compinit && compinit
```

  Para habilitar la finalización de comandos, utilice el comando integrado `complete`.

```
$ complete -C '/usr/local/bin/aws_completer' aws
```

  Agregue el comando anterior a `~/.zshrc` para que se ejecute cada vez que abra un nuevo shell.

- **tcsh**: la finalización de `tcsh` requiere un tipo de palabra y un patrón para definir el comportamiento de finalización.

```
> complete aws 'p/*/`aws_completer`/'
```

  Agregue el comando anterior a `~/.tcshrc` para que se ejecute cada vez que abra un nuevo shell.

Después de habilitar la finalización del comando, Verifique la finalización de comandos funciona.

Verifique la finalización de comandos

Tras habilitar la finalización de comandos, vuelva a cargar su shell, escriba parcialmente un comando y pulse la tecla Tab (Tabulación) para ver los comandos disponibles.

```
$ aws sTAB
s3              ses             sqs             sts             swf
s3api           sns             storagegateway  support
```

Configuración de la finalización de comandos en Windows

> **Note**
>
> Para obtener información sobre cómo PowerShell gestiona la finalización, incluidas las diversas claves de finalización, consulte about_Tab_Expansion en Documentos de Microsoft PowerShell.

Para habilitar la finalización de comandos para PowerShell en Windows, siga los pasos siguientes en PowerShell.

1. Abra el archivo `$PROFILE` con el siguiente comando.

   ```
   PS C:\> Notepad $PROFILE
   ```

   Si no dispone de un `$PROFILE`, cree un perfil de usuario mediante el siguiente comando.

   ```
   PS C:\> if (!(Test-Path -Path $PROFILE ))
   { New-Item -Type File -Path $PROFILE -Force }
   ```

   Para obtener más información sobre los perfiles de PowerShell, consulte Cómo utilizar perfiles en ISE de Windows PowerShell en el sitio web de Documentos de Microsoft.

2. Para habilitar la finalización de comandos, agregue el siguiente bloque de código a su perfil, guarde y luego cierre el archivo.

   ```
   Register-ArgumentCompleter -Native -CommandName aws -ScriptBlock {
       param($commandName, $wordToComplete, $cursorPosition)
           $env:COMP_LINE=$wordToComplete
           if ($env:COMP_LINE.Length -lt $cursorPosition){
               $env:COMP_LINE=$env:COMP_LINE + " "
           }
           $env:COMP_POINT=$cursorPosition
           aws_completer.exe | ForEach-Object {
               [System.Management.Automation.CompletionResult]::new($_, $_,
    'ParameterValue', $_)
           }
           Remove-Item Env:\COMP_LINE
           Remove-Item Env:\COMP_POINT
   ```

```
}
```

3. Tras habilitar la finalización de comandos, vuelva a cargar el shell, ingrese parcialmente un comando y pulse la tecla Tab (Tabulación) para recorrer los comandos disponibles.

```
$ aws sTab
```

```
$ aws s3
```

Para ver todos los comandos disponibles para completar, ingrese parcialmente un comando y pulse Ctrl (Control) + Space Espacio.

```
$ aws sCtrl + Space
s3              ses             sqs             sts             swf
s3api           sns             storagegateway  support
```

Reintentos de AWS CLI en la AWS CLI

En este tema se describe cómo AWS CLI podría ver las llamadas a servicios de AWS que fallan debido a problemas inesperados. Estos problemas pueden ocurrir en el lado del servidor o puede fallar debido a la limitación de velocidad del servicio de AWS al que está intentando llamar. Este tipo de errores generalmente no requieren un manejo especial y la llamada se realiza de nuevo automáticamente, a menudo después de un breve período de espera. La AWS CLI proporciona muchas características para ayudar a reintentar llamadas de cliente a AWS cuando se experimentan este tipo de errores o excepciones.

Temas

- Modos de reintento disponibles
- Configuración de un modo de reintento
- Visualización de registros de reintentos

Modos de reintento disponibles

La AWS CLI tiene varios modos para elegir según su versión:

- Modo de reintento estándar (predeterminado)

- Modo de reintento heredado
- Modo de reintento flexible

Modo de reintento estándar (predeterminado)

El modo `Standard` es un conjunto estándar de reglas de reintento en los SDK de AWS con más funcionalidad que el modo heredado y es el modo predeterminado para la AWS CLI. El modo estándar se creó para la versión 2 de la AWS CLI y se adaptó para la versión 1 de la AWS CLI. La funcionalidad del modo estándar incluye:

- Un valor predeterminado de 2 para los intentos máximos de reintento, haciendo un total de 3 intentos de llamada. Este valor se puede sobrescribir a través del parámetro de configuración de `max_attempts`.
- Reintentos para la siguiente lista ampliada de errores y excepciones:
  - Errores y excepciones transitorios
    - `RequestTimeout`
    - `RequestTimeoutException`
    - `PriorRequestNotComplete`
    - `ConnectionError`
    - `HTTPClientError`
  - Errores y excepciones de límites y de la limitación controlada del lado del servicio:
    - `Throttling`
    - `ThrottlingException`
    - `ThrottledException`
    - `RequestThrottledException`
    - `TooManyRequestsException`
    - `ProvisionedThroughputExceededException`
    - `TransactionInProgressException`
    - `RequestLimitExceeded`
    - `BandwidthLimitExceeded`
    - `LimitExceededException`
    - `RequestThrottled`

    - `SlowDown`
    - `EC2ThrottledException`

- Reintentos de códigos de error transitorios y no descriptivos. En concreto, estos códigos de estado HTTP: 500, 502, 503, 504.
- Cualquier reintento incluirá un retroceso exponencial por un factor base de 2 para un tiempo máximo de retroceso de 20 segundos.

Modo de reintento heredado

El modo `Legacy` utiliza un controlador de reintentos más antiguo con una funcionalidad limitada que incluye:

- Un valor predeterminado de 4 reintentos máximo, lo que hace un total de 5 intentos de llamada. Este valor se puede sobrescribir a través del parámetro de configuración de `max_attempts`.
- DynamoDB tiene un valor predeterminado de 9 reintentos como máximo, lo que hace un total de 10 intentos de llamada. Este valor se puede sobrescribir a través del parámetro de configuración de `max_attempts`.
- Reintentos para el siguiente limite de errores y excepciones:
    - Errores generales de toma o conexión:
        - `ConnectionError`
        - `ConnectionClosedError`
        - `ReadTimeoutError`
        - `EndpointConnectionError`
    - Errores y excepciones de límites y de la limitación controlada del lado del servicio:
        - `Throttling`
        - `ThrottlingException`
        - `ThrottledException`
        - `RequestThrottledException`
        - `ProvisionedThroughputExceededException`
- Reintentos de varios códigos de estado HTTP, incluidos 429, 500, 502, 503, 504 y 509.
- Cualquier reintento incluirá un retroceso exponencial por un factor base de 2.

Modo de reintento flexible

> **Warning**
>
> El modo flexible es un modo experimental y está sujeto a cambios, tanto en las características como en el comportamiento.

El modo de reintento `Adaptive` es un modo de reintento experimental que incluye todas las características del modo estándar. Además de las características del modo estándar, el modo flexible también presenta la limitación de la velocidad del lado del cliente mediante el uso del algoritmo token bucket y variables de límite de velocidad que se actualizan en forma dinámica con cada reintento. Este modo ofrece flexibilidad en los reintentos del lado del cliente que se adapta a la respuesta de estado del error y la excepción desde un servicio de AWS.

Con cada nuevo reintento, el modo flexible modifica las variables de límite de velocidad en función del error, la excepción o el código de estado HTTP presentado en la respuesta del servicio de AWS. Estas variables de límite de velocidad se utilizan para calcular una nueva tasa de llamada para el cliente. Cada excepción/error o respuesta HTTP no exitosa (proporcionada en la lista anterior) de un servicio de AWS actualiza las variables de límite de velocidad a medida que se producen reintentos hasta que se alcanza el éxito, se agota el token bucket o se alcanza el valor máximo de intentos configurado.

Configuración de un modo de reintento

La AWS CLI incluye una variedad de configuraciones de reintento, así como métodos de configuración que se deben tener en cuenta al crear el objeto cliente.

Métodos de configuración disponibles

En la AWS CLI, los usuarios pueden configurar reintentos de las siguientes maneras:

- Variables de entorno
- Archivo de configuración de la AWS CLI

Los usuarios pueden personalizar las siguientes opciones de reintento:

- Modo de reintento: especifica qué modo de reintento utiliza la AWS CLI. Como se ha comentado anteriormente, hay tres modos de reintento disponibles: heredado, estándar y adaptativo. El valor predeterminado de la AWS CLIla versión 2 de es estándar.
- Cantidad máxima de intentos: especifica el valor máximo de reintentos que utiliza el controlador de reintentos de AWS CLI, donde la llamada inicial cuenta para el valor que usted proporciona. El valor predeterminado se basa en su modo de reintento.

Definición de una configuración de reintento en las variables de entorno

Para definir la configuración de reintento para la AWS CLI, actualice las variables de entorno de su sistema operativo.

Las variables de entorno de reintento son:

- `AWS_RETRY_MODE`
- `AWS_MAX_ATTEMPTS`

Para obtener más información sobre las variables de entorno, consulte Configuración de variables de entorno para la AWS CLI.

Definición de una configuración de reintento en un archivo de configuración de AWS

Para cambiar la configuración de reintento, actualice su archivo de configuración global de la AWS. La ubicación predeterminada del archivo de configuración de la AWS es ~/.aws/config.

El siguiente es un ejemplo de un archivo de configuración de la AWS:

```
[default]
retry_mode = standard
max_attempts = 6
```

Para obtener más información sobre cómo usar archivos de configuración, consulte Opciones de los archivos de configuración y credenciales en la AWS CLI.

Visualización de registros de reintentos

La AWS CLI utiliza la metodología de reintento y el registro de Boto3. Puede utilizar la opción `--debug` en cualquier comando para recibir registros de depuración. Para obtener información sobre cómo utilizar la opción `--debug`, consulte Opciones de línea de comandos en la AWS CLI.

Si busca “reintento” en sus registros de depuración, encontrará la información sobre de reintentos que necesita. Las entradas del registro del cliente correspondientes a los reintentos dependen del modo de reintento habilitado.

Modo heredado:

Los mensajes de reintento se generan mediante botocore.retryhandler. Verá uno de los tres mensajes:

- `No retry needed`
- `Retry needed, action of: <action_name>`
- `Reached the maximum number of retry attempts: <attempt_number>`

Modo estándar o flexible:

Los mensajes de reintento se generan a través de botocore.retries.standard. Verá uno de los tres mensajes:

- `No retrying request`
- `Retry needed, retrying request after delay of: <delay_value>`
- `Retry needed but retry quota reached, not retrying request`

Para obtener el archivo completo de definición de los reintentos de botocore, consulte _retry.json en el Repositorio GitHub de botocore.

Uso de un proxy HTTP para la AWS CLI

Para acceder a AWS a través de servidores proxy, puede configurar las variables de entorno `HTTP_PROXY` y `HTTPS_PROXY` con los nombres de dominio de DNS o con las direcciones IP y los números de puerto que utilizan los servidores proxy.

Temas

- Uso de los ejemplos de la
- Autenticación en un proxy
- Uso de un proxy en instancias Amazon EC2
- Solución de problemas

Uso de los ejemplos de la

> **Note**
>
> En los ejemplos siguientes, se muestra el nombre de la variable de entorno con todas las letras en mayúscula. Sin embargo, si especifica una variable dos veces utilizando mayúsculas y minúsculas diferentes, prevalecen las letras minúsculas. Recomendamos que defina cada variable solo una vez para evitar la confusión de sistema y un comportamiento inesperado.

Los siguientes ejemplos muestran cómo puede utilizar la dirección IP explícita de su proxy o un nombre de DNS que se resuelve en la dirección IP de su proxy. Cualquiera puede ir seguido de dos puntos y el número de puerto al que se deben enviar las consultas.

Linux or macOS

```
$ export HTTP_PROXY=http://10.15.20.25:1234
$ export HTTP_PROXY=http://proxy.example.com:1234
$ export HTTPS_PROXY=http://10.15.20.25:5678
$ export HTTPS_PROXY=http://proxy.example.com:5678
```

Windows Command Prompt

Para configurar todas las sesiones

```
C:\> setx HTTP_PROXY http://10.15.20.25:1234
C:\> setx HTTP_PROXY http://proxy.example.com:1234
C:\> setx HTTPS_PROXY http://10.15.20.25:5678
C:\> setx HTTPS_PROXY http://proxy.example.com:5678
```

El uso de `setx` para establecer una variable de entorno cambia el valor usado en la sesión de símbolo del sistema actual y en todas las sesiones de símbolo del sistema que cree después de ejecutar el comando. La operación no afecta a otros comandos del shell que ya se están ejecutando en el momento de ejecutar el comando.

Para configurar solo para la sesión actual

El uso de `set` para configurar una variable de entorno cambia el valor usado hasta que finalice la sesión de símbolo de sistema actual o hasta que otorgue a la variable un valor diferente.

```
C:\> set HTTP_PROXY=http://10.15.20.25:1234
C:\> set HTTP_PROXY=http://proxy.example.com:1234
C:\> set HTTPS_PROXY=http://10.15.20.25:5678
C:\> set HTTPS_PROXY=http://proxy.example.com:5678
```

Autenticación en un proxy

> **Note**
>
> La AWS CLI no admite servidores proxy NTLM. Si utiliza un proxy del protocolo NTLM o Kerberos, es posible que pueda conectarse a través de un proxy de autenticación como Cntlm.

La AWS CLI admite la autenticación básica de HTTP. Especifique el nombre de usuario y la contraseña en la URL del proxy como se indica a continuación.

Linux or macOS

```
$ export HTTP_PROXY=http://username:password@proxy.example.com:1234
$ export HTTPS_PROXY=http://username:password@proxy.example.com:5678
```

Windows Command Prompt

Para configurar todas las sesiones

```
C:\> setx HTTP_PROXY http://username:password@proxy.example.com:1234
C:\> setx HTTPS_PROXY http://username:password@proxy.example.com:5678
```

Para configurar solo la sesión actual

```
C:\> set HTTP_PROXY=http://username:password@proxy.example.com:1234
C:\> set HTTPS_PROXY=http://username:password@proxy.example.com:5678
```

Uso de un proxy en instancias Amazon EC2

Si configura un proxy en una instancia de Amazon EC2 que se ha lanzado con un rol de IAM asociado, asegúrese de excluir la dirección utilizada para obtener acceso a los metadatos de la

instancia. Para ello, establezca la variable de entorno NO_PROXY en la dirección IP del servicio de metadatos de la instancia, 169.254.169.254. Esta dirección no varía.

Linux or macOS

```
$ export NO_PROXY=169.254.169.254
```

Windows Command Prompt

Para configurar todas las sesiones

```
C:\> setx NO_PROXY 169.254.169.254
```

Para configurar solo la sesión actual

```
C:\> set NO_PROXY=169.254.169.254
```

Solución de problemas

Si encuentra problemas con la AWS CLI, consulte the section called “Errores de solución de problemas” para los pasos de resolución de problemas. Para conocer los pasos más relevantes de la resolución de problemas, consulte the section called “Errores de certificado SSL”.

Uso de puntos de conexión en la AWS CLI

Para conectarse mediante programación a un Servicio de AWS, utilice un punto de conexión. Un punto de conexión es la dirección URL del punto de entrada de un servicio web de AWS. AWS Command Line Interface (AWS CLI) usa automáticamente el punto de conexión predeterminado para cada servicio de una Región de AWS, pero puede especificar un punto de conexión alternativo para las solicitudes de la API.

Temas sobre puntos de conexión

- Establecer punto de conexión para un solo comando
- Establecer un punto de conexión global para todos los Servicios de AWS
- Establecer para usar los puntos de conexión de FIPS para todos los Servicios de AWS
- Establecer para utilizar los puntos de conexión de doble pila para todos los Servicios de AWS

- Establecer puntos de conexión específicos del servicio
  - Puntos de conexión específicos del servicio: variables de entorno
  - Puntos de conexión específicos del servicio: archivo config compartido
  - Puntos de conexión específicos del servicio: lista de identificadores específicos del servicio
- Puntos de conexión basados en cuentas
- Prioridad de la configuración y los ajustes del punto de conexión

Establecer punto de conexión para un solo comando

Para invalidar la configuración del punto de conexión o las variables de entorno de un solo comando, utilice la opción de línea de comandos `--endpoint-url`. El siguiente ejemplo de comando usa una URL de punto de conexión de Amazon S3 personalizada.

```
$ aws s3 ls --endpoint-url http://localhost:4567
```

Establecer un punto de conexión global para todos los Servicios de AWS

Para dirigir las solicitudes de todos los servicios a una URL de punto de conexión personalizada, utilice una de las siguientes configuraciones:

- Variables de entorno:
  - `AWS_IGNORE_CONFIGURED_ENDPOINT_URLS`: Ignore las URL de punto de conexión configuradas.

    Linux or macOS

    ```
    $ export AWS_IGNORE_CONFIGURED_ENDPOINT_URLS=true
    ```

    Windows Command Prompt

    Para configurar todas las sesiones

    ```
    C:\> setx AWS_IGNORE_CONFIGURED_ENDPOINT_URLS true
    ```

    Para configurar solo la sesión actual

    ```
    C:\> set AWS_IGNORE_CONFIGURED_ENDPOINT_URLS=true
    ```

PowerShell

```
PS C:\> $Env:AWS_IGNORE_CONFIGURED_ENDPOINT_URLS="true"
```

- AWS_ENDPOINT_URL: Defina la URL del punto de conexión global.

  Linux or macOS

  ```
  $ export AWS_ENDPOINT_URL=http://localhost:4567
  ```

  Windows Command Prompt

  Para configurar todas las sesiones

  ```
  C:\> setx AWS_ENDPOINT_URL http://localhost:4567
  ```

  Para configurar solo la sesión actual

  ```
  C:\> set AWS_ENDPOINT_URL=http://localhost:4567
  ```

  PowerShell

  ```
  PS C:\> $Env:AWS_ENDPOINT_URL="http://localhost:4567"
  ```

- El archivo `config`:
  - ignore_configure_endpoint_urls: Ignore las URL de punto de conexión configuradas.

    ```
    ignore_configure_endpoint_urls = true
    ```

  - endpoint_url: Defina la URL del punto de conexión global.

    ```
    endpoint_url = http://localhost:4567
    ```

Los puntos de conexión específicos del servicio y la opción de línea de comandos `--endpoint-url` invalidan cualquier punto de conexión global.

Establecer para usar los puntos de conexión de FIPS para todos los Servicios de AWS

Para dirigir las solicitudes de todos los servicios para usar puntos de conexión de FIPS, utilice una de las siguientes opciones:

- AWS_USE_FIPS_ENDPOINT variable de entorno

  Linux or macOS

  ```
  $ export AWS_USE_FIPS_ENDPOINT=true
  ```

  Windows Command Prompt

  Para configurar todas las sesiones

  ```
  C:\> setx AWS_USE_FIPS_ENDPOINT true
  ```

  Para configurar solo la sesión actual

  ```
  C:\> set AWS_USE_FIPS_ENDPOINT=true
  ```

  PowerShell

  ```
  PS C:\> $Env:AWS_USE_FIPS_ENDPOINT="true"
  ```

- Configuración de archivos use_fips_endpoint.

  ```
  use_fips_endpoint = true
  ```

Algunos servicios de AWS ofrecen puntos de conexión compatibles que admiten el Estándar de procesamiento de la información federal (FIPS) 140-2 en algunas Regiones de AWS. Cuando el servicio de AWS es compatible con FIPS, esta configuración establece qué punto de conexión FIPS debe utilizar la AWS CLI. A diferencia de los puntos de conexión de AWS estándar, los puntos de conexión FIPS utilizan una biblioteca de software TLS que cumple con FIPS 140-2. Las empresas que trabajan con el gobierno de los Estados Unidos pueden requerir estos puntos de conexión.

Si esta configuración está habilitada pero no existe un punto de conexión FIPS para el servicio en la Región de AWS, es posible que el comando AWS produzca un error. En este caso, especifique manualmente el punto de conexión que se va a utilizar en el comando mediante la opción `--endpoint-url` o utilice los puntos de conexión específicos del servicio.

Para obtener más información sobre cómo especificar los puntos de conexión de FIPS por Región de AWS, consulte Puntos de conexión de FIPS por servicio.

Establecer para utilizar los puntos de conexión de doble pila para todos los Servicios de AWS

Para dirigir las solicitudes de todos los servicios para usar puntos de conexión de doble pila cuando estén disponibles, utilice una de las siguientes configuraciones:

- `AWS_USE_DUALSTACK_ENDPOINT` variable de entorno

  Linux or macOS

  ```
  $ export AWS_USE_DUALSTACK_ENDPOINT=true
  ```

  Windows Command Prompt

  Para configurar todas las sesiones

  ```
  C:\> setx AWS_USE_DUALSTACK_ENDPOINT true
  ```

  Para configurar solo la sesión actual

  ```
  C:\> set AWS_USE_DUALSTACK_ENDPOINT=true
  ```

  PowerShell

  ```
  PS C:\> $Env:AWS_USE_DUALSTACK_ENDPOINT="true"
  ```

- Configuración de archivos `use_dualstack_endpoint`.

```
use_dualstack_endpoint = true
```

Permite el uso de puntos de conexión de doble pila para enviar solicitudes de AWS. Para obtener más información sobre los puntos de conexión de doble pila, que admiten tráfico de IPv4 e IPv6, consulte Uso de puntos de conexión de doble pila de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service. Los puntos de conexión de doble pila están disponibles para algunos servicios en algunas regiones. Si no existe un punto de conexión de doble pila para el servicio o Región de AWS, la solicitud produce un error. Esta opción está deshabilitada de forma predeterminada.

Establecer puntos de conexión específicos del servicio

La configuración del punto de conexión específico del servicio ofrece la opción de utilizar un punto de conexión persistente de su elección para las solicitudes de la AWS CLI. Estas configuraciones proporcionan flexibilidad para admitir puntos de conexión locales, puntos de conexión de VPC y entornos de desarrollo de AWS locales de terceros. Se pueden usar diferentes puntos de conexión para los entornos de prueba y producción. Puede especificar una URL de punto de conexión para Servicios de AWS individuales.

Los puntos de conexión específicos del servicio se pueden especificar de las siguientes maneras:

- La opción de línea de comandos `--endpoint-url` para un solo comando.
- Variables de entorno:
  - `AWS_IGNORE_CONFIGURED_ENDPOINT_URLS`: Ignore todas las URL de punto de conexión configuradas, a menos que se especifiquen en la línea de comandos.
  - `AWS_ENDPOINT_URL_<SERVICE>`: Especifica un punto de conexión personalizado que se utiliza para un servicio específico, donde `<SERVICE>` se sustituye por el identificador de Servicio de AWS. Para ver todas las variables específicas del servicio, consulte the section called “Lista de identificadores específicos del servicio”.
- Archivo `config`:
  - `ignore_configure_endpoint_urls`: Ignore todas las URL de punto de conexión configuradas, a menos que se especifique el uso de variables de entorno o en la línea de comandos.
  - La sección `services` del archivo `config` combinada con la configuración del archivo `endpoint_url`.

Temas de puntos de conexión específicos del servicio:

- Puntos de conexión específicos del servicio: variables de entorno

- Puntos de conexión específicos del servicio: archivo config compartido
- Puntos de conexión específicos del servicio: lista de identificadores específicos del servicio

Puntos de conexión específicos del servicio: variables de entorno

Las variables de entorno invalidan la configuración del archivo de configuración, pero no invalidan las opciones especificadas en la línea de comandos. Use variables de entorno si quiere que todos los perfiles usen los mismos puntos de conexión en el dispositivo.

A continuación, se muestran variables de entorno específicas del servicio:

- `AWS_IGNORE_CONFIGURED_ENDPOINT_URLS`: Ignore todas las URL de punto de conexión configuradas, a menos que se especifiquen en la línea de comandos.

  Linux or macOS

  ```
  $ export AWS_IGNORE_CONFIGURED_ENDPOINT_URLS=true
  ```

  Windows Command Prompt

  Para configurar todas las sesiones

  ```
  C:\> setx AWS_IGNORE_CONFIGURED_ENDPOINT_URLS true
  ```

  Para configurar solo la sesión actual

  ```
  C:\> set AWS_IGNORE_CONFIGURED_ENDPOINT_URLS=true
  ```

  PowerShell

  ```
  PS C:\> $Env:AWS_IGNORE_CONFIGURED_ENDPOINT_URLS="true"
  ```

- `AWS_ENDPOINT_URL_<SERVICE>`: Especifica un punto de conexión personalizado que se utiliza para un servicio específico, donde `<SERVICE>` se sustituye por el identificador de Servicio de AWS. Para ver todas las variables específicas del servicio, consulte the section called “Lista de identificadores específicos del servicio”.

  Los siguientes ejemplos de variables de entorno establecen un punto de conexión para AWS Elastic Beanstalk:

Linux or macOS

```
$ export AWS_ENDPOINT_URL_ELASTIC_BEANSTALK=http://localhost:4567
```

Windows Command Prompt

Para configurar todas las sesiones

```
C:\> setx AWS_ENDPOINT_URL_ELASTIC_BEANSTALK http://localhost:4567
```

Para configurar solo la sesión actual

```
C:\> set AWS_ENDPOINT_URL_ELASTIC_BEANSTALK=http://localhost:4567
```

PowerShell

```
PS C:\> $Env:AWS_ENDPOINT_URL_ELASTIC_BEANSTALK="http://localhost:4567"
```

Para obtener más información sobre la configuración de las variables de entorno, consulte the section called “Variables de entorno”.

Puntos de conexión específicos del servicio: archivo **`config`** compartido

En el archivo compartido `config`, `endpoint_url` se usa en varias secciones. Para configurar un punto de conexión específico del servicio, use la configuración anidada `endpoint_url` en una clave de identificador de servicio dentro de una sección `services`. Para obtener más información sobre cómo definir una sección de `services` en el archivo compartido `config`, consulte the section called “`services`”.

En el siguiente ejemplo, se utiliza una sección de `services` para configurar una URL de punto de conexión específica del servicio para Amazon S3 y un punto de conexión global personalizado que se utiliza para todos los demás servicios:

```
[profile dev1]
endpoint_url = http://localhost:1234
services = s3-specific

[services testing-s3]
s3 =
```

```
  endpoint_url = http://localhost:4567
```

Un único perfil puede configurar puntos de conexión para varios servicios. El siguiente ejemplo establece las URL de punto de conexión específicas del servicio para Amazon S3 y AWS Elastic Beanstalk en el mismo perfil.

Para obtener una lista de todas las claves de identificación de servicio que se van a utilizar en la sección de `services`, consulte Lista de identificadores específicos del servicio.

```
[profile dev1]
services = testing-s3-and-eb

[services testing-s3-and-eb]
s3 =
  endpoint_url = http://localhost:4567
elastic_beanstalk =
  endpoint_url = http://localhost:8000
```

La sección de configuración de servicios se puede utilizar en varios perfiles. En el siguiente ejemplo, dos perfiles utilizan la misma definición de `services`:

```
[profile dev1]
output = json
services = testing-s3

[profile dev2]
output = text
services = testing-s3

[services testing-s3]
s3 =
  endpoint_url = https://localhost:4567
```

Puntos de conexión específicos del servicio: lista de identificadores específicos del servicio

El identificador de Servicio de AWS se basa en `serviceId` del modelo de la API, sustituyendo todos los espacios por guiones bajos y poniendo en minúsculas todas las letras.

La siguiente tabla muestra todos los identificadores específicos del servicio, las claves de archivo `config` y las variables de entorno.

Puntos de conexión basados en cuentas

Los puntos de conexión basados en cuentas se pueden especificar de las siguientes maneras:

- Variables de entorno
  - AWS_ACCOUNT_ID: especifica el ID del punto de conexión basado en la cuenta de AWS que se utilizará para las llamadas a los Servicios de AWS compatibles.

    Linux or macOS

    ```
    $ export AWS_ACCOUNT_ID=<account-id>
    ```

    Windows Command Prompt

    Para configurar todas las sesiones

    ```
    C:\> setx AWS_ACCOUNT_ID <account-id>
    ```

    Para configurar solo la sesión actual

    ```
    C:\> set AWS_ACCOUNT_ID=<account-id>
    ```

    PowerShell

    ```
    PS C:\> $Env:AWS_ACCOUNT_ID="<account-id>"
    ```

  - AWS_ACCOUNT_ID_ENDPOINT_MODE: especifica si se deben utilizar los ID de punto de conexión basados en cuentas de AWS para las llamadas a los Servicios de AWS compatibles. Se puede establecer en `preferred`, `disabled` o `required`. El valor predeterminado es `preferred`.

    Linux or macOS

    ```
    $ export AWS_ACCOUNT_ID_ENDPOINT_MODE=preferred
    ```

    Windows Command Prompt

    Para configurar todas las sesiones

    ```
    C:\> setx AWS_ACCOUNT_ID_ENDPOINT_MODE preferred
    ```

Para configurar solo la sesión actual

```
C:\> set AWS_ACCOUNT_ID_ENDPOINT_MODE=preferred
```

PowerShell

```
PS C:\> $Env:AWS_ACCOUNT_ID_ENDPOINT_MODE="preferred"
```

- El archivo `config`:
  - `aws_account_id`: especifica el ID del punto de conexión basado en la cuenta de AWS que se utilizará para las llamadas a los Servicios de AWS compatibles.

    ```
    aws_account_id = <account-id>
    ```

  - `account_id_endpoint_mode`: especifica si se deben utilizar los ID de punto de conexión basados en cuentas de AWS para las llamadas a los Servicios de AWS compatibles. Se puede establecer en `preferred`, `disabled` o `required`. El valor predeterminado es el preferido.

    ```
    account_id_endpoint_mode = preferred
    ```

Los puntos de conexión basados en cuentas ayudan a garantizar un alto rendimiento y escalabilidad, ya que utilizan el ID de cuenta de AWS para agilizar el enrutamiento de las solicitudes de Servicio de AWS para los servicios compatibles con esta característica. Cuando utiliza un proveedor de credenciales y un servicio que admite puntos de conexión basados en cuentas, la AWS CLI crea y utiliza automáticamente un punto de conexión basado en una cuenta en lugar de un punto de conexión regional.

Los puntos de conexión basados en cuentas utilizan el siguiente formato, donde `<account-id>` se sustituye por el ID de cuenta de AWS y `<region>` se sustituye por la Región de AWS:

```
https://<account-id>.myservice.<region>.amazonaws.com
```

De forma predeterminada en la AWS CLI, el modo de punto de conexión basado en la cuenta está configurado en `preferred`.

Prioridad de la configuración y los ajustes del punto de conexión

Los ajustes de configuración de punto de conexión se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. Los ajustes de configuración del punto de conexión de la AWS CLI tienen prioridad en el siguiente orden:

1. La opción de línea de comandos `--endpoint-url`.
2. Si está habilitada, la variable de entorno del punto de conexión `AWS_IGNORE_CONFIGURED_ENDPOINT_URLS` global o la configuración del perfil `ignore_configure_endpoint_urls` para ignorar los puntos de conexión personalizados.
3. El valor proporcionado por una variable de entorno específica del servicio `AWS_ENDPOINT_URL_<SERVICE>`, como `AWS_ENDPOINT_URL_DYNAMODB`.
4. Los valores proporcionados por las variables de entorno `AWS_USE_DUALSTACK_ENDPOINT`, `AWS_USE_FIPS_ENDPOINT` y `AWS_ENDPOINT_URL`.
5. La variable de entorno `AWS_ACCOUNT_ID_ENDPOINT_MODE` se establece en `preferred` o `required` mediante el ID de cuenta en la variable de entorno `AWS_ACCOUNT_ID` o la configuración de `aws_account_id`.
6. El valor de punto de conexión específico del servicio proporcionado por la configuración `endpoint_url` de una sección de `services` del archivo compartido `config`.
7. El valor proporcionado por la configuración `endpoint_url` en un `profile` de un archivo compartido `config`.
8. Configuración de `use_dualstack_endpoint`, `use_fips_endpoint` y `endpoint_url`.
9. La configuración `account_id_endpoint_mode` se establece en `preferred` o `required` mediante el ID de cuenta en la variable de entorno `AWS_ACCOUNT_ID` o la configuración de `aws_account_id`.
10. En último lugar, se utiliza cualquier URL de punto de conexión predeterminada para el Servicio de AWS respectivo. Para obtener una lista de los puntos de conexión de servicio estándar disponibles en cada región, consulte Regiones y puntos de enlace de AWS en la Referencia general de Amazon Web Services.

Credenciales de autenticación y acceso para la AWS CLI

Debe establecer cómo AWS CLI se autentica con AWS cuando desarrolla con los servicios de AWS. Para configurar las credenciales de acceso programático para la AWS CLI, elija una de las siguientes opciones. Las opciones están en orden de recomendación.

Tipo de autenticación	Finalidad	Instrucciones
Credenciales de la consola de administración de AWS	(Recomendado) Use credenciales de corto plazo iniciando sesión en la AWS CLI con las credenciales de la consola. Se recomienda utilizar usuarios raíz, usuarios de IAM o federación con IAM para el acceso a la cuenta de AWS	the section called “Credenciales de consola”
Credenciales a corto plazo de los usuarios del personal de IAM Identity Center	Use credenciales a corto plazo para un usuario del personal de IAM Identity Center. La práctica recomendada de seguridad es utilizar AWS Organizations con IAM Identity Center. Aquí se combinan las credenciales de corta duración con un directorio de usuarios, como el directorio integrado de IAM Identity Center o Active Directory.	the section called “Autenticación del Centro de identidades de IAM”
Credenciales a corto plazo de usuarios de IAM	Utilice las credenciales a corto plazo de los usuarios de IAM, que son más seguras que las credenciales a largo plazo. Si sus credenciales	the section called “Credenciales a corto plazo”

Tipo de autenticación	Finalidad	Instrucciones
	están comprometidas, tiene un tiempo limitado para usarlas antes de que caduquen.	
Los usuarios de IAM o IAM Identity Center en una instancia de Amazon EC2	Usar metadatos de la instancia de Amazon EC2 para consultar credenciales temporales mediante el rol asignado a la instancia de Amazon EC2.	the section called “Metadatos de Amazon EC2”
Asumir roles para los permisos	Emparejar otro método de credenciales y asumir un rol para el acceso temporal a los Servicios de AWS a los que su usuario podría no tener acceso.	the section called “Roles de IAM”
Credenciales a largo plazo de usuarios de IAM	(No recomendado) Usar credenciales a largo plazo, que no tienen fecha de caducidad.	the section called “Usuarios de IAM”
Almacenamiento externo de los usuarios del personal de IAM o IAM Identity Center	(No recomendado) Emparejar otro método de credenciales pero almacenar los valores de credenciales en una ubicación fuera de la AWS CLI. Este método es tan seguro como la ubicación externa en la que se almacenan las credenciales.	the section called “Credenciales externas”

Prioridad de configuración y credenciales

Las credenciales y las opciones de configuración se encuentran en varios lugares, como las variables de entorno del sistema o del usuario, los archivos de configuración de AWS locales o declarados explícitamente en la línea de comandos como un parámetro. Determinadas autenticaciones tienen prioridad sobre otras. La configuración de autenticación de la AWS CLI tiene prioridad y sigue este orden:

1. Opciones de línea de comandos: anula la configuración en cualquier otra ubicación, como los parámetros `--region`, `--output` y `--profile`.
2. Variables de entorno: puede almacenar valores en las variables de entorno de su sistema.
3. Asumir rol: asuma los permisos de un rol de IAM mediante la configuración o el comando `assume-role`.
4. Asumir rol con identidad web: asuma los permisos de un rol de IAM con identidad web mediante la configuración o el comando `assume-role-with-web-identity`.
5. AWS IAM Identity Center: los ajustes de configuración de IAM Identity Center guardados en el archivo `config` se actualizan al ejecutar el comando `aws configure sso`. A continuación, las credenciales se autentican al ejecutar el comando `aws sso login`. El archivo `config` se encuentra en `~/.aws/config` en Linux o macOS, o en `C:\Users\`*`USERNAME`*`\.aws\config` en Windows.
6. Archivo de credenciales: los archivos `credentials` y `config` se actualizan al ejecutar el comando `aws configure`. El archivo `credentials` se encuentra en `~/.aws/credentials` en Linux o macOS, o en `C:\Users\`*`USERNAME`*`\.aws\credentials` en Windows.
7. Proceso personalizado: obtenga sus credenciales de un origen externo.
8. Archivo de configuración: los archivos `credentials` y `config` se actualizan al ejecutar el comando `aws configure`. El archivo `config` se encuentra en `~/.aws/config` en Linux o macOS, o en `C:\Users\`*`USERNAME`*`\.aws\config` en Windows.
9. Credenciales contenedor: puede asociar un rol de IAM con cada una de las definiciones de tareas de Amazon Elastic Container Service (Amazon ECS). Las credenciales temporales de ese rol estarán disponibles para los contenedores de esa tarea. Para obtener más información, consulte Roles de IAM para tareas en la Guía para desarrolladores de Amazon Elastic Container Service.
10. Credenciales de perfil de instancia de Amazon EC2: puede asociar un rol de IAM con cada una de las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Las credenciales temporales de ese rol estarán disponibles para el código que se ejecute en la instancia. Las credenciales

se entregan a través del servicio de metadatos de Amazon EC2. Para obtener más información, consulte Roles de IAM para Amazon EC2 en la Guía del usuario de Amazon EC2 y Uso de perfiles de instancia en la Guía del usuario de IAM.

Temas adicionales en esta sección

- the section called “Autenticación del Centro de identidades de IAM”
- the section called “Credenciales a corto plazo”
- the section called “Roles de IAM”
- the section called “Usuarios de IAM”
- the section called “Metadatos de Amazon EC2”
- the section called “Credenciales externas”

Inicio de sesión para el desarrollo local de AWS con credenciales de consola

Puede usar sus credenciales de inicio de sesión de consola de administración de AWS actuales para el acceso mediante programación a servicios de AWS. Tras un flujo de autenticación basado en un navegador, AWS genera credenciales temporales que funcionan en todas las herramientas de desarrollo locales, como la AWS CLI, AWS Tools para PowerShell y los AWS SDK. Esta característica simplifica el proceso de configuración y administración de las credenciales de AWS CLI, especialmente si prefiere la autenticación interactiva en lugar de administrar las claves de acceso a largo plazo.

Con este proceso, puede autenticarse con las credenciales raíz creadas durante la configuración inicial de la cuenta, un usuario de IAM o una identidad federada del proveedor de identidad, y la AWS CLI administra automáticamente las credenciales temporales por usted. Este enfoque mejora la seguridad al eliminar la necesidad de almacenar localmente las credenciales a largo plazo.

Al ejecutar el comando `aws login`, puede seleccionar una de las sesiones de consola activas o iniciar sesión mediante el flujo de autenticación basado en el navegador, lo que generará credenciales temporales automáticamente. La CLI actualizará automáticamente estas credenciales durante un máximo de 12 horas.

Una vez configurada, la sesión se puede utilizar en la AWS CLI y en otros AWS SDK y herramientas.

Temas

- Requisitos previos
- Inicie sesión en la AWS CLI con el comando aws login.
- Ejecución de un comando con el perfil
- Cierre de sesión con el comando de cierre de sesión de AWS
- Solución de problemas
- Recursos relacionados

Requisitos previos

- Instale la CLI de AWS. Para obtener más información, consulte Instalación o actualización de la versión más reciente de AWS CLI. Se requiere una versión mínima de 2.32.0 para usar el comando `aws login`.
- Acceda para iniciar sesión en la consola de administración de AWS como usuario raíz, usuario de IAM o mediante federación con IAM. Si utiliza IAM Identity Center, vaya a Configuración de la autenticación de IAM Identity Center con la AWS CLI en su lugar.
- Asegúrese de que la identidad de IAM tiene los permisos adecuados. Adjunte la política administrada SignInLocalDevelopmentAccess al usuario de IAM, rol o grupo. Si inicia sesión como usuario raíz, no se requieren permisos adicionales.

Inicie sesión en la AWS CLI con el comando **`aws login`**.

Ejecute el comando `aws login` para autenticarse con las credenciales de la consola de administración de AWS existentes. Si no ha configurado un perfil anteriormente, se le solicitará información adicional. Para iniciar sesión o configurar un perfil siga los pasos que se indican a continuación.

1. En el terminal que prefiera, ejecute el comando `aws login`.

```
$ aws login
```

   Para iniciar sesión en un perfil con nombre o crear uno nuevo, use la opción `--profile`.

```
$ aws login --profile my-dev-profile
```

- Si se trata de un perfil nuevo o no se ha especificado ninguna región de AWS, la AWS CLI le solicitará que proporcione una región.

```
No AWS region has been configured. The AWS region is the geographic location of
your AWS resources.

If you've used AWS before and already have resources in your account, tell us
which region they were created in. If you haven't created resources in your
 account
before, you can pick the region closest to you:
https://docs.aws.amazon.com/global-infrastructure/latest/regions/aws-regions.html.
You are able to change the region in the CLI at any time with the command
`aws configure set region NEW_REGION`.

AWS Region [us-east-1]:
```

- Si el dispositivo que usa la AWS CLI no tiene un navegador, puede usar la opción `--remote` para proporcionar una URL para abrirla en un dispositivo con navegador.

```
$ aws login --remote
```

2. La AWS CLI intenta abrir el navegador predeterminado para el proceso de inicio de sesión de la cuenta de AWS.

```
Attempting to open the login page for `us-east-1` in your default browser.
If the browser does not open, use the following URL to complete your login:
https://signin.us-east-1.amazonaws.com/authorize?<abbreviated>

If you cannot connect to this URL, make sure that you have specified a valid region.
```

- Si usó la opción `--remote`, se muestran las instrucciones para iniciar el proceso de inicio de sesión de forma manual en función del tipo de autorización que está usando. La URL que se muestra es una URL única que comienza por https://us-east-1.signin.amazonaws.com/authorize. Una vez que complete el inicio de sesión en el navegador, tendrá que copiar y pegar el código de autorización resultante en la CLI.

```
Browser will not be automatically opened.
Please visit the following URL:
https://region.signin.amazonaws.com/authorize?<abbreviated>
```

```
Please enter the authorization code displayed in the browser:
```

3. En el navegador, seleccione las credenciales que desee utilizar en la lista que se muestra y, a continuación, vuelva al terminal.
   - Si el perfil que está configurando tiene una sesión de inicio de sesión previamente configurada que no coincide con la nueva sesión, la AWS CLI le pide que confirme que está cambiando la sesión que corresponde al perfil existente.

   ```
   Profile signin is already configured to use session
    arn:aws:iam::0123456789012:user/ReadOnly.
   Do you want to overwrite it to use arn:aws:iam::0123456789012:user/Admin instead?
    (y/n):.
   ```

4. Un mensaje final describe la configuración del perfil completada. Ahora puede utilizar este perfil para solicitar credenciales. Utilice el comando `aws login` para solicitar y recuperar realmente las credenciales necesarias para ejecutar comandos.

   El token de autenticación se almacena en caché en el disco en el directorio `.aws/login/cache` con un nombre de archivo basado en el perfil resuelto.

Archivo de configuración generado

Estos pasos dan como resultado la creación del perfil `default` en el archivo `config` similar al siguiente:

```
[default]
login_session = arn:aws:iam::0123456789012:user/username
region = us-east-1
```

Ejecución de un comando con el perfil

Una vez que haya iniciado sesión, puede utilizar sus credenciales para invocar comandos de la AWS CLI con el perfil asociado. En el ejemplo siguiente, se llama al comando `get-caller-identity` que usa el perfil `default`:

```
$ aws sts get-caller-identity
```

Para iniciar sesión en una sesión específica, utilice la opción `--profile`.

```
$ aws sts get-caller-identity --profile my-dev-profile
```

La AWS CLI y los SDK actualizarán automáticamente las credenciales almacenadas en caché cada 15 minutos, según sea necesario. La sesión general será válida hasta la duración de sesión establecida para la entidad principal de IAM (máximo de 12 horas), tras lo cual deberá volver a ejecutar `aws login`.

Cierre de sesión con el comando de cierre de sesión de AWS

Cuando haya terminado de utilizar la sesión, puede dejar que las credenciales caduquen o ejecutar el comando `aws logout` para eliminar las credenciales almacenadas en caché. Si no se especifica ningún perfil en la línea de comandos o en la variable de entorno `AWS_PROFILE`, el comando cierra la sesión del perfil predeterminado. En el ejemplo siguiente, se cierra la sesión del perfil predeterminado.

```
$ aws logout
```

Para cerrar sesión de una sesión específica, utilice la opción `--profile`.

```
$ aws logout --profile my-dev-profile
```

Para cerrar sesión en todos los perfiles que usan credenciales de inicio de sesión, use la opción `--all`.

```
$ aws logout --all
```

Credenciales almacenadas en caché

Las credenciales temporales en caché, así como los metadatos necesarios para actualizarlas, se almacenan de forma predeterminada en `~/.aws/login/cache` en Linux y macOS o `%USERPROFILE%\.aws\login\cache` en Windows.

Para almacenar la caché de credenciales de corta duración en una ubicación alternativa, establezca la variable de entorno `AWS_LOGIN_CACHE_DIRECTORY`.

Uso compartido de las credenciales de inicio de sesión como credenciales de proceso

Es posible que las versiones anteriores de los AWS SDK u otras herramientas de desarrollo aún no admitan las credenciales de consola. Como solución alternativa, puede configurar la AWS CLI para

que sirva como proveedor de credenciales de procesos. La CLI seguirá actualizando las credenciales según sea necesario y, al mismo tiempo, las compartirá con las herramientas configuradas para usar el perfil credential_process.

En este ejemplo, utilice la AWS CLI para iniciar sesión primero para el inicio de sesión del perfil:

```
$ aws login --profile signin
```

A continuación, configure manualmente un perfil con la opción credential_process, que apunta al perfil de inicio de sesión. Ahora puede configurar los SDK o las herramientas para que usen el perfil de proceso, que invocará la CLI para compartir las credenciales del perfil de inicio de sesión.

```
[profile signin]
login_session = arn:aws:iam::0123456789012:user/username
region = us-east-1

[profile process]
credential_process = aws configure export-credentials --profile signin --format process
region = us-east-1
```

Solución de problemas

Esta página contiene recomendaciones para solucionar problemas relacionados con el inicio de sesión para el desarrollo local de AWS mediante las credenciales de consola de la AWS CLI.

> **Note**
>
> Para solucionar otros problemas que puedan surgir al utilizar la AWS CLI, consulte Solución de errores para la AWS CLI.

Errores ExpiredToken o AccessDeniedException después de usar “Inicio de sesión de AWS”

Al ejecutar un comando de AWS CLI después de ejecutar `aws login` para un perfil determinado, es posible que se produzca un error de credenciales caducadas o no válidas.

```
$ aws s3 ls
```

```
An error occurred (ExpiredToken) when calling the ListBuckets operation: The provided
 token has expired.
```

Causa posible: tiene una combinación de credenciales existentes y las nuevas credenciales de inicio de sesión en ese perfil

Ejecute `aws configure list` o `aws configure list --profile <profile name>` para imprimir el lugar desde el que la CLI resuelve las credenciales para el perfil predeterminado o para el perfil dado.

Si la columna TYPE no es de inicio de sesión, significa que todavía hay un tipo diferente de credenciales establecido en el perfil de destino.

En este ejemplo, las credenciales se resuelven desde el archivo de credenciales compartido del directorio principal, que tiene prioridad sobre las credenciales de inicio de sesión.

```
$  aws configure list
NAME       : VALUE                   : TYPE             : LOCATION
profile    : <not set>               : None             : None
access_key : ****************MPLE     : shared-credentials-file :
secret_key : ****************EKEY     : shared-credentials-file :
region     : us-east-1               : config-file      : ~/.aws/config
```

Para solucionar este problema, elimine manualmente las credenciales existentes del archivo de configuración y credenciales del perfil de destino. Una vez que lo haga, debería ver las credenciales de inicio de sesión cuando se vuelva a ejecutar `aws configure list`.

```
$  aws configure list
NAME       : VALUE                   : TYPE             : LOCATION
profile    : <not set>               : None             : None
access_key : ****************MPLE     : login            :
secret_key : ****************EKEY     : login            :
region     : us-east-1               : config-file      : ~/.aws/config
```

Como opción alternativa, el uso de la opción `--debug` mostrará el lugar desde el que la CLI resuelve las credenciales.

El firewall bloquea el acceso de red cuando se ejecuta “Inicio de sesión de AWS”

Cuando se ejecuta `aws login`, es posible que aparezca una ventana emergente o un mensaje del software de firewall que impida que la AWS CLI acceda a la red

Causa posible: el firewall o el software de seguridad impiden que la AWS CLI abra el puerto utilizado para gestionar la devolución de llamada de OAuth.

Para evitar este problema, utilice la opción `--remote` en su lugar. Esto pedirá que se copie y pegue el código de autorización en lugar de utilizar la devolución de llamada de OAuth.

```
$ aws login --remote
```

Recursos relacionados

Los recursos adicionales son los siguientes.

- Instalación o actualización de la versión más reciente de AWS CLI
- `aws login` en la referencia de la AWS CLI versión 2
- `aws logout` en la referencia de la AWS CLI versión 2

Configuración de la autenticación de IAM Identity Center con la AWS CLI

En este tema se proporcionan instrucciones sobre cómo configurar laAWS CLI con AWS IAM Identity Center (IAM Identity Center) para recuperar las credenciales que permiten ejecutar comandos de la AWS CLI. Existen principalmente dos formas de autenticar a los usuarios con IAM Identity Center para que obtengan las credenciales que permiten ejecutar los comandos de AWS CLI a través del archivo `config`:

- (Recomendada) Configuración del proveedor de token de SSO.
- Configuración heredada no actualizable.

Para obtener información sobre el uso de autenticación de portador, que no utiliza ID de cuenta ni rol, consulte Configuración para utilizar la AWS CLI con CodeCatalyst en la Guía del usuario de Amazon CodeCatalyst.

> **Note**
>
> Para ver un proceso guiado sobre el uso de IAM Identity Center con los comandos de la AWS CLI, consulte the section called “Tutorial: AWS IAM Identity Center y Amazon S3”.

Temas

- the section called “Requisitos previos”
- the section called “Configurar el perfil con el asistente de `aws configure sso`”
- the section called “Configurar solo la sección `sso-session` con el asistente de `aws configure sso-session`”
- the section called “Configuración manual mediante el archivo `config`”
- the section called “Inicio de sesión en IAM Identity Center”
- the section called “Ejecución de un comando con el perfil de IAM Identity Center”
- the section called “Cierre de sesiones de IAM Identity Center”
- the section called “Solución de problemas”
- the section called “Recursos relacionados”

Requisitos previos

- Instale la AWS CLI. Para obtener más información, consulte the section called “Instalar o actualizar”.
- Primero debe tener acceso a la autenticación de SSO en el Centro de identidades de IAM. Elija uno de los siguientes métodos para acceder a las credenciales de AWS.

No he establecido el acceso a través de IAM Identity Center

Siga las instrucciones en Introducción en la Guía del usuario de AWS IAM Identity Center. Este proceso activa IAM Identity Center, crea un usuario administrativo y agrega un conjunto apropiado de permisos de privilegio mínimo.

> **Note**
>
> Cree un conjunto de permisos que aplique los permisos de privilegio mínimo. Le recomendamos que utilice el conjunto de permisos predefinido `PowerUserAccess`, a menos que su empleador haya creado un conjunto de permisos personalizado para este fin.

Salga del portal e inicie sesión de nuevo para ver las Cuentas de AWS, los detalles sobre el acceso programático y las opciones para `Administrator` o `PowerUserAccess`. Seleccione `PowerUserAccess` cuando trabaje con el SDK.

Ya tengo acceso a AWS a través de un proveedor de identidades federado administrado por mi empleador (como Azure AD u Okta)

Inicie sesión en AWS a través del portal de su proveedor de identidades. Si su administrador de la nube le ha concedido permisos `PowerUserAccess` (desarrollador), verá las Cuentas de AWS a las que tiene acceso y su conjunto de permisos. Junto al nombre de su conjunto de permisos, verá las opciones para acceder a las cuentas de forma manual o programática mediante ese conjunto de permisos.

Las implementaciones personalizadas pueden dar lugar a experiencias diferentes, como distintos nombres de conjuntos de permisos. Si no está seguro de qué configuración de permisos debe utilizar, contacte con su equipo de TI para obtener ayuda.

Ya tengo acceso a AWS a través del portal de acceso de AWS administrado por mi empleador

Inicie sesión en AWS a través del portal de acceso de AWS. Si su administrador de la nube le ha concedido permisos `PowerUserAccess` (desarrollador), verá las Cuentas de AWS a las que tiene acceso y su conjunto de permisos. Junto al nombre de su conjunto de permisos, verá las opciones para acceder a las cuentas de forma manual o programática mediante ese conjunto de permisos.

Ya tengo acceso a AWS a través de un proveedor de identidades federado administrado por mi empleador

Contacte con su equipo de TI para obtener ayuda.

Tras acceder a IAM Identity Center, recopile la información de IAM Identity Center realizando lo siguiente:

1. Recopilación de los valores `SSO Start URL` y `SSO Region` que necesita para ejecutar `aws configure sso`

    a. En el portal de acceso de AWS, seleccione el conjunto de permisos que utiliza para el desarrollo y seleccione el enlace Claves de acceso.

    b. En el cuadro de diálogo Obtener credenciales, elija la pestaña que coincida con su sistema operativo.

c. Elija el método de credenciales de IAM Identity Center para obtener los valores `SSO Start URL` y `SSO Region`.

2. Como alternativa, a partir de la versión 2.22.0, puede utilizar la URL del emisor en lugar de la URL de inicio. La URL del emisor se ubica en la consola de AWS IAM Identity Center en una de las siguientes ubicaciones:
   - En la página del panel, la URL del emisor aparece en el resumen de la configuración.
   - En la página de configuración, la URL del emisor se encuentra en los ajustes del origen de identidad.
3. Para obtener información sobre qué ámbitos se deben registrar, consulte Ámbitos de acceso de OAuth 2.0 en la Guía del usuario del IAM Identity Center.

Configurar el perfil con el asistente de `aws configure sso`

Para configurar un perfil de IAM Identity Center en la AWS CLI:

1. En el terminal que prefiera, ejecute el comando `aws configure sso`.

   (Recommended) IAM Identity Center

   Cree un nombre de sesión, proporcione la URL de inicio de IAM Identity Center o la URL del emisor, la Región de AWS que aloja el directorio de IAM Identity Center y el ámbito del registro.

   ```
   $ aws configure sso
   SSO session name (Recommended): my-sso
   SSO start URL [None]: https://my-sso-portal.awsapps.com/start
   SSO region [None]: us-east-1
   SSO registration scopes [None]: sso:account:access
   ```

   La autorización de la clave de prueba para el intercambio de códigos (PKCE) se utiliza de forma predeterminada para la AWS CLI a partir de la versión 2.22.0 y se debe utilizar en dispositivos con navegador. Para seguir utilizando la autorización de dispositivos, agregue la opción `--use-device-code`.

   ```
   $ aws configure sso --use-device-code
   ```

Legacy IAM Identity Center

Sáltese el nombre de sesión y proporcione su URL de inicio de IAM Identity Center y la región de AWS que aloja el directorio del Identity Center.

```
$ aws configure sso
SSO session name (Recommended):
SSO start URL [None]: https://my-sso-portal.awsapps.com/start
SSO region [None]:us-east-1
```

2. La AWS CLI intenta abrir su navegador predeterminado para el proceso de inicio de sesión de su cuenta de IAM Identity Center. El proceso puede pedirle que permita que la AWS CLI acceda a los datos. Dado que la AWS CLI se ha creado con el SDK para Python, los mensajes de permiso pueden contener variaciones del nombre `botocore`.
   - Si la AWS CLI no puede abrir el navegador, se muestran las instrucciones para iniciar el proceso de inicio de sesión de forma manual en función del tipo de autorización que está usando.

     PKCE authorization

     La autorización de la clave de prueba para el intercambio de códigos (PKCE) se utiliza de forma predeterminada para la AWS CLI a partir de la versión 2.22.0. La URL que se muestra es una URL única que comienza por *https://oidc.us-east-1.amazonaws.com/authorize*

     Las URL de autorización de la PKCE se deben abrir en el mismo dispositivo en el que está iniciando sesión y se deben usar en un dispositivo con navegador.

```
Attempting to automatically open the SSO authorization
 page in your
default browser.
If the browser does not open or you wish to use a
 different device to
authorize the request, open the following URL:

https://oidc.us-east-1.amazonaws.com/authorize?
<abbreviated>
```

Device authorization

En las versiones anteriores a 2.22.0, la AWS CLI utiliza la autorización de dispositivos OAuth 2.0. Puede habilitar este método en las versiones más recientes mediante la opción `--use-device-code`.

Las URL de autorización de dispositivo no se tienen que abrir en el mismo dispositivo en el que está iniciando sesión y se pueden usar en un dispositivo con o sin navegador.

```
If the browser does not open or you wish to use a
 different device to
authorize this request, open the following URL:
https://device.sso.us-west-2.amazonaws.com/

Then enter the code:
QCFK-N451
```

3. Seleccione la cuenta de AWS que desee utilizar de la lista que aparece. Si solo tiene autorización para usar una única cuenta, la AWS CLI selecciona esa cuenta automáticamente y omite la petición.

```
There are 2 AWS accounts available to you.
> DeveloperAccount, developer-account-admin@example.com (123456789011)
  ProductionAccount, production-account-admin@example.com (123456789022)
```

4. Seleccione el rol de IAM que desee utilizar en la lista que aparece. Si solo hay un rol disponible, la AWS CLI selecciona automáticamente ese rol y omite la petición.

```
Using the account ID 123456789011
There are 2 roles available to you.
> ReadOnly
  FullAccess
```

5. Especifique el formato de salida predeterminado, la Región de AWS predeterminada a la que se enviarán los comandos y un nombre para el perfil. Si especifica `default` como nombre de perfil, este perfil pasa a ser el perfil predeterminado. En el ejemplo siguiente, el usuario introduce una región predeterminada, un formato de salida predeterminado y el nombre del perfil.

```
Default client Region [None]: us-west-2<ENTER>
CLI default output format (json if not specified) [None]: json<ENTER>
```

```
Profile name [123456789011_ReadOnly]: my-dev-profile<ENTER>
```

6. Un mensaje final describe la configuración del perfil completada. Ahora puede utilizar este perfil para solicitar credenciales. Utilice el comando `aws sso login` para solicitar y recuperar realmente las credenciales necesarias para ejecutar comandos. Para obtener instrucciones, consulte Inicio de sesión en IAM Identity Center.

Archivo de configuración generado

Estos pasos dan como resultado la creación de una sección `sso-session` y un perfil con un nombre en el archivo `config` similar al siguiente:

IAM Identity Center

```
[profile my-dev-profile]
sso_session = my-sso
sso_account_id = 123456789011
sso_role_name = readOnly
region = us-west-2
output = json

[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_registration_scopes = sso:account:access
```

Legacy IAM Identity Center

```
[profile my-dev-profile]
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_region = us-east-1
sso_account_id = 123456789011
sso_role_name = readOnly
region = us-west-2
output = json
```

Configurar solo la sección **`sso-session`** con el asistente de **`aws configure sso-session`**

> **Note**
>
> Esta configuración no es compatible con IAM Identity Center heredado.

El comando `aws configure sso-session` solo actualiza las secciones `sso-session` del archivo `~/.aws/config`. Ejecute el comando `aws configure sso-session` y proporcione la URL de inicio de IAM Identity Center o la URL del emisor y la región de AWS que aloja el directorio del IAM Identity Center.

```
$ aws configure sso-session
SSO session name: my-sso
SSO start URL [None]: https://my-sso-portal.awsapps.com/start
SSO region [None]: us-east-1
SSO registration scopes [None]: sso:account:access
```

Configuración manual mediante el archivo **`config`**

La información de configuración de IAM Identity Center se almacena en el archivo `config` y se puede editar con un editor de texto. Para añadir manualmente compatibilidad con IAM Identity Center a un perfil con nombre, debe añadir claves y valores al archivo `config`.

Configuración del archivo de IAM Identity Center

La sección `sso-session` del archivo `config` se usa para agrupar las variables de configuración para adquirir los tokens de acceso SSO, que luego se pueden usar para adquirir credenciales de AWS. Se utilizan las siguientes configuraciones:

- (Obligatorio) `sso_start_url`
- (Obligatorio) `sso_region`
- `sso_account_id`
- `sso_role_name`
- `sso_registration_scopes`

Defina una sección `sso-session` y asóciela a un perfil. Los ajustes de `sso_start_url` y `sso_region` se deben definir dentro de la sección `sso-session`. Normalmente, `sso_account_id` y `sso_role_name` deben establecerse en la sección `profile` para que el SDK pueda solicitar las credenciales de SSO.

En el siguiente ejemplo se configura el SDK para que solicite credenciales de SSO y admita la actualización automática de tokens:

```
[profile dev]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = SampleRole

[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
```

Esto también permite reutilizar las configuraciones de `sso-session` en varios perfiles:

```
[profile dev]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = SampleRole

[profile prod]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = SampleRole2

[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
```

No obstante, `sso_account_id` y `sso_role_name` no son necesarios para todos los escenarios de configuración de token de SSO. Si su aplicación solo utiliza servicios de AWS que admiten la autenticación de portador, no son necesarias las credenciales de AWS tradicionales. La autenticación de portador es un esquema de autenticación HTTP que utiliza tokens de seguridad denominados tokens de portador. En este escenario, no se necesitan `sso_account_id` ni `sso_role_name`. Consulte la guía individual de su servicio de AWS para determinar si admite la autorización de token de portador.

Además, los ámbitos de registro pueden configurarse como parte de `sso-session`. El alcance es un mecanismo de OAuth 2.0 para limitar el acceso de una aplicación a la cuenta de un usuario. Una solicitud puede pedir uno o varios ámbitos y el token de acceso emitido a la solicitud se limitará a los ámbitos concedidos. Estos ámbitos definen los permisos cuya autorización se solicita para el cliente OIDC registrado y los tokens de acceso recuperados por el cliente. El siguiente ejemplo establece `sso_registration_scopes` para proporcionar acceso para enumerar cuentas/roles:

```
[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_registration_scopes = sso:account:access
```

El token de autenticación se almacena en caché en el disco en el directorio `sso/cache` con un nombre de archivo basado en el nombre de la sesión.

Archivo de configuración de IAM Identity Center heredado

> **Note**
>
> La actualización automática de tokens no se admite con la configuración no actualizable heredada. Le recomendamos que utilice la configuración del token de SSO.

Para agregar manualmente compatibilidad con IAM Identity Center a un perfil con nombre, debe agregar las siguientes claves y valores a la definición del perfil en el archivo `config`.

- `sso_start_url`
- `sso_region`
- `sso_account_id`
- `sso_role_name`

Puede incluir otras claves y valores válidos en el archivo `.aws/config`. A continuación, se muestra un ejemplo de perfil de IAM Identity Center:

```
[profile my-sso-profile]
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_region = us-west-2
```

```
sso_account_id = 111122223333
sso_role_name = SSOReadOnlyRole
region = us-west-2
output = json
```

Para ejecutar comandos, primero debe utilizar the section called “Inicio de sesión en IAM Identity Center” para solicitar y recuperar las credenciales temporales.

Para obtener más información sobre los archivos de `config` y `credentials`, consulte the section called “Opciones de configuración”.

Inicio de sesión en IAM Identity Center

> **Note**
>
> El proceso de inicio de sesión puede pedirle que permita que la AWS CLI acceda a sus datos. Dado que la AWS CLI se ha creado con el SDK para Python, los mensajes de permiso pueden contener variaciones del nombre `botocore`.

Para recuperar y almacenar en caché un conjunto de credenciales de IAM Identity Center, ejecute el siguiente comando de la AWS CLI para abrir su navegador predeterminado y comprobar que ha iniciado sesión en IAM Identity Center.

```
$ aws sso login --profile my-dev-profile
SSO authorization page has automatically been opened in your default browser.
Follow the instructions in the browser to complete this authorization request.
Successfully logged into Start URL: https://my-sso-portal.awsapps.com/start
```

Sus credenciales de IAM Identity Center se guardan en la caché y la AWS CLI las utiliza para recuperar de forma segura las credenciales de AWS del rol de IAM especificado en el perfil.

Si la AWS CLI no puede abrir su navegador

Si la AWS CLI no puede abrir el navegador de forma automática, se muestran las instrucciones para iniciar el proceso de inicio de sesión de forma manual en función del tipo de autorización que está usando.

PKCE authorization

La autorización de la clave de prueba para el intercambio de códigos (PKCE) se utiliza de forma predeterminada para la AWS CLI a partir de la versión 2.22.0. La URL que se muestra es una URL única que comienza por *https://oidc.us-east-1.amazonaws.com/authorize*

Las URL de autorización de la PKCE se deben abrir en el mismo dispositivo en el que está iniciando sesión y se deben usar en un dispositivo con navegador.

```
Attempting to automatically open the SSO authorization
 page in your
default browser.
If the browser does not open or you wish to use a
 different device to
authorize the request, open the following URL:

https://oidc.us-east-1.amazonaws.com/authorize?
<abbreviated>
```

Device authorization

En las versiones anteriores a 2.22.0, la AWS CLI utiliza la autorización de dispositivos OAuth 2.0. Puede habilitar este método en las versiones más recientes mediante la opción `--use-device-code`.

Las URL de autorización de dispositivo no se tienen que abrir en el mismo dispositivo en el que está iniciando sesión y se pueden usar en un dispositivo con o sin navegador.

```
If the browser does not open or you wish to use a
 different device to
authorize this request, open the following URL:
https://device.sso.us-west-2.amazonaws.com/

Then enter the code:
QCFK-N451
```

También puede especificar qué perfil de `sso-session` utilizar al iniciar la sesión utilizando el parámetro `--sso-session` del comando `aws sso login`. La opción `sso-session` no está disponible para IAM Identity Center heredado.

```
$ aws sso login --sso-session my-dev-session
```

A partir de la versión 2.22.0, la autorización de la PKCE es la predeterminada. Para usar la autorización del dispositivo para iniciar sesión, agregue la opción `--use-device-code`.

```
$ aws sso login --profile my-dev-profile --use-device-code
```

El token de autenticación se almacena en caché en el disco en el directorio `~/.aws/sso/cache` con un nombre de archivo basado en la `sso_start_url`.

Ejecución de un comando con el perfil de IAM Identity Center

Una vez que haya iniciado sesión, puede utilizar estas credenciales para invocar comandos de la AWS CLI con el perfil con nombre asociado. En el ejemplo siguiente se muestra un comando que usa un perfil:

```
$ aws sts get-caller-identity --profile my-dev-profile
```

Mientras haya iniciado sesión en IAM Identity Center y esas credenciales almacenadas en caché no hayan caducado, la AWS CLI renovará automáticamente las credenciales de AWS caducadas cuando sea necesario. Sin embargo, si sus credenciales de IAM Identity Center caducan, debe renovarlas explícitamente iniciando sesión de nuevo en la cuenta de IAM Identity Center.

Cierre de sesiones de IAM Identity Center

Cuando haya terminado de utilizar su perfil de IAM Identity Center, puede dejar que las credenciales caduquen o ejecutar el siguiente comando para eliminar las credenciales almacenadas en caché.

```
$ aws sso logout
Successfully signed out of all SSO profiles.
```

Solución de problemas

Si tiene problemas con la AWS CLI, consulte the section called “Errores de solución de problemas” para ver los pasos de solución de problemas.

Recursos relacionados

Los recursos adicionales son los siguientes.

- the section called “Conceptos de IAM Identity Center”
- the section called “Tutorial: AWS IAM Identity Center y Amazon S3”
- the section called “Instalar o actualizar”
- the section called “Opciones de configuración”
- `aws configure sso` en la AWS CLI version 2 Reference
- `aws configure sso-session` en la AWS CLI version 2 Reference
- `aws sso login` en la AWS CLI version 2 Reference
- `aws sso logout` en la AWS CLI version 2 Reference
- Setting up to use the AWS CLI with CodeCatalyst en la Guía del usuario de Amazon CodeCatalyst
- Ámbitos de acceso de OAuth 2.0 en la Guía del usuario del IAM Identity Center
- Tutoriales de introducción en la Guía del usuario del IAM Identity Center

Conceptos de AWS IAM Identity Center para la AWS CLI

En este tema se describen los conceptos clave de AWS IAM Identity Center (IAM Identity Center). IAM Identity Center es un servicio de IAM basado en la nube que simplifica la administración del acceso de los usuarios a múltiples Cuentas de AWS, aplicaciones, SDK y herramientas mediante la integración con los proveedores de identidad (IdP) existentes. Permite un inicio de sesión único seguro, la administración de permisos y la auditoría a través de un portal de usuarios centralizado, lo que agiliza el control de identidades y accesos para las organizaciones.

Temas

- Qué es IAM Identity Center
- Términos
- Cómo funciona IAM Identity Center
- Recursos adicionales

Qué es IAM Identity Center

IAM Identity Center es un servicio de administración de identidades y accesos (IAM) basado en la nube que le permite administrar de forma centralizada el acceso a múltiples Cuentas de AWS y aplicaciones empresariales.

Proporciona un portal de usuarios en el que los usuarios autorizados pueden acceder a las Cuentas de AWS y las aplicaciones para las que se les haya concedido permiso utilizando sus credenciales corporativas actuales. Esto permite a las organizaciones aplicar políticas de seguridad coherentes, así como agilizar la administración del acceso de los usuarios.

Independientemente del IdP que utilice, el Centro de identidades de IAM abstrae esas distinciones. Por ejemplo, puede conectar Microsoft Azure AD como se describe en el artículo del blog The Next Evolution in IAM Identity Center (La próxima evolución en el Centro de identidades de IAM).

> **Note**
>
> Para obtener información sobre el uso de autenticación de portador, que no utiliza ID de cuenta ni rol, consulte Configuración para utilizar la AWS CLI con CodeCatalyst en la Guía del usuario de Amazon CodeCatalyst.

Términos

Los términos más comunes en el uso de IAM Identity Center son los siguientes:

Proveedor de identidad (IdP)

: Un sistema de administración de identidades como IAM Identity Center, Microsoft Azure AD, Okta o su propio servicio de directorio corporativo.

AWS IAM Identity Center

: IAM Identity Center es el servicio de proveedor de identidades propiedad de AWS. Antes se le conocía como AWS Single Sign-On y los SDK y las herramientas conservan los espacios de nombres de las API de `sso` para garantizar la compatibilidad con versiones anteriores. Para más información, consulte IAM Identity Center rename en la Guía del usuario de AWS IAM Identity Center.

URL de Portal de acceso a AWS, URL de inicio del SSO, URL de inicio

: La URL exclusiva de IAM Identity Center de la organización para acceder a las Cuentas de AWS, los servicios y los recursos autorizados.

URL del emisor

: La URL del emisor exclusiva de IAM Identity Center de la organización para el acceso programático a las Cuentas de AWS, los servicios y los recursos autorizados. A partir de la

versión 2.22.0 de la AWS CLI, la URL del emisor se puede utilizar indistintamente con la URL de inicio.

Federación

Se trata del proceso que permite establecer la confianza entre IAM Identity Center y un proveedor de identidades a la hora de habilitar el inicio de sesión único (SSO).

Cuentas de AWS

Las Cuentas de AWS para las que se proporciona acceso a los usuarios a través de AWS IAM Identity Center.

Conjuntos de permisos, credenciales de AWS, credenciales de sigv4

Conjuntos predefinidos de permisos que se pueden asignar a usuarios o grupos para concederles acceso a los Servicios de AWS.

Ámbitos de registro, ámbitos de acceso, ámbitos

Los ámbitos son un mecanismo de OAuth 2.0 para limitar el acceso de una aplicación a la cuenta de un usuario. Una solicitud puede pedir uno o varios ámbitos y el token de acceso emitido a la solicitud se limita a los ámbitos concedidos. Para obtener información sobre los ámbitos, consulte Ámbitos de acceso en la Guía del usuario del IAM Identity Center.

Tokens, token de actualización, token de acceso

Los tokens son credenciales de seguridad temporales que se emiten en la autenticación. Estos tokens contienen información sobre su identidad y los permisos que se le han concedido.

Cuando accede a una aplicación o recurso de AWS a través del portal de IAM Identity Center, se presenta tu token a AWS para la autenticación y autorización. Esto permite a AWS verificar su identidad y asegurarse de que cuenta con los permisos necesarios para realizar las acciones solicitadas.

El token de autenticación se almacena en caché en el disco en el directorio `~/.aws/sso/cache` con un nombre de archivo JSON basado en el nombre de la sesión.

Sesión

Una sesión en IAM Identity Center hace referencia al período durante el cual un usuario está autenticado y autorizado a acceder a las aplicaciones o recursos de AWS. Cuando un usuario inicia sesión en el portal de IAM Identity Center, se establece una sesión y el token del usuario es válido durante un período específico. Para obtener más información sobre la duración de la sesión, consulte Set session duration en la Guía del usuario de AWS IAM Identity Center.

Durante la sesión, puede navegar entre diferentes aplicaciones y cuentas de AWS sin tener que volver a autenticarse, siempre y cuando la sesión permanezca activa. Cuando la sesión caduque, deberá volver a iniciar sesión para renovar el acceso.

Las sesiones de IAM Identity Center ayudan a proporcionar una experiencia de usuario fluida y, al mismo tiempo, aplican las prácticas recomendadas de seguridad mediante la limitación de la validez de las credenciales de acceso de los usuarios.

Concesión de códigos de autorización con clave de prueba para el intercambio de códigos (PKCE)

A partir de la versión 2.22.0, la clave de prueba para el intercambio de códigos (PKCE) es un flujo de concesión de autenticación de OAuth 2.0 para dispositivos con navegador. La PKCE es una forma sencilla y segura de autenticarse y obtener el consentimiento para acceder a los recursos de AWS desde ordenadores de sobremesa y dispositivos móviles con navegadores web. Este es el comportamiento de autorización predeterminado. Para obtener más información sobre la PKCE, consulte Authorization Code Grant with PKCE en la Guía del usuario de AWS IAM Identity Center.

Concesión de autorización de dispositivo

Un flujo de concesión de autenticación de OAuth 2.0 para dispositivos con o sin navegador web. Para obtener más información sobre cómo configurar la duración de las sesiones, consulte Device Authorization Grant en la Guía del usuario de AWS IAM Identity Center.

Cómo funciona IAM Identity Center

IAM Identity Center se integra con el proveedor de identidades de su organización, por ejemplo, IAM Identity Center, Microsoft Azure AD u Okta. Los usuarios se autentican con este proveedor de identidades y, a continuación, IAM Identity Center asigna dichas identidades a los permisos y accesos adecuados de su entorno de AWS.

En el siguiente flujo de trabajo de IAM Identity Center, se da por hecho que ya ha configurado la AWS CLI para utilizar IAM Identity Center:

1. Ejecute el comando `aws sso login` en el terminal que desee.
2. Inicie sesión en su Portal de acceso a AWS para comenzar una nueva sesión.
   - Al iniciar una nueva sesión, recibirá un token de actualización y un token de acceso que se almacena en la caché.
   - Si ya tiene una sesión activa, se reutiliza la sesión existente y caducará cuando lo haga la sesión existente.

3. En función del perfil que haya configurado en su archivo `config`, IAM Identity Center asume los conjuntos de permisos adecuados y le concede acceso a las Cuentas de AWS y aplicaciones correspondientes.
4. Las AWS CLI, los SDK y las herramientas utilizan su rol de IAM asumido para realizar llamadas a los Servicios de AWS, por ejemplo, para crear buckets de Amazon S3 hasta que caduque la sesión.
5. El token de acceso obtenido de IAM Identity Center se comprueba cada hora y se actualiza automáticamente mediante el token de actualización.
   - Si el token de acceso ha caducado, el SDK utiliza el token de actualización para obtener un nuevo token de acceso. A continuación, se comparan las duraciones de las sesiones de estos tokens y, si el token de actualización no ha caducado, IAM Identity Center proporciona un nuevo token de acceso.
   - Si el token de actualización ha caducado, no se proporcionan nuevos tokens de acceso y la sesión habrá finalizado.
6. Las sesiones finalizan cuando los tokens de actualización caducan o cuando cierra la sesión manualmente mediante el comando `aws sso logout`. Se eliminan las credenciales almacenadas en caché. Para seguir accediendo a los servicios mediante IAM Identity Center, debe iniciar una nueva sesión con el comando `aws sso login`.

Recursos adicionales

Los recursos adicionales son los siguientes.

- the section called “Autenticación del Centro de identidades de IAM”
- the section called “Tutorial: AWS IAM Identity Center y Amazon S3”
- the section called “Instalar o actualizar”
- the section called “Opciones de configuración”
- `aws configure sso` en la AWS CLI version 2 Reference
- `aws configure sso-session` en la AWS CLI version 2 Reference
- `aws sso login` en la AWS CLI version 2 Reference
- `aws sso logout` en la AWS CLI version 2 Reference
- Setting up to use the AWS CLI with CodeCatalyst en la Guía del usuario de Amazon CodeCatalyst
- IAM Identity Center rename en la Guía del usuario de AWS IAM Identity Center
- Ámbitos de acceso de OAuth 2.0 en la Guía del usuario del IAM Identity Center

- Set session duration en la Guía del usuario de AWS IAM Identity Center
- Tutoriales de introducción en la Guía del usuario del IAM Identity Center

Tutorial: uso de IAM Identity Center para ejecutar comandos de Amazon S3 en la AWS CLI

En este tema se describe cómo configurar la AWS CLI para autenticar a los usuarios con AWS IAM Identity Center (IAM Identity Center) actual, de manera que se recuperen las credenciales para ejecutar comandos de la AWS Command Line Interface (AWS CLI) para Amazon Simple Storage Service (Amazon S3).

Temas

- Paso 1: autenticación en IAM Identity Center
- Paso 2: recopilación de la información de IAM Identity Center
- Paso 3: creación de buckets de Amazon S3
- Paso 4: Instalar la AWS CLI
- Paso 5: configuración del perfil de la AWS CLI
- Paso 6: inicio de sesión en IAM Identity Center
- Paso 7: ejecución de comandos de Amazon S3
- Paso 8: cierre de sesión en IAM Identity Center
- Paso 9: eliminación de recursos
- Solución de problemas
- Recursos adicionales

Paso 1: autenticación en IAM Identity Center

Obtenga acceso a la autenticación de SSO en IAM Identity Center. Elija uno de los siguientes métodos para acceder a las credenciales de AWS.

No he establecido el acceso a través de IAM Identity Center

Siga las instrucciones en Introducción en la Guía del usuario de AWS IAM Identity Center. Este proceso activa IAM Identity Center, crea un usuario administrativo y agrega un conjunto apropiado de permisos de privilegio mínimo.

> **Note**
>
> Cree un conjunto de permisos que aplique los permisos de privilegio mínimo. Le recomendamos que utilice el conjunto de permisos predefinido `PowerUserAccess`, a menos que su empleador haya creado un conjunto de permisos personalizado para este fin.

Salga del portal e inicie sesión de nuevo para ver las Cuentas de AWS, los detalles sobre el acceso programático y las opciones para `Administrator` o `PowerUserAccess`. Seleccione `PowerUserAccess` cuando trabaje con el SDK.

Ya tengo acceso a AWS a través de un proveedor de identidades federado administrado por mi empleador (como Azure AD u Okta)

Inicie sesión en AWS a través del portal de su proveedor de identidades. Si su administrador de la nube le ha concedido permisos `PowerUserAccess` (desarrollador), verá las Cuentas de AWS a las que tiene acceso y su conjunto de permisos. Junto al nombre de su conjunto de permisos, verá las opciones para acceder a las cuentas de forma manual o programática mediante ese conjunto de permisos.

Las implementaciones personalizadas pueden dar lugar a experiencias diferentes, como distintos nombres de conjuntos de permisos. Si no está seguro de qué configuración de permisos debe utilizar, contacte con su equipo de TI para obtener ayuda.

Ya tengo acceso a AWS a través del portal de acceso de AWS administrado por mi empleador

Inicie sesión en AWS a través del portal de acceso de AWS. Si su administrador de la nube le ha concedido permisos `PowerUserAccess` (desarrollador), verá las Cuentas de AWS a las que tiene acceso y su conjunto de permisos. Junto al nombre de su conjunto de permisos, verá las opciones para acceder a las cuentas de forma manual o programática mediante ese conjunto de permisos.

Ya tengo acceso a AWS a través de un proveedor de identidades federado administrado por mi empleador

Contacte con su equipo de TI para obtener ayuda.

Paso 2: recopilación de la información de IAM Identity Center

Tras acceder a AWS, recopile la información que este contiene realizando lo siguiente:

1. Recopilación de los valores `SSO Start URL` y `SSO Region` que necesita para ejecutar `aws configure sso`

   a. En el portal de acceso de AWS, seleccione el conjunto de permisos que utiliza para el desarrollo y seleccione el enlace Claves de acceso.

   b. En el cuadro de diálogo Obtener credenciales, elija la pestaña que coincida con su sistema operativo.

   c. Elija el método de credenciales de IAM Identity Center para obtener los valores `SSO Start URL` y `SSO Region`.

2. Como alternativa, a partir de la versión 2.22.0, puede utilizar la nueva URL del emisor en lugar de la URL de inicio. La URL del emisor se ubica en la consola de AWS IAM Identity Center en una de las siguientes ubicaciones:
   - En la página del panel, la URL del emisor aparece en el resumen de la configuración.
   - En la página de configuración, la URL del emisor se encuentra en los ajustes del origen de identidad.
3. Para obtener información sobre qué ámbitos se deben registrar, consulte Ámbitos de acceso de OAuth 2.0 en la Guía del usuario del IAM Identity Center.

Paso 3: creación de buckets de Amazon S3

Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.

Para este tutorial, cree algunos buckets que pueda recuperar más tarde en una lista.

Paso 4: Instalar la AWS CLI

Para instalar la AWS CLI, siga las instrucciones de su sistema operativo. Para obtener más información, consulte the section called “Instalar o actualizar”.

Una vez instalada, puede verificar la instalación abriendo el terminal que prefiera y ejecutando el siguiente comando. Debería aparecer la versión instalada de la AWS CLI.

```
$ aws --version
```

Paso 5: configuración del perfil de la AWS CLI

Configure su perfil con uno de los siguientes métodos.

Configurar el perfil con el asistente de **`aws configure sso`**

La sección `sso-session` del archivo `config` se usa para agrupar las variables de configuración para adquirir los tokens de acceso SSO, que luego se pueden usar para adquirir credenciales de AWS. Se utilizan las siguientes configuraciones:

- (Obligatorio) `sso_start_url`
- (Obligatorio) `sso_region`
- `sso_account_id`
- `sso_role_name`
- `sso_registration_scopes`

Defina una sección `sso-session` y asóciela a un perfil. Los ajustes de `sso_start_url` y `sso_region` se deben definir dentro de la sección `sso-session`. Normalmente, `sso_account_id` y `sso_role_name` deben establecerse en la sección `profile` para que el SDK pueda solicitar las credenciales de SSO.

En el siguiente ejemplo se configura el SDK para que solicite credenciales de SSO y admita la actualización automática de tokens:

```
$ aws configure sso
SSO session name (Recommended): my-sso
SSO start URL [None]: https://my-sso-portal.awsapps.com/start
SSO region [None]: us-east-1
SSO registration scopes [None]: sso:account:access
```

La autorización de la clave de prueba para el intercambio de códigos (PKCE) se utiliza de forma predeterminada para la AWS CLI a partir de la versión 2.22.0 y se debe utilizar en dispositivos con navegador. Para seguir utilizando la autorización de dispositivos, agregue la opción `--use-device-code`.

```
$ aws configure sso --use-device-code
```

Configuración manual mediante el archivo **`config`**

La sección `sso-session` del archivo `config` se usa para agrupar las variables de configuración para adquirir los tokens de acceso SSO, que luego se pueden usar para adquirir credenciales de AWS. Se utilizan las siguientes configuraciones:

- (Obligatorio) sso_start_url
- (Obligatorio) sso_region
- sso_account_id
- sso_role_name
- sso_registration_scopes

Defina una sección `sso-session` y asóciela a un perfil. `sso_region` y`sso_start_url` deben establecerse en la sección `sso-session`. Normalmente, `sso_account_id` y `sso_role_name` deben establecerse en la sección `profile` para que el SDK pueda solicitar las credenciales de SSO.

En el siguiente ejemplo se configura el SDK para que solicite credenciales de SSO y admita la actualización automática de tokens:

```
[profile my-dev-profile]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = SampleRole

[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_registration_scopes = sso:account:access
```

El token de autenticación se almacena en caché en el disco en el directorio `~/.aws/sso/cache` con un nombre de archivo basado en el nombre de la sesión.

Paso 6: inicio de sesión en IAM Identity Center

> **Note**
>
> El proceso de inicio de sesión puede pedirle que permita que la AWS CLI acceda a sus datos. Dado que la AWS CLI se ha creado con el SDK para Python, los mensajes de permiso pueden contener variaciones del nombre `botocore`.

Para recuperar y almacenar en caché las credenciales de IAM Identity Center, ejecute el siguiente comando de la AWS CLI para abrir su navegador predeterminado y compruebe que ha iniciado sesión en IAM Identity Center.

```
$ aws sso login --profile my-dev-profile
```

A partir de la versión 2.22.0, la autorización de la PKCE es la predeterminada. Para usar la autorización del dispositivo para iniciar sesión, agregue la opción `--use-device-code`.

```
$ aws sso login --profile my-dev-profile --use-device-code
```

Paso 7: ejecución de comandos de Amazon S3

Para generar una lista de los buckets que creó anteriormente, utilice el comando `aws s3 ls`. En el siguiente ejemplo se enumeran todos los buckets de Amazon S3.

```
$ aws s3 ls
2018-12-11 17:08:50 my-bucket
2018-12-14 14:55:44 my-bucket2
```

Paso 8: cierre de sesión en IAM Identity Center

Cuando haya terminado de utilizar su perfil de IAM Identity Center, ejecute el siguiente comando para eliminar las credenciales almacenadas en caché.

```
$ aws sso logout
Successfully signed out of all SSO profiles.
```

Paso 9: eliminación de recursos

Cuando termine este tutorial, elimine todos los recursos que haya creado durante el tutorial y que ya no necesite, incluidos los buckets de Amazon S3.

Solución de problemas

Si tiene problemas con la AWS CLI, consulte the section called “Errores de solución de problemas” para ver los pasos comunes de solución de problemas.

Recursos adicionales

Los recursos adicionales son los siguientes.

- the section called “Conceptos de IAM Identity Center”
- the section called “Autenticación del Centro de identidades de IAM”
- the section called “Instalar o actualizar”
- the section called “Opciones de configuración”
- `aws configure sso` en la AWS CLI version 2 Reference
- `aws configure sso-session` en la AWS CLI version 2 Reference
- `aws sso login` en la AWS CLI version 2 Reference
- `aws sso logout` en la AWS CLI version 2 Reference
- Setting up to use the AWS CLI with CodeCatalyst en la Guía del usuario de Amazon CodeCatalyst
- Ámbitos de acceso de OAuth 2.0 en la Guía del usuario del IAM Identity Center
- Tutoriales de introducción en la Guía del usuario del IAM Identity Center

Autenticación con credenciales a corto plazo para la AWS CLI

Recomendamos configurar el SDK o la herramienta para utilizar la autenticación del Centro de identidades de IAM con opciones de duración de sesión ampliada. Sin embargo, puede copiar y utilizar las credenciales temporales que están disponibles en el portal de acceso de AWS. Las credenciales nuevas deberán copiarse cuando caduquen. Puede utilizar las credenciales temporales en un perfil o como valores para las propiedades del sistema y las variables de entorno.

1. Inicie sesión en el portal de acceso de AWS.
2. Siga estas instrucciones para copiar las credenciales del rol de IAM desde el portal de acceso de AWS.

    1. Para el paso 2 de las instrucciones vinculadas, elija la cuenta de AWS y el nombre del rol de IAM que le concede acceso para sus necesidades de desarrollo. Este rol suele tener un nombre como PowerUserAccess o Developer.
    2. Para el paso 4, seleccione la opción Agregar un perfil al archivo de credenciales de AWS y copie el contenido.

3. Cree o abra el archivo `credentials` compartido. Este archivo es `~/.aws/credentials` en sistemas Linux y macOS y `%USERPROFILE%\.aws\credentials` en Windows. Para obtener más información, consulte the section called “Opciones de configuración”.
4. Agregue el siguiente texto al archivo `credentials` compartido. Reemplace los valores de ejemplo por las credenciales que ha copiado.

```
[default]
aws_access_key_id = AKIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
aws_session_token =
 IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZVERYLONGSTRINGEXAMPLE
```

5. Agregue la región y el formato predeterminados que prefiera al archivo compartido `config`.

```
[default]
region=us-west-2
output=json

[profile user1]
region=us-east-1
output=text
```

Cuando el SDK cree un cliente de servicio, accederá a estas credenciales temporales y las utilizará para cada solicitud. La configuración del rol de IAM elegido en el paso 2a determina el tiempo de validez de las credenciales temporales. La duración máxima es de doce horas.

Repita estos pasos cada vez que caduquen las credenciales.

Uso de un rol de IAM de la AWS CLI

Un rol de AWS Identity and Access Management (IAM) es una herramienta de autorización que permite a un usuario conseguir permisos adicionales o distintos, u obtener permisos para realizar acciones en otra cuenta de AWS.

Temas

- Requisitos previos
- Información general del uso de roles de IAM
- Configuración y uso de un rol

- Uso de la autenticación multifactor
- Roles entre cuentas e ID externo
- Especificación de un nombre de sesión de rol para simplificar las auditorías
- Adopción de un rol con una identidad web
- Borrado de las credenciales almacenadas en memoria caché

Requisitos previos

Para utilizar los comandos de `iam`, debe instalar y configurar AWS CLI. Esto incluye la configuración de un perfil definido, como asumir que un rol está combinado con otro método de credenciales. Para obtener más información, consulte the section called “Instalar o actualizar”.

Información general del uso de roles de IAM

Puede configurar la AWS Command Line Interface (AWS CLI) para utilizar un rol de IAM definiendo un perfil para dicho rol en el archivo `~/.aws/config`.

En el siguiente ejemplo se muestra un perfil de rol llamado `marketingadmin`. Si ejecuta comandos con `--profile marketingadmin` (o lo especifica con la variable de entorno AWS_DEFAULT_PROFILE), la AWS CLI utiliza las credenciales definidas en un perfil separado de `user1` para adoptar el rol con el nombre de recurso de Amazon (ARN) `arn:aws:iam::123456789012:role/marketingadminrole`. Puede ejecutar cualquier operación permitida por los permisos asignados a ese rol.

```
[profile marketingadmin]
role_arn = arn:aws:iam::123456789012:role/marketingadminrole
source_profile = user1
```

Debe especificar un `source_profile` que apunte a un perfil con nombre independiente que contenga credenciales de usuario con permiso para utilizar el rol. En el ejemplo anterior, el perfil `marketingadmin` utiliza las credenciales en el perfil `user1`. Al especificar que un comando de la AWS CLI debe utilizar el perfil `marketingadmin`, la AWS CLI busca automáticamente las credenciales del perfil `user1` vinculado y las utiliza para solicitar credenciales temporales para el rol de IAM especificado. La CLI usa la operación sts:AssumeRole en segundo plano para llevar esto a cabo. Estas credenciales temporales se utilizan para ejecutar el comando de la AWS CLI solicitado. El rol especificado debe tener políticas de permisos de IAM asociadas que permitan que el comando de la AWS CLI solicitado se ejecute.

Para ejecutar un comando AWS CLI desde una instancia Amazon Elastic Compute Cloud (Amazon EC2) o un contenedor de Amazon Elastic Container Service (Amazon ECS), puede utilizar un rol de IAM asociado al perfil de instancia o al contenedor. Si no especifica ningún perfil o no establece ninguna variable de entorno, ese rol se utiliza directamente. De este modo, puede evitar el almacenamiento de las claves de acceso de larga duración en las instancias. También puede utilizar esos roles de instancia o contenedor solo para obtener credenciales para otro rol. Para ello, utilice `credential_source` (en lugar de `source_profile`) para especificar cómo encontrar las credenciales. El atributo `credential_source` es compatible con los siguientes valores:

- `Environment`: recupera las credenciales fuente de las variables de entorno.
- `Ec2InstanceMetadata`: utiliza el rol de IAM asociado al perfil de instancia de Amazon EC2.
- `EcsContainer`: utiliza el rol de IAM adjunto al contenedor de Amazon ECS.

En el siguiente ejemplo, se muestra el mismo rol `marketingadminrole` que se utilizó al hacer referencia a un perfil de instancia de Amazon EC2:

```
[profile marketingadmin]
role_arn = arn:aws:iam::123456789012:role/marketingadminrole
credential_source = Ec2InstanceMetadata
```

Cuando invoca un rol, tiene otras opciones que puede exigir; por ejemplo, el uso de la autenticación multifactor y de un ID externo (que compañías de terceros utilizan para acceder a los recursos de sus clientes). También puede especificar nombres de sesión de roles únicos que puedan auditarse más fácilmente en registros AWS CloudTrail.

Configuración y uso de un rol

Cuando se ejecutan comandos utilizando un perfil que especifica un rol de IAM, la AWS CLI emplea las credenciales del perfil fuente para llamar a AWS Security Token Service (AWS STS) y solicitar credenciales temporales para el rol especificado. El usuario del perfil fuente debe tener permiso para llamar a `sts:assume-role` en el rol del perfil especificado. El rol debe tener una relación de confianza que permita al usuario del perfil de origen utilizarlo. El proceso de recuperación y posterior uso de credenciales temporales en un rol a menudo se denomina asumir el rol.

Puede crear un rol en IAM con los permisos que quiera que adopten los usuarios siguiendo el procedimiento de Creación de un rol para delegar permisos a un usuario de IAM de la Guía del usuario de AWS Identity and Access Management. Si el rol y el usuario de del perfil de origen se

encuentran en la misma cuenta, puede introducir su propio ID de cuenta al configurar la relación de confianza del rol.

Después de crear el rol, modifique la relación de confianza para permitir que el usuario de lo asuma.

En el siguiente ejemplo se muestra una política de confianza que puede asociarse a un rol. Esta política permite asumir el rol a cualquier usuario de la cuenta 123456789012, si el administrador de dicha cuenta le concede de forma explícita el permiso `sts:AssumeRole`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

La política de confianza no concede permisos. El administrador de la cuenta debe delegar el permiso para asumir el rol a usuarios individuales asociando una política a los permisos adecuados. En el siguiente ejemplo, se muestra una política que puede asociarse a un usuario y que le permite asumir únicamente el rol `marketingadminrole`. Para obtener más información acerca de cómo conceder permisos de acceso a los usuarios para asumir un rol, consulte Conceción de permisos de usuario para cambiar de rol en la Guía del usuario de IAM.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
```

```
      "Resource": "arn:aws:iam::123456789012:role/marketingadminrole"
    }
  ]
}
```

El usuario no necesita permisos adicionales para ejecutar los comandos de la AWS CLI con el perfil del rol. En cambio, los permisos para ejecutar el comando proceden de los asociados al rol. Puede asociar políticas de permisos al rol para especificar qué acciones pueden realizarse en relación con qué recursos de AWS. Para obtener más información acerca de cómo asociar permisos a un rol (que funciona exactamente igual que para un usuario), consulte Cambio de permisos de un usuario de IAM en la Guía del usuario de IAM.

Ahora que ya tiene el perfil del rol, los permisos del rol, la relación de confianza del rol y los permisos de usuario configurados correctamente, puede utilizar el rol en la línea de comandos invocando la opción `--profile`. Por ejemplo, el siguiente comando llama al comando Amazon S3 de `ls` utilizando los permisos adjuntos al rol `marketingadmin` que se definieron en el ejemplo que se incluye al principio de este tema.

```
$ aws s3 ls --profile marketingadmin
```

Si desea utilizar el rol para varias llamadas, puede configurar la variable de entorno `AWS_PROFILE` para la sesión actual desde la línea de comandos. Siempre que esa variable de entorno se haya definido, no será necesario especificar la opción `--profile` en cada comando.

Linux o macOS

```
$ export AWS_PROFILE=marketingadmin
```

Windows

```
C:\> setx AWS_PROFILE marketingadmin
```

Para obtener información acerca de la configuración de los usuarios y los roles, consulte Identidades de IAM (usuarios, grupos y roles) y Roles de IAM en la Guía del usuario de IAM.

Uso de la autenticación multifactor

Para mayor seguridad, puede pedir a los usuarios que proporcionen una clave única generada a partir de un dispositivo de autenticación multifactor (MFA), un dispositivo U2F o una aplicación móvil cuando realicen una llamada utilizando el perfil del rol.

En primer lugar, puede elegir modificar la relación de confianza del rol de IAM para el que se requiere MFA. Esto impide que una persona utilice el rol sin autenticarse primero mediante MFA. A modo de ejemplo, vea la línea `Condition` en el siguiente ejemplo. Esta política permite a un usuario llamado `anika` adoptar el rol asociado a la política, pero solo si se autentica mediante MFA.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam::123456789012:user/anika" },
      "Action": "sts:AssumeRole",
      "Condition": { "Bool": { "aws:multifactorAuthPresent": true } }
    }
  ]
}
```

A continuación, agregue una línea al perfil del rol que especifique el ARN del dispositivo MFA del usuario. El siguiente archivo `config` de ejemplo muestra dos perfiles de rol que utilizan las claves de acceso del usuario `anika` para solicitar credenciales temporales para el rol `cli-role`. El usuario `anika` tiene permisos para asumir el rol, concedidos por la política de confianza del rol.

```
[profile role-without-mfa]
region = us-west-2
role_arn= arn:aws:iam::128716708097:role/cli-role
source_profile=cli-user

[profile role-with-mfa]
region = us-west-2
role_arn= arn:aws:iam::128716708097:role/cli-role
```

```
source_profile = cli-user
mfa_serial = arn:aws:iam::128716708097:mfa/cli-user

[profile cli-user]
region = us-west-2
output = json
```

El valor `mfa_serial` puede ser un ARN, tal como se muestra, o el número de serie de un token de MFA de hardware.

El primer perfil, `role-without-mfa`, no requiere MFA. Sin embargo, como la política de confianza asociada al rol del ejemplo anterior requiere MFA, cualquier intento de ejecutar un comando con este perfil produce un error.

```
$ aws iam list-users --profile role-without-mfa

An error occurred (AccessDenied) when calling the AssumeRole operation: Access denied
```

La segunda entrada del perfil, `role-with-mfa`, identifica el dispositivo MFA que se va a utilizar. Cuando el usuario intenta ejecutar un comando de la AWS CLI con este perfil, la AWS CLI le pide al usuario que introduzca la contraseña de un solo uso (OTP) proporcionada a través del dispositivo MFA. Si la autenticación MFA se realiza correctamente, el comando realiza la operación solicitada. La OTP no se muestra en la pantalla.

```
$ aws iam list-users --profile role-with-mfa
Enter MFA code for arn:aws:iam::123456789012:mfa/cli-user:
{
    "Users": [
        {
            ...
```

Roles entre cuentas e ID externo

Puede permitir que los usuarios de utilicen roles que pertenezcan a diferentes cuentas si configura el rol como un rol entre cuentas. Al crear un rol, establezca el tipo de rol en Another AWS account (Otra cuenta de), tal como se describe en Creating a Role to Delegate Permissions to an IAM user (Creación de un rol para delegar permisos a un usuario de IAM). Si lo desea, seleccione Require MFA (Requerir MFA). La opción Require MFA (Requerir NFA) configura la condición apropiada en la relación de confianza, tal y como se describe en Uso de la autenticación multifactor.

Si utiliza un ID externo para ofrecer mayor control sobre quién puede utilizar un rol entre cuentas, también debe añadir el parámetro `external_id` al perfil del rol. Esto se utiliza normalmente solo cuando la otra cuenta la controla alguien ajeno a su empresa u organización.

```
[profile crossaccountrole]
role_arn = arn:aws:iam::234567890123:role/SomeRole
source_profile = default
mfa_serial = arn:aws:iam::123456789012:mfa/saanvi
external_id = 123456
```

Especificación de un nombre de sesión de rol para simplificar las auditorías

Cuando muchas personas comparten un rol, la auditoría se convierte en un desafío más. Deseará asociar cada operación invocada con la persona que invocó la acción. Sin embargo, cuando la persona utiliza un rol, la asunción del rol por parte de la persona es una acción independiente de la invocación de una operación y debe relacionar manualmente las dos.

Puede simplificar este proceso especificando nombres de sesión de rol únicos cuando los usuarios asumen un rol. Para ello, añada un parámetro `role_session_name` a cada perfil con nombre en el archivo `config` que especifica un rol. El valor `role_session_name` se pasa a la operación `AssumeRole` y pasa a formar parte del ARN de la sesión de rol. También se incluye en los registros de AWS CloudTrail de todas las operaciones registradas.

Por ejemplo, podría crear un perfil basado en roles de la siguiente manera.

```
[profile namedsessionrole]
role_arn = arn:aws:iam::234567890123:role/SomeRole
source_profile = default
role_session_name = Session_Maria_Garcia
```

De este modo, la sesión del rol tendría el siguiente ARN.

```
arn:aws:iam::234567890123:assumed-role/SomeRole/Session_Maria_Garcia
```

Además, todos los registros de AWS CloudTrail incluyen el nombre de la sesión del rol en la información obtenida para cada operación.

Adopción de un rol con una identidad web

Puede configurar un perfil para indicar que la AWS CLI debe asumir un rol mediante la identidad federada web y Open ID Connect (OIDC). Al especificar esto en un perfil, la AWS CLI realiza automáticamente la llamada a AWS STS de `AssumeRoleWithWebIdentity` correspondiente.

> **Note**
>
> Cuando especifica un perfil que utiliza un rol de IAM, la AWS CLI realiza las llamadas correspondientes para recuperar las credenciales temporales. Estas credenciales se guardan en `~/.aws/cli/cache`. Los comandos de la AWS CLI posteriores que especifican el mismo perfil utilizan las credenciales temporales almacenadas en caché hasta que caducan. En ese momento, la AWS CLI actualiza automáticamente las credenciales.

Para recuperar y utilizar credenciales temporales utilizando identidades federadas web, puede especificar los siguientes valores de configuración en un perfil compartido:

role_arn

Especifica el ARN del rol que se va a adoptar.

web_identity_token_file

Especifica la ruta a un archivo que contiene un token de acceso de OAuth 2.0 o un ID de token de OpenID Connect proporcionado por el proveedor de identidad. La AWS CLI carga este archivo y pasa su contenido como el argumento `WebIdentityToken` de la operación `AssumeRoleWithWebIdentity`.

role_session_name

Especifica un nombre opcional que se aplica a esta sesión de asunción de rol.

A continuación, se muestra un ejemplo de la configuración mínima necesaria para configurar un rol de adopción con un perfil de identidad web:

```
# In ~/.aws/config

[profile web-identity]
role_arn=arn:aws:iam:123456789012:role/RoleNameToAssume
```

```
web_identity_token_file=/path/to/a/token
```

También puede establecer esta configuración utilizando variables de entorno:

AWS_ROLE_ARN

ARN del rol que se va a adoptar.

AWS_WEB_IDENTITY_TOKEN_FILE

La ruta al archivo de token de identidad web.

AWS_ROLE_SESSION_NAME

El nombre aplicado a esta sesión de asunción de rol.

> **Note**
>
> Actualmente, estas variables de entorno solo se aplican al rol que se va a adoptar con un proveedor de identidades web. No se aplican a la configuración general del proveedor de roles de adopción.

Borrado de las credenciales almacenadas en memoria caché

Al utilizar un rol, la AWS CLI almacena en caché localmente las credenciales temporales hasta que caducan. La próxima vez que intente utilizarlas, la AWS CLI intentará renovarlas en su nombre.

Si las credenciales temporales del rol se revocan, no se renuevan automáticamente y se producirá un error al intentar utilizarlas. Sin embargo, puede eliminar la caché para obligar a la AWS CLI a que recupere nuevas credenciales.

Linux o macOS

```
$ rm -r ~/.aws/cli/cache
```

Windows

```
C:\> del /s /q %UserProfile%\.aws\cli\cache
```

Autenticación con credenciales de usuario de IAM para la AWS CLI

> **Warning**
>
> Para evitar riesgos de seguridad, no utilice a los usuarios de IAM para la autenticación cuando desarrolle software especialmente diseñado o trabaje con datos reales. En cambio, utilice la federación con un proveedor de identidades como AWS IAM Identity Center.

En esta sección se explica cómo configurar las opciones básicas con un usuario de IAM. Entre ellas se incluyen sus credenciales de seguridad con los archivos `config` y `credentials`. En su lugar, consulte las instrucciones de configuración para AWS IAM Identity Center, consulte the section called "Autenticación del Centro de identidades de IAM".

Temas

- Paso 1: Crear el usuario de IAM
- Paso 2: Obtener las claves de acceso
- Paso 3: Configurar el AWS CLI
  - Uso de aws configure
  - Importación de claves de acceso mediante un archivo .CSV
  - Edición directa de los archivos config y credentials
- (Opcional) Uso de autenticación multifactor con las credenciales de usuario de IAM

Paso 1: Crear el usuario de IAM

Siga el procedimiento Creación de usuarios de IAM (consola) de la Guía del usuario de IAM para crear su usuario de IAM.

- Para Opciones de permiso, elija Adjuntar políticas directamente para indicar cómo desea asignar permisos a este usuario.
- La mayoría de los tutoriales del SDK "Introducción" utilizan el servicio Amazon S3 como ejemplo. Para proporcionar a su aplicación acceso completo a Amazon S3, seleccione la política `AmazonS3FullAccess` que desea asociar a este usuario.

Paso 2: Obtener las claves de acceso

1. Inicie sesión en Consola de administración de AWS y abra la consola IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la consola de IAM, seleccione Usuarios y, a continuación, seleccione el **`User name`** del usuario que creó anteriormente.
3. En la página del usuario, selecciona la página Credenciales de seguridad. A continuación, en Claves de acceso, seleccione Crear clave de acceso.
4. En el paso 1 de Crear clave de acceso, elija Interfaz de línea de comandos (CLI).
5. En el paso 2 de Crear clave de acceso, introduzca una etiqueta opcional y seleccione Siguiente.
6. En el paso 3 de Crear clave de acceso, seleccione Descargar archivo.csv para guardar un archivo `.csv` con la clave de acceso y la clave de acceso secreta de su usuario de IAM. Necesitará esta información más tarde.
7. Seleccione Done (Listo).

Paso 3: Configurar el AWS CLI

Para el uso general, AWS CLI necesita la siguiente información:

- ID de clave de acceso
- Clave de acceso secreta
- Región de AWS
- Formato de salida

La AWS CLI almacena esta información en un perfil (una colección de opciones) con el nombre `default` en el archivo `credentials`. De forma predeterminada, la información de este perfil se utiliza cuando se ejecuta un comando de la AWS CLI que no especifica explícitamente un perfil que se va a utilizar. Para obtener más información sobre el archivo `credentials`, consulte Opciones de los archivos de configuración y credenciales en la AWS CLI.

Utilice uno de los siguientes procedimientos para configurar la AWS CLI.

Temas

- Uso de aws configure
- Importación de claves de acceso mediante un archivo .CSV

- Edición directa de los archivos config y credentials

Uso de `aws configure`

Para el uso general, el comando `aws configure` es la forma más rápida de configurar la instalación de la AWS CLI. Este asistente de configuración le solicitará cada uno de los datos que necesita para empezar. A menos que se especifique lo contrario mediante el uso de la opción `--profile`, la AWS CLI almacena esta información en el perfil `default`.

En el siguiente ejemplo, se configura un perfil `default` con valores de ejemplo. Remplácelos con sus propios valores, tal y como se describe en las siguientes secciones.

```
$ aws configure
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
Default region name [None]: us-west-2
Default output format [None]: json
```

En el siguiente ejemplo, se configura un perfil denominado `userprod` con valores de ejemplo. Remplácelos con sus propios valores, tal y como se describe en las siguientes secciones.

```
$ aws configure --profile userprod
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
Default region name [None]: us-west-2
Default output format [None]: json
```

Importación de claves de acceso mediante un archivo .CSV

En lugar de utilizar `aws configure` para ingresar las claves de acceso, puede importar el archivo `.csv` de texto sin formato que descargó después de crear sus claves de acceso.

El archivo `.csv` debe contener los siguientes encabezados.

- Nombre de usuario: esta columna debe añadirse a su `.csv`. Se usa para crear el nombre del perfil utilizado en los archivos `config` y `credentials` al importar.
- ID de clave de acceso
- Clave de acceso secreta

> **Note**
>
> Durante la creación de las claves de acceso iniciales, una vez que cierre el cuadro de diálogo Descargar archivo .csv), no puede acceder a la clave de acceso secreta después de cerrar el cuadro de diálogo. Si necesita un archivo `.csv`, tendrá que crearlo con los encabezados necesarios y la información de sus claves de acceso almacenadas. Si no tiene acceso a la información sobre sus claves de acceso, deberá crear nuevas claves de acceso.

Para importar el archivo `.csv`, utilice el comando `aws configure import` con la opción `--csv` de la siguiente manera:

```
$ aws configure import --csv file://credentials.csv
```

Para obtener más información, consulte `aws_configure_import`.

Edición directa de los archivos **`config`** y **`credentials`**

Para editar directamente los archivos `config` y `credentials`, realice lo siguiente.

1. Cree o abra el archivo `credentials` de AWS compartido. Este archivo es `~/.aws/credentials` en sistemas Linux y macOS y `%USERPROFILE%\.aws\credentials` en Windows. Para obtener más información, consulte the section called “Opciones de configuración”.
2. Agregue el siguiente texto al archivo `credentials` compartido. Sustituya los valores de ejemplo del archivo `.csv` que descargó anteriormente y guarde el archivo.

   ```
   [default]
   aws_access_key_id = AKIAIOSFODNN7EXAMPLE
   aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
   ```

(Opcional) Uso de autenticación multifactor con las credenciales de usuario de IAM

Para mayor seguridad, puede usar una clave única generada a partir de un dispositivo de autenticación multifactor (MFA), un dispositivo U2F o una aplicación móvil cuando intente realizar una llamada.

Con el usuario de IAM habilitado para MFA, ejecute el comando `aws configure mfa-login` para configurar un nuevo perfil para usarlo con la autenticación multifactor (MFA) para el perfil especificado. Si no se especifica ningún perfil, la MFA se basa en el perfil `default`. Si no hay ningún perfil predeterminado configurado, el comando `mfa-login` le solicitará las credenciales de AWS antes de solicitar su información de MFA. En el ejemplo de comando siguiente, se usa la configuración predeterminada y se crea un perfil de MFA.

```
$ aws configure mfa-login
MFA serial number or ARN: arn:aws:iam::123456789012:mfa/MFADeviceName
MFA token code: 123456
Profile to update [session-MFADeviceName]:
Temporary credentials written to profile 'session-MFADeviceName'
Credentials will expire at 2023-05-19 18:06:10 UTC
To use these credentials, specify --profile session-MFADeviceName when running AWS CLI
 commands
```

Para actualizar un perfil existente, utilice el parámetro `--update-profile`.

```
$ aws configure mfa-login --profile myprofile --update-profile mfaprofile
MFA token code: 123456
Temporary credentials written to profile 'mfaprofile'
Credentials will expire at 2023-05-19 18:06:10 UTC
To use these credentials, specify --profile mfaprofile when running AWS CLI commands
```

Este comando actualmente solo admite hardware o software basado en autenticadores de contraseña de un solo uso (OTP). Actualmente, este comando no admite claves de acceso ni dispositivos U2F.

Para usar el perfil de MFA, use la opción `--profile` con los comandos.

```
$ aws s3 ls --profile mfaprofile
```

Para obtener más información sobre el uso de MFA con IAM, incluido cómo asignar MFA a un usuario de IAM, consulte Autenticación multifactor de AWS en IAM en la Guía del usuario de AWS Identity and Access Management.

Uso de metadatos de instancias de Amazon EC2 como credenciales en la AWS CLI

Cuando ejecuta la AWS CLI desde la instancia de Amazon Elastic Compute Cloud (Amazon EC2), puede simplificar el suministro de credenciales a sus comandos. Cada instancia de Amazon EC2 contiene metadatos que la AWS CLI puede consultar directamente para comprobar la existencia de credenciales temporales. Cuando se asocia un rol de IAM a la instancia, la AWS CLI recupera automáticamente y de forma segura las credenciales de los metadatos de la instancia.

Para deshabilitar este servicio, utilice la variable de entorno AWS_EC2_METADATA_DISABLED.

Temas

- Requisitos previos
- Configuración de un perfil para metadatos de Amazon EC2

Requisitos previos

Para usar credenciales de Amazon EC2 con la AWS CLI, debe completar lo siguiente:

- Instalar y configurar la AWS CLI. Para obtener más información, consulte the section called “Instalar o actualizar” y Credenciales de autenticación y acceso para la AWS CLI.
- Comprende los archivos de configuración y los perfiles con nombre. Para obtener más información, consulte Opciones de los archivos de configuración y credenciales en la AWS CLI.
- Ha creado un rol AWS Identity and Access Management (IAM) que tiene acceso a los recursos necesarios y ha asociado ese rol a la instancia de Amazon EC2 al lanzarla. Para obtener más información, consulte Políticas de IAM para Amazon EC2 en la Guía del usuario de Amazon EC2 y Concesión de acceso a aplicaciones que ejecutan instancias Amazon EC2 a los Recursos de AWS en la Guía del usuario de IAM.

Configuración de un perfil para metadatos de Amazon EC2

Para especificar que desea utilizar las credenciales disponibles en el perfil de instancia de Amazon EC2 de alojamiento, utilice la sintaxis siguiente en el perfil con nombre del archivo de configuración. Para obtener instrucciones adicionales, consulte estos pasos a continuación.

```
[profile profilename]
```

```
role_arn = arn:aws:iam::123456789012:role/rolename
credential_source = Ec2InstanceMetadata
region = region
```

1. Cree un perfil en su archivo de configuración.

   ```
   [profile profilename]
   ```

2. Agregue su rol arn de IAM que tenga acceso a los recursos necesarios.

   ```
   role_arn = arn:aws:iam::123456789012:role/rolename
   ```

3. Especifique `Ec2InstanceMetadata` como fuente de credenciales.

   ```
   credential_source = Ec2InstanceMetadata
   ```

4. Establezca su región.

   ```
   region = region
   ```

Ejemplo

El siguiente ejemplo presupone el rol *marketingadminrole* y utiliza la región *us-west-2* en un perfil de instancia de Amazon EC2 denominado *marketingadmin*.

```
[profile marketingadmin]
role_arn = arn:aws:iam::123456789012:role/marketingadminrole
credential_source = Ec2InstanceMetadata
region = us-west-2
```

Obtención de credenciales con un proceso externo en la AWS CLI

> **Warning**
>
> En el siguiente tema, se explica cómo se obtienen credenciales desde un proceso externo. Esto puede suponer un riesgo para la seguridad si el comando que genera las credenciales llega a estar accesible para usuarios o procesos no aprobados. Se recomienda utilizar las alternativas seguras y compatibles ofrecidas por la AWS CLI y AWS para reducir el riesgo de

que las credenciales se vean comprometidas. Asegúrese de proteger el archivo `config` y todos los archivos auxiliares y herramientas para evitar su divulgación.
Asegúrese de que la herramienta de credenciales personalizada no escriba ninguna información secreta en `StdErr`, ya que los SDK y la AWS CLI pueden capturar y registrar dicha información y podrían mostrarla a usuarios no autorizados.

Si tiene un método para generar o buscar credenciales que no sea directamente compatible con la AWS CLI, puede configurar la AWS CLI para usarla configurando el ajuste de `credential_process` en el archivo `config`.

Por ejemplo, puede incluir una entrada similar a la siguiente en el archivo `config`:

```
[profile developer]
credential_process = /opt/bin/awscreds-custom --username helen
```

Sintaxis

Para crear esta cadena de forma que sea compatible con cualquier sistema operativo, siga estas reglas:

- Si la ruta de acceso o el nombre del archivo contienen un espacio, rodee la ruta completa y el nombre del archivo con comillas dobles (" "). La ruta y el nombre de archivo solo pueden constar de los caracteres: A-Z a-z 0-9 - _ . espacio
- Si un nombre de parámetro o un valor de parámetro contienen un espacio, rodee ese elemento con comillas dobles (" "). Incluya solo el nombre o el valor, no el par.
- No incluya ninguna variable de entorno en las cadenas. Por ejemplo, no puede incluir `$HOME` ni `%USERPROFILE%`.
- No especifique la carpeta de inicio como ~. Debe especificar la ruta completa.

Ejemplo para Windows

```
credential_process = "C:\Path\To\credentials.cmd" parameterWithoutSpaces "parameter
 with spaces"
```

Ejemplo para Linux o macOS

```
credential_process = "/Users/Dave/path/to/credentials.sh" parameterWithoutSpaces
 "parameter with spaces"
```

Salida prevista del programa Credentials

La AWS CLI ejecuta el comando tal y como se especifica en el perfil y, a continuación, lee datos de STDOUT. El comando que especifique debe generar una salida JSON en STDOUT que se ajuste a la siguiente sintaxis.

```
{
  "Version": 1,
  "AccessKeyId": "an AWS access key",
  "SecretAccessKey": "your AWS secret access key",
  "SessionToken": "the AWS session token for temporary credentials",
  "Expiration": "ISO8601 timestamp when the credentials expire"
}
```

> **Note**
>
> En la fecha de publicación del presente documento, la clave `Version` debe establecerse en 1. Puede aumentar con el paso del tiempo a medida que la estructura evolucione.

La clave `Expiration` es una marca temporal con formato ISO8601. Si la clave `Expiration` no está presente en la salida de la herramienta, la CLI da por hecho que las credenciales son credenciales a largo plazo que no se actualizan. De otro modo, las credenciales se consideran credenciales temporales y se actualizan automáticamente volviendo a ejecutar el comando `credential_process` antes de que caduquen.

> **Note**
>
> La AWS CLI no almacena en caché credenciales de procesos externos de la forma que lo hace con las credenciales de asunción de rol. Si se requiere el almacenamiento en caché, debe implementarlo en el proceso externo.

El proceso externo puede devolver un código de devolución distinto de cero para indicar que se ha producido un error al intentar recuperar las credenciales.

Uso de AWS CLI

En esta sección se proporciona una descripción general completa del uso general, las características comunes y las opciones disponibles en la AWS Command Line Interface (AWS CLI), además de lo que figura en la sección de configuración the section called “puntos de conexión”.

Esta guía profundiza en los aspectos fundamentales de la escritura de comandos de la AWS CLI, incluida su estructura básica, el formato y las capacidades de filtrado. Al conocer estos elementos básicos, podrá crear comandos que se dirijan con precisión a los recursos y las acciones que necesita, sin necesidad de navegar por complejas consolas basadas en la web.

Además, aquí se destacan el contenido de ayuda y la documentación disponibles para la AWS CLI. Desde la ayuda de línea de comandos integrada hasta la completa guía de referencia de la versión 2 de la AWS CLI, tendrá acceso a información que le ayudará a explorar las características y capacidades de la AWS CLI.

Para ver ejemplos específicos del Servicio de AWS, consulte Ejemplos de AWS CLI en la guía de referencia de la versión 2 de la AWS CLI. Proporcionan información específica sobre los comandos y muestran ejemplos sobre cómo aprovechar la AWS CLI para varios Servicios de AWS.

> **Note**
>
> De forma predeterminada, la AWS CLI envía solicitudes a Servicios de AWS mediante HTTPS en el puerto TCP 443. Para utilizar la AWS CLI correctamente, debe poder realizar conexiones salientes en este puerto.

Temas de esta guía

- Acceso a la ayuda y a los recursos para la AWS CLI
- Estructura de comandos en la AWS CLI
- Especificación de valores de parámetros en la AWS CLI
- Activación y uso de los símbolos del sistema en la AWS CLI
- Control de la salida de comandos en la AWS CLI
- Códigos de retorno de la línea de comandos en la AWS CLI
- Uso de asistentes personalizados para ejecutar comandos interactivos en la AWS CLI
- Creación y uso de alias en la AWS CLI

- Solución de errores para la AWS CLI

Acceso a la ayuda y a los recursos para la AWS CLI

En este tema, se describe cómo acceder al contenido de ayuda de AWS Command Line Interface (AWS CLI).

Temas

- El comando de ayuda de AWS CLI integrado
- Guía de referencia de AWS CLI
- Documentación de la API
- Solución de errores
- Ayuda adicional

El comando de ayuda de AWS CLI integrado

Puede obtener ayuda para cualquier comando cuando utiliza la AWS Command Line Interface (AWS CLI). Para ello, simplemente escriba `help` al final del nombre de un comando.

Por ejemplo, el siguiente comando muestra la ayuda de las opciones generales de la AWS CLI generales y los comandos de nivel superior.

```
$ aws help
```

El comando siguiente muestra los comandos específicos de Amazon Elastic Compute Cloud (Amazon EC2) disponibles.

```
$ aws ec2 help
```

En el siguiente ejemplo se muestra información de ayuda detallada de la operación `DescribeInstances` de Amazon EC2. La ayuda incluye descripciones de los parámetros de entrada, los filtros disponibles y qué se incluye como salida. También incluye ejemplos que muestran cómo escribir variaciones comunes del comando.

```
$ aws ec2 describe-instances help
```

A partir de la versión `2.31.0` La visualización del comando `help` se configura mediante el ajuste `cli_help_output` y tiene los siguientes valores:

- (predeterminado) `terminal`: abra la página principal en el terminal.
- `browser`: abra la página principal como un archivo HTML local en el navegador predeterminado. Se imprime un aviso en el terminal cuando se abre el navegador predeterminado y un mensaje de error si la AWS CLI no puede abrir el navegador.
- `url`: imprima la URL de la guía de referencia de AWS CLI en línea de la versión de la AWS CLI que ha instalado. Se respetan los ajustes de la paginación del cliente, como la variable de entorno `AWS_PAGER`.

El contenido de ayuda de cada comando se divide en seis secciones:

Nombre

El nombre del comando.

```
NAME
       describe-instances -
```

Descripción

Una descripción de la operación de la API que el comando invoca.

```
DESCRIPTION
       Describes one or more of your instances.

       If you specify one or more instance IDs, Amazon EC2 returns information
       for those instances. If you do not specify  instance  IDs,  Amazon  EC2
       returns  information  for  all  relevant  instances.  If you specify an
       instance ID that is not valid, an error is returned. If you specify  an
       instance  that  you  do  not  own,  it  is not included in the returned
       results.
...
```

Sinopsis

La sintaxis básica para utilizar el comando y sus opciones. Si una opción aparece entre corchetes, significa que es opcional, que tiene un valor predeterminado o que existe una opción alternativa que puede utilizarse en su lugar.

```
SYNOPSIS
            describe-instances
          [--dry-run | --no-dry-run]
          [--instance-ids <value>]
          [--filters <value>]
          [--cli-input-json <value>]
          [--starting-token <value>]
          [--page-size <value>]
          [--max-items <value>]
          [--generate-cli-skeleton]
```

Por ejemplo, `describe-instances` tiene un comportamiento predeterminado que describe todas las instancias de la cuenta y la región de AWS actuales. Si lo desea, puede especificar una lista de `instance-ids` para describir una o varias instancias. `dry-run` es un indicador booleano opcional que no adopta ningún valor. Para utilizar un indicador booleano, especifique el valor aparece; en este caso, `--dry-run` o `--no-dry-run`. Del mismo modo, `--generate-cli-skeleton` no adopta un valor. Si existen condiciones para usar una opción, aparecen descritas en la sección `OPTIONS` o se muestran en los ejemplos.

Opciones

Una descripción de cada una de las opciones que aparecen en el resumen.

```
OPTIONS
       --dry-run | --no-dry-run (boolean)
          Checks whether you have the required  permissions  for  the  action,
          without actually making the request, and provides an error response.
          If you have the required permissions, the error response is  DryRun-
          Operation . Otherwise, it is UnauthorizedOperation .

       --instance-ids (list)
          One or more instance IDs.

          Default: Describes all your instances.
...
```

Ejemplos

Ejemplos que ilustran el uso del comando y sus opciones. Si no se proporciona un ejemplo de un comando o un caso de uso que necesite, solicítelo a través del enlace de comentarios de esta página o de la referencia de comandos de la AWS CLI en la página de ayuda del comando.

```
    EXAMPLES
    To describe an Amazon EC2 instance

    Command:

    aws ec2 describe-instances --instance-ids i-5203422c

    To describe all instances with the instance type m1.small

    Command:

    aws ec2 describe-instances --filters "Name=instance-type,Values=m1.small"

    To describe all instances with an Owner tag

    Command:

    aws ec2 describe-instances --filters "Name=tag-key,Values=Owner"
...
```

Output

Descripciones de cada uno de los campos y tipos de datos incluidos en la respuesta de AWS.

Para `describe-instances`, la salida es una lista de objetos de reserva, cada uno de los cuales contiene varios campos y objetos con información acerca de las instancias asociadas al mismo. Esta información procede de la documentación de la API para el tipo de datos de reserva que utiliza Amazon EC2.

```
OUTPUT
       Reservations -> (list)
          One or more reservations.

          (structure)
              Describes a reservation.

              ReservationId -> (string)
                 The ID of the reservation.

              OwnerId -> (string)
                 The ID of the AWS account that owns the reservation.

              RequesterId -> (string)
```

```
                The ID of the requester that launched the instances  on  your
                behalf (for example, AWS Management Console or Auto Scaling).

            Groups -> (list)
                One or more security groups.

                (structure)
                    Describes a security group.

                    GroupName -> (string)
                        The name of the security group.

                    GroupId -> (string)
                        The ID of the security group.

            Instances -> (list)
                One or more instances.

                (structure)
                    Describes an instance.

                    InstanceId -> (string)
                        The ID of the instance.

                    ImageId -> (string)
                        The ID of the AMI used to launch the instance.

                    State -> (structure)
                        The current state of the instance.

                        Code -> (integer)
                            The  low  byte represents the state. The high byte
                            is an opaque internal value and should be ignored.
...
```

Cuando la AWS CLI proporciona la salida en formato JSON, se convierte en una matriz de objetos de reserva, similar a la del siguiente ejemplo.

```
{
    "Reservations": [
        {
            "OwnerId": "012345678901",
            "ReservationId": "r-4c58f8a0",
```

```
            "Groups": [],
            "RequesterId": "012345678901",
            "Instances": [
                {
                    "Monitoring": {
                        "State": "disabled"
                    },
                    "PublicDnsName": "ec2-52-74-16-12.us-
west-2.compute.amazonaws.com",
                    "State": {
                        "Code": 16,
                        "Name": "running"
                    },
...
```

Cada objeto de reserva tiene campos que describen la reserva y una matriz de objetos de instancia, cada uno de ellos con sus propios campos (por ejemplo, `PublicDnsName`) y objetos (por ejemplo `State`) que los describen.

> **Usuarios de Windows**
>
> Puede añadir una barra vertical (|) a la salida del comando de ayuda al comando `more` para ver las páginas del archivo de ayuda una a una. Pulse la barra espaciadora o AvPág para avanzar por el documento y **q** para salir.
>
> ```
> C:\> aws ec2 describe-instances help | more
> ```

Guía de referencia de AWS CLI

Los archivos de ayuda contienen enlaces que no se pueden ver o visitar desde la línea de comandos. Puede consultar e interactuar con estos enlaces mediante la versión 2 de la guía de referencia de AWS CLI en línea. La referencia también tiene el contenido de la ayuda de todos los comandos de AWS CLI. Las descripciones se presentan para facilitar la navegación y la consulta en móviles, tabletas o equipos de escritorio.

Documentación de la API

Todos los comandos de la AWS CLI corresponden a solicitudes realizadas a la API pública de un servicio de AWS. Todos los servicios con una API pública tienen una referencia de API que puede

encontrarse en la página de inicio del servicio en el AWSsitio web Documentación de . El contenido de una referencia de API varía en función de cómo se construye la API y del protocolo utilizado. Normalmente, las referencias de API contienen información detallada sobre las acciones compatibles con la API, los datos enviados al servicio y desde este, y cualquier posible situación de error que pueda detectar el sistema.

Secciones de documentación de la API

- Acciones: información detallada de cada operación y sus parámetros (incluidas las restricciones de longitud o contenido, y valores predeterminados). Muestra los errores que pueden ocurrir con esta operación. Cada operación se corresponde con un subcomando de la AWS CLI.
- Tipos de datos: información detallada sobre las estructuras que un comando puede requerir como parámetro, o devolver en respuesta a una solicitud.
- Parámetros comunes: información detallada sobre los parámetros que utilizan todas las acciones de un servicio.
- Errores comunes: información detallada sobre los errores que cualquiera de las operaciones del servicio puede devolver.

El nombre y la disponibilidad de cada sección puede variar en función del servicio.

> **CLI específicas de los servicios**
>
> Algunos servicios tienen una CLI distinta que existía antes de que se creara una única AWS CLI para funcionar con todos los servicios. Las CLI específicas de los servicios tienen documentación aparte, a la que se accede con un enlace a la página de documentación del servicio. La documentación de las CLI específicas de los servicios no se aplica a AWS CLI.

Solución de errores

Para obtener ayuda a fin de diagnosticar y corregir errores de AWS CLI, consulte the section called “Errores de solución de problemas”.

Ayuda adicional

Para obtener ayuda adicional con sus problemas de AWS CLI, visite la Comunidad de AWS CLI en GitHub.

Estructura de comandos en la AWS CLI

En este tema se abordan cómo está estructurado el comando de la AWS Command Line Interface (AWS CLI) y cómo usar comandos de espera.

Temas

- Estructura de comandos
- Comandos de espera

Estructura de comandos

La AWS CLI utiliza una estructura de multiparte en la línea de comandos que deben especificarse en el siguiente orden:

1. La llamada base al programa de `aws`.
2. El comando de nivel superior, que normalmente corresponde a un servicio de AWS compatible con la AWS CLI.
3. El subcomando que especifica qué operación realizar.
4. Opciones o parámetros generales de la AWS CLI necesarios por la operación. Puede especificarlos en cualquier orden siempre que vayan detrás de las tres primeras partes. Si se especifica un parámetro exclusivo varias veces, solo se aplica el último valor.

```
$ aws <command> <subcommand> [options and parameters]
```

Los parámetros pueden tomar varios tipos de valores de entrada, como números, cadenas, listas, mapas y estructuras JSON. Los valores admitidos dependen del comando y los subcomandos que especifique.

Ejemplos

Amazon S3

En el siguiente ejemplo se enumeran todos los buckets de Amazon S3.

```
$ aws s3 ls
2018-12-11 17:08:50 amzn-s3-demo-bucket1
2018-12-14 14:55:44 amzn-s3-demo-bucket2
```

Para obtener más información acerca de los comandos de Simple Storage Service (Amazon S3), consulte `aws s3` en la Referencia de comandos de AWS CLI.

AWS CloudFormation

El siguiente ejemplo de comando `create-change-set` cambia el nombre de la pila de cloudformation a *`my-change-set`*.

```
$ aws cloudformation create-change-set --stack-name my-stack --change-set-name my-change-set
```

Para obtener más información acerca de los comandos de AWS CloudFormation, consulte `aws cloudformation` en la Referencia de comandos de AWS CLI.

Comandos de espera

Algunos servicios de AWS tienen comandos `wait` disponibles. Cualquier comando que use `aws wait` por lo general espera hasta que se completa un comando antes de ir al siguiente paso. Esto es especialmente útil para comandos multiparte o scripting, ya que puede utilizar un comando de espera para evitar pasar a pasos posteriores si el comando de espera falla.

La AWS CLI utiliza una estructura multiparte en la línea de comandos para el comando `wait` que debe especificarse en el siguiente orden:

1. La llamada base al programa de `aws`.
2. El comando de nivel superior, que normalmente corresponde a un servicio de AWS compatible con la AWS CLI.
3. El comando `wait`
4. El subcomando que especifica qué operación realizar.
5. Opciones o parámetros generales de la CLI necesarios por la operación. Puede especificarlos en cualquier orden siempre que vayan detrás de las tres primeras partes. Si se especifica un parámetro exclusivo varias veces, solo se aplica el último valor.

```
$ aws <command> wait <subcommand> [options and parameters]
```

Los parámetros pueden tomar varios tipos de valores de entrada, como números, cadenas, listas, mapas y estructuras JSON. Los valores admitidos dependen del comando y los subcomandos que especifique.

> **Note**
>
> No todos los servicios de AWS admiten comandos `wait`. Consulte la AWS CLIversión 2 de la guía de referencia de para ver si el servicio admite comandos `wait`.

Ejemplos

AWS CloudFormation

Los siguientes ejemplos de comandos `wait change-set-create-complete` se detienen y se reanudan solo después de que pueda confirmar que el conjunto de cambios *my-change-set* de la pila *my-stack* está listo para ejecutarse.

```
$ aws cloudformation wait change-set-create-complete --stack-name my-stack --change-set-name my-change-set
```

Para obtener más información acerca de los comandos `wait` de AWS CloudFormation, consulte `wait` en la Referencia de comandos de AWS CLI.

AWS CodeDeploy

Los ejemplos de comandos `wait deployment-successful` que se muestran a continuación se detienen hasta que se complete satisfactoriamente la implementación de *d-A1B2C3111*.

```
$ aws deploy wait deployment-successful --deployment-id d-A1B2C3111
```

Para obtener más información acerca de los comandos `wait` de AWS CodeDeploy, consulte `wait` en la Referencia de los comandos de AWS CLI.

Especificación de valores de parámetros en la AWS CLI

Muchos de los parámetros que se utilizan en AWS Command Line Interface (AWS CLI) son simples valores numéricos o de cadena, como el nombre del par de claves `my-key-pair` en el siguiente ejemplo de comando `aws ec2 create-key-pair`.

```
$ aws ec2 create-key-pair --key-name my-key-pair
```

El formato del comando puede variar entre terminales. Por ejemplo, la mayoría de los terminales distinguen entre mayúsculas y minúsculas, pero Powershell no distingue entre

mayúsculas y minúsculas. Esto significa que los dos ejemplos de comandos siguientes arrojarían resultados diferentes para los terminales que distinguen entre mayúsculas y minúsculas, ya que ven `MyFile*.txt` y `myfile*.txt` como parámetros diferentes.

Sin embargo, PowerShell procesaría estas solicitudes de la misma manera que ve `MyFile*.txt` y `myfile*.txt` como los mismos parámetros. En el siguiente ejemplo de comando se muestran estos parámetros con el comando `aws s3 cp`:

```
$ aws s3 cp . s3://amzn-s3-demo-bucket/path --include "MyFile*.txt"
$ aws s3 cp . s3://amzn-s3-demo-bucket/path --include "myfile*.txt"
```

Para obtener más información sobre no distinguir entre mayúsculas y minúsculas de casos en PowerShell, consulte about_Case-Sensitivity en la documentación de PowerShell.

A veces es necesario utilizar comillas o literales en las cadenas que incluyen caracteres especiales o de espacio. Las reglas en torno a este formato también pueden variar entre terminales. Para obtener más información sobre el uso de las comillas alrededor de parámetros complejos, consulte Entrecomillado de cadenas y uso de literales en la AWS CLI.

En estos temas se tratan las reglas de formato de terminal más habituales. Si tiene problemas para que su terminal reconozca los valores de los parámetros, asegúrese de revisar los temas de esta sección y también de consultar la documentación del terminal para conocer sus reglas de sintaxis específicas.

Temas de parámetros

- Tipos de parámetros comunes en la AWS CLI
- Entrecomillado de cadenas y uso de literales en la AWS CLI
- Carga de un parámetro de un archivo en la AWS CLI
- Esqueletos de la AWS CLI y archivos de entrada en la AWS CLI
- Uso de la sintaxis abreviada en la AWS CLI

Tipos de parámetros comunes en la AWS CLI

En esta sección, se describen algunos de los tipos de parámetros comunes y el formato requerido típico.

Si tiene problemas con el formato de un parámetro para un comando específico, compruebe la ayuda escribiendo **`help`** después del nombre del comando. La ayuda de cada subcomando incluye

el nombre y la descripción de una opción. El tipo de parámetro de la opción se muestra entre paréntesis. Para obtener más información acerca de obtener ayuda, consulte the section called "Obtención de ayuda".

Los tipos de parámetros incluyen:

- Cadena
- Timestamp
- Enumeración
- Booleano
- Entero
- Binario/blob (objeto binario grande) y blob en streaming
- Asignación
- Documento

Cadena

Los parámetros de cadena pueden contener caracteres alfanuméricos, símbolos y espacios en blanco del conjunto de caracteres ASCII. Las cadenas que contienen espacios en blanco se deben entrecomillar. Le recomendamos que no utilice símbolos ni espacios en blanco diferentes del carácter de espacio estándar, y que observe las reglas de entrecomillado del terminal para evitar resultados inesperados.

Algunos parámetros de cadena pueden aceptar datos binarios de un archivo. Consulte Archivos binarios para ver un ejemplo.

Timestamp

Las marcas temporales tienen un formato conforme a la norma ISO 8601. A menudo se conocen como parámetros "`DateTime`" o "`Date`".

```
$ aws ec2 describe-spot-price-history --start-time 2014-10-13T19:00:00Z
```

Los formatos aceptados son:

- *AAAA*-*MM*-*DD*T*hh*:*mm*:*ss.sssTZD (UTC)*, por ejemplo, 2014-10-01T20:30:00.000Z
- *AAAA*-*MM*-*DD*T*hh*:*mm*:*ss.sssTZD (con compensación)*, por ejemplo, 2014-10-01T12:30:00.000-08:00

- *AAAA*:*MM*:*DD*, por ejemplo, 2014-10-01
- Hora Unix en segundos; por ejemplo, 1412195400. Esto es lo que a veces se denomina fecha de inicio UNIX y representa el número de segundos desde la medianoche del 1 de enero de 1970 UTC.

De forma predeterminada, la versión 2 de la AWS CLI convierte todos los valores DateTime response al formato ISO 8601.

Puede establecer el formato de la marca de tiempo con el ajuste de archivo `cli_timestamp_format`.

Enumeración

Una o varias cadenas separadas por espacios. Si cualquiera de los elementos de cadena contiene un espacio, debe escribir dicho elemento entre comillas. Observe las normas de entrecomillado del terminal para evitar resultados inesperados

```
$ aws ec2 describe-spot-price-history --instance-types m1.xlarge m1.medium
```

Booleano

Marcador binario que activa o desactiva una opción. Por ejemplo, `ec2 describe-spot-price-history` tiene con un parámetro `--dry-run` booleano que, cuando se especifica, valida la consulta con el servicio sin ejecutar realmente una consulta.

```
$ aws ec2 describe-spot-price-history --dry-run
```

El resultado indica si el comando tenía el formato correcto o no. Este comando también incluye una versión `--no-dry-run` del parámetro que puede utilizarse para indicar de forma explícita que el comando debe ejecutarse con normalidad, aunque no es necesario incluirlo, ya que este es el comportamiento predeterminado.

Entero

Un número entero sin firma.

```
$ aws ec2 describe-spot-price-history --max-items 5
```

Binario/blob (objeto binario grande) y blob en streaming

En la AWS CLI, puede pasar un valor binario como una cadena directamente en la línea de comandos. Existen dos tipos de blobs:

- Blob
- Blob de streaming

Blob

Para pasar un valor a un parámetro con el tipo `blob`, debe especificar una ruta a un archivo local que contenga los datos binarios mediante el prefijo `fileb://`. Los archivos a los que se hace referencia mediante el prefijo `fileb://` siempre se tratan como binarios sin codificar. La ruta especificada se interpreta como una ruta relativa al directorio de trabajo actual. Por ejemplo, el parámetro `--plaintext` para `aws kms encrypt` es un blob.

```
$ aws kms encrypt \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --plaintext fileb://ExamplePlaintextFile \
    --output text \
    --query CiphertextBlob | base64 \
    --decode > ExampleEncryptedFile
```

> **Note**
>
> Por compatibilidad con versiones anteriores, puede utilizar el prefijo `file://`. Se utilizan dos formatos en función de la configuración de archivo `cli_binary_format` o de la opción de la línea de comandos `--cli-binary-format`:
>
> - Predeterminado para la AWS CLI versión 2. Si el valor de la configuración es `base64`, los archivos a los que se hace referencia mediante el prefijo `file://` se tratan como texto codificado en base64.
> - Predeterminado para la AWS CLI versión 1. Si el valor de la configuración es `raw-in-base64-out`, los archivos a los que se hace referencia mediante el prefijo `file://` se leen como texto y, a continuación, la AWS CLI intenta codificarlo en binario.

Para obtener más información, consulte la configuración de archivo `cli_binary_format` o la opción de la línea de comandos `--cli-binary-format`.

Blob de streaming

Los blobs de streaming como `aws cloudsearchdomain upload-documents` no utilizan prefijos. En cambio, los parámetros de blob de streaming se formatean mediante la ruta de archivo directa. En el siguiente ejemplo se utiliza la ruta de archivo directa `document-batch.json` para el comando `aws cloudsearchdomain upload-documents`:

```
$ aws cloudsearchdomain upload-documents \
    --endpoint-url https://doc-my-domain.us-west-1.cloudsearch.amazonaws.com \
    --content-type application/json \
    --documents document-batch.json
```

Asignación

Un conjunto de pares de clave-valor especificado en JSON o mediante la sintaxis abreviada de la CLI. En el siguiente ejemplo de JSON, se lee un elemento de una tabla de Amazon DynamoDB denominada my-table con un parámetro de mapa, `--key`. El parámetro especifica la clave principal denominada id con un valor numérico de 1 en una estructura JSON anidada.

Para conocer un uso más avanzado de JSON en una línea de comandos, considere usar un procesador JSON de línea de comandos, como `jq`, para crear cadenas JSON. Para obtener más información sobre `jq`, consulte el repositorio jq en GitHub.

```
$ aws dynamodb get-item --table-name my-table --key '{"id": {"N":"1"}}'

{
    "Item": {
        "name": {
            "S": "John"
        },
        "id": {
            "N": "1"
        }
    }
```

```
}
```

Documento

> **Note**
>
> La sintaxis abreviada no es compatible con los tipos de documento.

Los tipos de documento se utilizan para enviar datos sin necesidad de integrar JSON dentro de cadenas. El tipo de documento permite a los servicios proporcionar esquemas arbitrarios para que utilice tipos de datos más flexibles.

Esto permite enviar datos JSON sin necesidad de valores de escape. Por ejemplo, en lugar de utilizar la siguiente entrada JSON de escape:

```
{"document": "{\"key\":true}"}
```

Puede utilizar el tipo de documento que se muestra a continuación:

```
{"document": {"key": true}}
```

Valores válidos para tipos de documentos

Debido a la naturaleza flexible de los tipos de documentos, existen varios tipos de valores válidos. Entre los valores válidos se incluyen los siguientes:

Cadena

```
--option '"value"'
```

Número

```
--option 123
--option 123.456
```

Booleano

```
--option true
```

Nulo

```
--option null
```

Matriz

```
--option '["value1", "value2", "value3"]'
--option '["value", 1, true, null, ["key1", 2.34], {"key2": "value2"}]'
```

Objeto

```
--option '{"key": "value"}'
--option '{"key1": "value1", "key2": 123, "key3": true, "key4": null, "key5":
 ["value3", "value4"], "key6": {"value5": "value6"}'
```

Entrecomillado de cadenas y uso de literales en la AWS CLI

Hay dos maneras principales en las que se usan comillas simples y dobles en el AWS CLI.

- Usar comillas alrededor de cadenas que contienen espacios en blanco
- Uso de comillas dentro de cadenas

Usar comillas alrededor de cadenas que contienen espacios en blanco

Los nombres de los parámetros y sus valores están separados por espacios en la línea de comandos. Si un valor de cadena contiene un espacio incrustado, debe rodear toda la cadena con comillas para evitar que la AWS CLI malinterprete el espacio como un divisor entre el valor y el siguiente nombre del parámetro. El tipo de comillas que utilice depende del sistema operativo en el que esté ejecutando la AWS CLI.

Linux and macOS

Uso de comillas simples `' '`

```
$ aws ec2 create-key-pair --key-name 'my key pair'
```

Para obtener más información sobre el uso de las comillas, consulte documentación del usuario de su shell preferido.

PowerShell

Comillas simples (recomendadas)

Las marcas de comillas simples ' ' se llaman cadenas `verbatim`. La cadena se pasa al comando exactamente como se escribe, lo que significa que las variables de PowerShell no pasarán.

```
PS C:\> aws ec2 create-key-pair --key-name 'my key pair'
```

Comillas dobles

Las marcas de comillas dobles " " se llaman cadenas `expandable`. Las variables se pueden pasar en cadenas expandibles.

```
PS C:\> aws ec2 create-key-pair --key-name "my key pair"
```

Para obtener más información sobre el uso de las comillas, consulte Acerca de las reglas de entrecomillado en los Documentos de Microsoft PowerShell.

Windows command prompt

Uso de comillas dobles " ".

```
C:\> aws ec2 create-key-pair --key-name "my key pair"
```

Si lo desea, puede separar el nombre del parámetro del valor con un signo de igual = en lugar de un espacio. Normalmente, esto solo es necesario si el valor del parámetro comienza con un guion.

```
$ aws ec2 delete-key-pair --key-name=-mykey
```

Uso de comillas dentro de cadenas

Las cadenas pueden contener comillas y el shell puede requerir comillas de cierre para que funcionen correctamente. Uno de los tipos de valor de parámetro comunes es una cadena JSON. Esto es complejo, ya que incluye espacios y comillas dobles " " alrededor de cada nombre de elemento y valor en la estructura JSON. El modo en que introduzca parámetros con formato JSON en la línea de comandos varía en función de su sistema operativo.

Para conocer un uso más avanzado de JSON en la línea de comandos, considere usar un procesador JSON de línea de comandos, como `jq`, para crear cadenas JSON. Para obtener más información sobre `jq`, consulte el repositorio jq en GitHub.

Linux and macOS

Para que Linux y macOS interpreten cadenas en forma literal, use comillas simples `' '` para entrecomillar la estructura de datos JSON, como en el siguiente ejemplo. No necesita cerrar las comillas dobles incrustadas en la cadena JSON, ya que se las trata de manera literal. Dado que la cadena JSON está encerrada entre comillas simples, se deberá cerrar cualquier comilla simple en la cadena. Esto generalmente se logra usando una barra diagonal inversa antes de la comilla simple `\'`.

```
$ aws ec2 run-instances \
    --image-id ami-12345678 \
    --block-device-mappings '[{"DeviceName":"/dev/sdb","Ebs":
{"VolumeSize":20,"DeleteOnTermination":false,"VolumeType":"standard"}}]'
```

Para obtener más información sobre el uso de las comillas, consulte documentación del usuario de su shell preferido.

PowerShell

Utilice comillas simples `' '` o comillas dobles `" "`.

Comillas simples (recomendadas)

Las marcas de comillas simples `' '` se llaman cadenas `verbatim`. La cadena se pasa al comando exactamente como se escribe, lo que significa que las variables de PowerShell no pasarán.

Dado que las estructuras de datos JSON incluyen comillas dobles, sugerimos comillas simples `' '` para encerrarlas. Si usa comillas simples, no necesita cerrar las comillas dobles incrustadas en la cadena JSON. Sin embargo, debe cerrar cada comilla simple con una tilde invertido `` ` `` dentro de la estructura JSON.

```
PS C:\> aws ec2 run-instances `
    --image-id ami-12345678 `
    --block-device-mappings '[{"DeviceName":"/dev/sdb","Ebs":
{"VolumeSize":20,"DeleteOnTermination":false,"VolumeType":"standard"}}]'
```

Comillas dobles

Las marcas de comillas dobles " " se llaman cadenas `expandable`. Las variables se pueden pasar en cadenas expandibles.

Si usa comillas dobles, no necesita cerrar las comillas simples incrustadas en la cadena JSON. Sin embargo, debe cerrar cada comilla doble con un acento grave ` dentro de la estructura JSON, como con el siguiente ejemplo.

```
PS C:\> aws ec2 run-instances `
    --image-id ami-12345678 `
    --block-device-mappings "[{`"DeviceName`":`"/dev/sdb`",`"Ebs`":
{`"VolumeSize`":20,`"DeleteOnTermination`":false,`"VolumeType`":`"standard`"}}]"
```

Para obtener más información sobre el uso de las comillas, consulte Acerca de las reglas de entrecomillado en los Documentos de Microsoft PowerShell.

> **Warning**
>
> Antes de que PowerShell envíe un comando a la AWS CLI, determina si su comando se interpreta usando PowerShell típico o reglas de entrecomillado de `CommandLineToArgvW`. Cuando PowerShell procesa mediante `CommandLineToArgvW`, deben escaparse los caracteres con una barra invertida \.
> Para obtener más información sobre `CommandLineToArgvW` en PowerShell, consulte ¿Qué pasa con el extraño tratamiento de comillas y barras invertidas por CommandLineToArgVW? en Microsoft DevBlogs, Todos citan los argumentos de la línea de comandos de forma incorrecta en Microsoft Docs Blog yFunción CommandLineToArgVW en los Documentos de Microsoft.
> Comillas simples
> Las marcas de comillas simples ' ' se llaman cadenas `verbatim`. La cadena se pasa al comando exactamente como se escribe, lo que significa que las variables de PowerShell no pasarán. Los caracteres se escapan con una barra invertida\.
>
> ```
> PS C:\> aws ec2 run-instances `
>     --image-id ami-12345678 `
>     --block-device-mappings '[{\"DeviceName\":\"/dev/sdb\",\"Ebs\":
> {\"VolumeSize\":20,\"DeleteOnTermination\":false,\"VolumeType\":\"standard\"}}]'
> ```
>
> Comillas dobles

Las marcas de comillas dobles " " se llaman cadenas `expandable`. Las variables se pueden pasar en cadenas `expandable`. Para cadenas con comillas dobles, tiene que escapar dos veces usando `` `\ `` para cada comilla en lugar de usar solo un signo de acento. La barra invertida escapa la barra invertida y, a continuación, la barra invertida se utiliza como un carácter de escape para proceso `CommandLineToArgvW`.

```
PS C:\> aws ec2 run-instances `
    --image-id ami-12345678 `
    --block-device-mappings "[{`\"DeviceName`\":`\"/dev/sdb`\",`\"Ebs`\":
{`\"VolumeSize`\":20,`\"DeleteOnTermination`\":false,`\"VolumeType`\":`
\"standard`\"}}]"
```

Blobs (recomendado)
Para omitir las reglas de entrecomillado de PowerShell para la entrada de datos JSON, use Blobs para pasar los datos JSON directamente a la AWS CLI. Para obtener más información acerca de Blobs, consulte o Blob.

Windows command prompt

El símbolo del sistema de Windows requiere comillas dobles " " para entrecomillar la estructura de datos JSON. Además, para evitar que el procesador de comandos malinterprete las comillas dobles incrustadas en el JSON, también debe cerrar (precedido por un carácter de barra invertida \) cada comilla doble " dentro de la propia estructura de datos JSON, como en el siguiente ejemplo.

```
C:\> aws ec2 run-instances ^
    --image-id ami-12345678 ^
    --block-device-mappings "[{\"DeviceName\":\"/dev/sdb\",\"Ebs\":
{\"VolumeSize\":20,\"DeleteOnTermination\":false,\"VolumeType\":\"standard\"}}]"
```

El único caso en el que no se utiliza el carácter de cierre es con las comillas dobles de los extremos.

Carga de un parámetro de un archivo en la AWS CLI

Algunos parámetros esperan nombres de archivo como argumentos, desde los que la AWS CLI carga los datos. Otros parámetros le permiten especificar el valor del parámetro como texto escrito

en la línea de comandos o leído de un archivo. Tanto si un archivo es obligatorio como si es opcional, debe codificarlo correctamente para que la AWS CLI pueda entenderlo. La codificación del archivo debe coincidir con la configuración regional predeterminada del sistema de lectura. Esto se puede determinar utilizando el método Python `locale.getpreferredencoding()`.

Este método sirve para cargar un archivo para un único parámetro. Para obtener información sobre la carga de varios parámetros con un único archivo, consulte the section called “Generar una plantilla de esqueleto de la CLI”.

> **Note**
>
> De forma predeterminada, Windows PowerShell genera texto como UTF-16, lo que está en conflicto con la codificación UTF-8 utilizada por archivos JSON y muchos sistemas Linux. Le recomendamos que utilice `-Encoding ascii` con los comandos `Out-File` de PowerShell para asegurarse de que la AWS CLI puede leer el archivo resultante.

Temas

- Cómo cargar un parámetro de un archivo
- Archivos binarios
- Carga de un archivo como un valor sintáctico abreviado

Cómo cargar un parámetro de un archivo

En ocasiones, resulta conveniente cargar el valor de un parámetro desde un archivo en lugar de intentar escribirlo como un valor de parámetro de la línea de comandos, como, por ejemplo, cuando el parámetro es una cadena JSON compleja. Para especificar un archivo que contenga el valor, especifique la URL del archivo con el siguiente formato.

```
file://complete/path/to/file
```

- Los dos primeros caracteres de barra inclinada "/" forman parte de la especificación. Si la ruta requerida comienza con '/', el resultado será tres caracteres de barra inclinada: `file:///folder/file`.
- La dirección URL proporciona la ruta al archivo que incluye el contenido del parámetro real.
- Cuando se utilizan archivos con espacios o caracteres especiales, siga las normas de escape y entrecomillado para el terminal.

Las rutas de archivo en los siguientes ejemplos se interpretan como rutas relativas al directorio de trabajo actual.

Linux or macOS

```
// Read from a file in the current directory
$ aws ec2 describe-instances --filters file://filter.json

// Read from a file in /tmp
$ aws ec2 describe-instances --filters file:///tmp/filter.json

// Read from a file with a filename with whitespaces
$ aws ec2 describe-instances --filters 'file://filter content.json'
```

Windows command prompt

```
// Read from a file in C:\temp
C:\> aws ec2 describe-instances --filters file://C:\temp\filter.json

// Read from a file with a filename with whitespaces
C:\> aws ec2 describe-instances --filters "file://C:\temp\filter content.json"
```

La opción de prefijo `file://` admite ampliaciones tipo Unix, incluidas "~/", "`./`" y "`../`". En Windows, la expresión "~/" se amplía a su directorio de usuarios, guardado en la variable de entorno `%USERPROFILE%`. Por ejemplo, en Windows 10 normalmente tendría un directorio de usuarios en `%USERPROFILE%`.

Debe añadir el carácter de escape a los documentos JSON que están integrados como valor de otro documento JSON.

```
$ aws sqs create-queue --queue-name my-queue --attributes file://attributes.json
```

attributes.json

```
{
  "RedrivePolicy": "{\"deadLetterTargetArn\":\"arn:aws:sqs:us-
west-2:0123456789012:deadletter\", \"maxReceiveCount\":\"5\"}"
}
```

Archivos binarios

Para los comandos que toman datos binarios como un parámetro, especifique que los datos son contenido binario utilizando el prefijo `fileb://`. Los comandos que aceptan datos binarios son:

- **`aws ec2 run-instances`:** parámetro `--user-data`.
- **`aws s3api put-object`:** parámetro `--sse-customer-key`.
- **`aws kms decrypt`:** parámetro `--ciphertext-blob`.

En el siguiente ejemplo, se genera una clave AES binaria de 256 bits utilizando una herramienta de línea de comandos de Linux y después se proporciona dicha clave a Amazon S3 para cifrar un archivo cargado en el lado del servidor.

```
$ dd if=/dev/urandom bs=1 count=32 > sse.key
32+0 records in
32+0 records out
32 bytes (32 B) copied, 0.000164441 s, 195 kB/s
$ aws s3api put-object \
    --bucket amzn-s3-demo-bucket \
    --key test.txt \
    --body test.txt \
    --sse-customer-key fileb://sse.key \
    --sse-customer-algorithm AES256
{
    "SSECustomerKeyMD5": "iVg8oWa8sy714+FjtesrJg==",
    "SSECustomerAlgorithm": "AES256",
    "ETag": "\"a6118e84b76cf98bf04bbe14b6045c6c\""
}
```

Por ver otro ejemplo que haga referencia a un archivo que contenga parámetros con formato JSON, consulte Asociación de una política administrada de IAM a un usuario.

Carga de un archivo como un valor sintáctico abreviado

Cuando se utiliza una sintaxis abreviada en la que un valor es grande o complejo, suele ser más fácil cargarlo en un archivo como un valor. Para cargar un archivo como un valor sintáctico abreviado, el formato cambiará ligeramente. En lugar de `key=value`, usará el operador `@=`, en lugar del operador `=`. El valor `@=` se refiere a la AWS CLI que el valor se debe leer como una ruta de archivo y no como una cadena. En el siguiente ejemplo se muestra un par clave-valor que carga un archivo por su valor.

Linux or macOS

```
--option key@=file://template.txt
```

Windows

```
--option "key1@=file://template.txt"
```

En el siguiente ejemplo, se muestra la carga de un archivo de certificado para el comando `aws rolesanywhere create-trust-anchor`.

```
$ aws rolesanywhere create-trust-anchor --name TrustAnchor \
    --source sourceData={x509CertificateData@=file://root-
ca.crt},sourceType="CERTIFICATE_BUNDLE"  \
    --enabled
```

Para obtener más información sobre la sintaxis abreviada, consulte the section called “Sintaxis abreviada”.

Esqueletos de la AWS CLI y archivos de entrada en la AWS CLI

La mayoría de los comandos de la AWS CLI aceptan la importación de las entradas de parámetros de un archivo. Estas plantillas se pueden generar con la opción `generate-cli-skeleton` y, a continuación, se pueden importar con los parámetros `--cli-input-json` y `--cli-input-yaml`.

Temas

- Sobre esqueletos y archivos de entrada de AWS CLI
- Generación e importación de un esqueleto de comandos
- Combinación de archivos de entrada y parámetros de línea de comandos

Sobre esqueletos y archivos de entrada de AWS CLI

La mayoría de los comandos de AWS Command Line Interface (AWS CLI) pueden aceptar las entradas de parámetros desde un archivo con los parámetros `--cli-input-json` y `--cli-input-yaml`.

Esos mismos comandos usan el parámetro `--generate-cli-skeleton` para generar un archivo en formato JSON o YAML con todos los parámetros que pueda editar y completar. A continuación,

puede ejecutar el comando con el parámetro `--cli-input-json` o `--cli-input-yaml` y apuntar al archivo cumplimentado.

> **Important**
>
> Los comandos de la AWS CLI personalizados, como los comandos `aws s3` no admiten los parámetros `--generate-cli-skeleton` o `--cli-input-json` y `--cli-input-yaml` descritos en este tema. Para comprobar si un comando específico admite estos parámetros, ejecute el comando `help` correspondiente al comando que desee utilizar o consulte la guía de referencia de la versión 2 de AWS CLI.

`--generate-cli-skeleton` genera y muestra una plantilla de parámetros que puede personalizar y utilizar como entrada en un comando. La plantilla generada incluye todos los parámetros que admite el comando.

El parámetro `--generate-cli-skeleton` acepta uno de los siguientes valores:

- `input`: la plantilla generada incluye todos los parámetros de entrada formateados como JSON. Este es el valor predeterminado.
- `yaml-input`: la plantilla generada incluye todos los parámetros de entrada formateados como YAML.
- `output`: la plantilla generada incluye todos los parámetros de salida formateados como JSON. Actualmente, no puede solicitar los parámetros de salida en formato YAML.

Como la AWS CLI es esencialmente un "encapsulador" de la API del servicio, el archivo de esqueleto espera que el usuario haga referencia a todos los parámetros utilizando los nombres de parámetro de la API subyacente. Es probable que este nombre sea distinto al nombre del parámetro de la AWS CLI. Por ejemplo, un parámetro de la AWS CLI llamado `user-name` podría corresponderse con un parámetro de la API de servicio de AWS llamado `UserName` (observe cómo se usan las mayúsculas y que falta un guion). Le recomendamos que utilice la opción `--generate-cli-skeleton` para generar la plantilla con los nombres de parámetros "correctos" con el fin de evitar errores. Puede hacer referencia a la Guía de referencia de la API del servicio para ver los nombres de los parámetros esperados. Puede eliminar cualquier parámetro de la plantilla que no sea necesario y para el que no desee proporcionar un valor.

Por ejemplo, si ejecuta el siguiente comando, se genera la plantilla de parámetros para el comando Amazon Elastic Compute Cloud (Amazon EC2) run-instances.

JSON

En el siguiente ejemplo, se muestra cómo se genera una plantilla con formato JSON utilizando el valor predeterminado (`input`) en el parámetro `--generate-cli-skeleton`.

```
$ aws ec2 run-instances --generate-cli-skeleton
```

```
{
    "DryRun": true,
    "ImageId": "",
    "MinCount": 0,
    "MaxCount": 0,
    "KeyName": "",
    "SecurityGroups": [
        ""
    ],
    "SecurityGroupIds": [
        ""
    ],
    "UserData": "",
    "InstanceType": "",
    "Placement": {
        "AvailabilityZone": "",
        "GroupName": "",
        "Tenancy": ""
    },
    "KernelId": "",
    "RamdiskId": "",
    "BlockDeviceMappings": [
        {
            "VirtualName": "",
            "DeviceName": "",
            "Ebs": {
                "SnapshotId": "",
                "VolumeSize": 0,
                "DeleteOnTermination": true,
                "VolumeType": "",
                "Iops": 0,
                "Encrypted": true
            },
            "NoDevice": ""
        }
    ],
```

```
    "Monitoring": {
        "Enabled": true
    },
    "SubnetId": "",
    "DisableApiTermination": true,
    "InstanceInitiatedShutdownBehavior": "",
    "PrivateIpAddress": "",
    "ClientToken": "",
    "AdditionalInfo": "",
    "NetworkInterfaces": [
        {
            "NetworkInterfaceId": "",
            "DeviceIndex": 0,
            "SubnetId": "",
            "Description": "",
            "PrivateIpAddress": "",
            "Groups": [
                ""
            ],
            "DeleteOnTermination": true,
            "PrivateIpAddresses": [
                {
                    "PrivateIpAddress": "",
                    "Primary": true
                }
            ],
            "SecondaryPrivateIpAddressCount": 0,
            "AssociatePublicIpAddress": true
        }
    ],
    "IamInstanceProfile": {
        "Arn": "",
        "Name": ""
    },
    "EbsOptimized": true
}
```

YAML

En el ejemplo siguiente, se muestra cómo se genera una plantilla con formato YAML utilizando el valor `yaml-input` en el parámetro `--generate-cli-skeleton`.

```
$ aws ec2 run-instances --generate-cli-skeleton yaml-input
```

```
BlockDeviceMappings:  # The block device mapping entries.
- DeviceName: ''  # The device name (for example, /dev/sdh or xvdh).
  VirtualName: '' # The virtual device name (ephemeralN).
  Ebs: # Parameters used to automatically set up Amazon EBS volumes when the
 instance is launched.
    DeleteOnTermination: true  # Indicates whether the EBS volume is deleted on
 instance termination.
    Iops: 0 # The number of I/O operations per second (IOPS) that the volume
 supports.
    SnapshotId: '' # The ID of the snapshot.
    VolumeSize: 0 # The size of the volume, in GiB.
    VolumeType: st1 # The volume type. Valid values are: standard, io1, gp2, sc1,
 st1.
    Encrypted: true # Indicates whether the encryption state of an EBS volume is
 changed while being restored from a backing snapshot.
    KmsKeyId: '' # Identifier (key ID, key alias, ID ARN, or alias ARN) for a
 customer managed KMS key under which the EBS volume is encrypted.
  NoDevice: '' # Suppresses the specified device included in the block device
 mapping of the AMI.
ImageId: '' # The ID of the AMI.
InstanceType: c4.4xlarge # The instance type. Valid values are: t1.micro, t2.nano,
 t2.micro, t2.small, t2.medium, t2.large, t2.xlarge, t2.2xlarge, t3.nano, t3.micro,
 t3.small, t3.medium, t3.large, t3.xlarge, t3.2xlarge, t3a.nano, t3a.micro,
 t3a.small, t3a.medium, t3a.large, t3a.xlarge, t3a.2xlarge, m1.small, m1.medium,
 m1.large, m1.xlarge, m3.medium, m3.large, m3.xlarge, m3.2xlarge, m4.large,
 m4.xlarge, m4.2xlarge, m4.4xlarge, m4.10xlarge, m4.16xlarge, m2.xlarge, m2.2xlarge,
 m2.4xlarge, cr1.8xlarge, r3.large, r3.xlarge, r3.2xlarge, r3.4xlarge, r3.8xlarge,
 r4.large, r4.xlarge, r4.2xlarge, r4.4xlarge, r4.8xlarge, r4.16xlarge, r5.large,
 r5.xlarge, r5.2xlarge, r5.4xlarge, r5.8xlarge, r5.12xlarge, r5.16xlarge,
 r5.24xlarge, r5.metal, r5a.large, r5a.xlarge, r5a.2xlarge, r5a.4xlarge,
 r5a.8xlarge, r5a.12xlarge, r5a.16xlarge, r5a.24xlarge, r5d.large, r5d.xlarge,
 r5d.2xlarge, r5d.4xlarge, r5d.8xlarge, r5d.12xlarge, r5d.16xlarge, r5d.24xlarge,
 r5d.metal, r5ad.large, r5ad.xlarge, r5ad.2xlarge, r5ad.4xlarge, r5ad.8xlarge,
 r5ad.12xlarge, r5ad.16xlarge, r5ad.24xlarge, x1.16xlarge, x1.32xlarge, x1e.xlarge,
 x1e.2xlarge, x1e.4xlarge, x1e.8xlarge, x1e.16xlarge, x1e.32xlarge, i2.xlarge,
 i2.2xlarge, i2.4xlarge, i2.8xlarge, i3.large, i3.xlarge, i3.2xlarge, i3.4xlarge,
 i3.8xlarge, i3.16xlarge, i3.metal, i3en.large, i3en.xlarge, i3en.2xlarge,
 i3en.3xlarge, i3en.6xlarge, i3en.12xlarge, i3en.24xlarge, i3en.metal, hi1.4xlarge,
 hs1.8xlarge, c1.medium, c1.xlarge, c3.large, c3.xlarge, c3.2xlarge, c3.4xlarge,
 c3.8xlarge, c4.large, c4.xlarge, c4.2xlarge, c4.4xlarge, c4.8xlarge, c5.large,
 c5.xlarge, c5.2xlarge, c5.4xlarge, c5.9xlarge, c5.12xlarge, c5.18xlarge,
 c5.24xlarge, c5.metal, c5d.large, c5d.xlarge, c5d.2xlarge, c5d.4xlarge,
 c5d.9xlarge, c5d.18xlarge, c5n.large, c5n.xlarge, c5n.2xlarge, c5n.4xlarge,
```

```
 c5n.9xlarge, c5n.18xlarge, cc1.4xlarge, cc2.8xlarge, g2.2xlarge, g2.8xlarge,
 g3.4xlarge, g3.8xlarge, g3.16xlarge, g3s.xlarge, g4dn.xlarge, g4dn.2xlarge,
 g4dn.4xlarge, g4dn.8xlarge, g4dn.12xlarge, g4dn.16xlarge, cg1.4xlarge, p2.xlarge,
 p2.8xlarge, p2.16xlarge, p3.2xlarge, p3.8xlarge, p3.16xlarge, p3dn.24xlarge,
 d2.xlarge, d2.2xlarge, d2.4xlarge, d2.8xlarge, f1.2xlarge, f1.4xlarge, f1.16xlarge,
 m5.large, m5.xlarge, m5.2xlarge, m5.4xlarge, m5.8xlarge, m5.12xlarge, m5.16xlarge,
 m5.24xlarge, m5.metal, m5a.large, m5a.xlarge, m5a.2xlarge, m5a.4xlarge,
 m5a.8xlarge, m5a.12xlarge, m5a.16xlarge, m5a.24xlarge, m5d.large, m5d.xlarge,
 m5d.2xlarge, m5d.4xlarge, m5d.8xlarge, m5d.12xlarge, m5d.16xlarge, m5d.24xlarge,
 m5d.metal, m5ad.large, m5ad.xlarge, m5ad.2xlarge, m5ad.4xlarge, m5ad.8xlarge,
 m5ad.12xlarge, m5ad.16xlarge, m5ad.24xlarge, h1.2xlarge, h1.4xlarge, h1.8xlarge,
 h1.16xlarge, z1d.large, z1d.xlarge, z1d.2xlarge, z1d.3xlarge, z1d.6xlarge,
 z1d.12xlarge, z1d.metal, u-6tb1.metal, u-9tb1.metal, u-12tb1.metal, u-18tb1.metal,
 u-24tb1.metal, a1.medium, a1.large, a1.xlarge, a1.2xlarge, a1.4xlarge, a1.metal,
 m5dn.large, m5dn.xlarge, m5dn.2xlarge, m5dn.4xlarge, m5dn.8xlarge, m5dn.12xlarge,
 m5dn.16xlarge, m5dn.24xlarge, m5n.large, m5n.xlarge, m5n.2xlarge, m5n.4xlarge,
 m5n.8xlarge, m5n.12xlarge, m5n.16xlarge, m5n.24xlarge, r5dn.large, r5dn.xlarge,
 r5dn.2xlarge, r5dn.4xlarge, r5dn.8xlarge, r5dn.12xlarge, r5dn.16xlarge,
 r5dn.24xlarge, r5n.large, r5n.xlarge, r5n.2xlarge, r5n.4xlarge, r5n.8xlarge,
 r5n.12xlarge, r5n.16xlarge, r5n.24xlarge.
Ipv6AddressCount: 0 # [EC2-VPC] The number of IPv6 addresses to associate with the
 primary network interface.
Ipv6Addresses: # [EC2-VPC] The IPv6 addresses from the range of the subnet to
 associate with the primary network interface.
- Ipv6Address: ''  # The IPv6 address.
KernelId: '' # The ID of the kernel.
KeyName: '' # The name of the key pair.
MaxCount: 0 # [REQUIRED] The maximum number of instances to launch.
MinCount: 0 # [REQUIRED] The minimum number of instances to launch.
Monitoring: # Specifies whether detailed monitoring is enabled for the instance.
  Enabled: true  # [REQUIRED] Indicates whether detailed monitoring is enabled.
Placement: # The placement for the instance.
  AvailabilityZone: ''  # The Availability Zone of the instance.
  Affinity: '' # The affinity setting for the instance on the Dedicated Host.
  GroupName: '' # The name of the placement group the instance is in.
  PartitionNumber: 0 # The number of the partition the instance is in.
  HostId: '' # The ID of the Dedicated Host on which the instance resides.
  Tenancy: dedicated # The tenancy of the instance (if the instance is running in a
 VPC). Valid values are: default, dedicated, host.
  SpreadDomain: '' # Reserved for future use.
RamdiskId: '' # The ID of the RAM disk to select.
SecurityGroupIds: # The IDs of the security groups.
- ''
SecurityGroups: # [default VPC] The names of the security groups.
```

```
- ''
SubnetId: '' # [EC2-VPC] The ID of the subnet to launch the instance into.
UserData: '' # The user data to make available to the instance.
AdditionalInfo: '' # Reserved.
ClientToken: '' # Unique, case-sensitive identifier you provide to ensure the
 idempotency of the request.
DisableApiTermination: true # If you set this parameter to true, you can't terminate
 the instance using the Amazon EC2 console, CLI, or API; otherwise, you can.
DryRun: true # Checks whether you have the required permissions for the action,
 without actually making the request, and provides an error response.
EbsOptimized: true # Indicates whether the instance is optimized for Amazon EBS I/O.
IamInstanceProfile: # The IAM instance profile.
  Arn: ''  # The Amazon Resource Name (ARN) of the instance profile.
  Name: '' # The name of the instance profile.
InstanceInitiatedShutdownBehavior: stop # Indicates whether an instance stops or
 terminates when you initiate shutdown from the instance (using the operating system
 command for system shutdown). Valid values are: stop, terminate.
NetworkInterfaces: # The network interfaces to associate with the instance.
- AssociatePublicIpAddress: true  # Indicates whether to assign a public IPv4
 address to an instance you launch in a VPC.
  DeleteOnTermination: true # If set to true, the interface is deleted when the
 instance is terminated.
  Description: '' # The description of the network interface.
  DeviceIndex: 0 # The position of the network interface in the attachment order.
  Groups: # The IDs of the security groups for the network interface.
  - ''
  Ipv6AddressCount: 0 # A number of IPv6 addresses to assign to the network
 interface.
  Ipv6Addresses: # One or more IPv6 addresses to assign to the network interface.
  - Ipv6Address: ''  # The IPv6 address.
  NetworkInterfaceId: '' # The ID of the network interface.
  PrivateIpAddress: '' # The private IPv4 address of the network interface.
  PrivateIpAddresses: # One or more private IPv4 addresses to assign to the network
 interface.
  - Primary: true  # Indicates whether the private IPv4 address is the primary
 private IPv4 address.
    PrivateIpAddress: '' # The private IPv4 addresses.
  SecondaryPrivateIpAddressCount: 0 # The number of secondary private IPv4
 addresses.
  SubnetId: '' # The ID of the subnet associated with the network interface.
  InterfaceType: '' # The type of network interface.
PrivateIpAddress: '' # [EC2-VPC] The primary IPv4 address.
ElasticGpuSpecification: # An elastic GPU to associate with the instance.
- Type: ''  # [REQUIRED] The type of Elastic Graphics accelerator.
```

```
ElasticInferenceAccelerators: # An elastic inference accelerator to associate with
 the instance.
- Type: ''  # [REQUIRED]  The type of elastic inference accelerator.
TagSpecifications: # The tags to apply to the resources during launch.
- ResourceType: network-interface  # The type of resource to tag. Valid values
 are: client-vpn-endpoint, customer-gateway, dedicated-host, dhcp-options, elastic-
ip, fleet, fpga-image, host-reservation, image, instance, internet-gateway,
 launch-template, natgateway, network-acl, network-interface, reserved-instances,
 route-table, security-group, snapshot, spot-instances-request, subnet, traffic-
mirror-filter, traffic-mirror-session, traffic-mirror-target, transit-gateway,
 transit-gateway-attachment, transit-gateway-route-table, volume, vpc, vpc-peering-
connection, vpn-connection, vpn-gateway.
  Tags: # The tags to apply to the resource.
  - Key: ''  # The key of the tag.
    Value: '' # The value of the tag.
LaunchTemplate: # The launch template to use to launch the instances.
  LaunchTemplateId: ''  # The ID of the launch template.
  LaunchTemplateName: '' # The name of the launch template.
  Version: '' # The version number of the launch template.
InstanceMarketOptions: # The market (purchasing) option for the instances.
  MarketType: spot  # The market type. Valid values are: spot.
  SpotOptions: # The options for Spot Instances.
    MaxPrice: ''  # The maximum hourly price you're willing to pay for the Spot
 Instances.
    SpotInstanceType: one-time # The Spot Instance request type. Valid values are:
 one-time, persistent.
    BlockDurationMinutes: 0 # The required duration for the Spot Instances (also
 known as Spot blocks), in minutes.
    ValidUntil: 1970-01-01 00:00:00 # The end date of the request.
    InstanceInterruptionBehavior: terminate # The behavior when a Spot Instance is
 interrupted. Valid values are: hibernate, stop, terminate.
CreditSpecification: # The credit option for CPU usage of the T2 or T3 instance.
  CpuCredits: ''  # [REQUIRED] The credit option for CPU usage of a T2 or T3
 instance.
CpuOptions: # The CPU options for the instance.
  CoreCount: 0  # The number of CPU cores for the instance.
  ThreadsPerCore: 0 # The number of threads per CPU core.
CapacityReservationSpecification: # Information about the Capacity Reservation
 targeting option.
  CapacityReservationPreference: none  # Indicates the instance's Capacity
 Reservation preferences. Valid values are: open, none.
  CapacityReservationTarget: # Information about the target Capacity Reservation.
    CapacityReservationId: ''  # The ID of the Capacity Reservation.
HibernationOptions: # Indicates whether an instance is enabled for hibernation.
```

```
  Configured: true  # If you set this parameter to true, your instance is enabled
 for hibernation.
LicenseSpecifications: # The license configurations.
- LicenseConfigurationArn: ''  # The Amazon Resource Name (ARN) of the license
 configuration.
```

Generación e importación de un esqueleto de comandos

Para generar y utilizar un archivo de esqueleto de parámetros

1. Ejecute el comando con el parámetro `--generate-cli-skeleton` para producir la salida en formato JSON o YAML y dirigirla a un archivo para guardarla.

   JSON

   ```
   $ aws ec2 run-instances --generate-cli-skeleton input > ec2runinst.json
   ```

   YAML

   ```
   $ aws ec2 run-instances --generate-cli-skeleton yaml-input > ec2runinst.yaml
   ```

2. Abra el archivo de esqueleto de parámetros en el editor de texto y quite todos los parámetros que no necesite. Por ejemplo, puede reducir la plantilla hasta dejarla tal y como se muestra a continuación. Confirme que el código JSON o YAML del archivo sigue siendo válido después de eliminar los elementos que no necesita.

   JSON

   ```
   {
       "DryRun": true,
       "ImageId": "",
       "KeyName": "",
       "SecurityGroups": [
           ""
       ],
       "InstanceType": "",
       "Monitoring": {
           "Enabled": true
       }
   }
   ```

YAML

```
DryRun: true
ImageId: ''
KeyName: ''
SecurityGroups:
- ''
InstanceType:
Monitoring:
  Enabled: true
```

En este ejemplo, dejamos el parámetro `DryRun` establecido en `true` para utilizar la característica “dry run” (simulacro) de Amazon EC2. Esta característica le permite probar el comando de forma segura sin crear ni modificar ningún recurso.

3. Rellene los valores restantes con valores adecuados para su escenario. En este ejemplo, proporcionamos el tipo de instancia, el nombre de la clave, el grupo de seguridad y el identificador de Amazon Machine Image (AMI) que vamos a utilizar. En este ejemplo, se asume la Región de AWS predeterminada. La AMI `ami-dfc39aef` es una imagen de Amazon Linux de 64 bits alojada en la región `us-west-2`. Si utiliza una región diferente, debe encontrar el ID apropiado de la AMI que desea utilizar.

   JSON

   ```
   {
       "DryRun": true,
       "ImageId": "ami-dfc39aef",
       "KeyName": "mykey",
       "SecurityGroups": [
           "my-sg"
       ],
       "InstanceType": "t2.micro",
       "Monitoring": {
           "Enabled": true
       }
   }
   ```

   YAML

   ```
   DryRun: true
   ```

```
ImageId: 'ami-dfc39aef'
KeyName: 'mykey'
SecurityGroups:
- 'my-sg'
InstanceType: 't2.micro'
Monitoring:
  Enabled: true
```

4. Ejecute el comando con los parámetros completados pasando el archivo de plantilla relleno ya sea al parámetro `--cli-input-json` o `–cli-input-yaml` al utilizar el prefijo `file://`. La AWS CLI interpreta la ruta como relativa al directorio de trabajo actual. En el siguiente ejemplo, la AWS CLI busca el archivo en el directorio de trabajo actual.

   JSON

   ```
   $ aws ec2 run-instances --cli-input-json file://ec2runinst.json
   ```

   ```
   A client error (DryRunOperation) occurred when calling the RunInstances
    operation: Request would have succeeded, but DryRun flag is set.
   ```

   YAML

   ```
   $ aws ec2 run-instances --cli-input-yaml file://ec2runinst.yaml
   ```

   ```
   A client error (DryRunOperation) occurred when calling the RunInstances
    operation: Request would have succeeded, but DryRun flag is set.
   ```

   El error del simulacro indica que el código JSON o YAML está formado correctamente y que los valores de los parámetros son válidos. Si se informa de cualquier otro problema en la salida, corríjalo y repita el paso anterior hasta que aparezca el mensaje "`Request would have succeeded`".

5. Ahora puede establecer el parámetro `DryRun` en `false` para deshabilitar el simulacro.

   JSON

   ```
   {
       "DryRun": false,
       "ImageId": "ami-dfc39aef",
   ```

```
    "KeyName": "mykey",
    "SecurityGroups": [
        "my-sg"
    ],
    "InstanceType": "t2.micro",
    "Monitoring": {
        "Enabled": true
    }
}
```

YAML

```
DryRun: false
ImageId: 'ami-dfc39aef'
KeyName: 'mykey'
SecurityGroups:
- 'my-sg'
InstanceType: 't2.micro'
Monitoring:
  Enabled: true
```

6. Ejecute el comando para que `run-instances` lance una instancia de Amazon EC2 y muestre los detalles que se generan cuando el lanzamiento se realiza correctamente. El parámetro `--output` controla el formato de salida, independientemente del formato de la plantilla de parámetros de entrada.

   JSON

   ```
   $ aws ec2 run-instances --cli-input-json file://ec2runinst.json --output json
   ```

   ```
   {
       "OwnerId": "123456789012",
       "ReservationId": "r-d94a2b1",
       "Groups": [],
       "Instances": [
   ...
   ```

   YAML

   ```
   $ aws ec2 run-instances --cli-input-yaml file://ec2runinst.yaml --output yaml
   ```

```
OwnerId: '123456789012'
ReservationId: 'r-d94a2b1',
Groups":
- ''
Instances:
...
```

Combinación de archivos de entrada y parámetros de línea de comandos

Se puede usar un archivo de entrada para todos los parámetros o se puede combinar con los parámetros especificados en la AWS CLI. Puede utilizar esta característica para los ajustes que reutiliza con frecuencia en un archivo de entrada y, al mismo tiempo, conservar los ajustes individuales en el propio comando.

En los siguientes ejemplos de `aws ec2 run-instances`, se combinan el uso de un archivo de entrada y parámetros. Proporcionamos el tipo de instancia, el nombre de la clave, el grupo de seguridad y el identificador de la imagen de máquina de Amazon (AMI) que se va a utilizar y se asume la Región de AWS predeterminada. La AMI `ami-dfc39aef` es una imagen de Amazon Linux de 64 bits alojada en la región `us-west-2`. Si utiliza una región diferente, debe encontrar el ID apropiado de la AMI que desea utilizar.

JSON

Contenido del archivo JSON:

```
{
    "ImageId": "ami-dfc39aef",
    "KeyName": "mykey",
    "SecurityGroups": [
        "my-sg"
    ],
    "InstanceType": "t2.micro",
    "Monitoring": {
        "Enabled": true
    }
}
```

YAML

Contenido del archivo YAML:

```
ImageId: 'ami-dfc39aef'
KeyName: 'mykey'
SecurityGroups:
- 'my-sg'
InstanceType: 't2.micro'
Monitoring:
  Enabled: true
```

En el siguiente ejemplo, se utiliza el archivo de entrada en combinación con el parámetro `--dry-run` para realizar una actualización de prueba del comando para confirmar si tiene los permisos necesarios y si ha rellenado el archivo con valores válidos.

JSON

```
$ aws ec2 run-instances --cli-input-json file://ec2runinst.json --dry-run
```

```
A client error (DryRunOperation) occurred when calling the RunInstances operation:
 Request would have succeeded, but DryRun flag is set.
```

YAML

```
$ aws ec2 run-instances --cli-input-yaml file://ec2runinst.yaml --dry-run
```

```
A client error (DryRunOperation) occurred when calling the RunInstances operation:
 Request would have succeeded, but DryRun flag is set.
```

A continuación, en el siguiente ejemplo se utiliza el mismo archivo de entrada, pero con el parámetro `--no-dry-run` para ejecutar el comando en su totalidad.

JSON

```
$ aws ec2 run-instances --cli-input-json file://ec2runinst.json --no-dry-run --
output json
```

```
{
    "OwnerId": "123456789012",
    "ReservationId": "r-d94a2b1",
```

```
    "Groups": [],
    "Instances": [
...
```

YAML

```
$ aws ec2 run-instances --cli-input-yaml file://ec2runinst.yaml --no-dry-run --
output yaml
```

```
OwnerId: '123456789012'
ReservationId: 'r-d94a2b1',
Groups":
- ''
Instances:
...
```

Uso de la sintaxis abreviada en la AWS CLI

La AWS Command Line Interface (AWS CLI) puede aceptar muchos de sus parámetros de opciones en formato JSON. Sin embargo, resultaría tedioso escribir largas listas o estructuras de JSON en la línea de comandos. Para simplificarlo, la AWS CLI también admite una sintaxis abreviada que permite una representación de los parámetros de opciones más sencilla que si se usara el formato JSON íntegro.

Temas

- Parámetros de estructura con pares clave-valor
- Carga de un archivo como un valor sintáctico abreviado
- Uso de sintaxis abreviada con la AWS CLI

Parámetros de estructura con pares clave-valor

La sintaxis abreviada de la AWS CLI facilita a los usuarios la introducción de parámetros planos (con estructuras no anidadas). El formato consiste en una lista de pares de clave-valor separados por comas. Asegúrese de utilizar las reglas de comillas y caracteres de escape apropiadas para el terminal como sintaxis abreviada son cadenas.

Linux or macOS

```
--option key1=value1,key2=value2,key3=value3
```

Equivale al siguiente ejemplo con formato JSON.

```
--option '{"key1":"value1","key2":"value2","key3":"value3"}'
```

Windows

```
--option "key1=value1,key2=value2,key3=value3"
```

Equivale al siguiente ejemplo con formato JSON.

```
--option '{"key1":"value1","key2":"value2","key3":"value3"}'
```

No debe haber espacios en blanco entre cada uno de los pares de clave-valor separados por comas. A continuación, se muestra un ejemplo del comando de `update-table` de Amazon DynamoDB con la opción `--provisioned-throughput` especificada en modo abreviado.

```
$ aws dynamodb update-table \
    --provisioned-throughput ReadCapacityUnits=15,WriteCapacityUnits=10 \
    --table-name MyDDBTable
```

Esto equivale al siguiente ejemplo con formato JSON.

```
$ aws dynamodb update-table \
    --provisioned-throughput '{"ReadCapacityUnits":15,"WriteCapacityUnits":10}' \
    --table-name MyDDBTable
```

Carga de un archivo como un valor sintáctico abreviado

Cuando un valor es grande o complejo, suele ser más fácil cargarlo en un archivo como un valor. Para cargar un archivo como un valor sintáctico abreviado, el formato cambiará ligeramente. En lugar de `key=value`, usará el operador `@=`, en lugar del operador `=`. El valor `@=` se refiere a la AWS CLI que el valor se debe leer como una ruta de archivo y no como una cadena. Al cargar archivos en una sintaxis abreviada, se aplican las reglas de formato de archivo de la AWS CLI habituales. En el siguiente ejemplo se muestra un par clave-valor que carga un archivo por su valor.

Linux or macOS

```
--option key@=file://template.txt
```

Windows

```
--option "key1@=file://template.txt"
```

En el siguiente ejemplo, se muestra la carga de un archivo de certificado para el comando `aws rolesanywhere create-trust-anchor`.

```
$ aws rolesanywhere create-trust-anchor --name TrustAnchor \
    --source sourceData={x509CertificateData@=file://root-
ca.crt},sourceType="CERTIFICATE_BUNDLE"  \
    --enabled
```

Uso de sintaxis abreviada con la AWS CLI

Puede especificar los parámetros de entrada en una lista de dos formas: en JSON o en sintaxis abreviada. La sintaxis abreviada de la AWS CLI ha sido diseñada para que su inserción en listas con números, cadenas o estructuras no anidadas resulte más sencilla.

A continuación se muestra el formato básico, en el que los valores de la lista están separados por un único espacio.

```
--option value1 value2 value3
```

Esto equivale al siguiente ejemplo con formato JSON.

```
--option '[value1,value2,value3]'
```

Como ya hemos mencionado anteriormente, puede especificar una lista de números, una lista de cadenas o una lista de estructuras no anidadas en formato abreviado. A continuación, se muestra un ejemplo del comando `stop-instances` para Amazon Elastic Compute Cloud (Amazon EC2), en el que el parámetro de entrada (lista de cadenas) de la opción `--instance-ids` se especifica en forma abreviada.

```
$ aws ec2 stop-instances \
```

```
    --instance-ids i-1486157a i-1286157c i-ec3a7e87
```

Esto equivale al siguiente ejemplo con formato JSON.

```
$ aws ec2 stop-instances \
    --instance-ids '["i-1486157a","i-1286157c","i-ec3a7e87"]'
```

En el siguiente ejemplo se muestra el comando de `create-tags` de Amazon EC2, que toma una lista de estructuras no anidadas para la opción `--tags`. La opción `--resources` especifica el identificador de la instancia que debe etiquetarse.

```
$ aws ec2 create-tags \
    --resources i-1286157c \
    --tags Key=My1stTag,Value=Value1 Key=My2ndTag,Value=Value2
 Key=My3rdTag,Value=Value3
```

Esto equivale al siguiente ejemplo con formato JSON. El parámetro JSON está escrito en varias líneas para facilitar su lectura.

```
$ aws ec2 create-tags \
    --resources i-1286157c \
    --tags '[
        {"Key": "My1stTag", "Value": "Value1"},
        {"Key": "My2ndTag", "Value": "Value2"},
        {"Key": "My3rdTag", "Value": "Value3"}
    ]'
```

Activación y uso de los símbolos del sistema en la AWS CLI

Puede hacer que la versión 2 de la AWS CLI le pida comandos, parámetros y recursos cuando ejecute un comando de `aws`.

Temas

- Funcionamiento
- Características del mensaje automático
- Modos de mensaje automático
- Configuración del mensaje automático

Funcionamiento

Si está habilitado, el mensaje automático le permite utilizar la tecla ENTER (INTRO) para completar un comando introducido parcialmente. Después de presionar la tecla ENTER (INTRO), se sugieren comandos, parámetros y recursos en función de lo que siga escribiendo. Las sugerencias muestran el nombre del comando, parámetro o recurso a la izquierda y una descripción del mismo a la derecha. Para seleccionar y utilizar una sugerencia, utilice las teclas de flechas para resaltar una fila y, a continuación, presione la tecla de SPACE (ESPACIO). Cuando haya terminado de ingresar su comando, presione ENTER (INTRO) para usar el comando. En el siguiente ejemplo se muestra cómo se ve una lista sugerida de mensajes automáticos.

```
$ aws
> aws a
       accessanalyzer               Access Analyzer
       acm                          AWS Certificate Manager
       acm-pca                      AWS Certificate Manager Private Certificate
 Authority
       alexaforbusiness             Alexa For Business
       amplify                      AWS Amplify
```

Características del mensaje automático

El mensaje automático contiene las siguientes características útiles:

Panel de documentación

Proporciona la documentación de ayuda del comando actual. Para abrir la documentación, presione la tecla F3.

Finalización de comandos

Sugiere qué comandos de `aws` debería usar. Para ver una lista, ingrese parcialmente el comando. En el siguiente ejemplo se busca un servicio que comience con la letra `a`.

```
$ aws
> aws a
       accessanalyzer               Access Analyzer
       acm                          AWS Certificate Manager
       acm-pca                      AWS Certificate Manager Private Certificate
 Authority
       alexaforbusiness             Alexa For Business
```

```
        amplify                         AWS Amplify
```

Compleción de parámetros

Después de escribir un comando, el mensaje automático comienza a sugerir parámetros. Las descripciones de los parámetros incluyen el tipo de valor y una descripción del parámetro. Los parámetros necesarios se enumeran primero y se etiquetan según sean necesarios. En el siguiente ejemplo se muestra la lista de mensajes automáticos de parámetros para `aws dynamodb describe-table`.

```
$ aws dynamodb describe-table
> aws dynamodb describe-table
                               --table-name (required)  [string] The name of the
 table to describe.
                                --cli-input-json         [string] Reads arguments
 from the JSON string provided. The JSON string follows the format provide...
                                --cli-input-yaml         [string] Reads arguments
 from the YAML string provided. The YAML string follows the format provide...
                                --generate-cli-skeleton  [string] Prints a JSON
 skeleton to standard output without sending an API request. If provided wit...
```

Compleción de recursos

El mensaje automático realiza llamadas a la API de AWS utilizando las propiedades de recursos de AWS disponibles para sugerir valores de recursos. Esto permite que el mensaje automático sugiera posibles recursos que posee al introducir parámetros. En el siguiente ejemplo, el mensaje automático muestra los nombres de las tablas al rellenar el parámetro `--table-name` para el comando `aws dynamodb describe-table`.

```
$ aws dynamodb describe-table
> aws dynamodb describe-table --table-name
                                            Table1
                                            Table2
                                            Table3
```

Compleción abreviada

Para los parámetros que utilizan sintaxis abreviada, el mensaje automático sugiere los valores a utilizar. En el siguiente ejemplo, el mensaje automático muestra los valores de sintaxis abreviada para el parámetro `--placement` en el comando `aws ec2 run-instances`.

```
$ aws ec2 run-instances
> aws ec2 run-instances --placement
 AvailabilityZone=      [string] The Availability Zone of the instance. If not
 specified, an Availability Zone wil...
 Affinity=              [string] The affinity setting for the instance on the
 Dedicated Host. This parameter is no...
 GroupName=             [string] The name of the placement group the instance is in.
 PartitionNumber=       [integer] The number of the partition the instance is in.
 Valid only if the placement grou...
```

Compleción del archivo

Al rellenar los parámetros de los comandos `aws`, la compleción automática sugiere nombres de archivos locales después de usar el prefijo `file://` o `fileb://`. En el siguiente ejemplo, el mensaje automático sugiere archivos locales después de ingresar `--item file://` para el comando `aws ec2 run-instances`.

```
$ aws ec2 run-instances
> aws ec2 run-instances --item file://
                         item1.txt
                         file1.json
                         file2.json
```

Compleción de la región

Cuando se utiliza el parámetro global `--region`, el mensaje automático muestra las regiones posibles para seleccionar. En el siguiente ejemplo, el mensaje automático sugiere regiones en orden alfabético después de escribir `--region` para el comando `aws dynamodb list-tables`.

```
$ aws dynamodb list-tables
> aws dynamodb list-tables --region
                                    af-south-1
                                    ap-east-1
                                    ap-northeast-1
                                    ap-northeast-2
```

Compleción del perfil

Cuando se utiliza el parámetro global `--profile`, el mensaje automático muestra una lista de sus perfiles. En el siguiente ejemplo, el mensaje automático sugiere sus perfiles después de ingresar `--profile` para el comando `aws dynamodb list-tables`.

```
$ aws dynamodb list-tables
> aws dynamodb list-tables --profile
                                    profile1
                                    profile2
                                    profile3
```

Búsquedas confusas

Complete comandos y valores que contienen un conjunto específico de caracteres. En el siguiente ejemplo, el mensaje automático sugiere regiones que contienen `eu` después de ingresar `--region eu` para el comando `aws dynamodb list-tables`.

```
$ aws dynamodb list-tables
> aws dynamodb list-tables --region west
                                        eu-west-1
                                        eu-west-2
                                        eu-west-3
                                        us-west-1
```

Historial

Para ver y ejecutar los comandos utilizados anteriormente en el modo de mensaje automático, presione CTRL + R. El historial muestra los comandos anteriores que puede seleccionar mediante las teclas de flecha. En el ejemplo siguiente, se muestra el historial del modo de mensaje automático.

```
$ aws
> aws
        dynamodb list-tables
        s3 ls
```

Modos de mensaje automático

El mensaje automático para la versión 2 de AWS CLI se puede configurar en 2 modos:

- Modo completo: utiliza el mensaje automático cada vez que intenta ejecutar un comando `aws`, ya sea que lo llame manualmente usando el parámetro `--cli-auto-prompt` o lo habilite de forma permanente. Esto incluye presionar ENTER (INTRO) después de un comando completo o un comando incompleto.
- Modo parcial: utiliza el mensaje automático si un comando está incompleto o no se puede ejecutar debido a errores de validación del lado del cliente. Este modo es especialmente útil si tiene scripts preexistentes, runbooks, o solo desea que se le pregunte automáticamente sobre los comandos con los que no está familiarizado en lugar de preguntarle sobre cada comando.

Configuración del mensaje automático

Para configurar el mensaje automático, puede utilizar los siguientes métodos en orden de prioridad:

- Las opciones de línea de comandos habilitan o desactivan el mensaje automático para un solo comando. Use `--cli-auto-prompt` para solicitar un mensaje automático y `--no-cli-auto-prompt` para desactivarlo.
- Las variables del entorno utilizan la variable `aws_cli_auto_prompt`.
- Los archivos de configuración compartida usan la configuración`cli_auto_prompt`.

Control de la salida de comandos en la AWS CLI

En esra sección se describen las diferentes formas de controlar la salida de AWS Command Line Interface (AWS CLI). La personalización de la salida de la AWS CLI de su terminal puede mejorar la legibilidad, agilizar la automatización del scripting y facilitar la navegación a través de conjuntos de datos más grandes.

La AWS CLI admite varios formatos de salida, incluidos `json`, `text`, `yaml` y `table`. Algunos servicios tienen paginación del servidor para sus datos y la AWS CLI proporciona sus propias características del cliente para opciones de paginación adicionales.

Por último, la AWS CLI tiene filtrado tanto del servidor como del cliente que se puede usar de forma individual o conjuntamente para filtrar la salida de la AWS CLI.

Temas

- Salida de información confidencial
- Opciones de salida del servidor frente a las del cliente

- Configuración del formato de salida en la AWS CLI
- Uso de las opciones de paginación en la AWS CLI
- Filtrado de la salida en la AWS CLI

Salida de información confidencial

Algunas operaciones de la AWS CLI pueden dar como resultado información que podría considerarse confidencial, por ejemplo, la información de las variables de entorno. La exposición de esta información puede representar un riesgo para la seguridad en ciertas situaciones; por ejemplo, la información podría incluirse en los registros de integración e implementación continuos (CI/CD). Por lo tanto, es importante que revise cuándo se incluyen dichos resultados como parte de los registros y que los suprima cuando no los necesite.

Para obtener más información sobre la protección de datos confidenciales, consultethe section called "Protección de los datos".

Tenga en cuenta las siguientes prácticas recomendadas:

- Considere la posibilidad de recuperar los secretos mediante programación de un almacén de secretos, como. AWS Secrets Manager
- Revise el contenido de los registros de compilación para asegurarse de que no contienen información confidencial. Elija enfoques como canalizar a `/dev/null` o capturar la salida como una variable bash o PowerShell para suprimir las salidas de los comandos.

  El siguiente es un ejemplo de bash para redirigir la salida, pero no los errores, a `/dev/null`:

  ```
  $ aws s3 ls > /dev/null
  ```

  Para obtener información específica sobre cómo suprimir la salida del terminal, consulte la documentación del usuario del terminal que utilice.
- Tenga en cuenta el acceso a los registros y determine un acceso adecuado para el caso de uso.

Opciones de salida del servidor frente a las del cliente

La AWS CLI tiene filtrado tanto del servidor como del cliente que usted puede usar de forma individual o conjunta para filtrar la salida de la AWS CLI. El filtrado del servidor se procesa primero

y devuelve su salida para el filtrado del cliente. La API del servicio admite el filtrado del servidor. El filtrado del cliente está respaldado por el cliente AWS CLI mediante el uso del parámetro `--query`.

Las opciones de salida del servidor son características compatibles directamente con la API del servicio de Servicio de AWS. Los datos filtrados o paginados no se envían al cliente, lo que puede acelerar los tiempos de respuesta HTTP y mejorar el ancho de banda para conjuntos de datos más grandes.

Las opciones de salida del cliente son características creadas por la AWS CLI. Todos los datos se envían al cliente y, a continuación, la AWS CLI filtra o pagina el contenido que se muestra. Las operaciones del cliente no ahorran velocidad ni ancho de banda en el caso de conjuntos de datos más grandes.

Cuando las opciones del servidor y del cliente se utilizan juntas, las operaciones del servidor se completan primero y, después, se envían al cliente para las operaciones del cliente. De este modo se aprovechan los posibles ahorros de velocidad y ancho de banda de las opciones del servidor y, al mismo tiempo, se utilizan características adicionales de la AWS CLI para obtener el resultado deseado.

Configuración del formato de salida en la AWS CLI

Este tema describe los diferentes formatos de salida para la AWS Command Line Interface (AWS CLI). La AWS CLI admite los siguientes formatos de salida:

- **`json`**: la salida se formatea como una cadena JSON.
- **`yaml`**: la salida se formatea como una cadena YAML.
- **`yaml-stream`**: la salida se transmite y se formatea como una cadena YAML. El streaming permite un manejo más rápido de tipos de datos de gran tamaño.
- **`text`**: la salida tiene el formato de varias líneas de valores de cadena separados por tabuladores. Esto puede ser útil para pasar la salida a un procesador de texto, como `grep`, `sed` o `awk`.
- **`table`**: el resultado tiene el formato de una tabla en la que se usan los caracteres +|- para los bordes de celda. Normalmente, la información se presenta en un formato que es más fácil de leer que los demás formatos, pero que no es útil para programar.

Cómo seleccionar el formato de salida

Tal como se explica en el tema de configuración, el formato de salida se puede especificar de tres formas diferentes:

- Uso de la opciópn **`output`** en un perfil con nombre en el archivo **`config`**: el siguiente ejemplo establece el formato de la salida predeterminado como `text`.

```
[default]
output=text
```

- Uso de la variable de entorno de **`AWS_DEFAULT_OUTPUT`**: la siguiente salida establece el formato como `table` para los comandos de esta sesión de línea de comandos hasta que se cambie la variable o finalice la sesión. Con esta variable de entorno, se invalida cualquier valor establecido en el archivo `config`.

```
$ export AWS_DEFAULT_OUTPUT="table"
```

- Uso de la opción **`--output`** en la línea de comandos: el siguiente ejemplo establece la salida únicamente de este comando como `json`. El uso de esta opción en el comando anula cualquier variable de entorno definida actualmente o el valor en el archivo `config`.

```
$ aws swf list-domains --registration-status REGISTERED --output json
```

> **Important**
>
> El tipo de salida que especifique cambia cómo opera la opción `--query`:
>
> - Si especifica `--output text`, la salida se pagina antes de que se aplique el filtro `--query` y AWS CLI ejecuta la consulta una vez en cada página de la salida. Debido a esto, la consulta incluye el primer elemento que coincide en cada página, lo que puede dar lugar a una salida adicional inesperada. Para filtrar más la salida, puede usar otras herramientas de la línea de comandos como `head` o `tail`.
> - Si especifica `--output json`, `--output yaml` o `--output yaml-stream` la salida se procesará por completo como una única estructura nativa antes de aplicar el filtro `--query`. La AWS CLI ejecuta la consulta solo una vez en toda la estructura y produce un resultado filtrado que luego se ofrece como salida.

Formato de salida JSON

JSON es el formato de salida predeterminado de la AWS CLI. La mayoría de lenguajes de programación pueden decodificar fácilmente cadenas JSON con funciones integradas o con bibliotecas disponibles públicamente. Puede combinar la salida JSON con la opción —query de una forma eficaz para aplicar filtros y formato a la salida JSON de la AWS CLI.

Para aplicar un filtrado más avanzado que el que permite `--query`, considere la posibilidad de utilizar `jq`, un procesador JSON de línea de comandos. Puede descargarlo y consultar el tutorial oficial en http://stedolan.github.io/jq/.

A continuación, se muestra un ejemplo de una salida JSON:

```
$ aws iam list-users --output json
```

```
{
    "Users": [
        {
            "Path": "/",
            "UserName": "Admin",
            "UserId": "AIDA1111111111EXAMPLE",
            "Arn": "arn:aws:iam::123456789012:user/Admin",
            "CreateDate": "2014-10-16T16:03:09+00:00",
            "PasswordLastUsed": "2016-06-03T18:37:29+00:00"
        },
        {
            "Path": "/backup/",
            "UserName": "backup-user",
            "UserId": "AIDA2222222222EXAMPLE",
            "Arn": "arn:aws:iam::123456789012:user/backup/backup-user",
            "CreateDate": "2019-09-17T19:30:40+00:00"
        },
        {
            "Path": "/",
            "UserName": "cli-user",
            "UserId": "AIDA3333333333EXAMPLE",
            "Arn": "arn:aws:iam::123456789012:user/cli-user",
            "CreateDate": "2019-09-17T19:11:39+00:00"
        }
    ]
}
```

Formato de salida YAML

YAML es una buena opción para administrar la salida mediante programación con herramientas y servicios que emiten o consumen cadenas con formato YAML, como CloudFormation, que admite plantillas con formato YAML.

Para aplicar un filtrado más avanzado que el que permite `--query`, considere la posibilidad de utilizar `yq`, un procesador YAML de línea de comandos. Puede descargar `yq` en el repositorio de yq de GitHub.

A continuación, se muestra un ejemplo de una salida YAML.

```
$ aws iam list-users --output yaml
```

```
Users:
- Arn: arn:aws:iam::123456789012:user/Admin
  CreateDate: '2014-10-16T16:03:09+00:00'
  PasswordLastUsed: '2016-06-03T18:37:29+00:00'
  Path: /
  UserId: AIDA1111111111EXAMPLE
  UserName: Admin
- Arn: arn:aws:iam::123456789012:user/backup/backup-user
  CreateDate: '2019-09-17T19:30:40+00:00'
  Path: /backup/
  UserId: AIDA2222222222EXAMPLE
  UserName: arq-45EFD6D1-CE56-459B-B39F-F9C1F78FBE19
- Arn: arn:aws:iam::123456789012:user/cli-user
  CreateDate: '2019-09-17T19:30:40+00:00'
  Path: /
  UserId: AIDA3333333333EXAMPLE
  UserName: cli-user
```

Formato de salida de transmisión YAML

El formato `yaml-stream` aprovecha el formato YAML al tiempo que proporciona una visualización más receptiva/más rápida de los conjuntos de datos grandes mediante el streaming de datos a usted. Puede comenzar a ver y usar datos YAML antes de que se descargue toda la consulta.

Para aplicar un filtrado más avanzado que el que permite `--query`, considere la posibilidad de utilizar `yq`, un procesador YAML de línea de comandos. Puede descargar `yq` en el repositorio de yq de GitHub.

A continuación se muestra un ejemplo de la salida de `yaml-stream`.

```
$ aws iam list-users --output yaml-stream
```

```
- IsTruncated: false
  Users:
  - Arn: arn:aws:iam::123456789012:user/Admin
    CreateDate: '2014-10-16T16:03:09+00:00'
    PasswordLastUsed: '2016-06-03T18:37:29+00:00'
    Path: /
    UserId: AIDA1111111111EXAMPLE
    UserName: Admin
  - Arn: arn:aws:iam::123456789012:user/backup/backup-user
    CreateDate: '2019-09-17T19:30:40+00:00'
    Path: /backup/
    UserId: AIDA2222222222EXAMPLE
    UserName: arq-45EFD6D1-CE56-459B-B39F-F9C1F78FBE19
  - Arn: arn:aws:iam::123456789012:user/cli-user
    CreateDate: '2019-09-17T19:30:40+00:00'
    Path: /
    UserId: AIDA3333333333EXAMPLE
    UserName: cli-user
```

A continuación se muestra un ejemplo de salida `yaml-stream` en combinación con el uso del parámetro `--page-size` para paginar el contenido de YAML transmitido.

```
$ aws iam list-users --output yaml-stream --page-size 2
```

```
- IsTruncated: true
  Marker: ab1234cdef5ghi67jk8lmo9p/
q012rs3t445uv6789w0x1y2z/345a6b78c9d00/1efgh234ij56klmno78pqrstu90vwxyx
  Users:
  - Arn: arn:aws:iam::123456789012:user/Admin
    CreateDate: '2014-10-16T16:03:09+00:00'
    PasswordLastUsed: '2016-06-03T18:37:29+00:00'
    Path: /
    UserId: AIDA1111111111EXAMPLE
    UserName: Admin
  - Arn: arn:aws:iam::123456789012:user/backup/backup-user
    CreateDate: '2019-09-17T19:30:40+00:00'
    Path: /backup/
```

```
    UserId: AIDA2222222222EXAMPLE
    UserName: arq-45EFD6D1-CE56-459B-B39F-F9C1F78FBE19
- IsTruncated: false
  Users:
  - Arn: arn:aws:iam::123456789012:user/cli-user
    CreateDate: '2019-09-17T19:30:40+00:00'
    Path: /
    UserId: AIDA3333333333EXAMPLE
    UserName: cli-user
```

Formato de salida de texto

El formato `text` organiza la salida de la AWS CLI en líneas delimitadas por tabulaciones. Este formato funciona bien con herramientas de texto tradicionales de Unix, como `grep`, `sed` y `awk`, así como con el procesamiento de texto que realiza PowerShell.

El formato de salida de `text` sigue la estructura básica que se muestran a continuación. Las columnas se ordenan alfabéticamente según los nombres de las claves correspondientes del objeto JSON subyacente.

```
IDENTIFIER  sorted-column1 sorted-column2
IDENTIFIER2 sorted-column1 sorted-column2
```

A continuación se muestra un ejemplo de la salida de `text`. Cada campo está separado por tabulaciones de los demás, con una tabulación adicional si hay un campo vacío.

```
$ aws iam list-users --output text
```

```
USERS   arn:aws:iam::123456789012:user/Admin                2014-10-16T16:03:09+00:00
 2016-06-03T18:37:29+00:00   /          AIDA1111111111EXAMPLE   Admin
USERS   arn:aws:iam::123456789012:user/backup/backup-user   2019-09-17T19:30:40+00:00
                            /backup/   AIDA2222222222EXAMPLE   backup-user
USERS   arn:aws:iam::123456789012:user/cli-user             2019-09-17T19:11:39+00:00
                            /          AIDA3333333333EXAMPLE   cli-user
```

La cuarta columna es el campo `PasswordLastUsed` y está vacía en las dos últimas entradas, ya que esos usuarios nunca inician sesión en la Consola de administración de AWS.

Important

Le recomendamos encarecidamente que si especifica una salida *`text`*, utilice siempre la opción *`--query`* para garantizar un comportamiento coherente.
Esto se debe a que el formato de texto ordena alfabéticamente las columnas de salida por el nombre de la clave del objeto JSON subyacente que el servicio de AWS devuelve y podría haber recursos similares con distintos nombres de clave. Por ejemplo, la representación JSON de una instancia de Amazon EC2 basada en Linux podría tener elementos que no están presentes en la representación JSON de una instancia basada en Windows, o viceversa. Además, los recursos podrían tener elementos de valor de clave añadidos o eliminados en futuras actualizaciones, alterando el orden de las columnas. Aquí es donde `--query` incrementa la funcionalidad de la salida `text` para proporcionarle un control total sobre el formato de salida.
En el ejemplo siguiente, el comando especifica qué elementos se van a mostrar y define el orden de las columnas con la notación en lista `[key1, key2, ...]`. Esto le ofrece la plena confianza de que los valores de clave correctos se mostrarán siempre en la columna prevista. Por último, tenga en cuenta que la AWS CLI devuelve el valor `None` para las claves que no existen.

```
$ aws iam list-users --output text --query 'Users[*].
[UserName,Arn,CreateDate,PasswordLastUsed,UserId]'
```

```
Admin         arn:aws:iam::123456789012:user/Admin
 2014-10-16T16:03:09+00:00   2016-06-03T18:37:29+00:00   AIDA1111111111EXAMPLE
backup-user   arn:aws:iam::123456789012:user/backup-user
 2019-09-17T19:30:40+00:00   None                        AIDA2222222222EXAMPLE
cli-user      arn:aws:iam::123456789012:user/cli-backup
 2019-09-17T19:11:39+00:00   None                        AIDA3333333333EXAMPLE
```

El siguiente ejemplo muestra cómo se puede usar `grep` y `awk` con la salida `text` del comando `aws ec2 describe-instances`. El primer comando muestra la zona de disponibilidad, el estado actual y el ID de cada instancia en la salida `text`. El segundo comando procesa esa salida para mostrar únicamente los ID de instancia de todas las instancias en ejecución en la zona de disponibilidad `us-west-2a`.

```
$ aws ec2 describe-instances --query 'Reservations[*].Instances[*].
[Placement.AvailabilityZone, State.Name, InstanceId]' --output text
```

```
us-west-2a      running i-4b41a37c
us-west-2a      stopped i-a071c394
us-west-2b      stopped i-97a217a0
us-west-2a      running i-3045b007
us-west-2a      running i-6fc67758
```

```
$ aws ec2 describe-instances --query 'Reservations[*].Instances[*].
[Placement.AvailabilityZone, State.Name, InstanceId]' --output text | grep us-west-2a |
 grep running | awk '{print $3}'
```

```
i-4b41a37c
i-3045b007
i-6fc67758
```

El siguiente ejemplo va un paso más allá y muestra no solo cómo filtrar el resultado, sino cómo utilizar esa salida para automatizar los tipos de instancias cambiantes para cada instancia detenida.

```
$ aws ec2 describe-instances --query 'Reservations[*].Instances[*].[State.Name,
 InstanceId]' --output text |
> grep stopped |
> awk '{print $2}' |
> while read line;
> do aws ec2 modify-instance-attribute --instance-id $line --instance-type '{"Value":
 "m1.medium"}';
> done
```

La salida `text` también puede resultar útil en PowerShell. Como las columnas de la salida `text` están delimitadas por tabulaciones, puede dividir fácilmente la salida en una matriz utilizando el delimitador `` `t `` de PowerShell. El siguiente comando muestra el valor de la tercera columna (`InstanceId`) si la primera columna (`AvailabilityZone`) coincide con la cadena `us-west-2a`.

```
PS C:\>aws ec2 describe-instances --query 'Reservations[*].Instances[*].
[Placement.AvailabilityZone, State.Name, InstanceId]' --output text |
%{if ($_.split("`t")[0] -match "us-west-2a") { $_.split("`t")[2]; } }
```

```
-4b41a37c
```

```
i-a071c394
i-3045b007
i-6fc67758
```

Tenga en cuenta que, aunque en el ejemplo anterior se muestra cómo utilizar el parámetro `--query` para analizar los objetos JSON subyacentes y extraer la columna deseada, PowerShell dispone de una funcionalidad propia para gestionar JSON si la compatibilidad entre plataformas no es un problema. En lugar de tratar la salida como texto, como requieren la mayoría de los shells de comandos, PowerShell le permite utilizar el cmdlet `ConvertFrom-JSON` para producir un objeto estructurado jerárquicamente. A continuación, podrá acceder directamente al miembro que desee desde ese objeto.

```
(aws ec2 describe-instances --output json | ConvertFrom-
Json).Reservations.Instances.InstanceId
```

Tip

Si obtiene un texto en la salida y lo filtra con un solo campo utilizando el parámetro `--query`, la salida será una sola línea de valores separados por tabuladores. Para obtener cada valor en una línea independiente, puede colocar el campo de salida entre corchetes, tal y como se muestra en los siguientes ejemplos.
Salida de una sola línea separada por tabuladores:

```
$ aws iam list-groups-for-user --user-name susan  --output text --query
 "Groups[].GroupName"
```

```
HRDepartment    Developers      SpreadsheetUsers  LocalAdmins
```

Cada valor en su propia línea incluyendo `[GroupName]` entre corchetes:

```
$ aws iam list-groups-for-user --user-name susan  --output text --query
 "Groups[].[GroupName]"
```

```
HRDepartment
Developers
SpreadsheetUsers
LocalAdmins
```

Formato de salida de tabla

El formato `table` produce representaciones legibles para los humanos de la salida de la AWS CLI compleja en forma de tabla.

```
$ aws iam list-users --output table
```

```
-------------------------------------------------------------------------------------------------
|
 ListUsers                                                                                      |
+-----------------------------------------------------------------------------------------------
+
||
 Users                                                                                        ||
|+-----------------------------------------------------+--------------------------
+--------------------------+----------+----------------------+-------------+|
||                         Arn                          |       CreateDate          |
 PasswordLastUsed       |   Path   |        UserId         |   UserName  ||
|+-----------------------------------------------------+--------------------------
+--------------------------+----------+----------------------+-------------+|
||  arn:aws:iam::123456789012:user/Admin              | 2014-10-16T16:03:09+00:00 |
 2016-06-03T18:37:29+00:00 | /        | AIDA1111111111EXAMPLE | Admin       ||
||  arn:aws:iam::123456789012:user/backup/backup-user | 2019-09-17T19:30:40+00:00 |
                        | /backup/ | AIDA2222222222EXAMPLE | backup-user ||
||  arn:aws:iam::123456789012:user/cli-user           | 2019-09-17T19:11:39+00:00 |
                        | /        | AIDA3333333333EXAMPLE | cli-user    ||
+-------------------------------------------------------------------------------------------------
+
```

Puede combinar la opción `--query` con el formato `table` para mostrar un conjunto de elementos preseleccionados a partir de la salida en bruto. Observe las diferencias de la salida entre las notaciones de diccionario y lista: en el primer ejemplo los nombres de columna están ordenados alfabéticamente, y en el segundo ejemplo las columnas sin nombre se ordenan según lo definido por el usuario. Para obtener más información acerca de la opción `--query`, consulte Filtrado de la salida en la AWS CLI.

```
$ aws ec2 describe-volumes --query 'Volumes[*].
{ID:VolumeId,InstanceId:Attachments[0].InstanceId,AZ:AvailabilityZone,Size:Size}' --
output table
```

```
-----------------------------------------------------
```

```
|                  DescribeVolumes                  |
+------------+---------------+-------------+-------+
|     AZ     |      ID       | InstanceId  | Size  |
+------------+---------------+-------------+-------+
|  us-west-2a|  vol-e11a5288 |  i-a071c394 |  30   |
|  us-west-2a|  vol-2e410a47 |  i-4b41a37c |  8    |
+------------+---------------+-------------+-------+
```

```
$ aws ec2 describe-volumes --query 'Volumes[*].
[VolumeId,Attachments[0].InstanceId,AvailabilityZone,Size]' --output table
```

```
-------------------------------------------------
|                 DescribeVolumes                 |
+--------------+-------------+-------------+-----+
|  vol-e11a5288|  i-a071c394 |  us-west-2a |  30 |
|  vol-2e410a47|  i-4b41a37c |  us-west-2a |  8  |
+--------------+-------------+-------------+-----+
```

Uso de las opciones de paginación en la AWS CLI

En este tema se describen las diferentes formas de paginar la salida de AWS Command Line Interface (AWS CLI).

Hay principalmente dos formas de controlar la paginación desde laAWS CLI.

- Uso de parámetros de paginación del lado del servidor.
- Uso del programa de paginación del lado del cliente de salida predeterminado.

Los parámetros de paginación del lado del servidor procesan primero y cualquier salida se envía a la paginación del lado del cliente.

Paginación del lado del servidor

Para la mayoría de los comandos que pueden devolver una amplia lista de elementos, la AWS CLI tiene múltiples opciones del servidor para controlar el número de elementos que se incluyen en la salida cuando la AWS CLI llame a la API de un servicio para rellenar la lista. La API de servicio de AWS habilita la paginación del servidor en la AWS CLI, por lo que estas opciones solo funcionan si la API de servicio las habilita.

Las opciones para la mayoría de los comandos de la AWS CLI incluyen las siguientes opciones:

- Cómo usar el parámetro —no-paginate
- Cómo usar el parámetro —page-size
- Cómo usar el parámetro —max-items
- Cómo usar el parámetro —starting-token

De forma predeterminada, AWS CLI utiliza un tamaño de página determinado por el servicio individual y recupera todos los elementos disponibles. Por ejemplo, Simple Storage Service (Amazon S3) tiene un tamaño de página predeterminado de 1000. Si ejecuta `aws s3api list-objects` en un bucket de Simple Storage Service (Amazon S3) que contiene 3500 objetos, AWS CLI realiza cuatro llamadas a Simple Storage Service (Amazon S3) y se encarga de administrar por usted la lógica de paginación específica del servicio en segundo plano y de devolver los 3500 objetos en la salida final.

Para obtener información acerca de si un comando específico tiene paginación del servidor, consulte la Guía de referencia de la AWS CLI versión 2.

Cómo usar el parámetro —no-paginate

La opción `--no-paginate` desactiva los siguientes tokens de paginación en el lado del cliente. Cuando se utiliza un comando, de forma predeterminada, la AWS CLI realiza automáticamente varias llamadas para devolver todos los resultados posibles para crear paginación. Una llamada por cada página. La desactivación de la paginación hace la única llamada de la AWS CLI una vez para la primera página de resultados de comandos.

Por ejemplo, si ejecuta `aws s3api list-objects` en un bucket de Amazon S3 que contiene 3500 objetos, la AWS CLI solo realiza la primera llamada a Amazon S3, devolviendo solo los primeros 1000 objetos de la salida final.

```
$ aws s3api list-objects \
    --bucket amzn-s3-demo-bucket \
    --no-paginate
{
    "Contents": [
...
```

Cómo usar el parámetro —page-size

Si observa algún problema al ejecutar los comandos de la lista en un gran número de recursos, el tamaño de página predeterminado puede ser demasiado grande. Esto puede provocar las llamadas

a los servicios de AWS para superar el tiempo máximo permitido y generar un error de "tiempo de espera agotado". Puede utilizar la opción `--page-size` para especificar que la AWS CLI solicite un número menor de elementos de cada llamada al servicio de AWS. La AWS CLI recupera aun así la lista completa, pero realiza un mayor número de llamadas a la API en segundo plano y recupera un menor número de elementos con cada llamada. Esto ofrece a las llamadas individuales una mayor posibilidad de que tengan éxito sin que se agote el tiempo de espera. El cambio del tamaño de página no afecta a la salida; solo afecta a la cantidad de llamadas a la API que hay que realizar para generar la salida.

```
$ aws s3api list-objects \
    --bucket amzn-s3-demo-bucket \
    --page-size 100
{
    "Contents": [
...
```

Cómo usar el parámetro —max-items

Para incluir menos elementos a la vez en la salida de la AWS CLI, utilice la opción `--max-items`. La AWS CLI sigue administrando la paginación con el servicio tal y como se indicó anteriormente, pero solamente muestra a la vez el número de elementos especificado.

```
$ aws s3api list-objects \
    --bucket amzn-s3-demo-bucket \
    --max-items 100
{
    "NextToken": "eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ==",
    "Contents": [
...
```

Cómo usar el parámetro —starting-token

Si el número de elementos de salida (`--max-items`) es inferior al número total de elementos devueltos por las llamadas básicas a la API, la salida incluirá un `NextToken` que podrá pasar a un comando posterior para recuperar el siguiente conjunto de elementos. En el siguiente ejemplo se muestra cómo usar el valor `NextToken` devuelto por el ejemplo anterior y le permite recuperar los segundos 100 elementos.

> **Note**
>
> El parámetro `--starting-token` no puede ser nulo ni está vacío. Si el comando anterior no devuelve un valor `NextToken`, no hay más elementos para devolver y no es necesario llamar al comando de nuevo.

```
$ aws s3api list-objects \
    --bucket amzn-s3-demo-bucket \
    --max-items 100 \
    --starting-token eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ==
{
    "Contents": [
...
```

Puede que el servicio de AWS especificado no devuelva los elementos en el mismo orden cada vez que lo llame. Si especifica diferentes valores para `--page-size` y `--max-items`, puede obtener resultados inesperados en el que faltan elementos o están duplicados. Para evitar esto, utilice el mismo número con `--page-size` y `--max-items` para sincronizar la paginación de la AWS CLI con la del servicio subyacente. También puede recuperar la lista completa y realizar las operaciones de paginación necesarias de forma local.

Paginación del lado del cliente

La versión 2 de la AWS CLI proporciona el uso de un programa de paginación del lado del cliente para la salida. De forma predeterminada, esta función devuelve todas las salidas a través del programa de paginación predeterminado del sistema operativo.

En orden de prioridad, puede especificar la paginación de salida de estas dos maneras:

- Uso de la configuración de `cli_pager` en el archivo `config` en el perfil `default` o con nombre.
- Uso de la variable de entorno `AWS_PAGER`.
- Uso de la variable de entorno `PAGER`.

En orden de prioridad, puede deshabilitar todo el uso de un programa de paginación externo de las siguientes maneras:

- Use la opción de línea de comandos `--no-cli-pager` para desactivar la paginación para un solo uso de comando.
- Establezca la configuración `cli_pager` o la variable `AWS_PAGER` en una cadena vacía.

Temas de la paginación del lado del cliente:

- Cómo utilizar la configuración cli_pager
- Cómo definir la variable de entorno AWS_PAGER
- Cómo usar la opción —no-cli-pager
- Cómo usar marcadores de paginación

Cómo utilizar la configuración cli_pager

Puede guardar las opciones de configuración y las credenciales que utiliza con frecuencia en archivos que son mantenidos por la AWS CLI. La configuración de un perfil de nombre tiene prioridad sobre la configuración en el perfil `default`. Para obtener más información sobre los valores de configuración, consulte Opciones de los archivos de configuración y credenciales en la AWS CLI.

El siguiente ejemplo establece la paginación de salida predeterminada en el programa `less`.

```
[default]
cli_pager=less
```

En el ejemplo siguiente se establece el valor predeterminado para deshabilitar el uso de un paginador.

```
[default]
cli_pager=
```

Cómo definir la variable de entorno AWS_PAGER

El siguiente ejemplo establece la paginación de salida predeterminada en el programa `less`. Para obtener más información sobre las variables de entorno, consulte Configuración de variables de entorno para la AWS CLI.

Linux and macOS

```
$ export AWS_PAGER="less"
```

Windows

```
C:\> setx AWS_PAGER "less"
```

Cómo usar la opción —no-cli-pager

Para deshabilitar el uso de un paginador en un único comando, utilice la opción `--no-cli-pager`. Para obtener más información acerca de las opciones de línea de comandos, consulte Opciones de línea de comandos en la AWS CLI.

```
$ aws s3api list-objects \
    --bucket amzn-s3-demo-bucket \
    --no-cli-pager
{
    "Contents": [
...
```

Cómo usar marcadores de paginación

Puede especificar marcadores que se usarán automáticamente con el programa de paginación. Los marcadores dependen del programa de paginación que utilice. Los siguientes ejemplos son para los valores predeterminados típicos de `less` y `more`.

Linux and macOS

Si no especifica lo contrario, la versión 2 de AWS CLI que usa el paginador por defecto es `less`. Si no tiene el conjunto de variables de entorno `LESS`, la versión 2 de la AWS CLI utiliza los marcadores `FRX`. Puede combinar marcadores especificándolos al establecer el paginador AWS CLI.

En este ejemplo se usa el marcador `S`. Este marcador se combina con los marcadores predeterminados `FRX` para crear un marcador `FRXS`.

```
$ export AWS_PAGER="less -S"
```

Si no quiere utilizar ninguno de los marcadores `FRX`, puede negarlos. En el siguiente ejemplo se niega el marcador `F` para crear un marcador `RX` final.

```
$ export AWS_PAGER="less -+F"
```

Para obtener más información sobre los marcadores `less`, consulte menos en manpages.org.

Windows

Si no especifica lo contrario, la versión 2 de la AWS CLI del paginador utiliza por defecto `more` sin marcadores adicionales.

En el siguiente ejemplo se usa el parámetro `/c`.

```
C:\> setx AWS_PAGER "more /c"
```

Para obtener más información sobre `more` marcadores, consulte `more` en Documentos de Microsoft.

Filtrado de la salida en la AWS CLI

La AWS Command Line Interface (AWS CLI) tiene filtrado tanto del servidor como del cliente que usted puede usar de forma individual o juntos para filtrar su salida AWS CLI. El filtrado del lado del servidor se procesa primero y devuelve su salida para el filtrado del lado del cliente.

- El filtrado del lado del servidor es compatible con la API, y generalmente lo implementa con un parámetro `--filter`. El servicio solo devuelve resultados coincidentes que pueden acelerar los tiempos de respuesta HTTP para conjuntos de datos grandes.
- El filtrado del cliente está respaldado por el cliente AWS CLI mediante el uso del parámetro `--query`. Este parámetro tiene capacidades que el filtrado del servidor puede no tener.

Temas

- Filtrado en el servidor
- Filtrado del lado del cliente
- Combinación del filtrado del lado del cliente y del servidor
- Recursos adicionales

Filtrado en el servidor

El filtrado en el servidor en el AWS CLI se proporciona a través del API de servicio AWS. El servicio AWS solo devuelve los registros de la respuesta HTTP que coinciden con el filtro, lo que puede

acelerar los tiempos de respuesta HTTP para conjuntos de datos grandes. Dado que el filtrado del lado del servidor está definido por la API del servicio, los nombres de los parámetros y las funciones varían entre los servicios. Algunos nombres de parámetros comunes utilizados para filtrar son:

- `--filter` tales como ses y ce.
- `--filters` tales como ec2, autoescalado y rds.
- Nombres que empiezan por la palabra `filter`, por ejemplo `--filter-expression` para el comando `aws dynamodb scan`.

Para obtener información acerca de si un comando específico tiene filtrado del lado del servidor y las reglas de filtrado, consulte la AWS CLIversión 2 de la guía de referencia de .

Filtrado del lado del cliente

La AWS CLI ofrece capacidades de filtrado de salida basadas en JSON integradas con el parámetro `--query`. El parámetro `--query` es una potente herramienta que se puede utilizar para personalizar el contenido y el estilo de la salida. El parámetro `--query` toma la respuesta HTTP que regresa del servidor y filtra los resultados antes de mostrarlos. Dado que toda la respuesta HTTP se envía al cliente antes del filtrado, el filtrado del lado del cliente puede ser más lento que el filtrado del lado del servidor para grandes conjuntos de datos.

Las consultas usan sintaxis JMESPath para crear expresiones para filtrar la salida. Para obtener más información acerca de la sintaxis de JMesPath, consulte el Tutorial del sitio web JMESPath.

> **Important**
>
> El tipo de salida que especifique cambia cómo opera la opción `--query`:
>
> - Si especifica `--output text`, la salida se pagina antes de que se aplique el filtro `--query` y AWS CLI ejecuta la consulta una vez en cada página de la salida. Debido a esto, la consulta incluye el primer elemento que coincide en cada página, lo que puede dar lugar a una salida adicional inesperada. Para filtrar más la salida, puede usar otras herramientas de la línea de comandos como `head` o `tail`.
> - Si especifica `--output json`, `--output yaml` o `--output yaml-stream` la salida se procesará por completo como una única estructura nativa antes de aplicar el filtro `--query`. La AWS CLI ejecuta la consulta solo una vez en toda la estructura y produce un resultado filtrado que luego se ofrece como salida.

Temas de filtrado del lado del cliente

- Antes de comenzar
- Identificadores
- Cómo seleccionar de una lista
- Filtrado de datos anidados
- Aplanamiento de los resultados
- Filtrado para valores específicos
- Expresiones de canalización
- Filtrado para varios valores de identificador
- Agregado de etiquetas a valores de identificador
- Funciones
- Ejemplos --query avanzados

Antes de comenzar

> **Note**
>
> Estos ejemplos de expresiones de filtro están escritos para intérpretes de comandos de tipo Linux básicos. Cuando utilice estos ejemplos, asegúrese de utilizar las reglas de entrecomillado correctas para el intérprete de comandos del terminal. La forma en que el terminal interpreta las entradas puede cambiar enormemente lo que se envía a la AWS CLI. La forma en que el terminal lee las comillas simples `'`, las comillas dobles `"` o las comillas inversas `` ` `` puede cambiar la forma de leer el contenido.
> Para obtener más información, consulte the section called “Comillas con cadenas”.

En la siguiente salida JSON se muestra un ejemplo de lo que el parámetro `--query` puede producir. La salida describe tres volúmenes de Amazon EBS conectados a instancias independientes de Amazon EC2.

Ejemplo de resultado

```
$ aws ec2 describe-volumes
{
  "Volumes": [
    {
```

```
      "AvailabilityZone": "us-west-2a",
      "Attachments": [
        {
          "AttachTime": "2013-09-17T00:55:03.000Z",
          "InstanceId": "i-a071c394",
          "VolumeId": "vol-e11a5288",
          "State": "attached",
          "DeleteOnTermination": true,
          "Device": "/dev/sda1"
        }
      ],
      "VolumeType": "standard",
      "VolumeId": "vol-e11a5288",
      "State": "in-use",
      "SnapshotId": "snap-f23ec1c8",
      "CreateTime": "2013-09-17T00:55:03.000Z",
      "Size": 30
    },
    {
      "AvailabilityZone": "us-west-2a",
      "Attachments": [
        {
          "AttachTime": "2013-09-18T20:26:16.000Z",
          "InstanceId": "i-4b41a37c",
          "VolumeId": "vol-2e410a47",
          "State": "attached",
          "DeleteOnTermination": true,
          "Device": "/dev/sda1"
        }
      ],
      "VolumeType": "standard",
      "VolumeId": "vol-2e410a47",
      "State": "in-use",
      "SnapshotId": "snap-708e8348",
      "CreateTime": "2013-09-18T20:26:15.000Z",
      "Size": 8
    },
    {
      "AvailabilityZone": "us-west-2a",
      "Attachments": [
        {
          "AttachTime": "2020-11-20T19:54:06.000Z",
          "InstanceId": "i-1jd73kv8",
          "VolumeId": "vol-a1b3c7nd",
```

```
          "State": "attached",
          "DeleteOnTermination": true,
          "Device": "/dev/sda1"
        }
      ],
      "VolumeType": "standard",
      "VolumeId": "vol-a1b3c7nd",
      "State": "in-use",
      "SnapshotId": "snap-234087fb",
      "CreateTime": "2020-11-20T19:54:05.000Z",
      "Size": 15
    }
  ]
}
```

Identificadores

Los identificadores son las etiquetas de los valores de salida. Al crear filtros, se utilizan identificadores para reducir los resultados de la consulta. En el siguiente ejemplo de salida, se resaltan todos los identificadores como `Volumes`, `AvailabilityZone` y `AttachTime`.

```
$ aws ec2 describe-volumes
{
  "Volumes": [
    {
      "AvailabilityZone": "us-west-2a",
      "Attachments": [
        {
          "AttachTime": "2013-09-17T00:55:03.000Z",
          "InstanceId": "i-a071c394",
          "VolumeId": "vol-e11a5288",
          "State": "attached",
          "DeleteOnTermination": true,
          "Device": "/dev/sda1"
        }
      ],
      "VolumeType": "standard",
      "VolumeId": "vol-e11a5288",
      "State": "in-use",
      "SnapshotId": "snap-f23ec1c8",
      "CreateTime": "2013-09-17T00:55:03.000Z",
      "Size": 30
    },
```

```
    {
      "AvailabilityZone": "us-west-2a",
      "Attachments": [
        {
          "AttachTime": "2013-09-18T20:26:16.000Z",
          "InstanceId": "i-4b41a37c",
          "VolumeId": "vol-2e410a47",
          "State": "attached",
          "DeleteOnTermination": true,
          "Device": "/dev/sda1"
        }
      ],
      "VolumeType": "standard",
      "VolumeId": "vol-2e410a47",
      "State": "in-use",
      "SnapshotId": "snap-708e8348",
      "CreateTime": "2013-09-18T20:26:15.000Z",
      "Size": 8
    },
    {
      "AvailabilityZone": "us-west-2a",
      "Attachments": [
        {
          "AttachTime": "2020-11-20T19:54:06.000Z",
          "InstanceId": "i-1jd73kv8",
          "VolumeId": "vol-a1b3c7nd",
          "State": "attached",
          "DeleteOnTermination": true,
          "Device": "/dev/sda1"
        }
      ],
      "VolumeType": "standard",
      "VolumeId": "vol-a1b3c7nd",
      "State": "in-use",
      "SnapshotId": "snap-234087fb",
      "CreateTime": "2020-11-20T19:54:05.000Z",
      "Size": 15
    }
  ]
}
```


Para obtener más información, consulte Identificadores en el sitio web JMESPath.

Cómo seleccionar de una lista

Una lista o matriz es un identificador que va seguido de un corchete "`[`" como `Volumes` y `Attachments` en la the section called "Antes de comenzar".

Sintaxis

```
<listName>[ ]
```

Para filtrar todos los resultados de una matriz, puede usar la notación comodín. Las expresiones comodín son expresiones utilizadas para devolver elementos utilizando la notación `*`.

En el siguiente ejemplo se consulta todo el contenido de `Volumes`.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[*]'
[
  {
    "AvailabilityZone": "us-west-2a",
    "Attachments": [
      {
        "AttachTime": "2013-09-17T00:55:03.000Z",
        "InstanceId": "i-a071c394",
        "VolumeId": "vol-e11a5288",
        "State": "attached",
        "DeleteOnTermination": true,
        "Device": "/dev/sda1"
      }
    ],
    "VolumeType": "standard",
    "VolumeId": "vol-e11a5288",
    "State": "in-use",
    "SnapshotId": "snap-f23ec1c8",
    "CreateTime": "2013-09-17T00:55:03.000Z",
    "Size": 30
  },
  {
    "AvailabilityZone": "us-west-2a",
    "Attachments": [
      {
        "AttachTime": "2020-11-20T19:54:06.000Z",
        "InstanceId": "i-1jd73kv8",
```

```
        "VolumeId": "vol-a1b3c7nd",
        "State": "attached",
        "DeleteOnTermination": true,
        "Device": "/dev/sda1"
      }
    ],
    "VolumeType": "standard",
    "VolumeId": "vol-a1b3c7nd",
    "State": "in-use",
    "SnapshotId": "snap-234087fb",
    "CreateTime": "2020-11-20T19:54:05.000Z",
    "Size": 15
  }
]
```

Para ver un volumen específico en la matriz por índice, se llama al índice de matriz. Por ejemplo, el primer elemento de la matriz `Volumes` tiene un índice de 0, lo que resulta en la consulta `Volumes[0]`. Para obtener más información acerca de los índices de matriz, consulte Expresiones de índice en el Sitio web JMESPath.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[0]'
{
  "AvailabilityZone": "us-west-2a",
  "Attachments": [
    {
      "AttachTime": "2013-09-17T00:55:03.000Z",
      "InstanceId": "i-a071c394",
      "VolumeId": "vol-e11a5288",
      "State": "attached",
      "DeleteOnTermination": true,
      "Device": "/dev/sda1"
    }
  ],
  "VolumeType": "standard",
  "VolumeId": "vol-e11a5288",
  "State": "in-use",
  "SnapshotId": "snap-f23ec1c8",
  "CreateTime": "2013-09-17T00:55:03.000Z",
  "Size": 30
}
```

Para ver un rango específico de volúmenes por índice, utilice `slice` con la siguiente sintaxis, donde iniciar es el índice de matriz inicial, detener es el índice en el que el filtro deja de procesarse y paso es el intervalo de omisión.

Sintaxis

```
<arrayName>[<start>:<stop>:<step>]
```

Si se omite cualquiera de estos elementos de la expresión de sector, utilizan los siguientes valores predeterminados:

- Iniciar: el primer índice de la lista, 0.
- Detener: el último índice de la lista.
- Paso: sin saltar paso, donde el valor es 1.

Para devolver solo los dos primeros volúmenes, utilice un valor inicial de 0, un valor de detención de 2 y un valor de paso de 1, como se muestra en el siguiente ejemplo.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[0:2:1]'
[
  {
    "AvailabilityZone": "us-west-2a",
    "Attachments": [
      {
        "AttachTime": "2013-09-17T00:55:03.000Z",
        "InstanceId": "i-a071c394",
        "VolumeId": "vol-e11a5288",
        "State": "attached",
        "DeleteOnTermination": true,
        "Device": "/dev/sda1"
      }
    ],
    "VolumeType": "standard",
    "VolumeId": "vol-e11a5288",
    "State": "in-use",
    "SnapshotId": "snap-f23ec1c8",
    "CreateTime": "2013-09-17T00:55:03.000Z",
    "Size": 30
  },
  {
```

```
    "AvailabilityZone": "us-west-2a",
    "Attachments": [
      {
        "AttachTime": "2013-09-18T20:26:16.000Z",
        "InstanceId": "i-4b41a37c",
        "VolumeId": "vol-2e410a47",
        "State": "attached",
        "DeleteOnTermination": true,
        "Device": "/dev/sda1"
      }
    ],
    "VolumeType": "standard",
    "VolumeId": "vol-2e410a47",
    "State": "in-use",
    "SnapshotId": "snap-708e8348",
    "CreateTime": "2013-09-18T20:26:15.000Z",
    "Size": 8
  }
]
```

Dado que este ejemplo contiene valores predeterminados, puede acortar el segmento de `Volumes[0:2:1]` a `Volumes[:2]`.

En el ejemplo siguiente se omiten los valores predeterminados y se devuelve cada dos volúmenes de toda la matriz.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[::2]'
[
  {
    "AvailabilityZone": "us-west-2a",
    "Attachments": [
      {
        "AttachTime": "2013-09-17T00:55:03.000Z",
        "InstanceId": "i-a071c394",
        "VolumeId": "vol-e11a5288",
        "State": "attached",
        "DeleteOnTermination": true,
        "Device": "/dev/sda1"
      }
    ],
    "VolumeType": "standard",
    "VolumeId": "vol-e11a5288",
```

```
    "State": "in-use",
    "SnapshotId": "snap-f23ec1c8",
    "CreateTime": "2013-09-17T00:55:03.000Z",
    "Size": 30
  },
  {
    "AvailabilityZone": "us-west-2a",
    "Attachments": [
      {
        "AttachTime": "2020-11-20T19:54:06.000Z",
        "InstanceId": "i-1jd73kv8",
        "VolumeId": "vol-a1b3c7nd",
        "State": "attached",
        "DeleteOnTermination": true,
        "Device": "/dev/sda1"
      }
    ],
    "VolumeType": "standard",
    "VolumeId": "vol-a1b3c7nd",
    "State": "in-use",
    "SnapshotId": "snap-234087fb",
    "CreateTime": "2020-11-20T19:54:05.000Z",
    "Size": 15
  }
]
```

Los pasos también pueden utilizar números negativos para filtrar en el orden inverso de una matriz como se muestra en el siguiente ejemplo.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[::-2]'
[
  {
    "AvailabilityZone": "us-west-2a",
    "Attachments": [
      {
        "AttachTime": "2020-11-20T19:54:06.000Z",
        "InstanceId": "i-1jd73kv8",
        "VolumeId": "vol-a1b3c7nd",
        "State": "attached",
        "DeleteOnTermination": true,
        "Device": "/dev/sda1"
      }
```

```
    ],
    "VolumeType": "standard",
    "VolumeId": "vol-a1b3c7nd",
    "State": "in-use",
    "SnapshotId": "snap-234087fb",
    "CreateTime": "2020-11-20T19:54:05.000Z",
    "Size": 15
  },
  {
    "AvailabilityZone": "us-west-2a",
    "Attachments": [
      {
        "AttachTime": "2013-09-17T00:55:03.000Z",
        "InstanceId": "i-a071c394",
        "VolumeId": "vol-e11a5288",
        "State": "attached",
        "DeleteOnTermination": true,
        "Device": "/dev/sda1"
      }
    ],
    "VolumeType": "standard",
    "VolumeId": "vol-e11a5288",
    "State": "in-use",
    "SnapshotId": "snap-f23ec1c8",
    "CreateTime": "2013-09-17T00:55:03.000Z",
    "Size": 30
  }
]
```

Para obtener más información, consulte Sectores en el Sitio web JMESPath.

Filtrado de datos anidados

Para restringir el filtrado de `Volumes[*]` para los valores anidados, se utilizan subexpresiones agregando un punto y sus criterios de filtro.

Sintaxis

```
<expression>.<expression>
```

En el siguiente ejemplo se muestra toda la información de `Attachments`para todos los volúmenes.

```
$ aws ec2 describe-volumes \
```

```
    --query 'Volumes[*].Attachments'
[
  [
    {
      "AttachTime": "2013-09-17T00:55:03.000Z",
      "InstanceId": "i-a071c394",
      "VolumeId": "vol-e11a5288",
      "State": "attached",
      "DeleteOnTermination": true,
      "Device": "/dev/sda1"
    }
  ],
  [
    {
      "AttachTime": "2013-09-18T20:26:16.000Z",
      "InstanceId": "i-4b41a37c",
      "VolumeId": "vol-2e410a47",
      "State": "attached",
      "DeleteOnTermination": true,
      "Device": "/dev/sda1"
    }
  ],
  [
    {
      "AttachTime": "2020-11-20T19:54:06.000Z",
      "InstanceId": "i-1jd73kv8",
      "VolumeId": "vol-a1b3c7nd",
      "State": "attached",
      "DeleteOnTermination": true,
      "Device": "/dev/sda1"
    }
  ]
]
```

Para filtrar más los valores anidados, agregue la expresión para cada indentificador anidado. En el ejemplo siguiente, se muestran los `State` para todos los `Volumes`.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[*].Attachments[*].State'
[
  [
    "attached"
  ],
```

```
  [
    "attached"
  ],
  [
    "attached"
  ]
]
```

Aplanamiento de los resultados

Para obtener más información, consulte SubExpresiones en elSitio web JMESPath.

Puede aplanar los resultados de `Volumes[*].Attachments[*].State` eliminando la notación comodín que resulta en la consulta `Volumes[*].Attachments[].State`. El aplanamiento a menudo es útil para mejorar la legibilidad de los resultados.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[*].Attachments[].State'
[
  "attached",
  "attached",
  "attached"
]
```

Para obtener más información, consulte Aplanar en el Sitio web JMESPath.

Filtrado para valores específicos

Para filtrar valores específicos de una lista, utilice una expresión de filtro como se muestra en la siguiente sintaxis.

Sintaxis

```
? <expression> <comparator> <expression>]
```

Los comparadores de expresiones incluyen ==, !=, <, <=, > y >=. En el ejemplo siguiente se filtra para el `VolumeIds`, para todos los `Volumes` en un `AttachedState`.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[*].Attachments[?State==`attached`].VolumeId'
[
```

```
  [
    "vol-e11a5288"
  ],
  [
    "vol-2e410a47"
  ],
  [
    "vol-a1b3c7nd"
  ]
]
```

Esto se puede aplanar, lo que resulta en el siguiente ejemplo.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[*].Attachments[?State==`attached`].VolumeId[]'
[
  "vol-e11a5288",
  "vol-2e410a47",
  "vol-a1b3c7nd"
]
```

En el ejemplo siguiente se filtra para el `VolumeIds`, de todos los `Volumes` que tienen un tamaño inferior a 20.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[?Size < `20`].VolumeId'
[
  "vol-2e410a47",
  "vol-a1b3c7nd"
]
```

Para obtener más información, consulte Expresiones de filtro en el Sitio web JMESPath.

Expresiones de canalización

Puede canalizar los resultados de un filtro a una nueva lista y, a continuación, filtrar el resultado con otra expresión utilizando la siguiente sintaxis:

Sintaxis

```
<expression> | <expression>]
```

En el siguiente ejemplo se toman los resultados del filtro de la expresión `Volumes[*].Attachments[].InstanceId` y genera el primer resultado en la matriz.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[*].Attachments[].InstanceId | [0]'
"i-a071c394"
```

En este ejemplo, se crea primero la matriz a partir de la siguiente expresión.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[*].Attachments[].InstanceId'
"i-a071c394",
  "i-4b41a37c",
  "i-1jd73kv8"
```

Y luego devuelve el primer elemento de esa matriz.

```
"i-a071c394"
```

Para obtener más información, consulte Expresiones de canalización en el Sitio web JMESPath.

Filtrado para varios valores de identificador

Para filtrar por varios identificadores, utilice una lista de selección múltiple mediante la siguiente sintaxis:

Sintaxis

```
<listName>[].[<expression>, <expression>]
```

En el siguiente ejemplo, `VolumeId` y `VolumeType` se filtran en la lista `Volumes` lo que resulta en la siguiente expresión.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[].[VolumeId, VolumeType]'
[
  [
    "vol-e11a5288",
    "standard"
```

```
  ],
  [
    "vol-2e410a47",
    "standard"
  ],
  [
    "vol-a1b3c7nd",
    "standard"
  ]
]
```

Para agregar datos anidados a la lista, agregue otra lista de selección múltiple. El siguiente ejemplo amplía el ejemplo anterior al filtrar también `InstanceId` y `State` en la lista de `Attachments` anidada. Esto da como resultado la siguiente expresión.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[].[VolumeId, VolumeType, Attachments[].[InstanceId, State]]'
[
  [
    "vol-e11a5288",
    "standard",
    [
      [
        "i-a071c394",
        "attached"
      ]
    ]
  ],
  [
    "vol-2e410a47",
    "standard",
    [
      [
        "i-4b41a37c",
        "attached"
      ]
    ]
  ],
  [
    "vol-a1b3c7nd",
    "standard",
    [
      [
```

```
        "i-1jd73kv8",
        "attached"
      ]
    ]
  ]
]
```

Para que sea más legible, aplane la expresión como se muestra en el siguiente ejemplo.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[].[VolumeId, VolumeType, Attachments[].[InstanceId, State][]][]'
[
  "vol-e11a5288",
  "standard",
  [
    "i-a071c394",
    "attached"
  ],
  "vol-2e410a47",
  "standard",
  [
    "i-4b41a37c",
    "attached"
  ],
  "vol-a1b3c7nd",
  "standard",
  [
    "i-1jd73kv8",
    "attached"
  ]
]
```

Para obtener más información, consulte la Lista de selección múltiple en el Sitio web JMESPath.

Agregado de etiquetas a valores de identificador

Para facilitar la lectura de este resultado, utilice un hash de selección múltiple con la siguiente sintaxis.

Sintaxis

```
<listName>[].{<label>: <expression>, <label>: <expression>}
```

No es necesario que la etiqueta de identificación sea la misma que el nombre del identificador. En el ejemplo siguiente se utiliza la etiqueta `VolumeType` para los valores `VolumeType`.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[].{VolumeType: VolumeType}'
[
  {
    "VolumeType": "standard",
  },
  {
    "VolumeType": "standard",
  },
  {
    "VolumeType": "standard",
  }
]
```

Para mayor simplicidad, en el siguiente ejemplo se conservan los nombres de los identificadores de cada etiqueta y se muestra el `VolumeId`, `VolumeType`, `InstanceId` y `State` de todos los volúmenes:

```
$ aws ec2 describe-volumes \
    --query 'Volumes[].{VolumeId: VolumeId, VolumeType: VolumeType, InstanceId:
 Attachments[0].InstanceId, State: Attachments[0].State}'
[
  {
    "VolumeId": "vol-e11a5288",
    "VolumeType": "standard",
    "InstanceId": "i-a071c394",
    "State": "attached"
  },
  {
    "VolumeId": "vol-2e410a47",
    "VolumeType": "standard",
    "InstanceId": "i-4b41a37c",
    "State": "attached"
  },
  {
    "VolumeId": "vol-a1b3c7nd",
    "VolumeType": "standard",
    "InstanceId": "i-1jd73kv8",
    "State": "attached"
```

```
  }
]
```

Para obtener más información, consulte Hash de selección múltiple en el Sitio web JMESPath.

Funciones

La sintaxis JMESPath contiene muchas funciones que puede utilizar para sus consultas. Para obtener información sobre las funciones de JMESPath, consulte Funciones integradas en el Sitio web JMESPath.

Para demostrar cómo puede incorporar una función a sus consultas, en el siguiente ejemplo se utiliza la función `sort_by`. La función `sort_by` ordena una matriz utilizando una expresión como clave de ordenación utilizando la siguiente sintaxis:

Sintaxis

```
sort_by(<listName>, <sort expression>)[].<expression>
```

En el ejemplo siguiente se utiliza el ejemplo de hash de selección múltiple y ordena la salida por `VolumeId`.

```
$ aws ec2 describe-volumes \
    --query 'sort_by(Volumes, &VolumeId)[].{VolumeId: VolumeId, VolumeType: VolumeType,
 InstanceId: Attachments[0].InstanceId, State: Attachments[0].State}'
[
  {
    "VolumeId": "vol-2e410a47",
    "VolumeType": "standard",
    "InstanceId": "i-4b41a37c",
    "State": "attached"
  },
  {
    "VolumeId": "vol-a1b3c7nd",
    "VolumeType": "standard",
    "InstanceId": "i-1jd73kv8",
    "State": "attached"
  },
  {
    "VolumeId": "vol-e11a5288",
    "VolumeType": "standard",
    "InstanceId": "i-a071c394",
```

```
    "State": "attached"
  }
]
```

Para obtener más información, consulte sort_by en el Sitio web JMESPath.

Ejemplos **`--query`** avanzados

Para extraer información de un elemento específico

En el siguiente ejemplo, se usa el parámetro `--query` para encontrar un elemento específico en una lista y, a continuación, extrae la información de ese elemento. En el ejemplo, se muestran todas las `AvailabilityZones` asociadas con el punto de enlace de servicio especificado. Extrae el elemento de la lista `ServiceDetails` que tiene el `ServiceName` especificado; a continuación, genera el campo `AvailabilityZones` a partir de ese elemento seleccionado.

```
$ aws --region us-east-1 ec2 describe-vpc-endpoint-services \
    --query 'ServiceDetails[?ServiceName==`com.amazonaws.us-
east-1.ecs`].AvailabilityZones'
[
    [
        "us-east-1a",
        "us-east-1b",
        "us-east-1c",
        "us-east-1d",
        "us-east-1e",
        "us-east-1f"
    ]
]
```

Para mostrar instantáneas después de la fecha de creación especificada

En el siguiente ejemplo se muestra cómo enumerar todas las instantáneas que se han creado después de una fecha especificada, incluidos solo algunos de los campos disponibles en la salida.

```
$ aws ec2 describe-snapshots --owner self \
    --output json \
    --query 'Snapshots[?StartTime>=`2018-02-07`].
{Id:SnapshotId,VId:VolumeId,Size:VolumeSize}'
[
    {
        "id": "snap-0effb42b7a1b2c3d4",
```

```
        "vid": "vol-0be9bb0bf12345678",
        "Size": 8
    }
]
```

Para mostrar las AMI más recientes

En el siguiente ejemplo, se muestran las cinco imágenes de Amazon Machine (AMI) más reciente que ha creado, ordenadas de la más reciente y a la más antigua.

```
$ aws ec2 describe-images \
    --owners self \
    --query 'reverse(sort_by(Images,&CreationDate))[:5].{id:ImageId,date:CreationDate}'
[
    {
        "id": "ami-0a1b2c3d4e5f60001",
        "date": "2018-11-28T17:16:38.000Z"
    },
    {
        "id": "ami-0a1b2c3d4e5f60002",
        "date": "2018-09-15T13:51:22.000Z"
    },
    {
        "id": "ami-0a1b2c3d4e5f60003",
        "date": "2018-08-19T10:22:45.000Z"
    },
    {
        "id": "ami-0a1b2c3d4e5f60004",
        "date": "2018-05-03T12:04:02.000Z"
    },
    {
        "id": "ami-0a1b2c3d4e5f60005",
        "date": "2017-12-13T17:16:38.000Z"
    }
]
```

Para mostrar instancias de escalado automático en mal estado

El siguiente ejemplo muestra solo la `InstanceId` para las instancias en mal estado en el grupo de Auto Scaling especificado.

```
$ aws autoscaling describe-auto-scaling-groups \
```

```
    --auto-scaling-group-name My-AutoScaling-Group-Name \
    --output text \
    --query 'AutoScalingGroups[*].Instances[?HealthStatus==`Unhealthy`].InstanceId'
```

Para incluir volúmenes con la etiqueta especificada

En el siguiente ejemplo se describen todas las instancias con una etiqueta `test`. Siempre y cuando haya otra etiqueta al lado de `test` adjunta al volumen, el volumen se sigue devolviendo en los resultados.

La siguiente expresión para devolver todas las etiquetas con la etiqueta `test` en una matriz. Cualquier etiqueta de que no sea la etiqueta `test` contiene un valor `null`.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[*].Tags[?Value == `test`]'
```

Para excluir volúmenes con la etiqueta especificada

El siguiente ejemplo describe todas las instancias sin una etiqueta `test`. El uso de una expresión `?Value != `test`` simple no funciona para excluir un volumen ya que los volúmenes pueden tener varias etiquetas. Siempre y cuando haya otra etiqueta al lado de `test` adjunta al volumen, el volumen se sigue devolviendo en los resultados.

Para excluir todos los volúmenes con la etiqueta `test`, comience con la siguiente expresión para devolver todas las etiquetas con la etiqueta `test` en una matriz. Cualquier etiqueta de que no sea la etiqueta `test` contiene un valor `null`.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[*].Tags[?Value == `test`]'
```

Luego, filtre todos los resultados positivos `test` con la función `not_null`.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[?!not_null(Tags[?Value == `test`].Value)]'
```

Canalice los resultados para aplanar los que resultan en la siguiente consulta.

```
$ aws ec2 describe-volumes \
    --query 'Volumes[?!not_null(Tags[?Value == `test`].Value)] | []'
```

Combinación del filtrado del lado del cliente y del servidor

Se puede utilizar el filtrado del lado del cliente y del servidor juntos. El filtrado del lado del servidor se completa primero y envía los datos al cliente que luego el parámetro `--query` filtra. Si está utilizando conjuntos de datos grandes, usar primero el filtrado del lado del servidor puede reducir la cantidad de datos que se envían al cliente para cada AWS CLI, sin dejar de mantener la potente personalización que proporciona el filtrado del lado del cliente.

En el siguiente ejemplo se muestran los volúmenes de Amazon EC2 con el filtrado tanto del lado del cliente como del servidor. El servicio filtra una lista de todos los volúmenes asociados de la zona de disponibilidad `us-west-2a`. El parámetro `--query` limita aún más la salida a solo los volúmenes con un valor de `Size` mayor que 50 y muestra solo los campos especificados con nombres definidos por el usuario.

```
$ aws ec2 describe-volumes \
    --filters "Name=availability-zone,Values=us-west-2a" "Name=status,Values=attached"
 \
    --query 'Volumes[?Size > `50`].{Id:VolumeId,Size:Size,Type:VolumeType}'
[
    {
        "Id": "vol-0be9bb0bf12345678",
        "Size": 80,
        "VolumeType": "gp2"
    }
]
```

El siguiente ejemplo recupera una lista de imágenes que cumplen varios criterios. A continuación, utiliza el parámetro `--query` para ordenar la salida por `CreationDate`, que selecciona solo las más recientes. Finalmente, muestra el valor de `ImageId` de esa imagen.

```
$ aws ec2 describe-images \
    --owners amazon \
    --filters "Name=name,Values=amzn*gp2" "Name=virtualization-type,Values=hvm"
 "Name=root-device-type,Values=ebs" \
    --query "sort_by(Images, &CreationDate)[-1].ImageId" \
    --output text
ami-00ced3122871a4921
```

En el ejemplo siguiente, se muestra el número de volúmenes disponibles que son más de 1000 IOPS utilizando `length` para contar cuántos hay en una lista.

```
$ aws ec2 describe-volumes \
    --filters "Name=status,Values=available" \
    --query 'length(Volumes[?Iops > `1000`])'
3
```

En el siguiente ejemplo se recuperan los nombres de los grupos de escalado automático que están utilizando configuraciones de lanzamiento en la Región de AWS especificada que están usando pilas de CloudFormation.

```
$ aws autoscaling describe-auto-scaling-groups --region us-west-2 \
  --filters Name=tag-key,Values=aws:cloudformation:stack-name \
  --query 'AutoScalingGroups[?LaunchConfigurationName!=`null`].AutoScalingGroupName'
[
    "group-1",
    "group-2",
    "group-3"
]
```

Recursos adicionales

Solicitud automática de AWS CLI

Cuando comience a usar expresiones de filtro, puede usar la función de solicitud automática en la versión 2 de la AWS CLI. La característica de solicitud automática proporciona una vista previa al presionar la tecla F5. Para obtener más información, consulte the section called “Mensaje automático”.

Terminal JMESPath

Terminal JMesPath es un comando de terminal interactivo para experimentar con expresiones JMesPath que se utilizan para el filtrado del lado del cliente. al usar el comando `jpterm`, el terminal muestra los resultados inmediatos de la consulta a medida que usted escribe. Puede canalizar directamente la salida AWS CLI a la terminal, lo que permite la experimentación avanzada de consultas.

El siguiente ejemplo de canalizaciones `aws ec2 describe-volumes` sale directamente al terminal JMESPath.

```
$ aws ec2 describe-volumes | jpterm
```

Para obtener más información acerca del terminal JMESPath y las instrucciones de instalación, consulte Terminal JMESPath en GitHub.

Utilidad jq

La utilidad `jq` le proporciona una forma de transformar su salida en el lado del cliente a un formato de salida que desee. Para obtener más información sobre `jq` e instrucciones sobre la instalación, consulte jq en GitHub.

Códigos de retorno de la línea de comandos en la AWS CLI

El código de retorno suele ser un código oculto enviado después de ejecutar un comando de la AWS Command Line Interface (AWS CLI) que describe el estado del comando. Puede utilizar el comando `echo` para mostrar el código enviado desde el último comando de la AWS CLI y utilice estos códigos para determinar si un comando se ha realizado correctamente y por qué un comando puede tener un error. Además de los códigos de retorno, puede ver más detalles sobre un error ejecutando sus comandos con el conmutador `--debug`. Este conmutador produce un informe detallado de los pasos que usa la AWS CLI para procesar el comando e indica cuál fue el resultado de cada paso.

Para determinar el código de devolución de un comando de la AWS CLI, ejecute uno de los siguientes comandos inmediatamente después de ejecutar el comando de la CLI.

Linux and macOS

```
$ echo $?
0
```

Windows PowerShell

```
PS> echo $lastexitcode
0
```

Windows Command Prompt

```
C:\> echo %errorlevel%
0
```

A continuación se indican los valores código de devolución que se pueden devolver al finalizar la ejecución de un comando de la AWS Command Line Interface (AWS CLI).

Códig	Significado
0	El servicio respondió con un código de estado de respuesta HTTP de 200 que indica que AWS CLI no generó errores y el servicio de AWS al que se envía la solicitud.
1	Error en una o varias operaciones de transferencia de Amazon S3. Limitado a comandos de S3.
2	El significado de este código de devolución depende del comando: • Aplicable a todos los comandos de AWS CLI: no se pudo analizar el comando introduci do. Errores de análisis que pueden deberse, entre otras cosas, a falta de subcomandos o argumentos necesarios o al uso de comandos o argumentos desconocidos. • Limitado a comandos S3: uno o más archivos marcados para transferencia durante el proceso de transferencia. Sin embargo, el resto de los archivos marcados para transfere ncia se han transferido correctamente. Los archivos que se omiten durante el proceso de transferencia pueden ser: archivos que no existen; archivos de dispositivos orientados a caracteres, dispositivos orientados a bloques, colas FIFO o sockets, y archivos para los que el usuario no tiene permiso de lectura.
130	El comando se ha visto interrumpido por SIGINT. Esta es la señal que usted envió para cancelar un comando con `Ctrl+C`.
252	La sintaxis del comando no era válida, se proporcionó un parámetro desconocido o había un valor de parámetro incorrecto que impidió que el comando se ejecutara.
253	El entorno o la configuración del sistema no eran válidos. Si bien el comando proporcio nado puede ser válido en sentido sintáctico, la falta de configuración o credenciales impidió que el comando se ejecutara.
254	El comando se analizó correctamente y se realizó una solicitud al servicio especificado, pero el servicio devolvió un error. Esto por lo general indicará el uso incorrecto de la API u otros problemas específicos del servicio.
255	Error del comando. La AWS CLI o el servicio de AWS al que se había enviado la solicitud produjeron errores.

Uso de asistentes personalizados para ejecutar comandos interactivos en la AWS CLI

La AWS Command Line Interface (AWS CLI) proporciona la posibilidad de utilizar un asistente para algunos comandos. Para contribuir o ver la lista completa de asistentes de AWS CLI, consulte la carpeta de asistentes de AWS CLI en GitHub.

Funcionamiento

Similar a la consola de AWS, la AWS CLI tiene un asistente de interfaz de usuario que lo guía a través de la administración de sus recursos de AWS. Para utilizar el asistente, llame al subcomando `wizard` y el nombre del asistente después del nombre del servicio en un comando. La estructrura del comando es la siguiente:

Sintaxis:

```
$ aws <command> wizard <wizardName>
```

El siguiente ejemplo llama al asistente para crear una nueva tabla de `dynamodb`.

```
$ aws dynamodb wizard new-table
```

`aws configure` es el único asistente que no tiene un nombre de asistente. Cuando ejecute el asistente, ejecute el comando `aws configure wizard` como se muestra en el siguiente ejemplo:

```
$ aws configure wizard
```

Después de llamar a un asistente, se muestra un formulario en el shell. Para cada parámetro, se le proporciona una lista de opciones para seleccionar o se le pide que introduzca una cadena. Para seleccionar de una lista, utilice las teclas de flecha arriba y abajo y presione ENTER (INTRO). Para ver los detalles de una opción, presione la tecla de flecha derecha. Cuando haya terminado de completar un parámetro, pulse ENTER (INTRO).

```
$ aws configure wizard
What would you like to configure
> Static Credentials
  Assume Role
  Process Provider
```

```
  Additional CLI configuration
Enter the name of the profile:
Enter your Access Key Id:
Enter your Secret Access Key:
```

Para editar solicitudes anteriores, utilice MAYÚS + TAB. Para algunos asistentes, después de rellenar todas las solicitudes, puede obtener una vista previa de una plantilla de AWS CloudFormation o el comando AWS CLI completadas con su información. Este modo de vista previa es útil para aprender el AWS CLI, API de servicio y creación de plantillas para scripts.

Presione ENTER (INTRO) después de la vista previa o el último mensaje para ejecutar el comando final.

```
$ aws configure wizard
What would you like to configure
Enter the name of the profile: testWizard
Enter your Access Key Id: AB1C2D3EF4GH5I678J90K
Enter your Secret Access Key: ab1c2def34gh5i67j8k90l1mnop2qr3s45tu678v90
<ENTER>
```

Creación y uso de alias en la AWS CLI

Los alias son accesos directos que se pueden crear en la AWS Command Line Interface (AWS CLI) para acortar los comandos o secuencias de comandos que utiliza con frecuencia. Puede crear alias en el campo `alias` ubicado en la carpeta de configuración.

Temas

- Requisitos previos
- Paso 1: Creación del archivo de alias
- Paso 2: Creación de un alias
- Paso 3: Cómo llamar a un alias
- Ejemplos de repositorio de alias
- Recursos

Requisitos previos

Para utilizar los comandos de alias, debe seguir estos pasos:

- Instalar y configurar la AWS CLI. Para obtener más información, consulte the section called "Instalar o actualizar" y Credenciales de autenticación y acceso para la AWS CLI.
- Utilice como mínimo una versión de 1.11.24 o 2.0.0 de AWS CLI.
- (Opcional) Para usar scripts de bash de alias de AWS CLI, debe utilizar un terminal compatible con bash.

Paso 1: Creación del archivo de alias

Para crear el archivo `alias`, puede utilizar la navegación de archivos y un editor de texto, o utilizar su terminal preferido mediante el procedimiento paso a paso. Para crear rápidamente el archivo de alias, utilice el siguiente bloque de comandos.

Linux and macOS

```
$ mkdir -p ~/.aws/cli
$ echo '[toplevel]' > ~/.aws/cli/alias
```

Windows

```
C:\> md %USERPROFILE%\.aws\cli
C:\> echo [toplevel] > %USERPROFILE%/.aws/cli/alias
```

Para crear el archivo de alias

1. Cree una carpeta con el nombre `cli` en su carpeta de configuración de AWS CLI. De forma predeterminada, la carpeta de configuración es `~/.aws/` en Linux o macOS y `%USERPROFILE%\.aws\` en Windows. Puede crearla a través de la navegación de archivos o mediante el siguiente comando.

   Linux and macOS

   ```
   $ mkdir -p ~/.aws/cli
   ```

   Windows

   ```
   C:\> md %USERPROFILE%\.aws\cli
   ```

La ruta predeterminada resultante de la carpeta `cli` es `~/.aws/cli/` en Linux o macOS y `%USERPROFILE%\.aws\cli` en Windows.

2. En la carpeta `cli`, cree un archivo de texto con el nombre `alias` sin extensión y agréguele `[toplevel]` a la primera línea. Puede crear este archivo a través de su editor de texto preferido o utilizar el siguiente comando.

   Linux and macOS

   ```
   $ echo '[toplevel]' > ~/.aws/cli/alias
   ```

   Windows

   ```
   C:\> echo [toplevel] > %USERPROFILE%/.aws/cli/alias
   ```

Paso 2: Creación de un alias

Puede crear un alias mediante comandos básicos o scripting de bash.

Creación de un alias de comando básico

Puede crear su alias agregando un comando con la siguiente sintaxis en el archivo `alias` que creó en el paso anterior.

Sintaxis

```
aliasname = command [--options]
```

el *`nombre de alias`* es lo que usted llama su alias. El *`comando`* es el comando al que desea llamar, que puede incluir otros alias. Puede incluir opciones o parámetros en su alias, o agregarlos al llamar a su alias.

En el siguiente ejemplo se muestra cómo crear un alias llamado `aws whoami` con el comando `aws sts get-caller-identity`. Dado que este alias llama a un comando AWS CLI existente, puede escribir el comando sin el prefijo `aws`.

```
whoami = sts get-caller-identity
```

En el siguiente ejemplo se toma el ejemplo anterior `whoami` y se agregan las opciones de filtro `Account` y texto `output`.

```
whoami2 = sts get-caller-identity --query Account --output text
```

Creación de un alias de subcomando

> **Note**
>
> La característica de alias de subcomando requiere una versión de la AWS CLI mínima de 1.11.24 o 2.0.0

Puede crear un alias para subcomandos si agrega un comando mediante la siguiente sintaxis en el archivo `alias` que creó en el paso anterior.

Sintaxis

```
[command commandGroup]
aliasname = command [--options]
```

En *commandGroup* se indica el espacio de nombres del comando, por ejemplo, el comando `aws ec2 describe-regions` está en el grupo de comandos `ec2`. el *nombre de alias* es lo que usted llama su alias. El *comando* es el comando al que desea llamar, que puede incluir otros alias. Puede incluir opciones o parámetros en su alias, o agregarlos al llamar a su alias.

En el siguiente ejemplo se muestra cómo crear un alias llamado `aws ec2 regions` con el comando `aws ec2 describe-regions`. Dado que este alias llama a un comando AWS CLI existente en el espacio de nombres de comando `ec2`, puede escribir el comando sin el prefijo `aws ec2`.

```
[command ec2]
regions = describe-regions --query Regions[].RegionName
```

Para crear alias de comandos fuera del espacio de nombres del comando, anteponga al comando completo un signo de exclamación. En el siguiente ejemplo se muestra cómo crear un alias llamado `aws ec2 instance-profiles` con el comando `aws iam list-instance-profiles`.

```
[command ec2]
instance-profiles = !aws iam list-instance-profiles
```

> **Note**
>
> Los alias solo utilizan espacios de nombres de comando existentes y no puede crear nuevos. Por ejemplo, no puede crear un alias con la sección `[command johnsmith]` ya que el espacio de nombres de comando `johnsmith` no existe.

Creación de un alias de scripting bash

> **Warning**
>
> Para utilizar scripts bash de alias AWS CLI, debe usar un terminal compatible con bash

Puede crear un alias utilizando scripts bash para procesos más avanzados utilizando la siguiente sintaxis.

Sintaxis

```
aliasname =
    !f() {
        script content
}; f
```

El *nombre de alias* es lo que llama su alias y el *contenido de script* es el script que desea ejecutar al llamar al alias.

El siguiente ejemplo utiliza `opendns` para generar la dirección IP actual. Dado que puede usar alias en otros alias, el siguiente alias `myip` es útil para permitir o revocar el acceso a su dirección IP desde otros alias.

```
myip =
  !f() {
    dig +short myip.opendns.com @resolver1.opendns.com
  }; f
```

El siguiente ejemplo de script llama al alias anterior `aws myip` para autorizar la entrada de un grupo de seguridad de Amazon EC2 a su dirección IP.

```
authorize-my-ip =
  !f() {
    ip=$(aws myip)
    aws ec2 authorize-security-group-ingress --group-id ${1} --cidr $ip/32 --protocol
 tcp --port 22
  }; f
```

Cuando llama a alias que usan scripting de Bash, las variables siempre se pasan en el orden en que las ingresó. En el scripting de Bash, los nombres de las variables no se tienen en cuenta, solo el orden en que aparecen. En los siguientes ejemplos de alias `textalert`, la variable para la opción `--message` es la primera y la opción `--phone-number` es la segunda.

```
textalert =
  !f() {
    aws sns publish --message "${1}" --phone-number ${2}
  }; f
```

Paso 3: Cómo llamar a un alias

Para ejecutar el alias que creó en su archivo `alias` utilice la siguiente sintaxis. Puede agregar opciones adicionales al llamar a su alias.

Sintaxis

```
$ aws aliasname
```

En el siguiente ejemplo se utiliza el alias de comando `aws whoami`.

```
$ aws
 whoami
{
    "UserId": "A12BCD34E5FGHI6JKLM",
    "Account": "1234567890987",
    "Arn": "arn:aws:iam::1234567890987:user/userName"
}
```

El siguiente ejemplo utiliza el alias `aws whoami` con opciones adicionales para devolver solo el número `Account` en la salida `text`.

```
$ aws whoami --query Account --output
 text
1234567890987
```

En el siguiente ejemplo se utiliza el alias de subcomando `aws ec2 regions`.

```
$ aws ec2
 regions
[
    "ap-south-1",
    "eu-north-1",
    "eu-west-3",
    "eu-west-2",
...
```

Cómo llamar a un alias usando variables de scripting de Bash

Cuando se llama a alias que usan scripting de Bash, las variables se pasan en el orden en que se introducen. En el scripting de Bash, el nombre de las variables no se tiene en cuenta, solo el orden en que aparecen. Por ejemplo, en el siguiente alias `textalert`, la variable de la opción `--message` está primera y `--phone-number` está segunda.

```
textalert =
  !f() {
    aws sns publish --message "${1}" --phone-number ${2}
  }; f
```

Cuando llama al alias `textalert`, debe pasar variables en el mismo orden en que se ejecutan en el alias. En el siguiente ejemplo utilizamos las variables `$message` y `$phone`. La variable `$message` se pasa como `${1}` para la opción `--message` y la variable `$phone` se pasa como `${2}` para la opción `--phone-number`. Esto da como resultado una llamada correcta al alias `textalert` para enviar un mensaje.

```
$ aws textalert $message
 $phone
{
    "MessageId": "1ab2cd3e4-fg56-7h89-i01j-2klmn34567"
}
```

En el siguiente ejemplo, el orden se cambia al llamar al alias para `$phone` y `$message`. La variable `$phone` se pasa como `${1}` para la opción `--message` y la variable `$message` se pasa como `${2}` para la opción `--phone-number`. Dado que las variables están fuera de servicio, el alias pasa las variables de manera incorrecta. Esto provoca un error porque el contenido de `$message` no coinciden con los requisitos de formato de número de teléfono para la opción `--phone-number`.

```
$ aws textalert $phone
 $message
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help

Unknown options: text
```

Ejemplos de repositorio de alias

El repositorio de alias de AWS CLI en GitHub contiene ejemplos de alias de AWS CLI creados por el equipo de desarrolladores y la comunidad de AWS CLI. Puede usar todo el ejemplo del archivo `alias` o tomar alias individuales para su propio uso.

> **Warning**
>
> Al ejecutar los comandos de esta sección, se elimina su archivo `alias`existente. Para evitar sobrescribir el archivo de alias existente, cambie la ubicación de descarga.

Para utilizar alias del repositorio

1. Instala Git Para obtener instrucciones de instalación, consulte Introducción - Instalación de Git en la Documentación de Git.
2. Instale el comando `jp`. El comando `jp` se utiliza en el alias `tostring`. Para obtener instrucciones de instalación, consulte el archivo JMESPath (jp) README.md en GitHub.
3. Instale el comando `jq`. El comando `jq` se utiliza en el alias `tostring-with-jq`. Para obtener instrucciones de instalación, consulte el archivo JSON processor (jq) en GitHub.
4. Descargue el archivo `alias` de la siguiente manera:

- Ejecute los siguientes comandos que se descargan del repositorio y se copian el archivo `alias` en la carpeta de configuración.

  Linux and macOS

  ```
  $ git clone https://github.com/awslabs/awscli-aliases.git
  $ mkdir -p ~/.aws/cli
  $ cp awscli-aliases/alias ~/.aws/cli/alias
  ```

  Windows

  ```
  C:\> git clone https://github.com/awslabs/awscli-aliases.git
  C:\> md %USERPROFILE%\.aws\cli
  C:\> copy awscli-aliases\alias %USERPROFILE%\.aws\cli
  ```

- Descargue directamente desde el repositorio y guárdelo en la carpeta `cli` en su carpeta de configuración AWS CLI. De forma predeterminada, la carpeta de configuración es `~/.aws/` en Linux o macOS y `%USERPROFILE%\.aws\` en Windows.

5. Para verificar que los alias funcionan, ejecute el siguiente alias.

   ```
   $ aws whoami
   ```

   Esto muestra la misma respuesta que el comando `aws sts get-caller-identity`:

   ```
   {
       "Account": "012345678901",
       "UserId": "AIUAINBADX2VEG2TC6HD6",
       "Arn": "arn:aws:iam::012345678901:user/myuser"
   }
   ```

Recursos

- El repositorio de alias de AWS CLI en GitHub contiene ejemplos de alias de AWS CLI creados por el equipo de desarrolladores de AWS CLI y con la contribución de la comunidad de AWS CLI.
- El anuncio de la característica de alias de AWS re:Invent 2016: The Effective AWS CLI User en YouTube.
- `aws sts get-caller-identity`

- `aws ec2 describe-instances`
- `aws sns publish`

Solución de errores para la AWS CLI

En esta sección se describen los errores comunes y los pasos de solución de problemas que se deben seguir para resolver el problema. Le sugerimos seguir primero la solución de problemas generales.

Contenido

- Solución de problemas generales para probar primero
  - Compruebe su formato de comandos de la AWS CLI
  - Compruebe la Región de AWS que utiliza su comando de la AWS CLI.
  - Confirme que está ejecutando una versión reciente de la AWS CLI
  - Use la opción --debug
  - Habilite y revise los registros del historial del comando AWS CLI
  - Confirme que se ha configurado su AWS CLI
- Errores de comando no encontrado
- El comando "aws --version" devuelve una versión diferente a la instalada
- El comando "aws --version" devuelve una versión después de desinstalar la AWS CLI
- La AWS CLI ha procesado un comando con un nombre de parámetro incompleto
- Errores de acceso denegado
- Errores de credenciales y claves no válidas
- Errores de firma que no coincide
- Errores de certificado SSL
- Errores de JSON no válido
- Recursos adicionales

Solución de problemas generales para probar primero

Si recibe un error o encuentra un problema con la AWS CLI, le sugerimos los siguientes consejos generales para solucionar problemas.

(Volver arriba)

Compruebe su formato de comandos de la AWS CLI

Si aparece un error en el que se indica que no existe un comando o que no se reconoce un parámetro (`Parameter validation failed`) que según la documentación está disponible, es posible que el comando tenga un formato incorrecto. Le sugerimos que compruebe lo siguiente:

- Compruebe si hay errores ortográficos y de formato en el comando.
- Confirme que todas las comillas y caracteres de escape apropiados para su terminal son correctos en el comando.
- Generar un esqueleto de AWS CLI para confirmar la estructura del comando.
- Para JSON, consulte la solución de problemas para valores JSON. Si tiene problemas con su terminal para procesar el formato JSON, le sugerimos omitir las reglas de entrecomillado del terminal utilizando Blobs para pasar los datos JSON directamente a la AWS CLI.

Para obtener más información sobre cómo debe estructurarse un comando específico, consulte la Guía de referencia de la AWS CLI versión 2.

Volver arriba

Compruebe la Región de AWS que utiliza su comando de la AWS CLI.

> **Note**
>
> Cuanto utilice la AWS CLI, debe especificar una Región de AWS, ya sea de forma explícita o estableciendo una región predeterminada. Para obtener una lista de todas las Regiones de AWS que se pueden especificar, consulte Regiones y puntos de conexión de AWS en la Referencia general de Amazon Web Services. Los designadores de Región de AWS que la AWS CLI utiliza son los mismos nombres que aparecen en las URL y los puntos de conexión de servicio de Consola de administración de AWS.

Se pueden producir errores o resultados inesperados si un Servicio de AWS no está disponible para la Región de AWS especificada o si los recursos están ubicados en una Región de AWS diferente. La Región de AWS se ajusta de las siguientes formas, en el orden de prioridad:

- La opción de línea de comandos de la `--region`.

- La variable de entorno compatible con el SDK de la `AWS_REGION`.
- La variable de entorno de la `AWS_DEFAULT_REGION`.
- La configuración del perfil de la `region`.

Verifique que está usando la Región de AWS correcta para sus recursos.

Volver arriba

Confirme que está ejecutando una versión reciente de la AWS CLI

Si recibe un error que indica que un comando no existe, o que no reconoce un parámetro que en la Guía de referencia de la AWS CLI versión 2 se indica que está disponible, confirme primero que el comando tiene el formato correcto. Si el formato es correcto, le recomendamos que se actualice a la versión más reciente de la AWS CLI. Las versiones actualizadas de la AWS CLI se publican casi todos los días hábiles. Se incorporan nuevos servicios de AWS, características y parámetros en las nuevas versiones de la AWS CLI. La única manera de obtener acceso a los nuevos servicios, características o parámetros es actualizándose a una versión que se lanzara después de que ese elemento se incorporara por primera vez.

La forma de actualizar la versión de AWS CLI depende de si la instaló originalmente como se describe en the section called “Instalar o actualizar”.

Si ha utilizado uno de los instaladores del paquete, debe eliminar la instalación existente antes de descargar e instalar la versión más reciente para su sistema operativo.

Volver arriba

Use la opción `--debug`

Cuando la AWS CLI informa de un error que no entiende inmediatamente, o produce resultados que no espera, puede obtener más detalles sobre el error si ejecuta de nuevo el comando con la opción `--debug`. Con esta opción, la AWS CLI emite detalles sobre cada paso que realiza para procesar su comando. Los detalles de la salida pueden ayudarlo a determinar cuándo se produce el error y proporciona pistas sobre dónde comenzó.

Puede enviar el resultado a un archivo de texto para revisarlo posteriormente o enviarlo a AWS Support cuando se le solicite.

Cuando se incluye la opción `--debug`, algunos detalles son:

- Búsqueda de credenciales
- Análisis de los parámetros proporcionados
- Creación de la solicitud enviada a los servidores de AWS
- El contenido de la solicitud enviada a AWS
- El contenido de la respuesta sin procesar
- La salida con formato

A continuación, se muestra un ejemplo de la ejecución de un comando con y sin la opción `--debug`:

```
$ aws iam list-groups --profile MyTestProfile
{
    "Groups": [
        {
            "Path": "/",
            "GroupName": "MyTestGroup",
            "GroupId": "AGPA0123456789EXAMPLE",
            "Arn": "arn:aws:iam::123456789012:group/MyTestGroup",
            "CreateDate": "2019-08-12T19:34:04Z"
        }
    ]
}
```

```
$ aws iam list-groups --profile MyTestProfile --debug
2019-08-12 12:36:18,305 - MainThread - awscli.clidriver - DEBUG - CLI version: aws-
cli/1.16.215 Python/3.7.3 Linux/4.14.133-113.105.amzn2.x86_64 botocore/1.12.205
2019-08-12 12:36:18,305 - MainThread - awscli.clidriver - DEBUG - Arguments entered to
 CLI: ['iam', 'list-groups', '--debug']
2019-08-12 12:36:18,305 - MainThread - botocore.hooks - DEBUG - Event session-
initialized: calling handler <function add_scalar_parsers at 0x7fdf173161e0>
2019-08-12 12:36:18,305 - MainThread - botocore.hooks - DEBUG - Event session-
initialized: calling handler <function register_uri_param_handler at 0x7fdf17dec400>
2019-08-12 12:36:18,305 - MainThread - botocore.hooks - DEBUG - Event session-
initialized: calling handler <function inject_assume_role_provider_cache at
 0x7fdf17da9378>
2019-08-12 12:36:18,307 - MainThread - botocore.credentials - DEBUG - Skipping
 environment variable credential check because profile name was explicitly set.
2019-08-12 12:36:18,307 - MainThread - botocore.hooks - DEBUG - Event session-
initialized: calling handler <function attach_history_handler at 0x7fdf173ed9d8>
```

```
2019-08-12 12:36:18,308 - MainThread - botocore.loaders - DEBUG - Loading JSON
 file: /home/ec2-user/venv/lib/python3.7/site-packages/botocore/data/iam/2010-05-08/
service-2.json
2019-08-12 12:36:18,317 - MainThread - botocore.hooks - DEBUG - Event building-command-
table.iam: calling handler <function add_waiters at 0x7fdf1731a840>
2019-08-12 12:36:18,320 - MainThread - botocore.loaders - DEBUG - Loading JSON
 file: /home/ec2-user/venv/lib/python3.7/site-packages/botocore/data/iam/2010-05-08/
waiters-2.json
2019-08-12 12:36:18,321 - MainThread - awscli.clidriver - DEBUG - OrderedDict([('path-
prefix', <awscli.arguments.CLIArgument object at 0x7fdf171ac780>), ('marker',
 <awscli.arguments.CLIArgument object at 0x7fdf171b09e8>), ('max-items',
 <awscli.arguments.CLIArgument object at 0x7fdf171b09b0>)])
2019-08-12 12:36:18,322 - MainThread - botocore.hooks - DEBUG - Event building-
argument-table.iam.list-groups: calling handler <function add_streaming_output_arg at
 0x7fdf17316510>
2019-08-12 12:36:18,322 - MainThread - botocore.hooks - DEBUG - Event building-
argument-table.iam.list-groups: calling handler <function add_cli_input_json at
 0x7fdf17da9d90>
2019-08-12 12:36:18,322 - MainThread - botocore.hooks - DEBUG - Event building-
argument-table.iam.list-groups: calling handler <function unify_paging_params at
 0x7fdf17328048>
2019-08-12 12:36:18,326 - MainThread - botocore.loaders - DEBUG - Loading JSON
 file: /home/ec2-user/venv/lib/python3.7/site-packages/botocore/data/iam/2010-05-08/
paginators-1.json
2019-08-12 12:36:18,326 - MainThread - awscli.customizations.paginate - DEBUG -
 Modifying paging parameters for operation: ListGroups
2019-08-12 12:36:18,326 - MainThread - botocore.hooks - DEBUG - Event building-
argument-table.iam.list-groups: calling handler <function add_generate_skeleton at
 0x7fdf1737eae8>
2019-08-12 12:36:18,326 - MainThread - botocore.hooks - DEBUG - Event
 before-building-argument-table-parser.iam.list-groups: calling handler
 <bound method OverrideRequiredArgsArgument.override_required_args of
 <awscli.customizations.cliinputjson.CliInputJSONArgument object at 0x7fdf171b0a58>>
2019-08-12 12:36:18,327 - MainThread - botocore.hooks - DEBUG - Event
 before-building-argument-table-parser.iam.list-groups: calling handler
 <bound method GenerateCliSkeletonArgument.override_required_args of
 <awscli.customizations.generatecliskeleton.GenerateCliSkeletonArgument object at
 0x7fdf171c5978>>
2019-08-12 12:36:18,327 - MainThread - botocore.hooks - DEBUG - Event operation-
args-parsed.iam.list-groups: calling handler functools.partial(<function
 check_should_enable_pagination at 0x7fdf17328158>, ['marker', 'max-items'], {'max-
items': <awscli.arguments.CLIArgument object at 0x7fdf171b09b0>}, OrderedDict([('path-
prefix', <awscli.arguments.CLIArgument object at 0x7fdf171ac780>), ('marker',
 <awscli.arguments.CLIArgument object at 0x7fdf171b09e8>), ('max-items',
```

```
 <awscli.customizations.paginate.PageArgument object at 0x7fdf171c58d0>), ('cli-
input-json', <awscli.customizations.cliinputjson.CliInputJSONArgument object at
 0x7fdf171b0a58>), ('starting-token', <awscli.customizations.paginate.PageArgument
 object at 0x7fdf171b0a20>), ('page-size', <awscli.customizations.paginate.PageArgument
 object at 0x7fdf171c5828>), ('generate-cli-skeleton',
 <awscli.customizations.generatecliskeleton.GenerateCliSkeletonArgument object at
 0x7fdf171c5978>)]))
2019-08-12 12:36:18,328 - MainThread - botocore.hooks - DEBUG - Event load-cli-
arg.iam.list-groups.path-prefix: calling handler <awscli.paramfile.URIArgumentHandler
 object at 0x7fdf1725c978>
2019-08-12 12:36:18,328 - MainThread - botocore.hooks - DEBUG - Event load-cli-
arg.iam.list-groups.marker: calling handler <awscli.paramfile.URIArgumentHandler object
 at 0x7fdf1725c978>
2019-08-12 12:36:18,328 - MainThread - botocore.hooks - DEBUG - Event load-cli-
arg.iam.list-groups.max-items: calling handler <awscli.paramfile.URIArgumentHandler
 object at 0x7fdf1725c978>
2019-08-12 12:36:18,328 - MainThread - botocore.hooks - DEBUG -
 Event load-cli-arg.iam.list-groups.cli-input-json: calling handler
 <awscli.paramfile.URIArgumentHandler object at 0x7fdf1725c978>
2019-08-12 12:36:18,328 - MainThread - botocore.hooks - DEBUG -
 Event load-cli-arg.iam.list-groups.starting-token: calling handler
 <awscli.paramfile.URIArgumentHandler object at 0x7fdf1725c978>
2019-08-12 12:36:18,328 - MainThread - botocore.hooks - DEBUG - Event load-cli-
arg.iam.list-groups.page-size: calling handler <awscli.paramfile.URIArgumentHandler
 object at 0x7fdf1725c978>
2019-08-12 12:36:18,328 - MainThread - botocore.hooks - DEBUG - Event
 load-cli-arg.iam.list-groups.generate-cli-skeleton: calling handler
 <awscli.paramfile.URIArgumentHandler object at 0x7fdf1725c978>
2019-08-12 12:36:18,329 - MainThread - botocore.hooks - DEBUG
 - Event calling-command.iam.list-groups: calling handler
 <bound method CliInputJSONArgument.add_to_call_parameters of
 <awscli.customizations.cliinputjson.CliInputJSONArgument object at 0x7fdf171b0a58>>
2019-08-12 12:36:18,329 - MainThread - botocore.hooks - DEBUG -
 Event calling-command.iam.list-groups: calling handler <bound
 method GenerateCliSkeletonArgument.generate_json_skeleton of
 <awscli.customizations.generatecliskeleton.GenerateCliSkeletonArgument object at
 0x7fdf171c5978>>
2019-08-12 12:36:18,329 - MainThread - botocore.credentials - DEBUG - Looking for
 credentials via: assume-role
2019-08-12 12:36:18,329 - MainThread - botocore.credentials - DEBUG - Looking for
 credentials via: assume-role-with-web-identity
2019-08-12 12:36:18,329 - MainThread - botocore.credentials - DEBUG - Looking for
 credentials via: shared-credentials-file
```

```
2019-08-12 12:36:18,329 - MainThread - botocore.credentials - INFO - Found credentials
 in shared credentials file: ~/.aws/credentials
2019-08-12 12:36:18,330 - MainThread - botocore.loaders - DEBUG - Loading JSON file: /
home/ec2-user/venv/lib/python3.7/site-packages/botocore/data/endpoints.json
2019-08-12 12:36:18,334 - MainThread - botocore.hooks - DEBUG - Event choose-service-
name: calling handler <function handle_service_name_alias at 0x7fdf1898eb70>
2019-08-12 12:36:18,337 - MainThread - botocore.hooks - DEBUG - Event creating-client-
class.iam: calling handler <function add_generate_presigned_url at 0x7fdf18a028c8>
2019-08-12 12:36:18,337 - MainThread - botocore.regions - DEBUG - Using partition
 endpoint for iam, us-west-2: aws-global
2019-08-12 12:36:18,337 - MainThread - botocore.args - DEBUG - The s3 config key is not
 a dictionary type, ignoring its value of: None
2019-08-12 12:36:18,340 - MainThread - botocore.endpoint - DEBUG - Setting iam timeout
 as (60, 60)
2019-08-12 12:36:18,341 - MainThread - botocore.loaders - DEBUG - Loading JSON file: /
home/ec2-user/venv/lib/python3.7/site-packages/botocore/data/_retry.json
2019-08-12 12:36:18,341 - MainThread - botocore.client - DEBUG - Registering retry
 handlers for service: iam
2019-08-12 12:36:18,342 - MainThread - botocore.hooks - DEBUG - Event before-
parameter-build.iam.ListGroups: calling handler <function generate_idempotent_uuid at
 0x7fdf189b10d0>
2019-08-12 12:36:18,342 - MainThread - botocore.hooks - DEBUG - Event before-
call.iam.ListGroups: calling handler <function inject_api_version_header_if_needed at
 0x7fdf189b2a60>
2019-08-12 12:36:18,343 - MainThread - botocore.endpoint - DEBUG - Making
 request for OperationModel(name=ListGroups) with params: {'url_path': '/',
 'query_string': '', 'method': 'POST', 'headers': {'Content-Type': 'application/x-
www-form-urlencoded; charset=utf-8', 'User-Agent': 'aws-cli/1.16.215 Python/3.7.3
 Linux/4.14.133-113.105.amzn2.x86_64 botocore/1.12.205'}, 'body': {'Action':
 'ListGroups', 'Version': '2010-05-08'}, 'url': 'https://iam.amazonaws.com/',
 'context': {'client_region': 'aws-global', 'client_config': <botocore.config.Config
 object at 0x7fdf16e9a4a8>, 'has_streaming_input': False, 'auth_type': None}}
2019-08-12 12:36:18,343 - MainThread - botocore.hooks - DEBUG - Event request-
created.iam.ListGroups: calling handler <bound method RequestSigner.handler of
 <botocore.signers.RequestSigner object at 0x7fdf16e9a470>>
2019-08-12 12:36:18,343 - MainThread - botocore.hooks - DEBUG - Event choose-
signer.iam.ListGroups: calling handler <function set_operation_specific_signer at
 0x7fdf18996f28>
2019-08-12 12:36:18,343 - MainThread - botocore.auth - DEBUG - Calculating signature
 using v4 auth.
2019-08-12 12:36:18,343 - MainThread - botocore.auth - DEBUG - CanonicalRequest:
POST
/
```

```
content-type:application/x-www-form-urlencoded; charset=utf-8
host:iam.amazonaws.com
x-amz-date:20190812T193618Z

content-type;host;x-amz-date
5f776d91EXAMPLE9b8cb5eb5d6d4a787a33ae41c8cd6eEXAMPLEca69080e1e1f
2019-08-12 12:36:18,344 - MainThread - botocore.auth - DEBUG - StringToSign:
AWS4-HMAC-SHA256
20190812T193618Z
20190812/us-east-1/iam/aws4_request
ab7e367eEXAMPLE2769f178ea509978cf8bfa054874b3EXAMPLE8d043fab6cc9
2019-08-12 12:36:18,344 - MainThread - botocore.auth - DEBUG - Signature:
d85a0EXAMPLEb40164f2f539cdc76d4f294fe822EXAMPLE18ad1ddf58a1a3ce7
2019-08-12 12:36:18,344 - MainThread - botocore.endpoint - DEBUG - Sending
 http request: <AWSPreparedRequest stream_output=False, method=POST,
 url=https://iam.amazonaws.com/, headers={'Content-Type': b'application/
x-www-form-urlencoded; charset=utf-8', 'User-Agent': b'aws-cli/1.16.215
 Python/3.7.3 Linux/4.14.133-113.105.amzn2.x86_64 botocore/1.12.205',
 'X-Amz-Date': b'20190812T193618Z', 'Authorization': b'AWS4-HMAC-SHA256
 Credential=AKIA01234567890EXAMPLE-east-1/iam/aws4_request, SignedHeaders=content-
type;host;x-amz-date, Signature=d85a07692aceb401EXAMPLEa1b18ad1ddf58a1a3ce7EXAMPLE',
 'Content-Length': '36'}>
2019-08-12 12:36:18,344 - MainThread - urllib3.util.retry - DEBUG - Converted retries
 value: False -> Retry(total=False, connect=None, read=None, redirect=0, status=None)
2019-08-12 12:36:18,344 - MainThread - urllib3.connectionpool - DEBUG - Starting new
 HTTPS connection (1): iam.amazonaws.com:443
2019-08-12 12:36:18,664 - MainThread - urllib3.connectionpool - DEBUG - https://
iam.amazonaws.com:443 "POST / HTTP/1.1" 200 570
2019-08-12 12:36:18,664 - MainThread - botocore.parsers - DEBUG - Response headers:
 {'x-amzn-RequestId': '74c11606-bd38-11e9-9c82-559da0adb349', 'Content-Type': 'text/
xml', 'Content-Length': '570', 'Date': 'Mon, 12 Aug 2019 19:36:18 GMT'}
2019-08-12 12:36:18,664 - MainThread - botocore.parsers - DEBUG - Response body:
b'<ListGroupsResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">\n
 <ListGroupsResult>\n    <IsTruncated>false</IsTruncated>\n    <Groups>\n
  <member>\n        <Path>/</Path>\n        <GroupName>MyTestGroup</GroupName>
\n        <Arn>arn:aws:iam::123456789012:group/MyTestGroup</Arn>\n
 <GroupId>AGPA1234567890EXAMPLE</GroupId>\n        <CreateDate>2019-08-12T19:34:04Z</
CreateDate>\n      </member>\n    </Groups>\n  </ListGroupsResult>\n
 <ResponseMetadata>\n    <RequestId>74c11606-bd38-11e9-9c82-559da0adb349</RequestId>\n
 </ResponseMetadata>\n</ListGroupsResponse>\n'
2019-08-12 12:36:18,665 - MainThread - botocore.hooks - DEBUG - Event needs-
retry.iam.ListGroups: calling handler <botocore.retryhandler.RetryHandler object at
 0x7fdf16e9a780>
2019-08-12 12:36:18,665 - MainThread - botocore.retryhandler - DEBUG - No retry needed.
```

```
2019-08-12 12:36:18,665 - MainThread - botocore.hooks - DEBUG - Event after-
call.iam.ListGroups: calling handler <function json_decode_policies at 0x7fdf189b1d90>
{
    "Groups": [
        {
            "Path": "/",
            "GroupName": "MyTestGroup",
            "GroupId": "AGPA123456789012EXAMPLE",
            "Arn": "arn:aws:iam::123456789012:group/MyTestGroup",
            "CreateDate": "2019-08-12T19:34:04Z"
        }
    ]
}
```

Volver arriba

Habilite y revise los registros del historial del comando AWS CLI

Puede habilitar los registros del historial del comando AWS CLI con la configuración de archivo `cli_history`. Después de habilitar esta configuración, la AWS CLI registra el historial de comandos `aws`.

Puede hacer una lista de su historial con el comando `aws history list` y utilizar los command_ids resultantes en el comando `aws history show` para obtener más información. Para obtener más información, consulte `aws history` en la Guía de referencia de la AWS CLI.

Cuando se incluye la opción `--debug`, algunos detalles son:

- Llamadas de la API realizadas a botocore
- Códigos de estado
- Respuestas HTTP
- Encabezados
- Códigos de devolución

Puede usar esta información para confirmar que los datos de parámetros y las llamadas a la API se comportan de la manera esperada y, a continuación, puede deducir en qué etapa del proceso está fallando el comando.

Volver arriba

Confirme que se ha configurado su AWS CLI

Pueden producirse varios errores si los archivos `config` y `credentials` o su rol o usuario de IAM no están configurados correctamente. Para obtener más información sobre la resolución de errores con los archivos `config` y `credentials` o su usuario o roles de IAM, consulte the section called “Errores de acceso denegado” y the section called “Errores de credenciales y claves no válidas”.

Volver arriba

Errores de comando no encontrado

Este error significa que el sistema operativo no puede encontrar el comando de la AWS CLI. Puede que la instalación esté incompleta o sea necesario actualizarla.

Causa posible: está intentando utilizar una característica de AWS CLI más reciente que la versión instalada, o tiene un formato incorrecto

Ejemplo de texto de error:

```
$ aws s3 copy
aws: [ERROR]: argument operation: Found invalid choice 'copy'

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help
```

Pueden producirse varios errores si su comando tiene un formato incorrecto o si está utilizando una versión anterior a la publicación de la característica. Para obtener más información sobre la resolución de errores en torno a estos dos problemas, consulte the section called “Compruebe su formato de comandos de la AWS CLI” y the section called “Confirme que está ejecutando una versión reciente de la AWS CLI”.

Volver arriba

Causa posible: es necesario reiniciar el terminal después de la instalación

Ejemplo de texto de error:

```
$ aws --version
```

```
command not found: aws
```

Si el comando `aws` no se encuentra después de instalar o actualizar la AWS CLI, es posible que tenga que reiniciar su terminal para que reconozca las actualizaciones de `PATH`.

Volver arriba

Causa posible: la AWS CLI no se ha instalado completamente

Ejemplo de texto de error:

```
$ aws --version
command not found: aws
```

Si no se puede encontrar el comando `aws` después de instalar o actualizar la AWS CLI, es posible que no se haya instalado completamente. Intente reinstalar siguiendo los pasos correspondientes a la plataforma en the section called “Instalar o actualizar”.

Volver arriba

Causa posible: la AWS CLI no tiene permisos (Linux)

Si no se puede encontrar el comando `aws` después de instalar o actualizar la AWS CLI en Linux, es posible que no tenga permisos `execute` para la carpeta en la que se instaló. Ejecute el siguiente comando con el `PATH` a su instalación AWS CLI, para proporcionar permisos `chmod` para la AWS CLI:

```
$ sudo chmod -R 755 /usr/local/aws-cli/
```

Volver arriba

Causa posible: la variable **`PATH`** del sistema operativo no se ha actualizado durante la instalación

Ejemplo de texto de error:

```
$ aws --version
command not found: aws
```

Es posible que tenga que añadir el ejecutable `aws` a la variable de entorno `PATH` del sistema operativo. Para agregar AWS CLI a `PATH`, utilice las instrucciones siguientes correspondientes a su sistema operativo.

Linux and macOS

1. Busque el script de perfil de su shell en su directorio de usuario. Si no está seguro de cuál es el shell que tiene, ejecute `echo $SHELL`.

   ```
   $ ls -a ~
   .  ..  .bash_logout  .bash_profile  .bashrc  Desktop  Documents  Downloads
   ```

   - Bash – `.bash_profile`, `.profile`, o `.bash_login`
   - Zsh – `.zshrc`
   - Tcsh – `.tcshrc`, `.cshrc`, o `.login`

2. Añada un comando de exportación al script de su perfil. El siguiente comando agrega su bin local a la variable PATH actual.

   ```
   export PATH=/usr/local/bin:$PATH
   ```

3. Vuelva a cargar el perfil actualizado en la sesión actual.

   ```
   $ source ~/.bash_profile
   ```

Windows

1. En un símbolo del sistema de Windows, utilice el comando `where` con el parámetro `/R` *`path`* para encontrar la ubicación del archivo de `aws`. Los resultados devuelven todas las carpetas que contienen `aws`.

   ```
   C:\> where /R c:\ aws
   c:\Program Files\Amazon\AWSCLIV2\aws.exe
   ...
   ```

   De forma predeterminada, la versión 2 de AWS CLI se encuentra en:

   ```
   c:\Program Files\Amazon\AWSCLIV2\aws.exe
   ```

2. Pulse la tecla de Windows y escriba **`environment variables`**.
3. En la lista de sugerencias, elija Edit environment variables for your account (Editar variables de entorno para la cuenta).

4. Elija PATH y, a continuación, Edit (Edición de).
5. Agregue la ruta que encontró en el primer paso al campo Variable value (Valor de variable), por ejemplo, ***C:\Program Files\Amazon\AWSCLIV2\aws.exe***.
6. Elija OK (Aceptar) dos veces para aplicar la nueva configuración.
7. Cierre los símbolos del sistema en ejecución y vuelva a abrir la ventana de símbolo del sistema.

Volver arriba

El comando "**`aws --version`**" devuelve una versión diferente a la instalada

Es posible que su terminal le devuelva un valor de `PATH` para la AWS CLI distinto al que espera.

Causa posible: es necesario reiniciar el terminal después de la instalación

Si el comando `aws` muestra la versión incorrecta, es posible que tenga que reiniciar su terminal para que reconozca las actualizaciones de `PATH`. Todos los terminales abiertos deben estar cerrados, no solo el terminal activo.

Volver arriba

Causa posible: es necesario reiniciar el sistema después de la instalación

Si el comando `aws` muestra la versión incorrecta y el reinicio del terminal no funcionó, es posible que tenga que reiniciar el terminal para que reconozca las actualizaciones de `PATH`.

Volver arriba

Causa posible: tiene varias versiones de la AWS CLI

Si ha actualizado la AWS CLI y ha utilizado un método de instalación diferente al de su instalación anterior, podría provocar la instalación de varias versiones. Por ejemplo, si en Linux o macOS ha utilizado `pip` para su instalación actual, pero ha intentado la actualización mediante el archivo de instalación de `.pkg`, esto podría causar algunos conflictos, especialmente con su `PATH` apuntando a la versión antigua.

Para resolver esto, desinstale todas las versiones de la AWS CLI y realice una instalación limpia.

Después de desinstalar todas las versiones, siga las instrucciones correspondientes a su sistema operativo para instalar la versión que desee de la AWS CLI versión 1 o la AWS CLI versión 2.

> **Note**
>
> Si esto sucede después de haber instalado la AWS CLI versión 2 con una instalación preexistente de la AWS CLI versión 1, siga las instrucciones de migración en the section called “Instrucciones de migración”.

Volver arriba

El comando "**`aws --version`**" devuelve una versión después de desinstalar la AWS CLI

Esto suele ocurrir cuando todavía hay una AWS CLI instalada en algún lugar de su sistema.

Causa posible: es necesario reiniciar el terminal después de la desinstalación

Si el comando `aws --version` sigue funcionando, es posible que tenga que reiniciar su terminal para que reconozca las actualizaciones del terminal.

Volver arriba

Causa posible: tiene varias versiones de la AWS CLI en su sistema, o no ha utilizado el mismo método de desinstalación que usó para instalar originalmente la AWS CLI

Es posible que la AWS CLI no se desinstale correctamente si desinstaló la AWS CLI con un método diferente al que utilizó para instalarla, o si instaló varias versiones. Por ejemplo, si utilizó `pip` para su instalación actual, debe utilizar `pip` para desinstalarla. Para solucionarlo, desinstale AWS CLI con el mismo método que utilizó para instalarla.

1. Siga las instrucciones adecuadas para el sistema operativo y el método de instalación original para desinstalar la AWS CLI versión 1 y AWS CLI versión 2.
2. Cierre todos los terminales que tenga abiertos.
3. Abra su terminal preferido, ingrese el siguiente comando y confirme que no se devuelve ninguna versión.

```
$ aws --version
command not found: aws
```

Si todavía tiene una versión en la lista de salida, lo más probable es que la AWS CLI se haya instalado con un método diferente o que haya varias versiones. Si no sabe con qué método instaló la AWS CLI, siga las instrucciones de cada método de desinstalación para la AWS CLI versión 1 y la AWS CLI versión 2 adecuadas al sistema operativo hasta que no reciba ninguna salida de versión.

> **Note**
>
> Si ha utilizado un administrador de paquetes para instalar la AWS CLI (`pip`, `apt`, `brew`, etc.), debe utilizar el mismo administrador de paquetes para desinstalarla. Asegúrese de seguir las instrucciones proporcionadas por el administrador de paquetes sobre cómo desinstalar todas las versiones de un paquete.

Volver arriba

La AWS CLI ha procesado un comando con un nombre de parámetro incompleto

Posible causa: ha utilizado una abreviatura reconocida del parámetro de la AWS CLI

Dado que la AWS CLI se crea utilizando Python, la AWS CLI utiliza la biblioteca `argparse` de Python, incluido el argumento `allow_abbrev`. Las abreviaturas de los parámetros son reconocidas y procesadas por la AWS CLI.

El siguiente comando de ejemplo `create-change-set` cambia el nombre de la pila de CloudFormation. El parámetro `--change-set-n` se reconoce como una abreviatura de `--change-set-name` y la AWS CLI procesa el comando.

```
$ aws cloudformation create-change-set --stack-name my-stack --change-set-n my-change-set
```

Cuando su abreviatura pueda ser varios comandos, el parámetro no se reconocerá como abreviatura.

El siguiente comando de ejemplo `create-change-set` cambia el nombre de la pila de CloudFormation. El parámetro `--change-set-` no se reconoce como una abreviatura, ya que

existen múltiples parámetros de los que podría ser una abreviatura, como `--change-set-name` y `--change-set-type`. Por lo tanto la AWS CLI no procesa el comando.

```
$ aws cloudformation create-change-set --stack-name my-stack --change-set- my-change-set
```

> **Warning**
>
> No utilice abreviaturas de parámetros a propósito. No son fiables y no son compatibles con versiones anteriores. Si se agrega algún parámetro nuevo a un comando que confunda sus abreviaturas, se interrumpirán sus comandos.
> Además, si el parámetro es un argumento de un solo valor, puede provocar un comportamiento inesperado con sus comandos. Si se pasan varias instancias de un argumento de un solo valor, solo se ejecutará la última instancia. En el siguiente ejemplo, el parámetro `--filters` es un argumento de un solo valor. Se especifican los parámetros `--filters` y `--filter`. El parámetro `--filter` es una abreviatura de `--filters`. Esto hace que se apliquen dos instancias de `--filters` y solo se aplica el último argumento `--filter`.
>
> ```
> $ aws ec2 describe-vpc-peering-connections \
>     --filters Name=tag:TagName,Values=VpcPeeringConnection \
>     --filter Name=status-code,Values=active
> ```
>
> Confirme que utiliza parámetros válidos antes de ejecutar un comando para evitar comportamientos inesperados.

Volver arriba

Errores de acceso denegado

Causa posible: el archivo de programa de la AWS CLI no tiene el permiso "run" (ejecutar)

En Linux o macOS, asegúrese de que el programa `aws` tiene permisos de ejecución para el usuario que realiza la llamada. Normalmente, los permisos se establecen en `755`.

Para añadir permisos de ejecución al usuario, ejecute el siguiente comando sustituyendo *`~ /.local/bin/aws`* por la ruta que tiene el programa en el equipo.

```
$ chmod +x ~/.local/bin/aws
```

Volver arriba

Causa posible: su identidad de IAM no tiene permiso para realizar la operación

Ejemplo de texto de error:

```
$ aws s3 ls
An error occurred (AcessDenied) when calling the ListBuckets operation: Access
 denied.
```

Cuando ejecuta un comando de la AWS CLI, las operaciones de AWS se realizan en su nombre, utilizando credenciales que lo asocian a un rol o cuenta de IAM. Las políticas asociadas deben concederle permiso para llamar a las acciones de la API correspondientes a los comandos que ejecuta con la AWS CLI.

La mayoría de los comandos llaman a una única acción que tiene un nombre que coincide con el nombre del comando. Sin embargo, los comandos personalizados como `aws s3 sync` llamar a múltiples API. Mediante la `--debug` opción puede ver a qué API llama un comando.

Si sabe con seguridad que el usuario o rol tiene los permisos adecuados asignados por la política, compruebe que el comando de la AWS CLI utiliza las credenciales que espera. Consulte la siguiente sección sobre credenciales para verificar que las credenciales que utiliza la AWS CLI son las adecuadas.

Para obtener más información acerca de la asignación de permisos de IAM, consulte Información general sobre la administración del acceso: permisos y políticas en la Guía del usuario de IAM.

Volver arriba

Errores de credenciales y claves no válidas

Ejemplo de texto de error:

```
$ aws s3 ls
An error occurred (InvalidAccessKeyId) when calling the ListBuckets operation: The AWS
 Access Key Id
you provided does not exist in our records.
```

```
$ aws s3 ls
An error occurred (InvalidClientTokenId) when calling the ListBuckets operation: The
 security token
included in the request is invalid.
```

Causa posible: la AWS CLI está leyendo las credenciales incorrectas o de una ubicación inesperada

Puede que la AWS CLI esté leyendo las credenciales desde un lugar diferente al que espera, o que la información de su par de claves sea incorrecta. Puede ejecutar `aws configure list` para confirmar las credenciales que se utilizan.

En el siguiente ejemplo se muestra cómo comprobar las credenciales utilizadas para el perfil predeterminado.

```
$ aws configure list
NAME       : VALUE                : TYPE                   : LOCATION
profile    : <not set>            : None                   : None
access_key : ****************ABCD : shared-credentials-file :
secret_key : ****************ABCD : shared-credentials-file :
region     : us-west-2            : env                    : AWS_DEFAULT_REGION
```

En el siguiente ejemplo se muestra cómo comprobar las credenciales de un perfil con nombre.

```
$ aws configure list --profile dev01
NAME       : VALUE                : TYPE                   : LOCATION
profile    : dev01                : None                   : --profile
access_key : ****************ABCD : shared-credentials-file :
secret_key : ****************ABCD : shared-credentials-file :
region     : us-west-2            : config-file            : ~/.aws/config
```

Para confirmar los detalles de su par de claves, compruebe sus archivos `config` y `credentials`. Para obtener más información sobre los archivos `config` y `credentials`, consulte the section called “Opciones de configuración”. Para obtener más información sobre credenciales y autenticación, incluida la precedencia de las credenciales, consulte Credenciales de autenticación y acceso.

Volver arriba

Causa posible: el reloj del equipo no está sincronizado

Si está utilizando credenciales válidas, puede que el reloj no esté sincronizado. En Linux o macOS, ejecute `date` para verificar la hora.

```
$ date
```

Si el reloj del sistema no es correcto en unos minutos, utilice `ntpd` para sincronizarlo.

```
$ sudo service ntpd stop
$ sudo ntpdate time.nist.gov
$ sudo service ntpd start
$ ntpstat
```

En Windows, utilice las opciones de fecha y hora del Panel de control para configurar el reloj del sistema.

Volver arriba

Errores de firma que no coincide

Ejemplo de texto de error:

```
$ aws s3 ls
An error occurred (SignatureDoesNotMatch) when calling the ListBuckets operation: The
 request signature we
calculated does not match the signature you provided. Check your key and signing
 method.
```

Cuando la AWS CLI ejecuta un comando, envía una solicitud cifrada a los servidores de AWS para realizar las operaciones del servicio de AWS correspondientes. Sus credenciales (la clave de acceso y la clave secreta) se incluyen en el cifrado y permiten que AWS autentique a la persona que realiza la solicitud. Tal y como se indica a continuación, hay varias cosas que pueden interferir con el funcionamiento correcto de este proceso.

Causa posible: el reloj no está sincronizado con los servidores de AWS

Para protegerse de los ataques de reproducción, puede utilizar la hora actual durante el proceso de cifrado y descifrado. Si la hora del cliente y el servidor no coinciden en una cantidad superior

a la permitida, puede que el proceso produzca un error y se rechace la solicitud. Esto también puede ocurrir cuando ejecuta un comando en una máquina virtual cuyo reloj no está sincronizado con el reloj de la máquina host. Una causa posible es cuando la máquina virtual está en hibernación y tarda algún tiempo en reactivarse para sincronizar el reloj con la máquina host.

En Linux o macOS, ejecute `date` para verificar la hora.

```
$ date
```

Si el reloj del sistema no es correcto en unos minutos, utilice `ntpd` para sincronizarlo.

```
$ sudo service ntpd stop
$ sudo ntpdate time.nist.gov
$ sudo service ntpd start
$ ntpstat
```

En Windows, utilice las opciones de fecha y hora del Panel de control para configurar el reloj del sistema.

Volver arriba

Causa posible: el sistema operativo está administrando incorrectamente las claves de AWS que contienen determinados caracteres especiales

Si las claves de AWS incluyen determinados caracteres especiales, como `-`, `+`, `/` o `%`, algunas variantes del sistema operativo procesan la cadena de forma incorrecta y hacen que la cadena de clave se interprete incorrectamente.

Si procesa las claves utilizando otras herramientas o scripts, como herramientas que compilan el archivo de credenciales en una nueva instancia cuando se crea, esas herramientas y scripts podrían tratar los caracteres especiales de forma distinta, lo que hace que se transformen en algo que AWS ya no reconoce.

Sugerimos regenerar la clave secreta para obtener una que no incluya el carácter especial que causa problemas.

Volver arriba

Errores de certificado SSL

Causa posible: la AWS CLI no confía en el certificado de su proxy

Ejemplo de texto de error:

```
$ aws s3 ls
[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed
```

Cuando utiliza un comando de AWS CLI, se recibe un mensaje de error `[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed`. Esto se produce porque AWS CLI no confía en el certificado del proxy debido a que ciertos factores como el certificado del proxy están autofirmados, con su empresa establecida como la entidad de certificación (CA). Esto evita que la AWS CLI encuentre el certificado raíz de la CA de su empresa en el registro local de CA.

Para solucionarlo, indíquele a la AWS CLI dónde encontrar el archivo `.pem` de su empresa utilizando el ajuste de archivo de configuración del `ca_bundle`, la opción de línea de comandos de `--ca-bundle` o la variable de entorno de `AWS_CA_BUNDLE`.

Volver arriba

Causa posible: la configuración no apunta a la ubicación correcta del certificado raíz de la CA

Ejemplo de texto de error:

```
$ aws s3 ls
SSL validation failed for regionname [Errno 2] No such file or directory
```

Esto se debe a que la ubicación del archivo del paquete de la autoridad de certificación (CA) está configurada incorrectamente en la AWS CLI. Para solucionarlo, confirme dónde se encuentra su archivo `.pem` de su empresa y actualice la configuración de la AWS CLI mediante la opción del archivo de configuración `ca_bundle`, la opción de la línea de comandos `--ca-bundle` o la variable de entorno `AWS_CA_BUNDLE`.

Volver arriba

Causa posible: la configuración no está usando la Región de AWS correcta.

Ejemplo de texto de error:

```
$ aws s3 ls
[SSL: CERTIFICATE_ VERIFY_FAILED] certificate verify failed
```

Se pueden producir errores o resultados inesperados si un Servicio de AWS no está disponible para la Región de AWS especificada o si los recursos están ubicados en una Región de AWS diferente. Para ver los pasos de solución de problemas, consulte the section called “Compruebe la Región de AWS que utiliza su comando de la AWS CLI.”.

Volver arriba

Causa posible: es necesario actualizar su versión de TLS

Ejemplo de texto de error:

```
$ aws s3 ls
[SSL: UNSAFE_LEGACY_RENEGOTIATION_DISABLED] unsafe legacy renegotiation disabled
```

El Servicio de AWS utiliza una versión de TLS que no es compatible con la versión de TLS de su dispositivo. Para resolver este problema, actualice a una versión de TLS compatible. Para obtener más información, consulte the section called “Aplicación de una versión mínima de TLS”.

Volver arriba

Errores de JSON no válido

Ejemplo de texto de error:

```
$ aws dynamodb update-table \
    --provisioned-throughput '{"ReadCapacityUnits":15,WriteCapacityUnits":10}' \
    --table-name MyDDBTable
Error parsing parameter '--provisioned-throughput': Invalid JSON: Expecting property
 name enclosed in
double quotes: line 1 column 25 (char 24)
JSON received: {"ReadCapacityUnits":15,WriteCapacityUnits":10}
```

Cuando utiliza un comando de AWS CLI, se recibe un mensaje de error “`Invalid JSON`“. Suele ser un error que aparece cuando se introduce un comando con un formato JSON esperado y AWS CLI no puede leer el JSON correctamente.

Causa posible: no ha introducido un JSON válido para que lo use AWS CLI

Confirme que ha introducido un JSON válido para el comando. Le sugerimos que utilice un validador de JSON para el JSON con problemas de formato.

Para conocer un uso más avanzado de JSON en la línea de comandos, considere usar un procesador JSON de línea de comandos, como `jq`, para crear cadenas JSON. Para obtener más información sobre `jq`, consulte el repositorio jq en GitHub.

Volver arriba

Causa posible: las reglas de centrecomillado de su terminal impiden que se envíe un JSON válido a la AWS CLI

Antes de que la AWS CLI reciba cualquier cosa de un comando, su terminal procesa el comando utilizando sus propias reglas de entrecomillado y escapes. Debido a las reglas de formato de un terminal, es posible que parte del contenido JSON se elimine antes de que el comando se pase a la AWS CLI. Al formular comandos, asegúrese de usar sus reglas de entrecomillado del terminal.

Para solucionar problemas, utilice el comando `echo` para ver cómo el shell gestiona los parámetros:

```
$ echo {"ReadCapacityUnits":15,"WriteCapacityUnits":10}
ReadCapacityUnits:15 WriteCapacityUnits:10
```

```
$ echo '{"ReadCapacityUnits":15,"WriteCapacityUnits":10}'
{"ReadCapacityUnits":15,"WriteCapacityUnits":10}
```

Modifique su comando hasta que se devuelva su JSON válido.

Para obtener una solución más detallada, use el parámetro `--debug` para ver los registros de depuración, ya que muestran exactamente lo que se pasó a la AWS CLI:

```
$ aws dynamodb update-table \
    --provisioned-throughput '{"ReadCapacityUnits":15,WriteCapacityUnits":10}' \
    --table-name MyDDBTable \
    --debug
2022-07-19 22:25:07,741 - MainThread - awscli.clidriver - DEBUG - CLI version: aws-
cli/1.18.147
Python/2.7.18 Linux/5.4.196-119.356.amzn2int.x86_64 botocore/1.18.6
2022-07-19 22:25:07,741 - MainThread - awscli.clidriver - DEBUG - Arguments entered
 to CLI:
```

```
['dynamodb', 'update-table', '--provisioned-throughput',
 '{"ReadCapacityUnits":15,WriteCapacityUnits":10}',
 '--table-name', 'MyDDBTable', '--debug']
```

Use las reglas de entrecomillado de tu terminal para solucionar cualquier problema que tenga su entrada JSON cuando se envía a la AWS CLI. Para obtener más información sobre las reglas de entrecomillado, consulte the section called “Comillas con cadenas”.

> **Note**
>
> Si tiene problemas para obtener JSON válido en la AWS CLI, le recomendamos omitir las reglas de entrecomillado de un terminal para la entrada de datos JSON, use Blobs para pasar los datos JSON directamente a la AWS CLI. Para obtener más información acerca de Blobs, consulte o Blob.

Volver arriba

Recursos adicionales

Para obtener ayuda adicional con sus problemas de AWS CLI, visite la comunidad de la AWS CLI en GitHub o la comunidad AWS re:Post.

Volver arriba

Ejemplos para la AWS CLI

En este capítulo se proporciona una serie de ejemplos que muestran cómo utilizar AWS Command Line Interface (AWS CLI) con los Servicios de AWS.

La AWS CLI incluye los siguientes tipos de ejemplo en esta guía:

- Ejemplos de comandos guiados: ejemplos de comandos guiados para la guía del usuario de AWS CLI sobre cómo usar la AWS CLI con algunos Servicios de AWS. Suelen ser ejemplos más detallados que los ejemplos de la guía de referencia de la versión 2 de la AWS CLI.
- Ejemplos de comandos de AWS CLI: ejemplos de comandos de código abierto que también están disponibles en la guía de referencia de la versión 2 de la AWS CLI. Los ejemplos de comandos están alojados en el repositorio de la AWS CLI en GitHub.
- Ejemplos de código de la AWS CLI con script Bash: ejemplos de script bash de código abierto. Los ejemplos de script Bash están alojados en el Repositorio de ejemplos de código de AWS en GitHub.

> **Comentarios sobre los ejemplos**
>
> ¿No encuentra lo que necesita? Solicite un ejemplo de comando en el enlace Proporcionar comentarios al final de esta página o en la página de comandos correspondiente de la guía de referencia de la versión 2 de la AWS CLI.
> ¿Quiere contribuir? Contribuya con ejemplos de comandos de la AWS CLI en el repositorio de ejemplos de código de AWS en GitHub. Para obtener más información sobre cómo contribuir, consulte AWS CLI code example contribution quick steps en las páginas de GitHub.

Ejemplos de comandos guiados de la AWS CLI

La AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le permite interactuar con una amplia gama de Servicios de AWS mediante el uso de comandos en el intérprete de comandos de la línea de comandos. En esta sección se proporcionan ejemplos guiados que muestran cómo aprovechar la AWS CLI para acceder a algunos de los Servicios de AWS. Esto incluye algunos de los comandos de AWS CLI personalizados, como los comandos `aws s3` de alto

nivel. Estos ejemplos de comandos muestran las acciones más comunes que se utilizan en algunos Servicios de AWS y proporcionan recursos adicionales para obtener más información.

Tanto si es un usuario de AWS con experiencia como si es nuevo en la AWS CLI, estos ejemplos guiados le servirán de recurso para agilizar sus operaciones de AWS.

Para obtener una referencia completa de todos los comandos disponibles para cada Servicio de AWS, consulte la guía de referencia de la versión 2 de la AWS CLI. Además, puede utilizar la ayuda integrada de la línea de comandos para explorar la variedad de Servicios de AWS, comandos, opciones y características de la AWS CLI.

Para ver más ejemplos de comandos que no están disponibles en esta sección, consulte la sección de Ejemplos de comando de AWS CLI. Estos son ejemplos de comandos de código abierto que también están disponibles en la guía de referencia de la versión 2 de la AWS CLI. Los ejemplos de comandos están alojados en el repositorio de la AWS CLI en GitHub.

Para ver ejemplos de script bash de código abierto, consulte the section called “Ejemplos de script Bash”. Los ejemplos de script bash están alojados en el Repositorio de ejemplos de código de AWS en GitHub.

Servicios

- Amazon DynamoDB en la AWS CLI
- Uso de Amazon EC2 en la AWS CLI
- Uso de Amazon Glacier en la AWS CLI
- Uso de IAM en la AWS CLI
- Uso de Amazon S3 en la AWS CLI
- Acceso a Amazon SNS en la AWS CLI

Amazon DynamoDB en la AWS CLI

La AWS Command Line Interface (AWS CLI) ofrece soporte para todos los servicios de base de datos de AWS, incluido Amazon DynamoDB. Puede usar la AWS CLI para operaciones impromptu, como crear una tabla. También puede usarla para incluir operaciones de DynamoDB en scripts de utilidades.

Para obtener más información acerca del uso de AWS CLI con DynamoDB, consulte `dynamodb` en la Referencia de comandos de AWS CLI.

Para mostrar los comandos de la AWS CLI para DynamoDB, utilice el siguiente comando.

```
$ aws dynamodb help
```

Temas

- Requisitos previos
- Creación y uso de tablas de DynamoDB
- Uso de DynamoDB Local
- Recursos

Requisitos previos

Para ejecutar los comandos de `dynamodb`, debe:

- Instalar y configurar la AWS CLI. Para obtener más información, consulte the section called "Instalar o actualizar" y Credenciales de autenticación y acceso para la AWS CLI.

Creación y uso de tablas de DynamoDB

El formato de la línea de comandos se compone de un nombre de comando de DynamoDB, seguido de los parámetros de dicho comando. La AWS CLI permite utilizar la sintaxis abreviada de la CLI en los valores de los parámetros, además de todo el código JSON.

En el siguiente ejemplo, se crea una tabla llamada `MusicCollection`.

```
$ aws dynamodb create-table \
    --table-name MusicCollection \
    --attribute-definitions AttributeName=Artist,AttributeType=S
 AttributeName=SongTitle,AttributeType=S \
    --key-schema AttributeName=Artist,KeyType=HASH
 AttributeName=SongTitle,KeyType=RANGE \
    --provisioned-throughput ReadCapacityUnits=1,WriteCapacityUnits=1
```

A continuación, puede añadir nuevas líneas a la tabla con comandos similares a los que se muestran en el siguiente ejemplo. En estos ejemplos se usa una combinación de sintaxis abreviada y JSON.

```
$ aws dynamodb put-item \
```

```
    --table-name MusicCollection \
    --item '{
        "Artist": {"S": "No One You Know"},
        "SongTitle": {"S": "Call Me Today"} ,
        "AlbumTitle": {"S": "Somewhat Famous"}
      }' \
    --return-consumed-capacity TOTAL
{
    "ConsumedCapacity": {
        "CapacityUnits": 1.0,
        "TableName": "MusicCollection"
    }
}
```

```
$ aws dynamodb put-item \
    --table-name MusicCollection \
    --item '{
        "Artist": {"S": "Acme Band"},
        "SongTitle": {"S": "Happy Day"} ,
        "AlbumTitle": {"S": "Songs About Life"}
      }' \
    --return-consumed-capacity TOTAL
{
    "ConsumedCapacity": {
        "CapacityUnits": 1.0,
        "TableName": "MusicCollection"
    }
}
```

Puede resultar difícil crear código JSON válido en una única línea de comandos. Para facilitar la operación, la AWS CLI puede leer archivos JSON. Por ejemplo, fíjese en el fragmento de código JSON siguiente, que se almacena en un archivo denominado `expression-attributes.json`.

```
{
  ":v1": {"S": "No One You Know"},
  ":v2": {"S": "Call Me Today"}
}
```

Puede utilizar ese archivo para emitir una solicitud de `query` mediante la AWS CLI. En el siguiente ejemplo, se usa el contenido del archivo `expression-attributes.json` como valor del parámetro `--expression-attribute-values`.

```
$ aws dynamodb query --table-name MusicCollection \
    --key-condition-expression "Artist = :v1 AND SongTitle = :v2" \
    --expression-attribute-values file://expression-attributes.json
{
    "Count": 1,
    "Items": [
        {
            "AlbumTitle": {
                "S": "Somewhat Famous"
            },
            "SongTitle": {
                "S": "Call Me Today"
            },
            "Artist": {
                "S": "No One You Know"
            }
        }
    ],
    "ScannedCount": 1,
    "ConsumedCapacity": null
}
```

Uso de DynamoDB Local

Además de con DynamoDB, también puede usar la AWS CLI con DynamoDB Local. DynamoDB Local es un pequeño servidor y base de datos del lado del cliente que imita el servicio de DynamoDB. DynamoDB Local le permite escribir aplicaciones que usan la API de DynamoDB sin manipular realmente las tablas o los datos del servicio web de DynamoDB. En lugar de eso, todas las acciones de la API se redirigen a una base de datos local. lo que le permite ahorrar en rendimiento aprovisionado, almacenamiento de datos y tarifas de transferencia de datos.

Para obtener más información sobre DynamoDB Local y cómo usarlo con la AWS CLI, consulte las secciones siguientes de Guía de desarrollador de Amazon DynamoDB:

- DynamoDB Local
- Uso de la AWS CLI con DynamoDB Local

Recursos

referencia de AWS CLI:

- `aws dynamodb`
- `aws dynamodb create-table`
- `aws dynamodb put-item`
- `aws dynamodb query`

Referencia de servicio:

- DynamoDB Local en la Guía para desarrolladores de Amazon DynamoDB
- Uso de la AWS CLI con DynamoDB Local en la Guía para desarrolladores de Amazon DynamoDB

Uso de Amazon EC2 en la AWS CLI

Una introducción a Amazon Elastic Compute Cloud (EC2)
Introducción a Amazon EC2: Elastic Cloud Server y alojamiento con AWS

Amazon Elastic Compute Cloud (Amazon EC2) proporciona entornos informáticos virtuales altamente escalables y flexibles. Amazon EC2 le permite aprovisionar y administrar servidores virtuales, conocidos como instancias de Amazon EC2, para satisfacer una amplia gama de necesidades informáticas.

Las instancias de Amazon EC2 son máquinas virtuales que se pueden personalizar con varias configuraciones de CPU, memoria, almacenamiento y capacidades de red. Puede elegir entre una amplia selección de tipos de instancias, que van desde opciones ligeras y rentables hasta instancias potentes y de alto rendimiento, según los requisitos de la aplicación. Esta flexibilidad le permite adaptarse a las necesidades informáticas para optimizar el rendimiento y la rentabilidad.

Además, Amazon EC2 ofrece un conjunto de características que le permiten administrar los recursos informáticos de forma eficaz. Estas incluyen la capacidad de lanzar nuevas instancias con rapidez, crear imágenes de máquina personalizadas (AMI) para una implementación rápida y ampliar o reducir la capacidad informática según sea necesario.

Puede obtener acceso a las características de Amazon EC2 con la AWS Command Line Interface (AWS CLI). Para mostrar los comandos de la AWS CLI para Amazon EC2, utilice el siguiente comando.

```
aws ec2 help
```

Antes de ejecutar los comandos, defina sus credenciales predeterminadas. Para obtener más información, consulte Configuración de los ajustes de AWS CLI.

En este tema se muestran ejemplos de comandos de formato corto de la AWS CLI que realizan tareas comunes para Amazon EC2.

Para obtener ejemplos de formato largo de los comandos de la AWS CLI, consulte el repositorio de ejemplos de código de AWS CLI en GitHub.

Temas

- Creación, visualización y eliminación de pares de claves de Amazon EC2 en la AWS CLI
- Creación, configuración y eliminación de grupos de seguridad de Amazon EC2 en la AWS CLI
- Lanzamiento, enumeración y eliminación de instancias de Amazon EC2 en la AWS CLI
- Cambio de un tipo de instancia de Amazon EC2 con un script de Bash en la AWS CLI

Creación, visualización y eliminación de pares de claves de Amazon EC2 en la AWS CLI

Puede utilizar el AWS Command Line Interface (AWS CLI) para crear, mostrar y eliminar los pares de claves para Amazon Elastic Compute Cloud (Amazon EC2). Utilice un par de claves para conectarse a su instancia de Amazon EC2. Puede proporcionar el par de claves para Amazon EC2 al crear la instancia y, a continuación, utilice ese par de claves para autenticarse cuando se conecte a la instancia.

> **Note**
>
> Para ver ejemplos de comandos adicionales, consulte la AWS CLIguía de referencia de .

Temas

- Requisitos previos
- Crear un par de claves
- Mostrar un par de claves
- Eliminar un par de claves

- Referencias

Requisitos previos

Para ejecutar los comandos de `ec2`, debe:

- Instalar y configurar la AWS CLI. Para obtener más información, consulte the section called "Instalar o actualizar" y Credenciales de autenticación y acceso para la AWS CLI.
- Establezca sus permisos de IAM para permitir el acceso a Amazon EC2. Para obtener más información sobre los permisos de IAM para Amazon EC2, consulte Políticas de IAM para Amazon EC2 en la Guía del usuario de Amazon EC2.

Crear un par de claves

Para crear un par de claves, utilice el comando `aws ec2 create-key-pair` con la opción `--query` y la opción `--output text` para transferir su clave privada directamente a un archivo.

```
$ aws ec2 create-key-pair --key-name MyKeyPair --query 'KeyMaterial' --output text
 > MyKeyPair.pem
```

Para PowerShell, el redireccionamiento de `> file` adopta la codificación UTF-8 de forma predeterminada, que no se puede utilizar en algunos clientes SSH. Por lo tanto, debe convertir la salida transfiriéndola al comando `out-file` y establecer de forma explícita la codificación en `ascii`.

```
PS C:\>aws ec2 create-key-pair --key-name MyKeyPair --query 'KeyMaterial' --output text
 | out-file -encoding ascii -filepath MyKeyPair.pem
```

El archivo `MyKeyPair.pem` resultante tiene este aspecto.

```
-----BEGIN RSA PRIVATE KEY-----
EXAMPLEKEYKCAQEAy7WZhaDsrA1W3mRlQtvhwyORRX8gnxgDAfRt/gx42kWXsT4rXE/b5CpSgie/
vBoU7jLxx92pNHoFnByP+Dc21eyyz6CvjTmWA0JwfWiW5/akH7iO5dSrvC7dQkW2duV5QuUdE0QW
Z/aNxMniGQE6XAgfwlnXVBwrerrQo+ZWQeqiUwwMkuEbLeJFLhMCvYURpUMSC1oehm449ilx9X1F
G50TCFeOzfl8dqqCP6GzbPaIjiU19xX/azOR9V+tpUOzEL+wmXnZt3/nHPQ5xvD2OJH67km6SuPW
oPzev/D8V+x4+bHthfSjR9Y7DvQFjfBVwHXigBdtZcU2/wei8D/HYwIDAQABAoIBAGZ1kaEvnrqu
/uler7vgIn5m7lN5LKw4hJLAIW6tUT/fzvtcHK0SkbQCQXuriHmQ2MQyJX/0kn2NfjLV/ufGxbL1
mb5qwMGUnEpJaZD6QSSs3kICLwWUYUiGfc0uiSbmJoap/GTLU0W5Mfcv36PaBUNy5p53V6G7hXb2
bahyWyJNfjLe4M86yd2YK3V2CmK+X/BOsShnJ36+hjrXPPWmV3N9zEmCdJjA+K15DYmhm/tJWSD9
```

```
81oGk9TopEp7CkIfatEATyyZiVqoRq6k64iuM9JkA3OzdXzMQexXVJ1TLZVEH0E7bhlY9d8O1ozR
oQs/FiZNAx2iijCWyv0lpjE73+kCgYEA9mZtyhkHkFDpwrSM1APaL8oNAbbjwEy7Z5Mqfql+lIp1
YkriL0DbLXlvRAH+yHPRit2hHOjtUNZh4Axv+cpg09qbUI3+43eEy24B7G/Uh+GTfbjsXsOxQx/x
p9otyVwc7hsQ5TA5PZb+mvkJ5OBEKzet9XcKwONBYELGhnEPe7cCgYEA06Vgov6YHleHui9kHuws
ayav0elc5zkxjF9nfHFJRry21R1trw2Vdpn+9g481URrpzWVOEihvm+xTtmaZlSp//lkq75XDwnU
WA8gkn6O3QE3fq2yN98BURsAKdJfJ5RL1HvGQvTe10HLYYXpJnEkHv+Unl2ajLivWUt5pbBrKbUC
gYBjbO+OZk0sCcpZ29sbzjYjpIddErySIyRX5gV2uNQwAjLdp9PfN295yQ+BxMBXiIycWVQiw0bH
oMo7yykABY7Ozd5wQewBQ4AdSlWSX4nGDtsiFxWiI5sKuAAeOCbTosy1s8w8fxoJ5Tz1sdoxNeGs
Arq6Wv/G16zQuAE9zK9vvwKBgF+09VI/1wJBirsDGz9whVWfFPrTkJNvJZzYt69qezxlsjgFKshy
WBhd4xHZtmCqpBPlAymEjr/TOlbxyARmXMnIOWIAnNXMGB4KGSyl1mzSVAoQ+fqR+cJ3d0dyPl1j
jjb0Ed/NY8frlNDxAVHE8BSkdsx2f6ELEyBKJSRr9snRAoGAMrTwYneXzvTskF/S5Fyu0iOegLDa
NWUH38v/nDCgEpIXD5Hn3qAEcju1IjmbwlvtW+nY2jVhv7UGd8MjwUTNGItdb6nsYqM2asrnF3qS
VRkAKKKYeGjkpUfVTrW0YFjXkfcrR/V+QFL5OndHAKJXjW7a4ejJLncTzmZSpYzwApc=
-----END RSA PRIVATE KEY-----
```

Su clave privada no se almacena en AWS y solo se puede recuperar en el momento de crearla. No puede recuperarla más adelante. En vez de ello, si pierde la clave privada, debe crear un par de claves nuevo.

Si se está conectando a su instancia desde un equipo Linux, le recomendamos que utilice el siguiente comando para establecer los permisos de su archivo de clave privada de modo que solo usted pueda leerlo.

```
$ chmod 400 MyKeyPair.pem
```

Mostrar un par de claves

Se genera una "huella digital" a partir del par de claves, que puede utilizar para verificar que la clave privada que tiene en su equipo local coincide con la clave pública almacenada en AWS.

La huella digital es un valor hash SHA1 tomado a partir de una copia de la clave privada con codificación DER. Este valor se captura cuando se crea el par de claves y se almacena en AWS junto con la clave pública. Puede consultar la huella digital en la consola de Amazon EC2 o ejecutando el comando de la AWS CLI `aws ec2 describe-key-pairs`.

En el siguiente ejemplo se muestra la huella digital de `MyKeyPair`.

```
$ aws ec2 describe-key-pairs --key-name MyKeyPair
{
    "KeyPairs": [
        {
```

```
            "KeyName": "MyKeyPair",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f"
        }
    ]
}
```

Para obtener más información sobre las claves y huellas digitales, consulte Pares de claves de Amazon EC2 en la Guía del usuario de Amazon EC2.

Eliminar un par de claves

Para eliminar un par de claves, ejecute el comando `aws ec2 delete-key-pair`, sustituyendo *MyKeyPair* por el nombre del par de claves que desea eliminar.

```
$ aws ec2 delete-key-pair --key-name MyKeyPair
```

Referencias

referencia de AWS CLI:

- `aws ec2`
- `aws ec2 create-key-pair`
- `aws ec2 delete-key-pair`
- `aws ec2 describe-key-pairs`

Otra referencia:

- Documentación de Amazon Elastic Compute Cloud
- Para ver y contribuir al SDK de AWS y los ejemplos de código de AWS CLI, consulte el Repositorio de ejemplos de código de AWS en GitHub.

Creación, configuración y eliminación de grupos de seguridad de Amazon EC2 en la AWS CLI

Puede crear un grupo de seguridad para las instancias Amazon Elastic Compute Cloud (Amazon EC2) que básicamente funciona como un firewall, con reglas que determinan el tráfico de red que puede entrar y salir.

Utilice AWS Command Line Interface (AWS CLI) para crear un nuevo grupo de seguridad, añadir reglas a grupos de seguridad existentes y eliminar grupos de seguridad.

> **Note**
>
> Para ver ejemplos de comandos adicionales, consulte la AWS CLIguía de referencia de .

Temas

- Requisitos previos
- Creación de un grupo de seguridad
- Agregar reglas al grupo de seguridad
- Eliminación de un grupo de seguridad
- Referencias

Requisitos previos

Para ejecutar los comandos de `ec2`, debe:

- Instalar y configurar la AWS CLI. Para obtener más información, consulte the section called "Instalar o actualizar" y Credenciales de autenticación y acceso para la AWS CLI.
- Establezca sus permisos de IAM para permitir el acceso a Amazon EC2. Para obtener más información sobre los permisos de IAM para Amazon EC2, consulte Políticas de IAM para Amazon EC2 en la Guía del usuario de Amazon EC2.

Creación de un grupo de seguridad

Puede crear grupos de seguridad asociados a nubes privadas virtuales (VPC).

En el siguiente ejemplo de `aws ec2 create-security-group` se muestra cómo crear un grupo de seguridad para una VPC especificada.

```
$ aws ec2 create-security-group --group-name my-sg --description "My security group" --
vpc-id vpc-1a2b3c4d
{
    "GroupId": "sg-903004f8"
}
```

Para ver la información inicial para un grupo de seguridad, ejecute el comando de `aws ec2 describe-security-groups`. Solo puede hacer referencia a un grupo de seguridad de EC2-VPC por su `vpc-id`, no por su nombre.

```
$ aws ec2 describe-security-groups --group-ids sg-903004f8
{
    "SecurityGroups": [
        {
            "IpPermissionsEgress": [
                {
                    "IpProtocol": "-1",
                    "IpRanges": [
                        {
                            "CidrIp": "0.0.0.0/0"
                        }
                    ],
                    "UserIdGroupPairs": []
                }
            ],
            "Description": "My security group"
            "IpPermissions": [],
            "GroupName": "my-sg",
            "VpcId": "vpc-1a2b3c4d",
            "OwnerId": "123456789012",
            "GroupId": "sg-903004f8"
        }
    ]
}
```

Agregar reglas al grupo de seguridad

Cuando ejecute una instancia de Amazon EC2, debe habilitar reglas en el grupo de seguridad para permitir el tráfico de red entrante en el medio que utilice para conectarse a la imagen.

Por ejemplo, si lanza una instancia de Windows, normalmente debe añadir una regla para permitir el tráfico entrante en el puerto TCP 3389 (RDP) para dar soporte al protocolo de escritorio remoto (RDP). Si lanza una instancia de Linux, normalmente debe añadir una regla para permitir el tráfico entrante en el puerto TCP 22 (SSH) para dar soporte a las conexiones de SSH.

Use el comando `aws ec2 authorize-security-group-ingress` para añadir una regla a un grupo de seguridad. Uno de los parámetros obligatorios de este comando es la dirección IP pública

de su equipo, o la red (en forma de un intervalo de direcciones) al que su equipo está asociada, en notación CIDR.

> **Note**
>
> Proporcionamos el siguiente servicio, https://checkip.global.api.aws/, para determinar su dirección IP pública. Para encontrar otros servicios que puedan ayudarle a identificar su dirección IP, utilice el navegador para buscar"cuál es mi dirección IP". Si se conecta a través de un ISP o protegido por su firewall mediante una dirección IP dinámica (a través de una gateway NAT desde una red privada), su dirección puede cambiar de forma periódica. En ese caso, debe averiguar el rango de direcciones IP que utilizan los equipos cliente.

En el siguiente ejemplo se muestra cómo añadir una regla para RDP (puerto TCP 3389) a un grupo de seguridad EC2-VPC con el ID `sg-903004f8` utilizando su dirección IP.

Para empezar, busque su dirección IP.

```
$ curl https://checkip.amazonaws.com
x.x.x.x
```

Luego, puede agregar la dirección IP a su grupo de seguridad mediante la ejecución del comando `aws ec2 authorize-security-group-ingress`.

```
$ aws ec2 authorize-security-group-ingress --group-id sg-903004f8 --protocol tcp --port
 3389 --cidr x.x.x.x/x
```

El siguiente comando añade otra regla para habilitar SSH en instancias en el mismo grupo de seguridad.

```
$ aws ec2 authorize-security-group-ingress --group-id sg-903004f8 --protocol tcp --port
 22 --cidr x.x.x.x/x
```

Para ver los cambios realizados en el grupo de seguridad, ejecute el comando `aws ec2 describe-security-groups`.

```
$ aws ec2 describe-security-groups --group-ids sg-903004f8
{
    "SecurityGroups": [
```

```
        {
            "IpPermissionsEgress": [
                {
                    "IpProtocol": "-1",
                    "IpRanges": [
                        {
                            "CidrIp": "0.0.0.0/0"
                        }
                    ],
                    "UserIdGroupPairs": []
                }
            ],
            "Description": "My security group"
            "IpPermissions": [
                {
                    "ToPort": 22,
                    "IpProtocol": "tcp",
                    "IpRanges": [
                        {
                            "CidrIp": "x.x.x.x/x"
                        }
                    ]
                    "UserIdGroupPairs": [],
                    "FromPort": 22
                }
            ],
            "GroupName": "my-sg",
            "OwnerId": "123456789012",
            "GroupId": "sg-903004f8"
        }
    ]
}
```

Eliminación de un grupo de seguridad

Para eliminar un grupo de seguridad, ejecute el comando `aws ec2 delete-security-group`.

> **Note**
>
> No puede eliminar un grupo de seguridad que esté conectado actualmente a un entorno.

El siguiente ejemplo de comando elimina un grupo de seguridad EC2-VPC.

```
$ aws ec2 delete-security-group --group-id sg-903004f8
```

Referencias

referencia de AWS CLI:

- aws ec2
- aws ec2 authorize-security-group-ingress
- aws ec2 create-security-group
- aws ec2 delete-security-group
- aws ec2 describe-security-groups

Otra referencia:

- Documentación de Amazon Elastic Compute Cloud
- Para ver y contribuir al SDK de AWS y los ejemplos de código de AWS CLI, consulte el Repositorio de ejemplos de código de AWS en GitHub.

Lanzamiento, enumeración y eliminación de instancias de Amazon EC2 en la AWS CLI

Puede utilizar la AWS Command Line Interface (AWS CLI) para lanzar, enumerar y eliminar instancias de Amazon Elastic Compute Cloud (Amazon EC2). Si lanza una instancia que no figura en la capa gratuita de AWS, se le facturará en cuanto la lance y se le cobrará el tiempo en que la instancia esté funcionando, aunque permanezca inactiva.

> **Note**
>
> Para ver ejemplos de comandos adicionales, consulte la Guía de la referencia de la AWS CLI.

Temas

- Requisitos previos
- iniciar la instancia
- Agregar un dispositivo de bloques a la instancia

- Agregar una etiqueta a la instancia
- Conéctese a su instancia
- Enumerar las instancias
- Eliminar la instancia
- Referencias

Requisitos previos

Para ejecutar los comandos `ec2` en este tema, debe hacer lo siguiente:

- Instalar y configurar la AWS CLI. Para obtener más información, consulte the section called "Instalar o actualizar", y Credenciales de autenticación y acceso para la AWS CLI.
- Establezca sus permisos de IAM para permitir el acceso a Amazon EC2. Para obtener más información sobre los permisos de IAM para Amazon EC2, consulte Políticas de IAM para Amazon EC2 en la Guía del usuario de Amazon EC2.
- Cree un par de claves y un grupo de seguridad.
- Seleccione una Amazon Machine Image (AMI) y anotar su ID de AMI. Para obtener más información, consulte Búsqueda de una AMI apta en la Guía del usuario de Amazon EC2.

iniciar la instancia

Para lanzar una instancia de Amazon EC2 utilizando la AMI que ha seleccionado, utilice el comando `aws ec2 run-instances`. Puede lanzar la instancia en una nube privada virtual (VPC).

Al principio, la instancia aparece en el estado `pending`, pero cambia al estado `running` después de unos minutos.

En el siguiente ejemplo se muestra cómo lanzar una instancia `t2.micro` en la subred especificada de una VPC. Sustituya los valores del parámetro *`en cursiva`* por sus propios valores.

```
$ aws ec2 run-instances --image-id ami-xxxxxxxx --count 1 --instance-type t2.micro --
key-name MyKeyPair --security-group-ids sg-903004f8 --subnet-id subnet-6e7f829e
{
    "OwnerId": "123456789012",
    "ReservationId": "r-5875ca20",
    "Groups": [
        {
            "GroupName": "my-sg",
```

```
            "GroupId": "sg-903004f8"
        }
    ],
    "Instances": [
        {
            "Monitoring": {
                "State": "disabled"
            },
            "PublicDnsName": null,
            "Platform": "windows",
            "State": {
                "Code": 0,
                "Name": "pending"
            },
            "EbsOptimized": false,
            "LaunchTime": "2013-07-19T02:42:39.000Z",
            "PrivateIpAddress": "10.0.1.114",
            "ProductCodes": [],
            "VpcId": "vpc-1a2b3c4d",
            "InstanceId": "i-5203422c",
            "ImageId": "ami-173d747e",
            "PrivateDnsName": "ip-10-0-1-114.ec2.internal",
            "KeyName": "MyKeyPair",
            "SecurityGroups": [
                {
                    "GroupName": "my-sg",
                    "GroupId": "sg-903004f8"
                }
            ],
            "ClientToken": null,
            "SubnetId": "subnet-6e7f829e",
            "InstanceType": "t2.micro",
            "NetworkInterfaces": [
                {
                    "Status": "in-use",
                    "SourceDestCheck": true,
                    "VpcId": "vpc-1a2b3c4d",
                    "Description": "Primary network interface",
                    "NetworkInterfaceId": "eni-a7edb1c9",
                    "PrivateIpAddresses": [
                        {
                            "PrivateDnsName": "ip-10-0-1-114.ec2.internal",
                            "Primary": true,
                            "PrivateIpAddress": "10.0.1.114"
```

```
                    }
                ],
                "PrivateDnsName": "ip-10-0-1-114.ec2.internal",
                "Attachment": {
                    "Status": "attached",
                    "DeviceIndex": 0,
                    "DeleteOnTermination": true,
                    "AttachmentId": "eni-attach-52193138",
                    "AttachTime": "2013-07-19T02:42:39.000Z"
                },
                "Groups": [
                    {
                        "GroupName": "my-sg",
                        "GroupId": "sg-903004f8"
                    }
                ],
                "SubnetId": "subnet-6e7f829e",
                "OwnerId": "123456789012",
                "PrivateIpAddress": "10.0.1.114"
            }
        ],
        "SourceDestCheck": true,
        "Placement": {
            "Tenancy": "default",
            "GroupName": null,
            "AvailabilityZone": "us-west-2b"
        },
        "Hypervisor": "xen",
        "BlockDeviceMappings": [
            {
                "DeviceName": "/dev/sda1",
                "Ebs": {
                    "Status": "attached",
                    "DeleteOnTermination": true,
                    "VolumeId": "vol-877166c8",
                    "AttachTime": "2013-07-19T02:42:39.000Z"
                }
            }
        ],
        "Architecture": "x86_64",
        "StateReason": {
            "Message": "pending",
            "Code": "pending"
        },
```

```
            "RootDeviceName": "/dev/sda1",
            "VirtualizationType": "hvm",
            "RootDeviceType": "ebs",
            "Tags": [
                {
                    "Value": "MyInstance",
                    "Key": "Name"
                }
            ],
            "AmiLaunchIndex": 0
        }
    ]
}
```

Agregar un dispositivo de bloques a la instancia

Cada instancia que lance tiene un volumen de dispositivo raíz asociado. Puede utilizar la asignación de dispositivos de bloques para especificar los volúmenes adicionales de Amazon Elastic Block Store (Amazon EBS) o los volúmenes de almacén de instancias que desea asociar a una instancia en el momento de lanzarla.

Para añadir un dispositivo de bloque a la instancia, especifique la opción `--block-device-mappings` cuando utilice `run-instances`.

El siguiente parámetro de ejemplo aprovisiona un volumen estándar de Amazon EBS con un tamaño de 20 GB y lo asigna a su instancia con el identificador `/dev/sdf`.

```
--block-device-mappings "[{\"DeviceName\":\"/dev/sdf\",\"Ebs\":{\"VolumeSize\":20,
\"DeleteOnTermination\":false}}]"
```

En el siguiente ejemplo se agrega un volumen de Amazon EBS, asignado a `/dev/sdf`, a partir de una instantánea existente. Una instantánea representa una imagen que se carga en el volumen por usted. Cuando se especifica una instantánea, no es necesario especificar un tamaño de volumen; será lo suficientemente grande como para almacenar la imagen. Sin embargo, si especifica un tamaño, este deberá ser igual o mayor que el tamaño de la instantánea.

```
--block-device-mappings "[{\"DeviceName\":\"/dev/sdf\",\"Ebs\":{\"SnapshotId\":\"snap-
a1b2c3d4\"}}]"
```

En el siguiente ejemplo se añaden dos volúmenes a la instancia. El número de volúmenes disponibles para su instancia depende del tipo de instancia.

```
--block-device-mappings "[{\"DeviceName\":\"/dev/sdf\",\"VirtualName\":\"ephemeral0\"},
{\"DeviceName\":\"/dev/sdg\",\"VirtualName\":\"ephemeral1\"}]"
```

En el siguiente ejemplo se crea el mapeo (`/dev/sdj`), pero no se aprovisiona un volumen para la instancia.

```
--block-device-mappings "[{\"DeviceName\":\"/dev/sdj\",\"NoDevice\":\"\"}]"
```

Para obtener más información, consulte Asignación de dispositivos de bloques en la Guía del usuario de Amazon EC2.

Agregar una etiqueta a la instancia

Una etiqueta es una marca que se asigna a un recurso de AWS. Le permite añadir metadatos a los recursos que puede utilizar para distintos fines. Para obtener más información, consulte Etiquetado de los recursos en la Guía del usuario de Amazon EC2.

En el siguiente ejemplo se muestra cómo añadir una etiqueta con el nombre de clave "`Name`" y el valor "`MyInstance`" a la instancia especificada, mediante el comando `aws ec2 create-tags`.

```
$ aws ec2 create-tags --resources i-5203422c --tags Key=Name,Value=MyInstance
```

Conéctese a su instancia

Puede conectarse a su instancia mientras se esté ejecutando y utilizarla como si fuera un equipo que tiene delante. Para obtener más información, consulte Conexión a la instancia de Amazon EC2 en la Guía del usuario de Amazon EC2.

Enumerar las instancias

Puede utilizar la AWS CLI para mostrar las instancias y ver información de las mismas. Puede incluir todas sus instancias en la lista o filtrar los resultados en función de las instancias que le interesen.

Los siguientes ejemplos muestran cómo utilizar el comando `aws ec2 describe-instances`.

El siguiente comando muestra todas sus instancias.

```
$ aws ec2 describe-instances
```

El siguiente comando filtra únicamente las instancias `t2.micro` de la lista y devuelve únicamente los valores `InstanceId` para cada coincidencia.

```
$ aws ec2 describe-instances --filters "Name=instance-type,Values=t2.micro" --query
 "Reservations[].Instances[].InstanceId"
[
    "i-05e998023d9c69f9a"
]
```

El siguiente comando muestra todas las instancias que tienen la etiqueta `Name=MyInstance`.

```
$ aws ec2 describe-instances --filters "Name=tag:Name,Values=MyInstance"
```

El siguiente comando muestra las instancias que tiene y que se iniciaron con cualquiera de las siguientes AMI: `ami-x0123456`, `ami-y0123456y` `ami-z0123456`.

```
$ aws ec2 describe-instances --filters "Name=image-id,Values=ami-x0123456,ami-
y0123456,ami-z0123456"
```

Eliminar la instancia

Puede usar la AWS CLI para terminar (eliminar) una instancia de Amazon EC2 cuando ya no la necesite.

> **Important**
>
> La terminación de una instancia es permanente e irreversible.
> Después de terminar una instancia, ya no podrá conectarse a esta ni recuperarla. Todos los volúmenes de Amazon EBS asociados que estén configurados para eliminarse en la terminación también se eliminan de manera permanente y no se pueden recuperar. Todos los datos almacenados en volúmenes de almacén de instancias se perderán de forma permanente. Para obtener más información, consulte Cómo funciona la terminación de instancias.
> Antes de terminar una instancia, asegúrese de haber realizado una copia de seguridad en un almacenamiento persistente de todos los datos que necesite retener después de la terminación.

En cuanto el estado de la instancia cambie a `shutting-down` o a `terminated`, dejará de incurrir en costos por ella. Si desea volver a conectarse a una instancia más adelante, utilice stop-instances en lugar de `terminate-instances`. Para obtener más información, consulte Finalizar una instancia en la Guía del usuario de Amazon EC2.

En el ejemplo siguiente, se muestra cómo eliminar una instancia mediante el comando aws ec2 terminate-instances.

```
$ aws ec2 terminate-instances --instance-ids i-5203422c
{
    "TerminatingInstances": [
        {
            "InstanceId": "i-5203422c",
            "CurrentState": {
                "Code": 32,
                "Name": "shutting-down"
            },
            "PreviousState": {
                "Code": 16,
                "Name": "running"
            }
        }
    ]
}
```

Referencias

AWS CLI referencia de:

- aws ec2
- aws ec2 create-tags
- aws ec2 describe-instances
- aws ec2 run-instances
- aws ec2 terminate-instances

Otra referencia:

- Documentación de Amazon Elastic Compute Cloud
- Para ver y contribuir al SDK de AWS y los ejemplos de código de AWS CLI, consulte el Repositorio de ejemplos de código de AWS en GitHub.

Cambio de un tipo de instancia de Amazon EC2 con un script de Bash en la AWS CLI

Este ejemplo de scripting de Bash para Amazon EC2 cambia el tipo de instancia de una instancia de Amazon EC2 con el método AWS Command Line Interface (AWS CLI). Detiene la instancia si se está ejecutando, cambia el tipo de instancia y, a continuación, si se solicita, reinicia la instancia. Los scripts de shell son programas diseñados para ejecutarse en una interfaz de línea de comandos.

> **Note**
>
> Para ver ejemplos de comandos adicionales, consulte la AWS CLIguía de referencia de .

Temas

- Antes de comenzar
- Acerca de este ejemplo
- Parámetros
- Archivos
- Referencias

Antes de comenzar

Antes de que pueda ejecutar cualquiera de los siguientes ejemplos, se debe completar lo siguiente.

- Instalar y configurar la AWS CLI. Para obtener más información, consulte the section called “Instalar o actualizar” y Credenciales de autenticación y acceso para la AWS CLI.
- El perfil que utilice debe tener permisos que permitan que se realicen las operaciones de la AWS mediante ejemplos.
- Una instancia de Amazon EC2 en ejecución en la cuenta para la que tiene permiso para detener y modificar. Si ejecuta el script de prueba, inicia una instancia, prueba el cambio del tipo y, a continuación, termina la instancia.
- Como práctica recomendada de AWS, conceda privilegios mínimos a este código o solo los permisos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegios mínimos en la Guía del usuario de AWS Identity and Access Management (IAM).
- Este código no ha sido probado en todas las regiones de AWS. Algunos servicios de AWS solo están disponibles en regiones específicas. Para obtener más información, consulte Puntos de enlace de servicio y cuotas en la Guía de referencia general de AWS.

- La ejecución de este código puede resultar en cargos en su cuenta de AWS. Es su responsabilidad asegurarse de que los recursos creados por este script se eliminen cuando haya terminado con ellos.

Acerca de este ejemplo

Este ejemplo se escribe como una función en el archivo de script de shell `change_ec2_instance_type.sh` que puede `source` desde otro script o desde la línea de comandos. Cada archivo de script contiene comentarios que describen cada una de las funciones. Una vez la función esté en la memoria, puede invocarla desde la línea de comandos. Por ejemplo, los siguientes comandos cambian el tipo de instancia especificada a `t2.nano`:

```
$ source ./change_ec2_instance_type.sh
$ ./change_ec2_instance_type -i *instance-id* -t new-type
```

Para obtener el ejemplo completo y los archivos de script descargables, consulte el Cambio del tipo de instancia de Amazon EC2 en AWS Ejemplos de código en GitHub.

Parámetros

-i-(string) Especifica el ID de instancia que se va a modificar.

-t-(string)Especifica el tipo de instancia de Amazon EC2 al que se va a cambiar.

-r-(switch) De forma predeterminada, no se establece. Si se configura `-r`, reinicia la instancia después del modificador de tipo.

-f-(switch) De forma predeterminada, el script solicita al usuario que confirme el cierre de la instancia antes de realizar el cambio. Si se configura `-f`, la función no le pide al usuario antes de apagar la instancia para hacer el cambio de tipo

-v-(switch) De forma predeterminada, el script funciona silenciosamente y muestra la salida solo en caso de error. Si se configura `-v`, la función muestra el estado a lo largo de su operación.

Archivos

`change_ec2_instance_type.sh`

El archivo de script principal contiene la función `change_ec2_instance_type()` que realiza las siguientes tareas:

- Comprueba que existe la instancia de Amazon EC2 especificada.

- A menos que se seleccione `-f`, advierte al usuario antes de detener la instancia.
- Cambia el tipo de instancia
- Si configura `-r`, reinicia la instancia y confirma que la instancia se está ejecutando

Ver el código de `change_ec2_instance_type.sh` en GitHub.

`test_change_ec2_instance_type.sh`

El script del archivo `test_change_ec2_instance_type.sh` prueba las diversas rutas de código para la función de `change_ec2_instance_type`. Si todos los pasos del script de prueba funcionan correctamente, este elimina todos los recursos que ha creado.

Puede ejecutar el script de prueba con los siguientes parámetros:

- -v-(switch)Cada prueba muestra un estado de superación/fallo a medida que se ejecutan. De forma predeterminada, las pruebas se ejecutan silenciosamente y la salida incluye solo el estado final de aprobado o error.
- -i-(switch) El script se detiene después de cada prueba para permitirle examinar los resultados intermedios de cada paso. Le permite examinar el estado actual de la instancia mediante la consola de Amazon EC2. El script pasa al siguiente paso después de presionar ENTER (INTRO) en el símbolo del sistema.

Ver el código de `test_change_ec2_instance_type.sh` en GitHub.

`awsdocs_general.sh`

El archivo de script `awsdocs_general.sh` contiene funciones de uso general utilizadas en ejemplos avanzados para el AWS CLI.

Ver el código de `awsdocs_general.sh` en GitHub.

Referencias

referencia de AWS CLI:

- `aws ec2`
- `aws ec2 describe-instances`
- `aws ec2 modify-instance-attribute`

- `aws ec2 start-instances`
- `aws ec2 stop-instances`
- `aws ec2 wait instance-running`
- `aws ec2 wait instance-stopped`

Otra referencia:

- Documentación de Amazon Elastic Compute Cloud
- Para ver y contribuir al SDK de AWS y los ejemplos de código de AWS CLI, consulte el Repositorio de ejemplos de código de AWS en GitHub.

Uso de Amazon Glacier en la AWS CLI

Introducción a Amazon Glacier
Introducción a Amazon Glacier

En este tema se muestran ejemplos de los comandos de la AWS CLI que realizan tareas comunes para Amazon Glacier. En los ejemplos se muestra cómo utilizar la AWS CLI para cargar un archivo de gran tamaño en Amazon Glacier dividiéndolo en partes más pequeñas y cargándolas desde la línea de comandos.

Puede acceder a las características de Amazon Glacier con la AWS Command Line Interface (AWS CLI). Para mostrar los comandos de la AWS CLI para Amazon Glacier, utilice el siguiente comando.

```
aws glacier help
```

> **Note**
>
> Para obtener más ejemplos de referencia de comandos y ver otros ejemplos, consulte `aws glacier` en la Referencia de comandos de AWS CLI.

Temas

- Requisitos previos

- Creación de un almacén de Amazon Glacier
- Preparación de un archivo para cargarlo
- Inicio de una carga multiparte y carga de archivos
- Finalización de la carga
- Recursos

Requisitos previos

Para ejecutar los comandos de `glacier`, debe:

- Instalar y configurar la AWS CLI. Para obtener más información, consulte the section called "Instalar o actualizar", y Credenciales de autenticación y acceso para la AWS CLI.
- Este tutorial utiliza varias herramientas de línea de comandos que normalmente vienen preinstaladas en los sistemas operativos tipo Unix, como Linux y macOS. Los usuarios de Windows pueden usar las mismas herramientas instalando Cygwin y ejecutando los comandos desde el terminal de Cygwin. Se indicará en cada caso si hay disponibles utilidades y comandos nativos de Windows que realicen las mismas funciones.

Creación de un almacén de Amazon Glacier

Cree un almacén con el comando `create-vault`.

```
$ aws glacier create-vault --account-id - --vault-name myvault
{
    "location": "/123456789012/vaults/myvault"
}
```

> **Note**
>
> Todos los comandos de Amazon Glacier requieren un parámetro de ID de cuenta. Utilice el carácter de guion (`--account-id -`) para utilizar la cuenta actual.

Preparación de un archivo para cargarlo

Cree un archivo para la carga de prueba. Los comandos siguientes crean un archivo llamado *`largefile`* que contiene exactamente 3 MiB de datos aleatorios.

Linux o macOS

```
$ dd if=/dev/urandom of=largefile bs=3145728 count=1
1+0 records in
1+0 records out
3145728 bytes (3.1 MB) copied, 0.205813 s, 15.3 MB/s
```

dd es una utilidad que copia un número de bytes de un archivo de entrada en un archivo de salida. En el ejemplo anterior se usa el archivo de dispositivo de sistema `/dev/urandom` como origen de datos aleatorios. `fsutil` realiza una función similar en Windows.

Windows

```
C:\> fsutil file createnew largefile 3145728
File C:\temp\largefile is created
```

A continuación, divida el archivo en fragmentos de 1 MiB (1 048 576 bytes) con un divisor de archivos.

```
$ split -b 1048576 --verbose largefile chunk
creating file `chunkaa'
creating file `chunkab'
creating file `chunkac'
```

Inicio de una carga multiparte y carga de archivos

Cree una carga multiparte en Amazon Glacier con el comando `initiate-multipart-upload`.

```
$ aws glacier initiate-multipart-upload --account-id - --archive-description "multipart
 upload test" --part-size 1048576 --vault-name myvault
{
    "uploadId": "19gaRezEXAMPLES6Ry5YYdqthHOC_kGRCT03L9yetr220UmPtBYKk-
OssZtLqyFu7sY1_lR7vgFuJV6NtcV5zpsJ",
    "location": "/123456789012/vaults/myvault/multipart-
uploads/19gaRezEXAMPLES6Ry5YYdqthHOC_kGRCT03L9yetr220UmPtBYKk-
OssZtLqyFu7sY1_lR7vgFuJV6NtcV5zpsJ"
}
```

Amazon Glacier requiere especificar el tamaño de cada parte en bytes (1 MiB en este ejemplo), el nombre del almacén y el ID de cuenta para configurar la carga multiparte. La AWS CLI genera un

ID de carga al completarse la operación. Guarde el ID de carga en una variable de shell para su uso posterior.

Linux o macOS

```
$ UPLOADID="19gaRezEXAMPLES6Ry5YYdqthHOC_kGRCT03L9yetr220UmPtBYKk-
OssZtLqyFu7sY1_lR7vgFuJV6NtcV5zpsJ"
```

Windows

```
C:\> set UPLOADID="19gaRezEXAMPLES6Ry5YYdqthHOC_kGRCT03L9yetr220UmPtBYKk-
OssZtLqyFu7sY1_lR7vgFuJV6NtcV5zpsJ"
```

A continuación, use el comando upload-multipart-part para cargar cada una de las tres partes.

```
$ aws glacier upload-multipart-part --upload-id $UPLOADID --body chunkaa --range 'bytes
 0-1048575/*' --account-id - --vault-name myvault
{
    "checksum": "e1f2a7cd6e047fa606fe2f0280350f69b9f8cfa602097a9a026360a7edc1f553"
}
$ aws glacier upload-multipart-part --upload-id $UPLOADID --body chunkab --range 'bytes
 1048576-2097151/*' --account-id - --vault-name myvault
{
    "checksum": "e1f2a7cd6e047fa606fe2f0280350f69b9f8cfa602097a9a026360a7edc1f553"
}
$ aws glacier upload-multipart-part --upload-id $UPLOADID --body chunkac --range 'bytes
 2097152-3145727/*' --account-id - --vault-name myvault
{
    "checksum": "e1f2a7cd6e047fa606fe2f0280350f69b9f8cfa602097a9a026360a7edc1f553"
}
```

> **Note**
>
> En el ejemplo anterior se usa el signo de dólar ($) para hacer referencia al contenido de la variable de shell UPLOADID en Linux. En la línea de comandos de Windows, inserte un signo de porcentaje (%) a ambos lados del nombre de la variable (por ejemplo, %UPLOADID%).

Debe especificar el intervalo de bytes de cada parte al cargarla, para que Amazon Glacier pueda volver a ensamblarlas en el orden adecuado. Cada parte tiene 1048576 bytes, por lo que la primera

ocupa los bytes del 0 al 1048575, la segunda del 1048576 al 2097151 y la tercera del 2097152 al 3145727.

Finalización de la carga

Amazon Glacier requiere un algoritmo hash en árbol del archivo original para poder confirmar que todas las partes cargadas llegan a AWS intactas.

Para calcular un algoritmo hash en árbol, divida el archivo en partes de 1 MiB y calcule un hash SHA-256 binario de cada fragmento. A continuación, divida la lista de hashes en pares, combine los dos hashes binarios de cada par y tome los hashes de los resultados. Repita este proceso hasta que solo quede un hash. Si hay un número impar de hashes en cualquier nivel, páselo al nivel siguiente sin modificarlo.

La clave para calcular un algoritmo hash en árbol correctamente al usar utilidades de línea de comandos es almacenar cada hash en formato binario y convertir a hexadecimal solamente en el último paso. Si la versión hexadecimal de cualquier hash del árbol se combina o se convierte a algoritmo hash, se obtendrá un resultado incorrecto.

> **Note**
>
> Los usuarios de Windows pueden utilizar el comando `type` en lugar de `cat`. OpenSSL está disponible para Windows en OpenSSL.org.

Para calcular un algoritmo hash en árbol

1. Divida el archivo original en partes de 1 MiB, si no lo ha hecho aún.

```
$ split --bytes=1048576 --verbose largefile chunk
creating file `chunkaa'
creating file `chunkab'
creating file `chunkac'
```

2. Calcule y almacene el hash SHA-256 binario de cada fragmento.

```
$ openssl dgst -sha256 -binary chunkaa > hash1
$ openssl dgst -sha256 -binary chunkab > hash2
$ openssl dgst -sha256 -binary chunkac > hash3
```

3. Combine los dos primeros hashes y tome el hash binario del resultado.

```
$ cat hash1 hash2 > hash12
$ openssl dgst -sha256 -binary hash12 > hash12hash
```

4. Combine el hash principal de los fragmentos `aa` y `ab` con el hash del fragmento `ac` y cree un hash del resultado, esta vez con formato hexadecimal. Almacene el resultado en una variable de shell.

```
$ cat hash12hash hash3 > hash123
$ openssl dgst -sha256 hash123
SHA256(hash123)= 9628195fcdbcbbe76cdde932d4646fa7de5f219fb39823836d81f0cc0e18aa67
$ TREEHASH=9628195fcdbcbbe76cdde932d4646fa7de5f219fb39823836d81f0cc0e18aa67
```

Por último, complete la carga con el comando `complete-multipart-upload`, que toma el tamaño del archivo original en bytes, el valor final del algoritmo hash en árbol en formato hexadecimal, su ID de cuenta y el nombre del almacén.

```
$ aws glacier complete-multipart-upload --checksum $TREEHASH --archive-size 3145728 --
upload-id $UPLOADID --account-id - --vault-name myvault
{
    "archiveId": "d3AbWhE0YE1m6f_fI1jPG82F8xzbMEEZmrAlLGAAONJAzo5QdP-
N83MKqd96Unspoa5H5lItWX-sK8-QS0ZhwsyGiu9-R-
kwWUyS1dSBlmgPPWkEbeFfqDSav053rU7FvVLHfRc6hg",
    "checksum": "9628195fcdbcbbe76cdde932d4646fa7de5f219fb39823836d81f0cc0e18aa67",
    "location": "/123456789012/vaults/myvault/archives/
d3AbWhE0YE1m6f_fI1jPG82F8xzbMEEZmrAlLGAAONJAzo5QdP-N83MKqd96Unspoa5H5lItWX-sK8-
QS0ZhwsyGiu9-R-kwWUyS1dSBlmgPPWkEbeFfqDSav053rU7FvVLHfRc6hg"
}
```

También puede comprobar el estado del almacén con el comando `describe-vault`.

```
$ aws glacier describe-vault --account-id - --vault-name myvault
{
    "SizeInBytes": 3178496,
    "VaultARN": "arn:aws:glacier:us-west-2:123456789012:vaults/myvault",
    "LastInventoryDate": "2018-12-07T00:26:19.028Z",
    "NumberOfArchives": 1,
    "CreationDate": "2018-12-06T21:23:45.708Z",
    "VaultName": "myvault"
}
```

> **Note**
>
> El estado del almacén se actualiza una vez al día. Consulte Trabajar con almacenes para obtener más información.

Ahora puede quitar sin problemas el fragmento y los archivos hash que ha creado.

```
$ rm chunk* hash*
```

Para obtener más información sobre las cargas multiparte, consulte Carga de archivos grandes por partes y Cálculo de sumas de comprobación en la Guía para desarrolladores de Amazon Glacier.

Recursos

AWS CLI referencia de:

- `aws glacier`
- `aws glacier complete-multipart-upload`
- `aws glacier create-vault`
- `aws glacier describe-vault`
- `aws glacier initiate-multipart-upload`

Referencia de servicio:

- Guía para desarrolladores de Amazon Glacier
- Carga de archivos grandes por partes en la Guía para desarrolladores de Amazon Glacier
- Cálculo de sumas de comprobación en la Guía para desarrolladores de Amazon Glacier
- Uso de almacenes en la Guía para desarrolladores de Amazon Glacier

Uso de IAM en la AWS CLI

Introducción a AWS Identity and Access Management
Introducción a AWS Identity and Access Management

Puede obtener acceso a las características de AWS Identity and Access Management (IAM) con la AWS Command Line Interface (AWS CLI). Para mostrar los comandos de la AWS CLI para IAM, utilice el siguiente comando.

```
aws iam help
```

En este tema se muestran ejemplos de comandos de la AWS CLI que realizan tareas comunes para IAM.

Antes de ejecutar los comandos, defina sus credenciales predeterminadas. Para obtener más información, consulte Configuración de los ajustes de AWS CLI.

Para obtener más información sobre el servicio IAM, consulte la Guía del usuario de AWS Identity and Access Management.

Temas

- Creación de un grupo y usuarios de IAM
- Asociación de una política administrada de IAM a un usuario
- Cómo establecer una contraseña inicial para un usuario de IAM
- Creación de una clave de acceso para un usuario de IAM

Creación de un grupo y usuarios de IAM

Para crear un grupo y añadirle un usuario

1. Utilice el comando `create-group` para crear el grupo.

```
$ aws iam create-group --group-name MyIamGroup
{
    "Group": {
        "GroupName": "MyIamGroup",
        "CreateDate": "2018-12-14T03:03:52.834Z",
        "GroupId": "AGPAJNUJ2W4IJVEXAMPLE",
        "Arn": "arn:aws:iam::123456789012:group/MyIamGroup",
        "Path": "/"
    }
}
```

2. Use el comando `create-user` para crear el usuario.

```
$ aws iam create-user --user-name MyUser
{
    "User": {
        "UserName": "MyUser",
        "Path": "/",
        "CreateDate": "2018-12-14T03:13:02.581Z",
        "UserId": "AIDAJY2PE5XUZ4EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:user/MyUser"
    }
}
```

3. Use el comando add-user-to-group para agregar el usuario al grupo.

```
$ aws iam add-user-to-group --user-name MyUser --group-name MyIamGroup
```

4. Para verificar que el grupo `MyIamGroup` contiene `MyUser`, use el comando get-group.

```
$ aws iam get-group --group-name MyIamGroup
{
    "Group": {
        "GroupName": "MyIamGroup",
        "CreateDate": "2018-12-14T03:03:52Z",
        "GroupId": "AGPAJNUJ2W4IJVEXAMPLE",
        "Arn": "arn:aws:iam::123456789012:group/MyIamGroup",
        "Path": "/"
    },
    "Users": [
        {
            "UserName": "MyUser",
            "Path": "/",
            "CreateDate": "2018-12-14T03:13:02Z",
            "UserId": "AIDAJY2PE5XUZ4EXAMPLE",
            "Arn": "arn:aws:iam::123456789012:user/MyUser"
        }
    ],
    "IsTruncated": "false"
}
```

Asociación de una política administrada de IAM a un usuario

La política de este ejemplo ofrece al usuario "Power User Access" (acceso avanzado).

Para asociar una política administrada de IAM a un usuario

1. Determine el nombre de recurso de Amazon (ARN) de la política que desea asociar. El siguiente comando usa `list-policies` para buscar el ARN de la política con el nombre `PowerUserAccess`. A continuación, almacena dicho ARN en una variable de entorno.

```
$ export POLICYARN=$(aws iam list-policies --query 'Policies[?
PolicyName==`PowerUserAccess`].{ARN:Arn}' --output text)      ~
$ echo $POLICYARN
arn:aws:iam::aws:policy/PowerUserAccess
```

2. Para adjuntar la política, utilice el comando `attach-user-policy` y haga referencia a la variable de entorno que contiene el ARN de política.

```
$ aws iam attach-user-policy --user-name MyUser --policy-arn $POLICYARN
```

3. Verifique que la política se ha adjuntado al usuario ejecutando el comando `list-attached-user-policies`.

```
$ aws iam list-attached-user-policies --user-name MyUser
{
    "AttachedPolicies": [
        {
            "PolicyName": "PowerUserAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/PowerUserAccess"
        }
    ]
}
```

Para obtener más información, consulte Recursos de administración de acceso. Este tema incluye vínculos a información general sobre permisos y políticas, además de vínculos a ejemplos de políticas para obtener acceso a Amazon S3, Amazon EC2 y otros servicios.

Cómo establecer una contraseña inicial para un usuario de IAM

El comando siguiente utiliza `create-login-profile` para configurar una contraseña inicial en el usuario especificado. Cuando el usuario inicia sesión por primera vez, se le solicitará que cambie la contraseña y elija una que solo él conozca.

```
$ aws iam create-login-profile --user-name MyUser --password My!User1Login8P@ssword --
password-reset-required
{
    "LoginProfile": {
        "UserName": "MyUser",
        "CreateDate": "2018-12-14T17:27:18Z",
        "PasswordResetRequired": true
    }
}
```

Puede usar el comando `update-login-profile` para cambiar la contraseña de un usuario.

```
$ aws iam update-login-profile --user-name MyUser --password My!User1ADifferentP@ssword
```

Creación de una clave de acceso para un usuario de IAM

Puede utilizar el comando `create-access-key` para crear una clave de acceso para un usuario. Una clave de acceso es un conjunto de credenciales de seguridad que se compone de un ID de clave de acceso y una clave secreta.

Un usuario solo puede crear dos claves de acceso al mismo tiempo. Si intenta crear un tercer conjunto, el comando devuelve un error `LimitExceeded`.

```
$ aws iam create-access-key --user-name MyUser
{
    "AccessKey": {
        "UserName": "MyUser",
        "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "Status": "Active",
        "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
        "CreateDate": "2018-12-14T17:34:16Z"
    }
}
```

Utilice el comando `delete-access-key` para eliminar una clave de acceso para un usuario. Especifique la clave de acceso que quiera eliminar mediante el ID de clave de acceso.

```
$ aws iam delete-access-key --user-name MyUser --access-key-id AKIAIOSFODNN7EXAMPLE
```

Uso de Amazon S3 en la AWS CLI

Una introducción a Amazon Simple Storage Service (Amazon S3)

Introducción a Amazon Simple Storage Service (Amazon S3): almacenamiento en la nube en AWS

Para obtener acceso a las características de Amazon Simple Storage Service (Amazon S3), utilice la AWS Command Line Interface (AWS CLI). Amazon S3 es un servicio de almacenamiento de objetos altamente escalable y duradero. Amazon S3 está diseñado para ofrecer una capacidad de almacenamiento prácticamente ilimitada, lo que lo convierte en una solución ideal para una amplia gama de necesidades de almacenamiento y administración de datos.

Amazon S3 permite almacenar y recuperar cualquier cantidad de datos en forma de objetos, desde archivos pequeños hasta conjuntos de datos de gran tamaño. Cada objeto se almacena en un contenedor denominado bucket, al que se puede acceder y que se puede administrar mediante la Consola de administración de AWS o programáticamente mediante los AWS SDK, las herramientas y la AWS CLI.

Amazon S3, con almacenamiento básico, también ofrece una gama de características que incluyen la administración del ciclo de vida, el control de versiones, la escalabilidad y la seguridad. Se integran con otros Servicios de AWS, lo que le permite crear soluciones basadas en la nube que se adapten a sus necesidades.

La AWS CLI ofrece dos niveles de comandos para obtener acceso a Amazon S3:

- s3: comandos de alto nivel personalizados, creados específicamente para AWS CLI, que simplifican la realización de tareas comunes, como crear, manipular, eliminar y sincronizar objetos y buckets.
- s3api: expone el acceso directo a todas las operaciones de la API de Simple Storage Service (Amazon S3), lo que le permite llevar a cabo operaciones avanzadas.

Temas de esta guía:

- Uso de comandos de alto nivel (s3) en la AWS CLI
- Uso de comandos de nivel de API (s3api) en la AWS CLI
- Ejemplo de scripts para el ciclo de vida para un bucket de Amazon S3 en la AWS CLI

Uso de comandos de alto nivel (s3) en la AWS CLI

En este tema se describe alguno de los comandos que puede utilizar para administrar los buckets y los objetos de Amazon S3 mediante comandos `aws s3` en la AWS CLI. Para ver los comandos que no se tratan en este tema y ejemplos de comandos adicionales, consulte los comandos `aws s3` en la Referencia de la AWS CLI.

Los comandos de `aws s3` de alto nivel simplifican la administración de objetos de Amazon S3. Estos comandos le permiten administrar el contenido de Amazon S3 dentro de sí mismo y con directorios locales.

Temas

- Requisitos previos
- Antes de comenzar
- Crear un bucket
- Lista de buckets y objetos
- Eliminar buckets
- Eliminar objetos
- Mover objetos
- Copia de objetos
- Sincronización de objetos
- Opciones utilizadas con frecuencia para los comandos s3
- Recursos

Requisitos previos

Para ejecutar los comandos de `s3`, debe:

- Instalar y configurar la AWS CLI. Para obtener más información, consulte the section called “Instalar o actualizar”, y Credenciales de autenticación y acceso para la AWS CLI.
- El perfil que utilice debe tener permisos que permitan las operaciones que AWS realizó por los ejemplos.
- Comprenda estos términos de Amazon S3:
  - Bucket: una carpeta de Amazon S3 de nivel superior.
  - Prefijo: una carpeta de Amazon S3 en un bucket.

- Objeto: cualquier artículo alojado en un bucket de Amazon S3.

Antes de comenzar

En esta sección se describen algunas cosas que hay que tener en cuenta antes de utilizar los comandos de `aws s3`.

Cargas de objetos grandes

Cuando utiliza comandos `aws s3` para cargar objetos grandes en un bucket de Amazon S3, la AWS CLI automáticamente realiza una carga multiparte. Los errores de carga no pueden reanudarse cuando se usan estos comandos de `aws s3`.

Si la carga multiparte falla debido a que se agota el tiempo de espera, o si canceló en forma manual en la AWS CLI, la AWS CLI detiene la carga y limpia los archivos que se han creado. Este proceso puede tardar varios minutos.

Si el proceso de carga o limpieza multiparte se cancela por un comando de cierre o un error del sistema, los archivos creados permanecen en el bucket de Amazon S3. Para limpiar la carga multiparte, utilice el comando s3api abort-multipart-upload.

Propiedades de archivo y etiquetas en copias multiparte

Cuando se utiliza la versión 1 de la AWS CLI de comandos en el espacio de nombres de `aws s3` para copiar un archivo de una ubicación de bucket de Amazon S3 a otra ubicación de bucket de Amazon S3, y esa operación utiliza la copia multiparte, no se copian propiedades de archivo del objeto fuente en el objeto de destino.

De forma predeterminada, los comandos de la versión 2 de la AWS CLI del espacio de nombres de `s3` que realizan copias multiparte transfieren todas las etiquetas y el siguiente conjunto de propiedades del origen a la copia de destino: `content-type`, `content-language`, `content-encoding`, `content-disposition`, `cache-control`, `expires` y `metadata`.

Esto puede dar lugar a llamadas de la API de AWS adicionales al punto de enlace de Amazon S3 que no se habrían realizado si hubiera utilizado la versión 1 de la AWS CLI. Estos pueden incluir: `HeadObject`, `GetObjectTagging` y `PutObjectTagging`.

Si necesita cambiar este comportamiento predeterminado en los comandos de la versión 2 de la AWS CLI, utilice el parámetro `--copy-props` para especificar una de las siguientes opciones:

- predeterminada: el valor predeterminado. Especifica que la copia incluye todas las etiquetas asociadas al objeto de origen y las propiedades abarcadas por el parámetro `--metadata-directive` utilizado para copias no multiparte: `content-type`, `content-language`, `content-encoding`, `content-disposition`, `cache-control`, `expires` y `metadata`.
- directiva de metadatos: especifica que la copia incluye solo las propiedades abarcadas por el parámetro `--metadata-directive` utilizado para copias no multiparte. No copia ninguna etiqueta.
- ninguno: especifica que la copia no incluye ninguna de las propiedades del objeto fuente.

Crear un bucket

Utilice el comando `s3 mb` para crear un bucket. Los nombres de los buckets deben ser globalmente únicos (únicos en todo Amazon S3) y deben ser compatibles con DNS.

Los nombres de los buckets pueden contener minúsculas, números, guiones y puntos. Los nombres de los buckets solo pueden empezar y terminar con una letra o número, y no pueden contener un punto junto a un guion u otro punto.

Sintaxis

```
$ aws s3 mb <target> [--options]
```

Ejemplos de s3 mb

En el siguiente ejemplo se crea el bucket `s3://amzn-s3-demo-bucket`.

```
$ aws s3 mb s3://amzn-s3-demo-bucket
```

Lista de buckets y objetos

Para mostrar los buckets, carpetas u objetos, utilice el comando `s3 ls`. El uso del comando sin destino u opciones muestra todos los buckets.

Sintaxis

```
$ aws s3 ls <target> [--options]
```

Para ver algunas opciones comunes que se pueden utilizar con este comando y ejemplos, consulte Opciones utilizadas con frecuencia para los comandos s3. Para ver una lista completa de las opciones disponibles, consulte `s3 ls` en la Referencia de comandos de AWS CLI.

Ejemplos de s3 ls

En el siguiente ejemplo se enumeran todos los buckets de Amazon S3.

```
$ aws s3 ls
2018-12-11 17:08:50 amzn-s3-demo-bucket1
2018-12-14 14:55:44 amzn-s3-demo-bucket2
```

El siguiente comando muestra todos los objetos y prefijos de un bucket. En este resultado de ejemplo, el prefijo `example/` tiene un archivo llamado `MyFile1.txt`.

```
$ aws s3 ls s3://amzn-s3-demo-bucket
                           PRE example/
2018-12-04 19:05:48          3 MyFile1.txt
```

Para filtrar la salida por un prefijo específico, inclúyalo en el comando. El siguiente comando muestra los objetos en *`bucket-name/example/`* (es decir, los objetos que estén en *`bucket-name`* filtrados por el prefijo *`example/`*).

```
$ aws s3 ls s3://amzn-s3-demo-bucket/example/
2018-12-06 18:59:32          3 MyFile1.txt
```

Para mostrar solo los buckets y los objetos de una región específica, use las opciones de `--region`

```
$ aws s3 ls --region us-east-2
2018-12-06 18:59:32          3 MyFile1.txt
```

Si tiene una lista grande de buckets y objetos, puede paginar los resultados con las opciones `--max-items` o `--page-size`. La opción `--max-items` limita el número total de buckets y objetos que se devuelven en una llamada y la opción `--page-size` limita el número de objetos que se muestran en una página.

```
$ aws s3 ls --max-items 100 --page-size 10
```

Para obtener más información sobre paginación, consulte the section called “--page-size” y the section called “--max-items”.

Eliminar buckets

Para eliminar un bucket, utilice el comando `s3 rb`.

Sintaxis

```
$ aws s3 rb <target> [--options]
```

Ejemplos de s3 rb

En el siguiente ejemplo se quita el bucket `s3://amzn-s3-demo-bucket`.

```
$ aws s3 rb s3://amzn-s3-demo-bucket
```

De forma predeterminada, el bucket debe estar vacío para que la operación se realice correctamente. Para eliminar un bucket que no esté vacío, debe incluir la opción `--force`. Si utiliza un bucket versionado que contenga objetos eliminados previamente, pero que se conservan, este comando no le permitirá eliminar el bucket. En primer lugar, debe eliminar todo el contenido.

El siguiente ejemplo elimina todos los objetos y los prefijos en el bucket, luego elimina el bucket.

```
$ aws s3 rb s3://amzn-s3-demo-bucket --force
```

Eliminar objetos

Para eliminar objetos en un bucket o en el directorio local, utilice el comando `s3 rm`.

Sintaxis

```
$ aws s3 rm  <target> [--options]
```

Para ver algunas opciones comunes que se pueden utilizar con este comando y ejemplos, consulte Opciones utilizadas con frecuencia para los comandos s3. Para ver una lista completa de opciones, consulte `s3 rm` en la Referencia de comandos de AWS CLI.

Ejemplos de s3 rm

En el siguiente ejemplo se elimina `filename.txt` de `s3://amzn-s3-demo-bucket/example`.

```
$ aws s3 rm s3://amzn-s3-demo-bucket/example/filename.txt
```

En el siguiente ejemplo se eliminan todos los objetos de `s3://amzn-s3-demo-bucket/example` utilizando la opción `--recursive`.

```
$ aws s3 rm s3://amzn-s3-demo-bucket/example --recursive
```

Mover objetos

Use el comando `s3 mv` para mover objetos de un bucket o un directorio local. El comando `s3 mv` copia el objeto de origen o el archivo de origen en el destino especificado y, a continuación, elimina dicho objeto o archivo.

Sintaxis

```
$ aws s3 mv <source> <target> [--options]
```

Para ver algunas opciones comunes que se pueden utilizar con este comando y ejemplos, consulte Opciones utilizadas con frecuencia para los comandos s3. Para ver una lista completa de las opciones disponibles, consulte `s3 mv` en la Referencia de comandos de AWS CLI.

> **Warning**
>
> Si utiliza algún tipo de ARN de punto de acceso o alias de punto de acceso en las URI de origen o destino de Amazon S3, debe prestar especial atención a que los URI de Amazon S3 de origen y destino se resuelvan en diferentes buckets subyacentes. Si los buckets de origen y destino son los mismos, el archivo u objeto de origen se puede mover sobre sí mismo, lo que puede provocar la eliminación accidental dicho archivo u objeto. Para comprobar que los buckets de origen y destino no son los mismos, utilice el parámetro `--validate-same-s3-paths` o defina la variable de entorno `AWS_CLI_S3_MV_VALIDATE_SAME_S3_PATHS` en `true`.

Ejemplos de s3 mv

En el siguiente ejemplo se mueven todos los objetos de `s3://amzn-s3-demo-bucket/example` a `s3://amzn-s3-demo-bucket/`.

```
$ aws s3 mv s3://amzn-s3-demo-bucket/example s3://amzn-s3-demo-bucket/
```

En el siguiente ejemplo se mueve un archivo local del directorio de trabajo actual al bucket de Amazon S3 con el comando de `s3 mv`.

```
$ aws s3 mv filename.txt s3://amzn-s3-demo-bucket
```

En el siguiente ejemplo se mueve un archivo del bucket de Amazon S3 a su directorio de trabajo actual, donde `./` especifica su directorio de trabajo actual.

```
$ aws s3 mv s3://amzn-s3-demo-bucket/filename.txt ./
```

Copia de objetos

Use el comando `s3 cp` para copiar objetos de un bucket o un directorio local.

Sintaxis

```
$ aws s3 cp <source> <target> [--options]
```

Puede usar el parámetro guión para el streaming de archivos a la entrada estándar (`stdin`) o salida estándar (`stdout`).

> **Warning**
>
> Si está utilizando PowerShell, el shell podría alterar la codificación de un CRLF o agregar un CRLF a la entrada o salida canalizada, o a la salida redirigida.

El comando `s3 cp` utiliza la siguiente sintaxis para cargar una secuencia de archivos desde `stdin` hasta un bucket especificado.

Sintaxis

```
$ aws s3 cp - <target> [--options]
```

El comando `s3 cp` utiliza la siguiente sintaxis para descargar una secuencia de archivos de Amazon S3 para `stdout`.

Sintaxis

```
$ aws s3 cp <target> [--options] -
```

Para ver algunas opciones comunes que se pueden utilizar con este comando y ejemplos, consulte Opciones utilizadas con frecuencia para los comandos s3. Para ver una lista completa de opciones, consulte `s3 cp` en la Referencia de comandos de AWS CLI.

`s3 cp`Ejemplos de

El siguiente ejemplo copia todos los registros de `s3://amzn-s3-demo-bucket/example` a `s3://amzn-s3-demo-bucket/`.

```
$ aws s3 cp s3://amzn-s3-demo-bucket/example s3://amzn-s3-demo-bucket/
```

En el siguiente ejemplo se copian un archivo local del directorio de trabajo actual en el bucket de Amazon S3 con el`s3 cp`comando.

```
$ aws s3 cp filename.txt s3://amzn-s3-demo-bucket
```

En el siguiente ejemplo se copia un archivo de su bucket de Amazon S3 en su directorio de trabajo actual, donde `./` especifica su directorio de trabajo actual.

```
$ aws s3 cp s3://amzn-s3-demo-bucket/filename.txt ./
```

En el siguiente ejemplo se utiliza la repetición para transmitir el texto “hola mundo” al archivo `s3://bucket-name/filename.txt`.

```
$ echo "hello world" | aws s3 cp - s3://amzn-s3-demo-bucket/filename.txt
```

En el ejemplo siguiente se transmite el archivo `s3://amzn-s3-demo-bucket/filename.txt` a `stdout` y se imprime el contenido en la consola.

```
$ aws s3 cp s3://amzn-s3-demo-bucket/filename.txt -
hello world
```

En el siguiente ejemplo se transmiten los contenidos de `s3://bucket-name/pre` a `stdout`, se utiliza el comando `bzip2` para comprimir los archivos y se carga el nuevo archivo comprimido llamado `key.bz2` a `s3://bucket-name`.

```
$ aws s3 cp s3://amzn-s3-demo-bucket/pre - | bzip2 --best | aws s3 cp - s3://amzn-s3-
demo-bucket/key.bz2
```

Sincronización de objetos

El comando `s3 sync` sincroniza el contenido de un bucket y un directorio o los contenidos de dos buckets. Normalmente, `s3 sync` copia archivos u objetos que estén desactualizados o que falten entre el origen y el destino. Sin embargo, también puede introducir la opción `--delete` para quitar archivos u objetos desde el destino que no se encuentran en el origen.

Sintaxis

```
$ aws s3 sync <source> <target> [--options]
```

Para ver algunas opciones comunes que se pueden utilizar con este comando y ejemplos, consulte Opciones utilizadas con frecuencia para los comandos s3. Para ver una lista completa de opciones, consulte `s3 sync` en la Referencia de comandos de AWS CLI.

Ejemplos de sincronización de s3

En el siguiente ejemplo se sincroniza el contenido de un prefijo Amazon S3 llamado ruta en el bucket denominado amzn-s3-demo-bucket con el directorio activo actual.

`s3 sync` actualiza los archivos que tengan un tamaño o tiempo de modificación diferente que los archivos con el mismo nombre en el destino. La salida muestra las operaciones específica realizadas durante la sincronización. Observe que la operación sincroniza de forma recursiva el subdirectorio `MySubdirectory` y su contenido con `s3://amzn-s3-demo-bucket/path/MySubdirectory`.

```
$ aws s3 sync . s3://amzn-s3-demo-bucket/path
upload: MySubdirectory\MyFile3.txt to s3://amzn-s3-demo-bucket/path/MySubdirectory/
MyFile3.txt
upload: MyFile2.txt to s3://amzn-s3-demo-bucket/path/MyFile2.txt
upload: MyFile1.txt to s3://amzn-s3-demo-bucket/path/MyFile1.txt
```

En el siguiente ejemplo, que amplía el anterior, se muestra cómo funciona la opción `--delete`.

```
// Delete local file
$ rm ./MyFile1.txt
```

```
// Attempt sync without --delete option - nothing happens
$ aws s3 sync . s3://amzn-s3-demo-bucket/path

// Sync with deletion - object is deleted from bucket
$ aws s3 sync . s3://amzn-s3-demo-bucket/path --delete
delete: s3://amzn-s3-demo-bucket/path/MyFile1.txt

// Delete object from bucket
$ aws s3 rm s3://amzn-s3-demo-bucket/path/MySubdirectory/MyFile3.txt
delete: s3://amzn-s3-demo-bucket/path/MySubdirectory/MyFile3.txt

// Sync with deletion - local file is deleted
$ aws s3 sync s3://amzn-s3-demo-bucket/path . --delete
delete: MySubdirectory\MyFile3.txt

// Sync with Infrequent Access storage class
$ aws s3 sync . s3://amzn-s3-demo-bucket/path --storage-class STANDARD_IA
```

Cuando se utiliza la opción `--delete`, las opciones `--exclude` y `--include` pueden filtrar archivos u objetos para eliminarlos durante una operación de `s3 sync`. En este caso, la cadena del parámetro debe especificar qué archivos se deben excluir o incluir en la eliminación, en el contexto del directorio o bucket de destino. A continuación se muestra un ejemplo.

```
Assume local directory and s3://amzn-s3-demo-bucket/path currently in sync and each
 contains 3 files:
MyFile1.txt
MyFile2.rtf
MyFile88.txt
'''

// Sync with delete, excluding files that match a pattern. MyFile88.txt is deleted,
 while remote MyFile1.txt is not.
$ aws s3 sync . s3://amzn-s3-demo-bucket/path --delete --exclude "path/MyFile?.txt"
delete: s3://amzn-s3-demo-bucket/path/MyFile88.txt
'''

// Sync with delete, excluding MyFile2.rtf - local file is NOT deleted
$ aws s3 sync s3://amzn-s3-demo-bucket/path . --delete --exclude "./MyFile2.rtf"
download: s3://amzn-s3-demo-bucket/path/MyFile1.txt to MyFile1.txt
'''

// Sync with delete, local copy of MyFile2.rtf is deleted
```

```
$ aws s3 sync s3://amzn-s3-demo-bucket/path . --delete
delete: MyFile2.rtf
```

Opciones utilizadas con frecuencia para los comandos s3

Las siguientes opciones se utilizan con frecuencia para los comandos descritos en este tema. Para obtener una lista completa de las opciones que puede utilizar en un comando, consulte el comando específico en la Guía de referencia de la AWS CLI versión 2.

acl

`s3 sync` y `s3 cp` pueden utilizar la opción `--acl`. Esto le permite configurar los permisos de acceso para archivos copiados en Amazon S3. La opción `--acl` admite los valores `private`, `public-read` y `public-read-write`. Para obtener más información, consulte ACL predefinidas en la Guía del usuario de Amazon S3.

```
$ aws s3 sync . s3://amzn-s3-demo-bucket/path --acl public-read
```

excluya

Cuando utiliza el comando `s3 cp`, `s3 mv`, `s3 sync` o `s3 rm`, puede filtrar los resultados mediante la opción `--exclude` o `--include`. La opción `--exclude` establece reglas para excluir únicamente objetos del comando y las opciones se aplican en el orden especificado. Esto se muestra en el siguiente ejemplo.

```
Local directory contains 3 files:
MyFile1.txt
MyFile2.rtf
MyFile88.txt

// Exclude all .txt files, resulting in only MyFile2.rtf being copied
$ aws s3 cp . s3://amzn-s3-demo-bucket/path --exclude "*.txt"

// Exclude all .txt files but include all files with the "MyFile*.txt" format,
 resulting in, MyFile1.txt, MyFile2.rtf, MyFile88.txt being copied
$ aws s3 cp . s3://amzn-s3-demo-bucket/path --exclude "*.txt" --include
 "MyFile*.txt"

// Exclude all .txt files, but include all files with the "MyFile*.txt" format,
 but exclude all files with the "MyFile?.txt" format resulting in, MyFile2.rtf and
 MyFile88.txt being copied
```

```
$ aws s3 cp . s3://amzn-s3-demo-bucket/path --exclude "*.txt" --include
 "MyFile*.txt" --exclude "MyFile?.txt"
```

incluir

Cuando utiliza el comando `s3 cp`, `s3 mv`, `s3 sync` o `s3 rm`, puede filtrar los resultados utilizando la opción `--exclude` o `--include`. La opción `--include` establece reglas para incluir únicamente objetos específicos para el comando y las opciones se aplican en el orden especificado. Esto se muestra en el siguiente ejemplo.

```
Local directory contains 3 files:
MyFile1.txt
MyFile2.rtf
MyFile88.txt

// Include all .txt files, resulting in MyFile1.txt and MyFile88.txt being copied
$ aws s3 cp . s3://amzn-s3-demo-bucket/path --include "*.txt"

// Include all .txt files but exclude all files with the "MyFile*.txt" format,
 resulting in no files being copied
$ aws s3 cp . s3://amzn-s3-demo-bucket/path --include "*.txt" --exclude
 "MyFile*.txt"

// Include all .txt files, but exclude all files with the "MyFile*.txt" format, but
 include all files with the "MyFile?.txt" format resulting in MyFile1.txt being
 copied

$ aws s3 cp . s3://amzn-s3-demo-bucket/path --include "*.txt" --exclude
 "MyFile*.txt" --include "MyFile?.txt"
```

concesión

Los comandos `s3 cp`, `s3 mv` y `s3 sync` incluyen una opción `--grants` que puede usar para conceder permisos sobre el objeto a usuarios o grupos específicos. Configure la opción `--grants` para obtener una lista de permisos mediante la siguiente sintaxis. Reemplace `Permission`, `Grantee_Type` y `Grantee_ID` por sus propios valores.

Sintaxis

```
--grants Permission=Grantee_Type=Grantee_ID
         [Permission=Grantee_Type=Grantee_ID ...]
```

Cada valor contiene los siguientes elementos:

- *Permiso*: especifica los permisos concedidos. Se puede establecer en `read`, `readacl`, `writeacl` o `full`.
- *Tipo de beneficiario*: especifica cómo identificar al beneficiario. Se puede establecer en `uri`, `emailaddress` o `id`.
- *Grantee_ID*: especifica el beneficiario del permiso según *Grantee_Type*.
  - `uri`: URI del grupo. Para obtener más información, consulte la sección ¿Quién es un beneficiario?
  - `emailaddress`: dirección de correo electrónico de la cuenta.
  - `id`: ID canónico de la cuenta.

Para obtener más información acerca de cómo controlar el acceso a Amazon S3, consulte la sección de Control de acceso.

En el siguiente ejemplo se copia un objeto en un bucket. Concede permisos `read` sobre el objeto a todos los usuarios y permisos `full` (`read`, `readacl` y `writeacl`) a la cuenta asociada con `user@example.com`.

```
$ aws s3 cp file.txt s3://amzn-s3-demo-bucket/ --grants read=uri=http://
acs.amazonaws.com/groups/global/AllUsers full=emailaddress=user@example.com
```

También puede especificar una clase de almacenamiento no predeterminada (`REDUCED_REDUNDANCY` o `STANDARD_IA`) para los objetos que se cargan en Amazon S3. Para ello, utilice la opción `--storage-class`.

```
$ aws s3 cp file.txt s3://amzn-s3-demo-bucket/ --storage-class REDUCED_REDUNDANCY
```

no-overwrite

Los comandos `s3 cp`, `s3 mv` y `s3 sync` incluyen una opción de `--no-overwrite` que puede utilizar para evitar que se sobrescriban los objetos que ya existen en el destino.

En el ejemplo siguiente, se copia un objeto de un bucket al directorio local solo si aún no existe en el directorio local.

```
$ aws s3 cp --no-overwrite s3://amzn-s3-demo-bucket/file.txt file.txt
```

En el ejemplo siguiente, se copian de forma recursiva archivos de un directorio local a un bucket. Solo copiará archivos que ya no existen en el bucket.

```
$ aws s3 cp --recursive --no-overwrite /path/to/demo-files/ s3://amzn-s3-demo-bucket/demo-files/
```

En el ejemplo siguiente, se mueve un objeto de un directorio local a un bucket solo si aún no existe en la ubicación de destino del bucket.

```
$ aws s3 mv --no-overwrite file.txt s3://amzn-s3-demo-bucket/file.txt
```

En el ejemplo siguiente, se sincronizan archivos de un directorio local a un bucket. Solo sincronizará archivos que ya no existen en el bucket de destino.

```
$ aws s3 sync --no-overwrite /path/to/demo-files/ s3://amzn-s3-demo-bucket/demo-files/
```

recursive

Cuando use esta opción, el comando se ejecuta en todos los objetos o archivos del directorio especificado o con el prefijo indicado. En el siguiente ejemplo se elimina `s3://amzn-s3-demo-bucket/path` y todos sus contenidos.

```
$ aws s3 rm s3://amzn-s3-demo-bucket/path --recursive
```

Recursos

AWS CLI referencia de:

- `aws s3`
- `aws s3 cp`
- `aws s3 mb`
- `aws s3 mv`
- `aws s3 ls`
- `aws s3 rb`
- `aws s3 rm`

- `aws s3 sync`

Referencia de servicio:

- Uso de buckets de Amazon S3 en la Guía del usuario de Amazon S3
- Uso de objetos de Amazon S3 en la Guía del usuario de Amazon S3
- Listado jerárquico de las claves con un prefijo y un delimitador en la Guía del usuario de Amazon S3
- Anulación de cargas multiparte a un bucket de S3 con AWS SDK para .NET (bajo nivel) en la Guía del usuario de Amazon S3

Uso de comandos de nivel de API (s3api) en la AWS CLI

Los comandos de nivel de API (incluidos en el conjunto de comandos de `s3api`) proporcionan acceso directo a las API de Amazon Simple Storage Service (Amazon S3) y permiten realizar algunas operaciones no expuestas en los comandos de `s3` de alto nivel. Estos comandos son el equivalente de los otros servicios de AWS que proporcionan acceso de nivel de API a la funcionalidad de los servicios. Para obtener más información acerca de los comandos `s3`, consulte Uso de comandos de alto nivel (s3) en la AWS CLI

En este tema, se incluyen ejemplos en los que se muestra cómo se usan los comandos de más bajo nivel que se asignan a las API de Amazon S3. Además, puede encontrar ejemplos para cada comando de API de S3 en la sección `s3api` de la Guía de referencia de la AWS CLI versión 2.

Temas

- Requisitos previos
- Aplicación de una ACL personalizada
- Configuración de una política de registro
- Recursos

Requisitos previos

Para ejecutar los comandos de `s3api`, debe:

- Instalar y configurar la AWS CLI. Para obtener más información, consulte the section called “Instalar o actualizar”, y Credenciales de autenticación y acceso para la AWS CLI.

- El perfil que utilice debe tener permisos que permitan las operaciones que AWS realizó por los ejemplos.
- Comprenda estos términos de Amazon S3:
  - Bucket: una carpeta de Amazon S3 de nivel superior.
  - Prefijo: una carpeta de Amazon S3 en un bucket.
  - Objeto: cualquier artículo alojado en un bucket de Amazon S3.

Aplicación de una ACL personalizada

Con los comandos de alto nivel, puede utilizar la opción `--acl` para aplicar las listas de control de acceso (ACL) predefinidas en objetos de Amazon S3. Sin embargo, no puede usar ese comando para establecer ACL en todo el bucket. Sin embargo, puede hacerlo con el comando por API `put-bucket-acl`.

En el siguiente ejemplo se muestra cómo conceder control total a dos usuarios de AWS (user1@example.com y user2@example.com) y permisos de lectura a todos los usuarios. El identificador para "everyone" (todos) proviene de un URI especial que se pasa como parámetro.

```
$ aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --grant-full-control
 'emailaddress="user1@example.com",emailaddress="user2@example.com"' --grant-read
 'uri="http://acs.amazonaws.com/groups/global/AllUsers"'
```

Para obtener más información acerca de cómo construir las ACL, consulte PUT Bucket acl en la Referencia de la API de Amazon Simple Storage Service. Los comandos ACL de `s3api` en la CLI, como `put-bucket-acl`, usan la misma notación abreviada de argumentos.

Configuración de una política de registro

El comando de la API `put-bucket-logging` configura una política de registro del bucket.

En el siguiente ejemplo, se concede al usuario de AWS user@example.com control total sobre los archivos de registro, y todos los usuarios tendrán acceso de lectura a ellos. Tenga en cuenta que el comando `put-bucket-acl` también es necesario para conceder al sistema de entrega de registros de Amazon S3 (especificado por un URI) los permisos necesarios para leer y escribir los registros en el bucket.

```
$ aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --grant-read-acp 'URI="http://
acs.amazonaws.com/groups/s3/LogDelivery"' --grant-write 'URI="http://acs.amazonaws.com/
groups/s3/LogDelivery"'
```

```
$ aws s3api put-bucket-logging --bucket amzn-s3-demo-bucket --bucket-logging-status
 file://logging.json
```

El archivo `logging.json` del comando anterior contiene lo siguiente.

```
{
  "LoggingEnabled": {
    "TargetBucket": "amzn-s3-demo-bucket",
    "TargetPrefix": "amzn-s3-demo-bucketLogs/",
    "TargetGrants": [
      {
        "Grantee": {
          "Type": "AmazonCustomerByEmail",
          "EmailAddress": "user@example.com"
        },
        "Permission": "FULL_CONTROL"
      },
      {
        "Grantee": {
          "Type": "Group",
          "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
        },
        "Permission": "READ"
      }
    ]
  }
}
```

Recursos

AWS CLI referencia de:

- aws s3api
- aws s3api put-bucket-acl
- aws s3api put-bucket-logging

Referencia de servicio:

- Uso de buckets de Amazon S3 en la Guía del usuario de Amazon S3
- Uso de objetos de Amazon S3 en la Guía del usuario de Amazon S3

- Listado jerárquico de las claves con un prefijo y un delimitador en la Guía del usuario de Amazon S3
- Anulación de cargas multiparte a un bucket de S3 con AWS SDK para .NET (bajo nivel) en la Guía del usuario de Amazon S3

Ejemplo de scripts para el ciclo de vida para un bucket de Amazon S3 en la AWS CLI

En este tema se utiliza un ejemplo de scripting de Bash para las operaciones del ciclo de vida del bucket de Amazon S3 mediante la AWS Command Line Interface (AWS CLI). En este ejemplo de scripting se utiliza el conjunto de comandos de `aws s3api`. Los scripts de shell son programas diseñados para ejecutarse en una interfaz de línea de comandos.

Temas

- Antes de comenzar
- Acerca de este ejemplo
- Archivos
- Referencias

Antes de comenzar

Antes de que pueda ejecutar cualquiera de los siguientes ejemplos, se debe completar lo siguiente.

- Instalar y configurar la AWS CLI. Para obtener más información, consulte the section called “Instalar o actualizar”, y Credenciales de autenticación y acceso para la AWS CLI.
- El perfil que utilice debe tener permisos que permitan las operaciones que AWS realizó por los ejemplos.

- Como práctica recomendada de AWS, conceda a este código privilegios mínimos o solo los permisos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Concesión de mínimos privilegios en la Guía del usuario de IAM.
- Este código no se ha probado en todas las regiones de AWS. Algunos servicios de AWS solo están disponibles en regiones específicas. Para obtener más información, consulte Puntos de enlace de servicio y cuotas en la Guía de referencia general de AWS.

- La ejecución de este código puede resultar en cargos en su cuenta de AWS. Es su responsabilidad asegurarse de que los recursos creados por este script se eliminen cuando haya terminado con ellos.

El servicio Amazon S3 utiliza los siguientes términos:

- Bucket: una carpeta de Amazon S3 de nivel superior.
- Prefijo: una carpeta de Amazon S3 en un bucket.
- Objeto: cualquier artículo alojado en un bucket de Amazon S3.

Acerca de este ejemplo

En este ejemplo se muestra cómo interactuar con algunas de las operaciones básicas de Amazon S3 mediante un conjunto de funciones en archivos de script de shell. Las funciones se encuentran en el archivo de script de shell llamado `bucket-operations.sh`. Puede llamar a estas funciones en otro archivo. Cada archivo de script contiene comentarios que describen cada una de las funciones.

Para ver los resultados intermedios de cada paso, ejecute el script con un parámetro `-i`. Para ver el estado actual del bucket o su contenido, puede usar la consola de Amazon S3. El scripting solo pasa al siguiente paso cuando se pulsa Enter (Intro) en el símbolo del sistema.

Para obtener el ejemplo completo y los archivos de script descargables, consulte Operaciones del ciclo de vida de bucket de Amazon S3 en el Repositorio de ejemplos de código deAWS en GitHub.

Archivos

El ejemplo contiene los siguientes archivos:

bucket-operations.sh

Este archivo de script principal puede obtenerse de otro archivo. Incluye funciones que realizan las siguientes tareas:

- Creación de un bucket y verificación de que existe
- Copia de un archivo desde el equipo local a un bucket
- Copia de un archivo desde una ubicación de bucket a otra ubicación de bucket
- Listado de contenidos de un bucket
- Eliminación a archivos desde un bucket

- Eliminar un bucket

Vea el código de `bucket-operations.sh` en GitHub.

test-bucket-operations.sh

El archivo de script de shell `test-bucket-operations.sh` muestra cómo llamar a las funciones mediante el suministro de archivo `bucket-operations.sh` y el llamando a cada una de las funciones. Después de llamar a las funciones, el script de prueba elimina todos los recursos que creó.

Vea el código de `test-bucket-operations.sh` en GitHub.

awsdocs-general.sh

El archivo de script `awsdocs-general.sh` contiene funciones de uso general utilizadas en ejemplos de código avanzados para la AWS CLI.

Vea el código de `awsdocs-general.sh` en GitHub.

Referencias

AWS CLI referencia de:

- `aws s3api`
- `aws s3api create-bucket`
- `aws s3api copy-object`
- `aws s3api delete-bucket`
- `aws s3api delete-object`
- `aws s3api head-bucket`
- `aws s3api list-objects`
- `aws s3api put-object`

Otra referencia:

- Uso de buckets de Amazon S3 en la Guía del usuario de Amazon S3

- Uso de objetos de Amazon S3 en la Guía del usuario de Amazon S3
- Para ver y contribuir al AWS SDK y los ejemplos de código de AWS CLI, consulte el Repositorio de ejemplos de código de AWS en GitHub.

Acceso a Amazon SNS en la AWS CLI

Puede acceder a las características de Amazon Simple Notification Service (Amazon SNS) a través de AWS Command Line Interface (AWS CLI). Para mostrar la lista de los comandos de AWS CLI para Amazon SNS, utilice el siguiente comando.

```
aws sns help
```

Antes de ejecutar los comandos, defina sus credenciales predeterminadas. Para obtener más información, consulte Configuración de los ajustes de AWS CLI.

En este tema se muestran ejemplos de comandos de la AWS CLI que realizan tareas comunes para Amazon SNS.

Temas

- Crear un tema
- Suscripción a un tema
- Publicar en un tema
- Cancelación de la suscripción a un tema
- Eliminación de un tema

Crear un tema

Para crear un tema, utilice el comando `sns create-topic` y especifique el nombre que desea asignar al tema.

```
$ aws sns create-topic --name my-topic
{
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
}
```

Anote el valor de `TopicArn` de la respuesta, que utilizará más adelante para publicar un mensaje.

Suscripción a un tema

Para suscribirse a un tema, utilice el comando `sns subscribe`.

En el siguiente ejemplo se especifica el protocolo `email` y una dirección de correo electrónico para el `notification-endpoint`.

```
$ aws sns subscribe --topic-arn arn:aws:sns:us-west-2:123456789012:my-topic --
protocol email --notification-endpoint saanvi@example.com
{
    "SubscriptionArn": "pending confirmation"
}
```

AWS envía inmediatamente un mensaje de confirmación a la dirección de correo electrónico que ha especificado en el comando `subscribe`. El mensaje de correo electrónico tiene este texto.

```
You have chosen to subscribe to the topic:
arn:aws:sns:us-west-2:123456789012:my-topic
To confirm this subscription, click or visit the following link (If this was in error
 no action is necessary):
Confirm subscription
```

Cuando el destinatario hace clic en el enlace Confirm subscription (Confirmar suscripción), el navegador del destinatario muestra un mensaje de notificación con información similar a la siguiente.

```
Subscription confirmed!

You have subscribed saanvi@example.com to the topic:my-topic.

Your subscription's id is:
arn:aws:sns:us-west-2:123456789012:my-topic:1328f057-de93-4c15-512e-8bb22EXAMPLE

If it was not your intention to subscribe, click here to unsubscribe.
```

Publicar en un tema

Para enviar un mensaje a todos los suscriptores de un tema, utilice el comando `sns publish`.

En el siguiente ejemplo se envía el mensaje “Hola mundo” a todos los suscriptores del tema especificado.

```
$ aws sns publish --topic-arn arn:aws:sns:us-west-2:123456789012:my-topic --
message "Hello World!"
{
    "MessageId": "4e41661d-5eec-5ddf-8dab-2c867EXAMPLE"
}
```

En este ejemplo, AWS envía un mensaje de correo electrónico con el texto “Hola mundo” a `saanvi@example.com`.

Cancelación de la suscripción a un tema

Para cancelar la suscripción a un tema y dejar de recibir los mensajes que se publican en él, utilice el comando `sns unsubscribe` y especifique el ARN del tema del que desea cancelar la suscripción.

```
$ aws sns unsubscribe --subscription-arn arn:aws:sns:us-west-2:123456789012:my-
topic:1328f057-de93-4c15-512e-8bb22EXAMPLE
```

Para verificar que se ha cancelado la suscripción correctamente, utilice el comando `sns list-subscriptions` para confirmar que el ARN ya no aparece en la lista.

```
$ aws sns list-subscriptions
```

Eliminación de un tema

Para eliminar un tema, ejecute el comando `sns delete-topic`.

```
$ aws sns delete-topic --topic-arn arn:aws:sns:us-west-2:123456789012:my-topic
```

Para verificar que AWS ha eliminado el tema correctamente, utilice el comando `sns list-topics` para confirmar que el tema ya no aparece en la lista.

```
$ aws sns list-topics
```

Ejemplos de comando de AWS CLI

En los ejemplos de código de este tema se muestra cómo utilizar AWS Command Line Interface con AWS.

Los conceptos básicos son ejemplos de código que muestran cómo realizar las operaciones esenciales dentro de un servicio.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica a través de llamadas a varias funciones dentro del servicio o combinado con otros Servicios de AWS.

Algunos servicios contienen categorías de ejemplo adicionales que muestran cómo aprovechar las bibliotecas o funciones específicas del servicio.

Services

- Ejemplos de ACM que utilizan la AWS CLI
- Ejemplos de API Gateway que utilizan la AWS CLI
- Ejemplos de API de WebSocket y HTTP de API Gateway que utilizan la AWS CLI
- Ejemplos de API de administración de puertas de enlace de API que utilizan la AWS CLI
- Ejemplos de App Mesh que utilizan la AWS CLI
- Ejemplos de App Runner que utilizan la AWS CLI
- AWS AppConfig Ejemplos de usando AWS CLI
- Ejemplos de Auto Scaling de aplicaciones que utilizan la AWS CLI
- Ejemplos de Application Discovery Service que utilizan la AWS CLI
- Ejemplos de señales de aplicación que utilizan AWS CLI
- Ejemplos de AppRegistry que utilizan la AWS CLI
- Ejemplos de Athena que utilizan la AWS CLI
- Ejemplos de escalado automático que utilizan la AWS CLI
- Ejemplos de Auto Scaling Plans que utilizan la AWS CLI
- AWS Backup Ejemplos de usando AWS CLI
- AWS Batch Ejemplos de usando AWS CLI
- AWS Budgets Ejemplos de usando AWS CLI
- Ejemplos de Amazon Chime que utilizan la AWS CLI
- Ejemplos de API de control en la nube que utilizan la AWS CLI

- AWS Cloud Map Ejemplos de usando AWS CLI
- AWS Cloud9 Ejemplos de usando AWS CLI
- CloudFormation Ejemplos de usando AWS CLI
- Ejemplos de CloudFront que utilizan la AWS CLI
- Ejemplos de Amazon CloudSearch que utilizan la AWS CLI
- Ejemplos de CloudTrail que utilizan la AWS CLI
- Ejemplos de CloudWatch que utilizan la AWS CLI
- Ejemplos de registros de CloudWatch que utilizan la AWS CLI
- Ejemplos de Monitor de red de CloudWatch que utilizan la AWS CLI
- Ejemplos de CloudWatch Observability Access Monitor que utilizan AWS CLI
- Ejemplos del administrador de observabilidad de CloudWatch que utiliza AWS CLI
- Ejemplos de CloudWatch Synthetics con AWS CLI
- Ejemplos de CodeArtifact que utilizan la AWS CLI
- Ejemplos de CodeBuild que utilizan la AWS CLI
- Ejemplos de CodeCommit que utilizan la AWS CLI
- Ejemplos de CodeDeploy que utilizan la AWS CLI
- Ejemplos del Revisor de CodeGuru que utilizan la AWS CLI
- Ejemplos de CodePipeline que utilizan la AWS CLI
- Ejemplos de notificaciones de AWS CodeStar que utilizan la AWS CLI
- Ejemplos de CodeConnections que utilizan la AWS CLI
- Ejemplos de identidades de Amazon Cognito que utilizan la AWS CLI
- Ejemplos del proveedor de identidades Amazon Cognito que utilizan la AWS CLI
- Ejemplos de Amazon Comprehend que utilizan la AWS CLI
- Ejemplos de Amazon Comprehend Medical que utilizan la AWS CLI
- AWS Config Ejemplos de usando AWS CLI
- Ejemplos de Amazon Connect que utilizan la AWS CLI
- AWS Cost and Usage Report Ejemplos de usando AWS CLI
- Ejemplos del Cost Explorer Service que utilizan la AWS CLI
- Ejemplos de Firehose que utilizan la AWS CLI
- Ejemplos de Amazon Data Lifecycle Manager que utilizan la AWS CLI

- AWS Data Pipeline Ejemplos de usando AWS CLI
- Ejemplos de DataSync que utilizan la AWS CLI
- Ejemplos de DAX que utilizan la AWS CLI
- Ejemplos de Detective que utilizan la AWS CLI
- Ejemplos de Device Farm que utilizan la AWS CLI
- Direct Connect Ejemplos de usando AWS CLI
- Directory Service Ejemplos de usando AWS CLI
- Ejemplos de datos de Directory Service que utilizan AWS CLI
- AWS DMS Ejemplos de usando AWS CLI
- Ejemplos de Amazon DocumentDB que utilizan la AWS CLI
- Ejemplos de DynamoDB que utilizan la AWS CLI
- Ejemplos de DynamoDB que utilizan la AWS CLI
- Ejemplos de Amazon EC2 que utilizan la AWS CLI
- Ejemplos de Amazon EC2 Instance Connect que utilizan la AWS CLI
- Ejemplos de Amazon ECR que utilizan la AWS CLI
- Ejemplos de Amazon ECR Public que utilizan la AWS CLI
- Ejemplos de Amazon ECS que utilizan la AWS CLI
- Ejemplos de Amazon EFS que utilizan la AWS CLI
- Ejemplos de Amazon EKS que utilizan la AWS CLI
- Ejemplos de Elastic Beanstalk que utilizan la AWS CLI
- ELB: ejemplos de la versión 1 mediante AWS CLI
- ELB: ejemplos de la versión 2 mediante AWS CLI
- Ejemplos de ElastiCache que utilizan la AWS CLI
- Ejemplos de MediaStore que utilizan la AWS CLI
- Ejemplos de Amazon EMR que utilizan la AWS CLI
- Ejemplos de Amazon EMR en EKS que utilizan la AWS CLI
- Ejemplos de EventBridge que utilizan la AWS CLI
- Ejemplos de canalizaciones de EventBridge con la AWS CLI
- Ejemplos de Firewall Manager que utilizan la AWS CLI

- AWS FIS Ejemplos de usando AWS CLI
- Ejemplos de servidores de Amazon GameLift que utilizan la AWS CLI
- Ejemplos de Amazon Glacier que utilizan AWS CLI
- Ejemplos de Global Accelerator que utilizan la AWS CLI
- AWS Glue Ejemplos de usando AWS CLI
- Ejemplos de GuardDuty que utilizan la AWS CLI
- AWS Health Ejemplos de usando AWS CLI
- Ejemplos de HealthImaging que utilizan la AWS CLI
- Ejemplos de HealthLake que utilizan la AWS CLI
- Ejemplos de HealthOmics que utilizan la AWS CLI
- Ejemplos de IAM que utilizan la AWS CLI
- Ejemplos del Analizador de acceso de IAM que utilizan la AWS CLI
- Ejemplos de Image Builder que utilizan la AWS CLI
- Ejemplos de Incident Manager que utilizan la AWS CLI
- Ejemplos de contactos de Incident Manager que utilizan la AWS CLI
- Ejemplos de Amazon Inspector que utilizan la AWS CLI
- AWS IoT Ejemplos de usando AWS CLI
- AWS IoT Analytics Ejemplos de usando AWS CLI
- Ejemplos de Device Advisor que utilizan la AWS CLI
- AWS IoT data Ejemplos de usando AWS CLI
- AWS IoT Events Ejemplos de usando AWS CLI
- AWS IoT Events-Data Ejemplos de usando AWS CLI
- AWS IoT Greengrass Ejemplos de usando AWS CLI
- AWS IoT Greengrass V2 Ejemplos de usando AWS CLI
- Publicación de AWS IoT Jobs SDK Ejemplos de usando AWS CLI
- AWS IoT SiteWise Ejemplos de usando AWS CLI
- AWS IoT Things Graph Ejemplos de usando AWS CLI
- AWS IoT Wireless Ejemplos de usando AWS CLI
- Ejemplos de Amazon IVS que utilizan la AWS CLI

- Ejemplos de Chat de Amazon IVS que utilizan la AWS CLI
- Ejemplos de Transmisión en tiempo real de Amazon IVS que utilizan la AWS CLI
- Ejemplos de Amazon Kendra que utilizan la AWS CLI
- Ejemplos de Kinesis que utilizan la AWS CLI
- AWS KMS Ejemplos de usando AWS CLI
- Ejemplos de Lake Formation que utilizan la AWS CLI
- Ejemplos de Lambda que utilizan la AWS CLI
- Ejemplos de License Manager que utilizan la AWS CLI
- Lightsail Ejemplos de usando AWS CLI
- Ejemplos de Macie que utilizan la AWS CLI
- Ejemplos de Amazon Managed Grafana que utilizan la AWS CLI
- Ejemplos de MediaConnect que utilizan la AWS CLI
- Ejemplos de MediaConvert que utilizan la AWS CLI
- Ejemplos de MediaLive que utilizan la AWS CLI
- Ejemplos de MediaPackage que utilizan la AWS CLI
- Ejemplos de VOD de MediaPackage que utilizan la AWS CLI
- Ejemplos de planos de datos de MediaStore que utilizan la AWS CLI
- Ejemplos de MediaTailor que utilizan la AWS CLI
- Ejemplos de MemoryDB que utilizan la AWS CLI
- Ejemplos de Amazon MSK que utilizan la AWS CLI
- Ejemplos de monitor del flujo de red mediante AWS CLI
- Ejemplos de Network Manager que utilizan la AWS CLI
- Ejemplos de OpenSearch Service que utilizan la AWS CLI
- Ejemplos de Organizations que utilizan la AWS CLI
- AWS Outposts Ejemplos de usando AWS CLI
- AWS Payment Cryptography Ejemplos de usando AWS CLI
- Ejemplos de planos de datos de AWS Payment Cryptography que utilizan la AWS CLI
- Ejemplos de Amazon Pinpoint que utilizan la AWS CLI
- Ejemplos de Amazon Polly que utilizan la AWS CLI
- Lista de precios de AWS Ejemplos de usando AWS CLI

- AWS Private CA Ejemplos de usando AWS CLI
- AWS Proton Ejemplos de usando AWS CLI
- Ejemplos de Amazon RDS usando AWS CLI
- Ejemplos de servicio de datos de Amazon RDS que utilizan la AWS CLI
- Ejemplos de información de rendimiento de Amazon RDS que utilizan la AWS CLI
- Ejemplos de Amazon Redshift que utilizan la AWS CLI
- Ejemplos de Amazon Rekognition usando AWS CLI
- AWS RAM Ejemplos de usando AWS CLI
- Ejemplos de Resource Explorer que utilizan la AWS CLI
- Ejemplos de Resource Groups que utilizan la AWS CLI
- Ejemplos de la API para Resource Groups Tagging que utilizan la AWS CLI
- Ejemplos de Route 53 que utilizan la AWS CLI
- Ejemplos de registro de dominios de Route 53 usando AWS CLI
- Ejemplos de Perfiles de Route 53 que utilizan la AWS CLI
- Ejemplos de Route 53 Resolver que utilizan la AWS CLI
- Ejemplos de Amazon S3 que utilizan la AWS CLI
- Ejemplos de Amazon S3 Control que utilizan la AWS CLI
- Ejemplos de Secrets Manager que utilizan la AWS CLI
- Ejemplos de CSPM de Security Hub que utilizan la AWS CLI
- Ejemplos de Security Lake que utilizan la AWS CLI
- AWS Serverless Application Repository Ejemplos de usando AWS CLI
- Ejemplos de Service Catalog que utilizan la AWS CLI
- Ejemplos de Service Quotas que utilizan la AWS CLI
- Ejemplos de Amazon SES que utilizan la AWS CLI
- Ejemplos de Shield que utilizan la AWS CLI
- Ejemplos de Signer que utilizan la AWS CLI
- Ejemplos de Snowball Edge que utilizan la AWS CLI
- Ejemplos de Amazon SNS que utilizan la AWS CLI
- Ejemplos de Amazon SQS usando AWS CLI
- Ejemplos de Storage Gateway que utilizan la AWS CLI

- AWS STS Ejemplos de usando AWS CLI
- Soporte Ejemplos de usando AWS CLI
- Ejemplos de Amazon SWF que utilizan la AWS CLI
- Ejemplos de Systems Manager que utilizan la AWS CLI
- Ejemplos de Amazon Textract que utilizan la AWS CLI
- Ejemplos de Amazon Transcribe que utilizan la AWS CLI
- Ejemplos de Amazon Translate que utilizan la AWS CLI
- Trusted Advisor Ejemplos de usando AWS CLI
- Ejemplos de Verified Permissions que utilizan la AWS CLI
- Ejemplos de VPC Lattice que utilizan la AWS CLI
- AWS WAF Classic Ejemplos de usando AWS CLI
- AWS WAF Classic Regional Ejemplos de usando AWS CLI
- AWS WAFV2 Ejemplos de usando AWS CLI
- Ejemplos de WorkDocs que utilizan la AWS CLI
- Ejemplos de Amazon WorkMail que utilizan la AWS CLI
- Ejemplos de flujo de mensajes de Amazon WorkMail que utilizan la AWS CLI
- Ejemplos de WorkSpaces que utilizan la AWS CLI
- Ejemplos de X-Ray que utilizan la AWS CLI

Ejemplos de ACM que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con ACM.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-tags-to-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-tags-to-certificate`.

AWS CLI

Adición de etiquetas a un certificado de ACM existente

El siguiente comando `add-tags-to-certificate` añade dos etiquetas al certificado especificado. Utilice un espacio para separar varias etiquetas:

```
aws acm add-tags-to-certificate --certificate-
arn arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012 --
tags Key=Admin,Value=Alice Key=Purpose,Value=Website
```

- Para obtener información sobre la API, consulte AddTagsToCertificate en la Referencia de comandos de la AWS CLI.

`delete-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-certificate`.

AWS CLI

Eliminación de un certificado de ACM de su cuenta

El siguiente comando `delete-certificate` elimina el certificado con el ARN especificado:

```
aws acm delete-certificate --certificate-
arn arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012
```

- Para obtener información sobre la API, consulte DeleteCertificate en la Referencia de comandos de la AWS CLI.

`describe-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-certificate`.

AWS CLI

Recuperación de los campos incluidos en un certificado de ACM

El siguiente comando `describe-certificate` recupera todos los campos del certificado con el ARN especificado:

```
aws acm describe-certificate --certificate-
arn arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012
```

Se muestra una salida similar a la siguiente:

```
{
  "Certificate": {
    "CertificateArn":
 "arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012",
    "CreatedAt": 1446835267.0,
    "DomainName": "www.example.com",
    "DomainValidationOptions": [
      {
        "DomainName": "www.example.com",
        "ValidationDomain": "www.example.com",
        "ValidationEmails": [
          "hostmaster@example.com",
          "admin@example.com",
          "owner@example.com.whoisprivacyservice.org",
          "tech@example.com.whoisprivacyservice.org",
          "admin@example.com.whoisprivacyservice.org",
          "postmaster@example.com",
          "webmaster@example.com",
          "administrator@example.com"
        ]
      },
      {
        "DomainName": "www.example.net",
        "ValidationDomain": "www.example.net",
        "ValidationEmails": [
          "postmaster@example.net",
          "admin@example.net",
          "owner@example.net.whoisprivacyservice.org",
          "tech@example.net.whoisprivacyservice.org",
          "admin@example.net.whoisprivacyservice.org",
          "hostmaster@example.net",
```

```
            "administrator@example.net",
            "webmaster@example.net"
          ]
        }
      ],
      "InUseBy": [],
      "IssuedAt": 1446835815.0,
      "Issuer": "Amazon",
      "KeyAlgorithm": "RSA-2048",
      "NotAfter": 1478433600.0,
      "NotBefore": 1446768000.0,
      "Serial": "0f:ac:b0:a3:8d:ea:65:52:2d:7d:01:3a:39:36:db:d6",
      "SignatureAlgorithm": "SHA256WITHRSA",
      "Status": "ISSUED",
      "Subject": "CN=www.example.com",
      "SubjectAlternativeNames": [
        "www.example.com",
        "www.example.net"
      ]
    }
}
```

- Para obtener información sobre la API, consulte DescribeCertificate en la Referencia de comandos de la AWS CLI.

`export-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `export-certificate`.

AWS CLI

Exportación de un certificado privado emitido por una entidad de certificación privada

En el siguiente comando `export-certificate`, se exporta un certificado privado, una cadena de certificados y una clave privada, que se pueden ver en la pantalla:

```
aws acm export-certificate --certificate-
arn arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012 --
passphrase file://path-to-passphrase-file
```

Para exportar el certificado, la cadena y la clave privada a un archivo local, utilice el siguiente comando:

```
aws acm export-certificate --certificate-
arn arn:aws:acm:region:sccount:certificate/12345678-1234-1234-1234-123456789012 --
passphrase file://path-to-passphrase-file > c:\temp\export.txt
```

- Para obtener información sobre la API, consulte ExportCertificate en la Referencia de comandos de la AWS CLI.

`get-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-certificate`.

AWS CLI

Recuperación de un certificado de ACM

El siguiente comando `get-certificate` recupera el certificado del ARN especificado y de la cadena de certificados:

```
aws acm get-certificate --certificate-
arn arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012
```

Se muestra una salida similar a la siguiente:

```
{
  "Certificate": "-----BEGIN CERTIFICATE-----
MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----",

  "CertificateChain": "-----BEGIN CERTIFICATE-----
```

```
MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----",
"-----BEGIN CERTIFICATE-----
MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----",
"-----BEGIN CERTIFICATE-----
MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
```

```
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----"
}
```

- Para obtener más información sobre la API, consulte GetCertificate en la Referencia de comandos de la AWS CLI.

`import-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-certificate`.

AWS CLI

Importación de un certificado a ACM.

El siguiente comando `import-certificate` importa un certificado a ACM. Reemplace los nombres de los archivos por los suyos:

```
aws acm import-certificate --certificate file://Certificate.pem --certificate-
chain file://CertificateChain.pem --private-key file://PrivateKey.pem
```

- Para obtener información sobre la API, consulte ImportCertificate en la Referencia de comandos de la AWS CLI.

`list-certificates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-certificates`.

AWS CLI

Creación de una lista de los certificados de ACM de una cuenta de AWS

El siguiente comando `list-certificates` muestra los ARN de los certificados de su cuenta:

```
aws acm list-certificates
```

El comando anterior produce un resultado similar al siguiente:

```
{
```

```
    "CertificateSummaryList": [
        {
            "CertificateArn":
 "arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012",
            "DomainName": "www.example.com"
        },
        {
            "CertificateArn": "arn:aws:acm:region:account:certificate/aaaaaaaa-bbbb-
cccc-dddd-eeeeeeeeeeee",
            "DomainName": "www.example.net"
        }
    ]
}
```

Puede decidir cuántos certificados quiere mostrar cada vez que llame a `list-certificates`. Por ejemplo, si tiene cuatro certificados y no quiere mostrar más de dos a la vez, establezca el argumento `max-items` en 2, como se muestra en el siguiente ejemplo:

```
aws acm list-certificates --max-items 2
```

Se mostrarán dos ARN de certificado y un valor `NextToken`:

```
"CertificateSummaryList": [
  {
    "CertificateArn": "arn:aws:acm:region:account: \
            certificate/12345678-1234-1234-1234-123456789012",
    "DomainName": "www.example.com"
  },
  {
    "CertificateArn": "arn:aws:acm:region:account: \
             certificate/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",
    "DomainName": "www.example.net"
  }
  ],
    "NextToken": "9f4d9f69-275a-41fe-b58e-2b837bd9ba48"
```

Para mostrar los dos certificados siguientes de su cuenta, establezca este valor `NextToken` en la próxima llamada:

```
aws acm list-certificates --max-items 2 --next-token 9f4d9f69-275a-41fe-
b58e-2b837bd9ba48
```

Puede filtrar su salida mediante el argumento `certificate-statuses`. El siguiente comando muestra los certificados que tienen el estado PENDING_VALIDATION:

```
aws acm list-certificates --certificate-statuses PENDING_VALIDATION
```

También puede filtrar la salida mediante el argumento `includes`. El siguiente comando muestra los certificados filtrados en las siguientes propiedades. Los certificados que se van a mostrar:

```
- Specify that the RSA algorithm and a 2048 bit key are used to generate key pairs.
- Contain a Key Usage extension that specifies that the certificates can be used to
 create digital signatures.
- Contain an Extended Key Usage extension that specifies that the certificates can
 be used for code signing.

aws acm list-certificates --max-items 10 --includes
 extendedKeyUsage=CODE_SIGNING,keyUsage=DIGITAL_SIGNATURE,keyTypes=RSA_2048
```

- Para obtener información sobre la API, consulte ListCertificates en la Referencia de comandos de la AWS CLI.

`list-tags-for-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-certificate`.

AWS CLI

Creación de una lista las etiquetas aplicadas a un certificado de ACM

El siguiente comando `list-tags-for-certificate` muestra las etiquetas aplicadas a un certificado de su cuenta:

```
aws acm list-tags-for-certificate --certificate-
arn arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012
```

El comando anterior produce un resultado similar al siguiente:

```
{
  "Tags": [
      {
          "Value": "Website",
```

```
            "Key": "Purpose"
        },
        {
            "Value": "Alice",
            "Key": "Admin"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListTagsForCertificate en la Referencia de comandos de la AWS CLI.

`remove-tags-from-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-tags-from-certificate`.

AWS CLI

Eliminación de una etiqueta de un certificado de ACM

El siguiente comando `remove-tags-from-certificate` elimina las dos etiquetas del certificado especificado. Utilice un espacio para separar varias etiquetas:

```
aws acm remove-tags-from-certificate --certificate-
arn arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012 --
tags Key=Admin,Value=Alice Key=Purpose,Value=Website
```

- Para obtener información sobre la API, consulte RemoveTagsFromCertificate en la Referencia de comandos de la AWS CLI.

`request-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `request-certificate`.

AWS CLI

Solicitud de un nuevo certificado de ACM

El siguiente comando `request-certificate` solicita un nuevo certificado para el dominio www.example.com mediante la validación de DNS:

```
aws acm request-certificate --domain-name www.example.com --validation-method DNS
```

Puede introducir un token de idempotencia para distinguir entre las llamadas a `request-certificate`.

```
aws acm request-certificate --domain-name www.example.com --validation-method DNS --
idempotency-token 91adc45q
```

Puede introducir uno o varios nombres alternativos de asunto para solicitar un certificado que proteja más de un dominio de ápex:

```
aws acm request-certificate --domain-name example.com --validation-method DNS --
idempotency-token 91adc45q --subject-alternative-names www.example.net
```

Puede introducir un nombre alternativo que también se pueda utilizar para acceder a su sitio web:

```
aws acm request-certificate --domain-name example.com --validation-method DNS --
idempotency-token 91adc45q --subject-alternative-names www.example.com
```

Puede utilizar un asterisco (*) como comodín para crear un certificado para varios subdominios del mismo dominio:

```
aws acm request-certificate --domain-name example.com --validation-method DNS --
idempotency-token 91adc45q --subject-alternative-names *.example.com
```

También puede introducir varios nombres alternativos:

```
aws acm request-certificate --domain-name example.com --validation-method DNS --
subject-alternative-names b.example.com c.example.com d.example.com
```

Si utiliza el correo electrónico para la validación, puede introducir las opciones de validación del dominio para especificar el dominio al que se enviará el correo electrónico de validación:

```
aws acm request-certificate --domain-name example.com --validation-
method EMAIL --subject-alternative-names www.example.com --domain-validation-
options DomainName=example.com,ValidationDomain=example.com
```

El siguiente comando cancela el registro de transparencia de certificados cuando solicita un certificado nuevo:

```
aws acm request-certificate --domain-name www.example.com --validation-method DNS --
options CertificateTransparencyLoggingPreference=DISABLED --idempotency-token 184627
```

- Para obtener información sobre la API, consulte RequestCertificate en la Referencia de comandos de la AWS CLI.

`resend-validation-email`

En el siguiente ejemplo de código, se muestra cómo utilizar `resend-validation-email`.

AWS CLI

Reenvío del correo electrónico de validación de su solicitud de certificado de ACM

El siguiente comando `resend-validation-email` indica a la autoridad de certificación de Amazon que envíe un correo electrónico de validación a las direcciones correspondientes:

```
aws acm resend-validation-email --certificate-
arn arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012 --
domain www.example.com --validation-domain example.com
```

- Para obtener información sobre la API, consulte ResendValidationEmail en la Referencia de comandos de la AWS CLI.

`update-certificate-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-certificate-options`.

AWS CLI

Actualización de las opciones de certificado

En el siguiente comando `update-certificate-options`, se cancela el registro de transparencia de certificados:

```
aws acm update-certificate-options --certificate-
arn arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012 --
options CertificateTransparencyLoggingPreference=DISABLED
```

- Para obtener información sobre la API, consulte UpdateCertificateOptions en la Referencia de comandos de la AWS CLI.

Ejemplos de API Gateway que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante AWS Command Line Interface con una puerta de enlace de API.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-api-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-api-key`.

AWS CLI

Creación de una clave de API que esté habilitada para una API y una etapa existentes

Comando:

```
aws apigateway create-api-key --name 'Dev API Key' --description 'Used for
 development' --enabled --stage-keys restApiId='a1b2c3d4e5',stageName='dev'
```

- Para obtener información sobre la API, consulte CreateApiKey en la Referencia de comandos de la AWS CLI.

`create-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-authorizer`.

AWS CLI

Ejemplo 1: cómo crear un autorizador personalizado de API Gateway basado en tokens para la API

En el siguiente ejemplo de `create-authorizer`, se crea un autorizador basado en tokens.

```
aws apigateway create-authorizer \
    --rest-api-id 1234123412 \
    --name 'First_Token_Custom_Authorizer' \
    --type TOKEN \
    --authorizer-uri 'arn:aws:apigateway:us-west-2:lambda:path/2015-03-31/functions/
arn:aws:lambda:us-west-2:123412341234:function:customAuthFunction/invocations' \
    --identity-source 'method.request.header.Authorization' \
    --authorizer-result-ttl-in-seconds 300
```

Salida:

```
{
    "authType": "custom",
    "name": "First_Token_Custom_Authorizer",
    "authorizerUri": "arn:aws:apigateway:us-west-2:lambda:path/2015-03-31/functions/
arn:aws:lambda:us-west-2:123412341234:function:customAuthFunction/invocations",
    "authorizerResultTtlInSeconds": 300,
    "identitySource": "method.request.header.Authorization",
    "type": "TOKEN",
    "id": "z40xj0"
}
```

Ejemplo 2: cómo crear un autorizador personalizado de API Gateway basado en grupos de usuarios de Cognito para la API

En el siguiente ejemplo de `create-authorizer`, se crea un autorizador personalizado de API Gateway basado en grupos de usuarios de Cognito.

```
aws apigateway create-authorizer \
    --rest-api-id 1234123412 \
    --name 'First_Cognito_Custom_Authorizer' \
    --type COGNITO_USER_POOLS \
    --provider-arns 'arn:aws:cognito-idp:us-east-1:123412341234:userpool/us-
east-1_aWcZeQbuD' \
    --identity-source 'method.request.header.Authorization'
```

Salida:

```
{
    "authType": "cognito_user_pools",
```

```
    "identitySource": "method.request.header.Authorization",
    "name": "First_Cognito_Custom_Authorizer",
    "providerARNs": [
        "arn:aws:cognito-idp:us-east-1:342398297714:userpool/us-east-1_qWbZzQhzE"
    ],
    "type": "COGNITO_USER_POOLS",
    "id": "5yid1t"
}
```

Ejemplo 3: cómo crear un autorizador personalizado de API Gateway basado solicitudes para la API

En el siguiente ejemplo de `create-authorizer`, se crea un autorizador basado solicitudes.

```
aws apigateway create-authorizer \
    --rest-api-id 1234123412 \
    --name 'First_Request_Custom_Authorizer' \
    --type REQUEST \
    --authorizer-uri 'arn:aws:apigateway:us-west-2:lambda:path/2015-03-31/functions/
arn:aws:lambda:us-west-2:123412341234:function:customAuthFunction/invocations' \
    --identity-source 'method.request.header.Authorization,context.accountId' \
    --authorizer-result-ttl-in-seconds 300
```

Salida:

```
{
    "id": "z40xj0",
    "name": "First_Request_Custom_Authorizer",
    "type": "REQUEST",
    "authType": "custom",
    "authorizerUri": "arn:aws:apigateway:us-west-2:lambda:path/2015-03-31/functions/
arn:aws:lambda:us-west-2:123412341234:function:customAuthFunction/invocations",
    "identitySource": "method.request.header.Authorization,context.accountId",
    "authorizerResultTtlInSeconds": 300
}
```

- Para obtener información sobre la API, consulte CreateAuthorizer en la Referencia de comandos de la AWS CLI.

`create-base-path-mapping`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-base-path-mapping`.

AWS CLI

Creación de la asignación de ruta base para un nombre de dominio personalizado

Comando:

```
aws apigateway create-base-path-mapping --domain-name subdomain.domain.tld --rest-api-id 1234123412 --stage prod --base-path v1
```

- Para obtener información sobre la API, consulte CreateBasePathMapping en la Referencia de comandos de la AWS CLI.

`create-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-deployment`.

AWS CLI

Para implementar los recursos configurados para una API en una nueva etapa

Comando:

```
aws apigateway create-deployment --rest-api-id 1234123412 --stage-name dev --stage-description 'Development Stage' --description 'First deployment to the dev stage'
```

Para implementar los recursos configurados para una API en una etapa existente

Comando:

```
aws apigateway create-deployment --rest-api-id 1234123412 --stage-name dev --description 'Second deployment to the dev stage'
```

Para implementar los recursos configurados para una API en una etapa existente con variables de etapa

aws apigateway create-deployment --rest-api-id 1234123412 --stage-name dev --description 'Third deployment to the dev stage' --variables key='value',otherKey='otherValue'

- Para obtener información sobre la API, consulte CreateDeployment en la Referencia de comandos de la AWS CLI.

`create-domain-name-access-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-domain-name-access-association`.

AWS CLI

Creación de una asociación de acceso a nombres de dominio

En el siguiente ejemplo de `create-domain-name-access-association`, se crea una asociación de acceso a un nombre de dominio entre un nombre de dominio personalizado privado y un punto de conexión de VPC.

```
aws apigateway create-domain-name-access-association \
    --domain-name-arn arn:aws:apigateway:us-west-2:111122223333:/domainnames/
my.private.domain.tld+abcd1234 \
    --access-association-source vpce-abcd1234efg \
    --access-association-source-type VPCE
```

Salida:

```
{
    "domainNameAccessAssociationArn": "arn:aws:apigateway:us-west-2:012345678910:/
domainnameaccessassociations/domainname/my.private.domain.tld/vpcesource/vpce-
abcd1234efg
    "accessAssociationSource": "vpce-abcd1234efg",
    "accessAssociationSourceType": "VPCE",
    "domainNameArn" : "arn:aws:apigateway:us-west-2:111122223333:/domainnames/
private.example.com+abcd1234"
}
```

Para obtener más información, consulte Nombres de dominio personalizados para las API privadas en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte CreateDomainNameAccessAssociation en Referencia de comandos de AWS CLI.

`create-domain-name`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-domain-name`.

AWS CLI

Ejemplo 1: creación de un nombre de dominio público personalizado

En el siguiente ejemplo de `create-domain-name`, se crea un nombre de dominio personalizado público.

```
aws apigateway create-domain-name \
    --domain-name 'my.domain.tld' \
    --certificate-name 'my.domain.tld cert'\
    --certificate-arn 'arn:aws:acm:us-east-1:012345678910:certificate/fb1b9770-
a305-495d-aefb-27e5e101ff3'
```

Salida:

```
{
    "domainName": "my.domain.tld",
    "certificateName": "my.domain.tld cert",
    "certificateArn": "arn:aws:acm:us-east-1:012345678910:certificate/fb1b9770-
a305-495d-aefb-27e5e101ff3",
    "certificateUploadDate": "2024-10-08T11:29:49-07:00",
    "distributionDomainName": "abcd1234.cloudfront.net",
    "distributionHostedZoneId": "Z2FDTNDATAQYW2",
    "endpointConfiguration": {
        "types": [
            "EDGE"
        ]
    },
    "domainNameStatus": "AVAILABLE",
    "securityPolicy": "TLS_1_2"
}
```

Para obtener más información, consulte Nombre de dominio personalizado para las API de REST públicas en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

Ejemplo 2: creación de un nombre de dominio privado personalizado

En el siguiente ejemplo de `create-domain-name`, se crea un nombre de dominio personalizado privado.

```
aws apigateway create-domain-name \
    --domain-name 'my.private.domain.tld' \
```

```
    --certificate-name 'my.domain.tld cert' \
    --certificate-arn 'arn:aws:acm:us-east-1:012345678910:certificate/fb1b9770-
a305-495d-aefb-27e5e101ff3' \
    --endpoint-configuration '{"types": ["PRIVATE"]}' \
    --security-policy 'TLS_1_2' \
    --policy file://policy.json
```

Contenido de `policy.json`:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "execute-api:Invoke",
            "Resource": [
                "execute-api:/*"
            ]
        },
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "execute-api:Invoke",
            "Resource": [
                "execute-api:/*"
            ],
            "Condition" : {
                "StringNotEquals": {
                    "aws:SourceVpce": "vpce-abcd1234efg"
                }
            }
        }
    ]
}
```

Salida:

```
{
    "domainName": "my.private.domain.tld",
    "domainNameId": "abcd1234",
    "domainNameArn": "arn:aws:apigateway:us-east-1:012345678910:/domainnames/
my.private.domain.tld+abcd1234",
```

```
    "certificateArn": "arn:aws:acm:us-east-1:012345678910:certificate/fb1b9770-
a305-495d-aefb-27e5e101ff3",
    "certificateUploadDate": "2024-09-10T10:31:20-07:00",
    "endpointConfiguration": {
        "types": [
            "PRIVATE"
        ]
    },
    "domainNameStatus": "AVAILABLE",
    "securityPolicy": "TLS_1_2",
    "policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":
\"Allow\",\"Principal\":\"*\",\"Action\":\"execute-api:Invoke\",\"Resource\":
\"arn:aws:execute-api:us-east-1:012345678910:/domainnames/my.private.domain.tld
+abcd1234\"},{\"Effect\":\"Deny\",\"Principal\":\"*\",\"Action\":\"execute-
api:Invoke\",\"Resource\":\"arn:aws:execute-api:us-east-1:012345678910:/domainnames/
my.private.domain.tld+abcd1234\",\"Condition\":{\"StringNotEquals\":{\"aws:SourceVpc
\":\"vpc-1a2b3c4d\"}}}]}"
}
```

Para obtener más información, consulte Nombre de dominio personalizado para las API de REST públicas en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte CreateDomainName en la Referencia de comandos de la AWS CLI.

`create-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-model`.

AWS CLI

Creación de un modelo para una API

Comando:

```
aws apigateway create-model --rest-api-id 1234123412 --name 'firstModel' --
description 'The First Model' --content-type 'application/json'  --schema
 '{ "$schema": "http://json-schema.org/draft-04/schema#", "title": "firstModel",
 "type": "object", "properties": { "firstProperty" : { "type": "object",
 "properties": { "key": { "type": "string" } } } } }'
```

Salida:

```
{
    "contentType": "application/json",
    "description": "The First Model",
    "name": "firstModel",
    "id": "2rzg0l",
    "schema": "{ \"$schema\": \"http://json-schema.org/draft-04/schema#\", \"title
\": \"firstModel\", \"type\": \"object\", \"properties\": { \"firstProperty
\" : { \"type\": \"object\", \"properties\": { \"key\": { \"type\": \"string
\" } } } } }"
}
```

- Para obtener información sobre la API, consulte CreateModel en la Referencia de comandos de la AWS CLI.

`create-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-resource`.

AWS CLI

Creación de un recurso en una API

Comando:

```
aws apigateway create-resource --rest-api-id 1234123412 --parent-id a1b2c3 --path-
part 'new-resource'
```

- Para obtener información sobre la API, consulte CreateResource en la Referencia de comandos de la AWS CLI.

`create-rest-api`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-rest-api`.

AWS CLI

Creación de una API

Comando:

```
aws apigateway create-rest-api --name 'My First API' --description 'This is my first
 API'
```

Para crear una API duplicada a partir de una API existente

Comando:

```
aws apigateway create-rest-api --name 'Copy of My First API' --description 'This is
 a copy of my first API' --clone-from 1234123412
```

- Para obtener información sobre la API, consulte CreateRestApi en la Referencia de comandos de la AWS CLI.

`create-stage`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-stage`.

AWS CLI

Creación de una etapa en una API que contenga una implementación existente

Comando:

```
aws apigateway create-stage --rest-api-id 1234123412 --stage-name 'dev' --
description 'Development stage' --deployment-id a1b2c3
```

Creación de una etapa en una API que contenga una implementación existente y variables de etapa personalizadas

Comando:

```
aws apigateway create-stage --rest-api-id 1234123412 --stage-name 'dev'
 --description 'Development stage' --deployment-id a1b2c3 --variables
 key='value',otherKey='otherValue'
```

- Para obtener información sobre la API, consulte CreateStage en la Referencia de comandos de la AWS CLI.

`create-usage-plan-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-usage-plan-key`.

AWS CLI

Asociación de una clave de API existente a un plan de uso

Comando:

```
aws apigateway create-usage-plan-key --usage-plan-id a1b2c3 --key-type "API_KEY" --
key-id 4vq3yryqm5
```

- Para obtener información sobre la API, consulte CreateUsagePlanKey en la Referencia de comandos de la AWS CLI.

`create-usage-plan`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-usage-plan`.

AWS CLI

Creación de un plan de uso con límites de cuota y limitación que se restablezca a principios de mes

Comando:

```
aws apigateway create-usage-plan --name "New Usage Plan" --description "A new usage
 plan" --throttle burstLimit=10,rateLimit=5 --quota limit=500,offset=0,period=MONTH
```

- Para obtener información sobre la API, consulte CreateUsagePlan en la Referencia de comandos de la AWS CLI.

`delete-api-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-api-key`.

AWS CLI

Eliminación de una clave de API

Comando:

```
aws apigateway delete-api-key --api-key 8bklk8bl1k3sB38D9B3l0enyWT8c09B30lkq0blk
```

- Para obtener información sobre la API, consulte DeleteApiKey en la Referencia de comandos de la AWS CLI.

`delete-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-authorizer`.

AWS CLI

Eliminación de un autorizador personalizado de una API

Comando:

```
aws apigateway delete-authorizer --rest-api-id 1234123412 --authorizer-id 7gkfbo
```

- Para obtener detalles sobre la API, consulte DeleteAuthorizer en la Referencia de comandos de la AWS CLI.

`delete-base-path-mapping`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-base-path-mapping`.

AWS CLI

Eliminación de la asignación de ruta base de un nombre de dominio personalizado

Comando:

```
aws apigateway delete-base-path-mapping --domain-name 'api.domain.tld' --base-path
 'dev'
```

- Para obtener información sobre la API, consulte DeleteBasePathMapping en la Referencia de comandos de la AWS CLI.

`delete-client-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-client-certificate`.

AWS CLI

Eliminación de un certificado de cliente

Comando:

```
aws apigateway delete-client-certificate --client-certificate-id a1b2c3
```

- Para obtener información sobre la API, consulte DeleteClientCertificate en la Referencia de comandos de la AWS CLI.

`delete-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-deployment`.

AWS CLI

Para eliminar una implementación en una API

Comando:

```
aws apigateway delete-deployment --rest-api-id 1234123412 --deployment-id a1b2c3
```

- Para obtener información sobre la API, consulte DeleteDeployment en la Referencia de comandos de la AWS CLI.

`delete-domain-name-access-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-domain-name-access-association`.

AWS CLI

Eliminación de una asociación de acceso a nombres de dominio

En el siguiente ejemplo de `delete-domain-name-access-association`, se elimina una asociación de acceso a un nombre de dominio entre un nombre de dominio personalizado privado y un punto de conexión de VPC.

```
aws apigateway delete-domain-name-access-association \
```

```
    --domain-name-access-association-arn arn:aws:apigateway:us-west-2:012345678910:/
domainnameaccessassociations/domainname/my.private.domain.tld/vpcesource/vpce-
abcd1234efg
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Nombres de dominio personalizados para las API privadas en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte DeleteDomainNameAccessAssociation en Referencia de comandos de la AWS CLI.

`delete-domain-name`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-domain-name`.

AWS CLI

Eliminación de un nombre de dominio personalizado

Comando:

```
aws apigateway delete-domain-name --domain-name 'api.domain.tld'
```

- Para obtener información sobre la API, consulte DeleteDomainName en la Referencia de comandos de la AWS CLI.

`delete-integration-response`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-integration-response`.

AWS CLI

Eliminación de una respuesta de integración de un recurso, método y código de estado determinados en una API

Comando:

```
aws apigateway delete-integration-response --rest-api-id 1234123412 --resource-
id a1b2c3 --http-method GET --status-code 200
```

- Para obtener información sobre la API, consulte DeleteIntegrationResponse en la Referencia de comandos de la AWS CLI.

`delete-integration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-integration`.

AWS CLI

Eliminación de una integración de un recurso y método determinados en una API

Comando:

```
aws apigateway delete-integration --rest-api-id 1234123412 --resource-id a1b2c3 --
http-method GET
```

- Para obtener información sobre la API, consulte DeleteIntegration en la Referencia de comandos de la AWS CLI.

`delete-method-response`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-method-response`.

AWS CLI

Eliminación de una respuesta de método de un recurso, método y código de estado determinados en una API

Comando:

```
aws apigateway delete-method-response --rest-api-id 1234123412 --resource-id a1b2c3
 --http-method GET --status-code 200
```

- Para obtener información sobre la API, consulte DeleteMethodResponse en la Referencia de comandos de la AWS CLI.

`delete-method`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-method`.

AWS CLI

Eliminación de un método de un recurso determinado en una API

Comando:

```
aws apigateway delete-method --rest-api-id 1234123412 --resource-id a1b2c3 --http-method GET
```

- Para obtener información sobre la API, consulte DeleteMethod en la Referencia de comandos de AWS CLI.

`delete-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-model`.

AWS CLI

Eliminación de un modelo en una API determinada

Comando:

```
aws apigateway delete-model --rest-api-id 1234123412 --model-name 'customModel'
```

- Para obtener información sobre la API, consulte DeleteModel en la Referencia de comandos de la AWS CLI.

`delete-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-resource`.

AWS CLI

Eliminación de un recurso en una API

Comando:

```
aws apigateway delete-resource --rest-api-id 1234123412 --resource-id a1b2c3
```

- Para obtener información sobre la API, consulte DeleteResource en la Referencia de comandos de la AWS CLI.

`delete-rest-api`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-rest-api`.

AWS CLI

Eliminación de una API

Comando:

```
aws apigateway delete-rest-api --rest-api-id 1234123412
```

- Para obtener información sobre la API, consulte DeleteRestApi en la Referencia de comandos de la AWS CLI.

`delete-stage`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-stage`.

AWS CLI

Para eliminar una etapa en una API

Comando:

```
aws apigateway delete-stage --rest-api-id 1234123412 --stage-name 'dev'
```

- Para obtener información sobre la API, consulte DeleteStage en la Referencia de comandos de la AWS CLI.

`delete-usage-plan-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-usage-plan-key`.

AWS CLI

Eliminación de una clave de API de un plan de uso

Comando:

```
aws apigateway delete-usage-plan-key --usage-plan-id a1b2c3 --key-
id 1NbjQzMReAkeEQPNAW8r3dXsU2rDD7fc7f2Sipnu
```

- Para obtener información sobre la API, consulte DeleteUsagePlanKey en la Referencia de comandos de la AWS CLI.

`delete-usage-plan`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-usage-plan`.

AWS CLI

Eliminación de un plan de uso

Comando:

```
aws apigateway delete-usage-plan --usage-plan-id a1b2c3
```

- Para obtener información sobre la API, consulte DeleteUsagePlan en la Referencia de comandos de la AWS CLI.

`flush-stage-authorizers-cache`

En el siguiente ejemplo de código, se muestra cómo utilizar `flush-stage-authorizers-cache`.

AWS CLI

Vaciado de todas las entradas de la caché del autorizador en una etapa

Comando:

```
aws apigateway flush-stage-authorizers-cache --rest-api-id 1234123412 --stage-
name dev
```

- Para obtener información sobre la API, consulte FlushStageAuthorizersCache en la Referencia de comandos de la AWS CLI.

`flush-stage-cache`

En el siguiente ejemplo de código, se muestra cómo utilizar `flush-stage-cache`.

AWS CLI

Vaciado de la caché de una etapa de la API

En el siguiente ejemplo de `flush-stage-cache`, se vacía la caché de una etapa.

```
aws apigateway flush-stage-cache \
    --rest-api-id 1234123412 \
    --stage-name dev
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Vaciar la caché de etapas de API en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte FlushStageCache en la Referencia de comandos de la AWS CLI.

`generate-client-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `generate-client-certificate`.

AWS CLI

Creación de un certificado SSL del cliente

Comando:

```
aws apigateway generate-client-certificate --description 'My First Client
 Certificate'
```

- Para obtener información sobre la API, consulte GenerateClientCertificate en la Referencia de comandos de la AWS CLI.

`get-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-account`.

AWS CLI

Para obtener la configuración de cuenta de API Gateway

Comando:

```
aws apigateway get-account
```

Salida:

```
{
    "cloudwatchRoleArn": "arn:aws:iam::123412341234:role/
APIGatewayToCloudWatchLogsRole",
    "throttleSettings": {
        "rateLimit": 500.0,
        "burstLimit": 1000
    }
}
```

- Para obtener información sobre la API, consulte GetAccount en la Referencia de comandos de la AWS CLI.

`get-api-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-api-key`.

AWS CLI

Para obtener información acerca de una clave de API específica

Comando:

```
aws apigateway get-api-key --api-key 8bklk8bl1k3sB38D9B3l0enyWT8c09B30lkq0blk
```

Salida:

```
{
    "description": "My first key",
    "enabled": true,
    "stageKeys": [
        "a1b2c3d4e5/dev",
        "e5d4c3b2a1/dev"
    ],
    "lastUpdatedDate": 1456184515,
    "createdDate": 1456184452,
    "id": "8bklk8bl1k3sB38D9B3l0enyWT8c09B30lkq0blk",
    "name": "My key"
}
```

- Para obtener información sobre la API, consulte GetApiKey en la Referencia de comandos de la AWS CLI.

`get-api-keys`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-api-keys`.

AWS CLI

Para obtener la lista de claves de API

Comando:

```
aws apigateway get-api-keys
```

Salida:

```
{
    "items": [
        {
            "description": "My first key",
            "enabled": true,
            "stageKeys": [
                "a1b2c3d4e5/dev",
                "e5d4c3b2a1/dev"
            ],
            "lastUpdatedDate": 1456184515,
            "createdDate": 1456184452,
            "id": "8bklk8bl1k3sB38D9B3l0enyWT8c09B30lkq0blk",
            "name": "My key"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetApiKeys en la Referencia de comandos de la AWS CLI.

`get-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-authorizer`.

AWS CLI

Para obtener la configuración del autorizador por API de API Gateway

Comando:

```
aws apigateway get-authorizer --rest-api-id 1234123412 --authorizer-id gfi4n3
```

Salida:

```
{
    "authorizerResultTtlInSeconds": 300,
    "name": "MyAuthorizer",
    "type": "TOKEN",
    "identitySource": "method.request.header.Authorization",
    "authorizerUri": "arn:aws:apigateway:us-west-2:lambda:path/2015-03-31/functions/
arn:aws:lambda:us-west-2:123412341234:function:authorizer_function/invocations",
    "id": "gfi4n3"
}
```

- Para obtener información sobre la API, consulte GetAuthorizer en la Referencia de comandos de la AWS CLI.

`get-authorizers`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-authorizers`.

AWS CLI

Para obtener la lista de autorizadores de una API de REST

Comando:

```
aws apigateway get-authorizers --rest-api-id 1234123412
```

Salida:

```
{
    "items": [
        {
            "name": "MyAuthorizer",
```

```
            "authorizerUri": "arn:aws:apigateway:us-west-2:lambda:path/2015-03-31/
functions/arn:aws:lambda:us-west-2:123412341234:function:My_Authorizer_Function/
invocations",
            "authorizerResultTtlInSeconds": 300,
            "identitySource": "method.request.header.Authorization",
            "type": "TOKEN",
            "id": "gfi4n3"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetAuthorizers en la Referencia de comandos de la AWS CLI.

`get-base-path-mapping`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-base-path-mapping`.

AWS CLI

Obtención de la asignación de ruta base para un nombre de dominio personalizado

Comando:

```
aws apigateway get-base-path-mapping --domain-name subdomain.domain.tld --base-
path v1
```

Salida:

```
{
    "basePath": "v1",
    "restApiId": "1234w4321e",
    "stage": "api"
}
```

- Para obtener información sobre la API, consulte GetBasePathMapping en la Referencia de comandos de la AWS CLI.

`get-base-path-mappings`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-base-path-mappings`.

AWS CLI

Para obtener las asignaciones de ruta base de un nombre de dominio personalizado

Comando:

```
aws apigateway get-base-path-mappings --domain-name subdomain.domain.tld
```

Salida:

```
{
    "items": [
        {
            "basePath": "(none)",
            "restApiId": "1234w4321e",
            "stage": "dev"
        },
        {
            "basePath": "v1",
            "restApiId": "1234w4321e",
            "stage": "api"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetBasePathMappings en la Referencia de comandos de la AWS CLI.

`get-client-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-client-certificate`.

AWS CLI

Para obtener un certificado de cliente

Comando:

```
aws apigateway get-client-certificate --client-certificate-id a1b2c3
```

- Para obtener información sobre la API, consulte GetClientCertificate en la Referencia de comandos de la AWS CLI.

`get-client-certificates`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-client-certificates`.

AWS CLI

Para obtener una lista de certificados de cliente

Comando:

```
aws apigateway get-client-certificates
```

Salida:

```
{
    "items": [
        {
            "pemEncodedCertificate": "-----BEGIN CERTIFICATE----- <certificate
 content> -----END CERTIFICATE-----",
            "clientCertificateId": "a1b2c3",
            "expirationDate": 1483556561,
            "description": "My Client Certificate",
            "createdDate": 1452020561
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetClientCertificates en la Referencia de comandos de la AWS CLI.

`get-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-deployment`.

AWS CLI

Para obtener información acerca de una implementación

Comando:

```
aws apigateway get-deployment --rest-api-id 1234123412 --deployment-id ztt4m2
```

Salida:

```
{
    "description": "myDeployment",
    "id": "ztt4m2",
    "createdDate": 1455218022
}
```

- Para obtener información sobre la API, consulte GetDeployment en la Referencia de comandos de la AWS CLI.

`get-deployments`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-deployments`.

AWS CLI

Para obtener una lista de implementaciones de una API de REST

Comando:

```
aws apigateway get-deployments --rest-api-id 1234123412
```

Salida:

```
{
    "items": [
        {
            "createdDate": 1453797217,
            "id": "0a2b4c",
            "description": "Deployed my API for the first time"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetDeployments en la Referencia de comandos de la AWS CLI.

`get-domain-name-access-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-domain-name-access-associations`.

AWS CLI

Ejemplo 1: muestra de todas las asociaciones de acceso a nombres de dominio

En el siguiente ejemplo de `get-domain-name-access-associations`, se muestran todas las asociaciones de acceso a nombres de dominio.

```
aws apigateway get-domain-name-access-associations
```

Salida:

```
{
    "items": [
        {
        "domainNameAccessAssociationArn": "arn:aws:apigateway:us-
west-2:012345678910:/domainnameaccessassociations/domainname/my.private.domain.tld/
vpcesource/vpce-abcd1234efg
        "accessAssociationSource": "vpce-abcd1234efg",
        "accessAssociationSourceType": "VPCE",
        "domainNameArn" : "arn:aws:apigateway:us-west-2:111122223333:/domainnames/
private.example.com+abcd1234"
        }
    ]
}
```

Para obtener más información, consulte Nombres de dominio personalizados para las API privadas en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

Ejemplo 2: muestra de todas las asociaciones de acceso a nombres de dominio que pertenecen a esta cuenta de AWS

En el siguiente ejemplo de `get-domain-name-access-associations`, se muestran todas las asociaciones de acceso a nombres de dominio que pertenecen a la cuenta de AWS actual.

```
aws apigateway get-domain-name-access-associations \
```

```
    --resource-owner SELF
```

Salida:

```
{
    "items": [
        {
        "domainNameAccessAssociationArn": "arn:aws:apigateway:us-
west-2:012345678910:/domainnameaccessassociations/domainname/my.private.domain.tld/
vpcesource/vpce-abcd1234efg
        "accessAssociationSource": "vpce-abcd1234efg",
        "accessAssociationSourceType": "VPCE",
        "domainNameArn" : "arn:aws:apigateway:us-west-2:111122223333:/domainnames/
private.example.com+abcd1234"
        }
    ]
}
```

Para obtener más información, consulte Nombres de dominio personalizados para las API privadas en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetDomainNameAccessAssociations en la Referencia del comando de la AWS CLI.

`get-domain-name`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-domain-name`.

AWS CLI

Ejemplo 1: obtención de información sobre un nombre de dominio personalizado público

En el siguiente ejemplo de `get-domain-name`, se obtiene información sobre un nombre de dominio personalizado público.

```
aws apigateway get-domain-name \
    --domain-name api.domain.tld
```

Salida:

```
{
```

```
    "domainName": "api.domain.tld",
    "distributionDomainName": "d1a2f3a4c5o6d.cloudfront.net",
    "certificateName": "uploadedCertificate",
    "certificateUploadDate": 1462565487
}
```

Para obtener más información, consulte Nombre de dominio personalizado para las API de REST públicas en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

Ejemplo 2: obtención de información sobre un nombre de dominio personalizado privado

En el siguiente ejemplo de `get-domain-name`, se obtiene información sobre un nombre de dominio personalizado privado.

```
aws apigateway get-domain-name \
    --domain-name api.private.domain.tld \
    --domain-name-id abcd1234
```

Salida:

```
{
    "domainName": "my.private.domain.tld",
    "domainNameId": "abcd1234",
    "domainNameArn": "arn:aws:apigateway:us-east-1:012345678910:/domainnames/
my.private.domain.tld+abcd1234",
    "certificateArn": "arn:aws:acm:us-east-1:012345678910:certificate/fb1b9770-
a305-495d-aefb-27e5e101ff3",
    "certificateUploadDate": "2024-09-10T10:31:20-07:00",
    "endpointConfiguration": {
        "types": [
            "PRIVATE"
        ]
    },
    "domainNameStatus": "AVAILABLE",
    "securityPolicy": "TLS_1_2",
    "policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":
\"Allow\",\"Principal\":\"*\",\"Action\":\"execute-api:Invoke\",\"Resource\":
\"arn:aws:execute-api:us-east-1:012345678910:/domainnames/my.private.domain.tld
+abcd1234\"},{\"Effect\":\"Deny\",\"Principal\":\"*\",\"Action\":\"execute-
api:Invoke\",\"Resource\":\"arn:aws:execute-api:us-east-1:012345678910:/domainnames/
my.private.domain.tld+abcd1234\",\"Condition\":{\"StringNotEquals\":{\"aws:SourceVpc
\":\"vpc-1a2b3c4d\"}}}]}"
```

```
}
```

Para obtener más información, consulte Nombre de dominio personalizado para las API de REST públicas en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetDomainName en la Referencia de comandos de la AWS CLI.

`get-domain-names`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-domain-names`.

AWS CLI

Ejemplo 1: obtención de una lista de nombres de dominio personalizados

El comando `get-domain-names` siguiente obtiene una lista de nombres de dominio.

```
aws apigateway get-domain-names
```

Salida:

```
{
    "items": [
        {
            "distributionDomainName": "d9511k3l09bkd.cloudfront.net",
            "certificateUploadDate": 1452812505,
            "certificateName": "my_custom_domain-certificate",
            "domainName": "subdomain.domain.tld"
        }
    ]
}
```

Para obtener más información, consulte Nombres de dominio personalizados para las API privadas en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

Ejemplo 2: obtención de una lista de nombres de dominio personalizados que pertenecen a esta cuenta de AWS

El comando `get-domain-names` siguiente obtiene una lista de nombres de dominio que pertenecen a esta cuenta de AWS.

```
aws apigateway get-domain-names \
    --resource-owner SELF
```

Salida:

```
{
    "items": [
        {
            "domainName": "my.domain.tld",
            "domainNameArn": "arn:aws:apigateway:us-east-1::/domainnames/
my.private.domain.tld",
            "certificateUploadDate": "2024-08-15T17:02:55-07:00",
            "regionalDomainName": "d-abcd1234.execute-api.us-east-1.amazonaws.com",
            "regionalHostedZoneId": "Z1UJRXOUMOOFQ8",
            "regionalCertificateArn": "arn:aws:acm:us-
east-1:012345678910:certificate/fb1b9770-a305-495d-aefb-27e5e101ff3",
            "endpointConfiguration": {
                "types": [
                    "REGIONAL"
                ]
            },
            "domainNameStatus": "AVAILABLE",
            "securityPolicy": "TLS_1_2"
        },
        {
            "domainName": "my.private.domain.tld",
            "domainNameId": "abcd1234",
            "domainNameArn": "arn:aws:apigateway:us-east-1:012345678910:/
domainnames/my.private.domain.tld+abcd1234",
            "certificateArn": "arn:aws:acm:us-east-1:012345678910:certificate/
fb1b9770-a305-495d-aefb-27e5e101ff3",
            "certificateUploadDate": "2024-11-26T11:44:40-08:00",
            "endpointConfiguration": {
                "types": [
                    "PRIVATE"
                ]
            },
            "domainNameStatus": "AVAILABLE",
            "securityPolicy": "TLS_1_2"
        }
    ]
}
```

Para obtener más información, consulte Nombres de dominio personalizados para las API privadas en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

Ejemplo 3: obtención de una lista de nombres de dominio personalizados que pertenecen a otras cuentas de AWS con las que puede crear una asociación de acceso a nombres de dominio.

El comando `get-domain-names` siguiente obtiene una lista de los nombres de dominio que pertenecen a otras cuentas de AWS a las que tiene acceso para crear una asociación de acceso a nombres de dominio.

```
aws apigateway get-domain-names \
    --resource-owner OTHER_ACCOUNTS
```

Salida:

```
{
    "items": [
        {
            "domainName": "my.private.domain.tld",
            "domainNameId": "abcd1234",
            "domainNameArn": "arn:aws:apigateway:us-east-1:012345678910:/
domainnames/my.private.domain.tld+abcd1234"
        }
    ]
}
```

Para obtener más información, consulte Nombres de dominio personalizados para las API privadas en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetDomainNames en la Referencia de comandos de la AWS CLI.

`get-export`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-export`.

AWS CLI

Para obtener la plantilla Swagger de JSON de una etapa

Comando:

```
aws apigateway get-export --rest-api-id a1b2c3d4e5 --stage-name dev --export-
type swagger /path/to/filename.json
```

Para obtener la plantilla Swagger de JSON + las extensiones de API Gateway para una etapa

Comando:

```
aws apigateway get-export --parameters extensions='integrations' --rest-api-
id a1b2c3d4e5 --stage-name dev --export-type swagger /path/to/filename.json
```

Para obtener la plantilla Swagger de JSON + las extensiones de Postman de una etapa

Comando:

```
aws apigateway get-export --parameters extensions='postman' --rest-api-id a1b2c3d4e5
 --stage-name dev --export-type swagger /path/to/filename.json
```

- Para obtener información sobre la API, consulte GetExport en la Referencia de comandos de la AWS CLI.

`get-integration-response`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-integration-response`.

AWS CLI

Para obtener la configuración de la respuesta de integración para un método HTTP definido en un recurso de la API de REST

Comando:

```
aws apigateway get-integration-response --rest-api-id 1234123412 --resource-
id y9h6rt --http-method GET --status-code 200
```

Salida:

```
{
    "statusCode": "200",
    "responseTemplates": {
        "application/json": null
```

```
    }
}
```

- Para obtener información sobre la API, consulte GetIntegrationResponse en la Referencia de comandos de la AWS CLI.

`get-integration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-integration`.

AWS CLI

Para obtener la configuración de la integración para un método HTTP definido en un recurso de la API de REST

Comando:

```
aws apigateway get-integration --rest-api-id 1234123412 --resource-id y9h6rt --http-method GET
```

Salida:

```
{
    "httpMethod": "POST",
    "integrationResponses": {
        "200": {
            "responseTemplates": {
                "application/json": null
            },
            "statusCode": "200"
        }
    },
    "cacheKeyParameters": [],
    "type": "AWS",
    "uri": "arn:aws:apigateway:us-west-2:lambda:path/2015-03-31/functions/
arn:aws:lambda:us-west-2:123412341234:function:My_Function/invocations",
    "cacheNamespace": "y9h6rt"
}
```

- Para obtener información sobre la API, consulte GetIntegration en la Referencia de comandos de la AWS CLI.

get-method-response

En el siguiente ejemplo de código, se muestra cómo utilizar `get-method-response`.

AWS CLI

Para obtener la configuración del recurso de respuesta de método para un método HTTP definido en un recurso de la API de REST

Comando:

```
aws apigateway get-method-response --rest-api-id 1234123412 --resource-id y9h6rt --
http-method GET --status-code 200
```

Salida:

```
{
    "responseModels": {
        "application/json": "Empty"
    },
    "statusCode": "200"
}
```

- Para obtener información sobre la API, consulte GetMethodResponse en la Referencia de comandos de la AWS CLI.

get-method

En el siguiente ejemplo de código, se muestra cómo utilizar `get-method`.

AWS CLI

Para obtener la configuración del recurso de método para un método HTTP definido en un recurso de la API de REST

Comando:

```
aws apigateway get-method --rest-api-id 1234123412 --resource-id y9h6rt --http-
method GET
```

Salida:

```
{
    "apiKeyRequired": false,
    "httpMethod": "GET",
    "methodIntegration": {
        "integrationResponses": {
            "200": {
                "responseTemplates": {
                    "application/json": null
                },
                "statusCode": "200"
            }
        },
        "cacheKeyParameters": [],
        "uri": "arn:aws:apigateway:us-west-2:lambda:path/2015-03-31/functions/
arn:aws:lambda:us-west-2:123412341234:function:My_Function/invocations",
        "httpMethod": "POST",
        "cacheNamespace": "y9h6rt",
        "type": "AWS"
    },
    "requestParameters": {},
    "methodResponses": {
        "200": {
            "responseModels": {
                "application/json": "Empty"
            },
            "statusCode": "200"
        }
    },
    "authorizationType": "NONE"
}
```

- Para obtener información sobre la API, consulte GetMethod en la Referencia de comandos de la AWS CLI.

`get-model-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-model-template`.

AWS CLI

Para obtener la plantilla de asignación de un modelo definido en una API de REST

Comando:

```
aws apigateway get-model-template --rest-api-id 1234123412 --model-name Empty
```

Salida:

```
{
    "value": "#set($inputRoot = $input.path('$'))\n{ }"
}
```

- Para obtener información sobre la API, consulte GetModelTemplate en la Referencia de comandos de la AWS CLI.

`get-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-model`.

AWS CLI

Para obtener la configuración de un modelo definido en una API de REST

Comando:

```
aws apigateway get-model --rest-api-id 1234123412 --model-name Empty
```

Salida:

```
{
    "contentType": "application/json",
    "description": "This is a default empty schema model",
    "name": "Empty",
    "id": "etd5w5",
    "schema": "{\n  \"$schema\": \"http://json-schema.org/draft-04/schema#\",\n
 \"title\" : \"Empty Schema\",\n  \"type\" : \"object\"\n}"
}
```

- Para obtener información sobre la API, consulte GetModel en la Referencia de comandos de la AWS CLI.

`get-models`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-models`.

AWS CLI

Para obtener una lista de modelos de una API de REST

Comando:

```
aws apigateway get-models --rest-api-id 1234123412
```

Salida:

```
{
    "items": [
        {
            "description": "This is a default error schema model",
            "schema": "{\n  \"$schema\" : \"http://json-schema.org/draft-04/schema#
\",\n  \"title\" : \"Error Schema\",\n  \"type\" : \"object\",\n  \"properties\" :
 {\n    \"message\" : { \"type\" : \"string\" }\n  }\n}",
            "contentType": "application/json",
            "id": "7tpbze",
            "name": "Error"
        },
        {
            "description": "This is a default empty schema model",
            "schema": "{\n  \"$schema\": \"http://json-schema.org/draft-04/schema#
\",\n  \"title\" : \"Empty Schema\",\n  \"type\" : \"object\"\n}",
            "contentType": "application/json",
            "id": "etd5w5",
            "name": "Empty"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetModels en la Referencia de comandos de la AWS CLI.

`get-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource`.

AWS CLI

Para obtener información sobre un recurso

Comando:

```
aws apigateway get-resource --rest-api-id 1234123412 --resource-id zwo0y3
```

Salida:

```
{
    "path": "/path",
    "pathPart": "path",
    "id": "zwo0y3",
    "parentId": "uyokt6ij2g"
}
```

- Para obtener detalles sobre la API, consulte GetResource en la Referencia de comandos de la AWS CLI.

`get-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resources`.

AWS CLI

Obtención de una lista de recursos para una API de REST

Comando:

```
aws apigateway get-resources --rest-api-id 1234123412
```

Salida:

```
{
    "items": [
        {
            "path": "/resource/subresource",
            "resourceMethods": {
                "POST": {}
            },
```

```
            "id": "024ace",
            "pathPart": "subresource",
            "parentId": "ai5b02"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte GetResources en la Referencia de comandos de la AWS CLI.

`get-rest-api`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-rest-api`.

AWS CLI

Para obtener información sobre una API

Comando:

```
aws apigateway get-rest-api --rest-api-id 1234123412
```

Salida:

```
{
    "name": "myAPI",
    "id": "o1y243m4f5",
    "createdDate": 1453416433
}
```

- Para obtener información sobre la API, consulte GetRestApi en la Referencia de comandos de la AWS CLI.

`get-rest-apis`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-rest-apis`.

AWS CLI

Para obtener una lista de las API de REST

Comando:

```
aws apigateway get-rest-apis
```

Salida:

```
{
    "items": [
        {
            "createdDate": 1438884790,
            "id": "12s44z21rb",
            "name": "My First API"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetRestApis en la Referencia de comandos de la AWS CLI.

`get-sdk`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-sdk`.

AWS CLI

Para obtener el SDK para Android de una etapa de API de REST

Comando:

```
aws apigateway get-sdk --rest-api-id 1234123412 --stage-name dev --sdk-type android
 --parameters
 groupId='com.mycompany',invokerPackage='com.mycompany.clientsdk',artifactId='Mycompany-
client',artifactVersion='1.0.0' /path/to/android_sdk.zip
```

Salida:

```
{
    "contentType": "application/octet-stream",
    "contentDisposition": "attachment; filename=\"android_2016-02-22_23-52Z.zip\""
}
```

Para obtener el SDK para IOS de una etapa de API de REST

Comando:

```
aws apigateway get-sdk --rest-api-id 1234123412 --stage-name dev --sdk-
type objectivec --parameters classPrefix='myprefix' /path/to/iOS_sdk.zip
```

Salida:

```
{
    "contentType": "application/octet-stream",
    "contentDisposition": "attachment; filename=\"objectivec_2016-02-22_23-52Z.zip
\""
}
```

Para obtener el SDK para Javascript de una etapa de API de REST

Comando:

```
aws apigateway get-sdk --rest-api-id 1234123412 --stage-name dev --sdk-
type javascript /path/to/javascript_sdk.zip
```

Salida:

```
{
    "contentType": "application/octet-stream",
    "contentDisposition": "attachment; filename=\"javascript_2016-02-22_23-52Z.zip
\""
}
```

- Para obtener información sobre la API, consulte GetSdk en la Referencia de comandos de la AWS CLI.

`get-stage`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-stage`.

AWS CLI

Para obtener información sobre una etapa de la API

Comando:

```
aws apigateway get-stage --rest-api-id 1234123412 --stage-name dev
```

Salida:

```
{
    "stageName": "dev",
    "cacheClusterSize": "0.5",
    "cacheClusterEnabled": false,
    "cacheClusterStatus": "NOT_AVAILABLE",
    "deploymentId": "rbh1fj",
    "lastUpdatedDate": 1466802961,
    "createdDate": 1460682074,
    "methodSettings": {
        "*/*": {
            "cacheTtlInSeconds": 300,
            "loggingLevel": "INFO",
            "dataTraceEnabled": false,
            "metricsEnabled": true,
            "unauthorizedCacheControlHeaderStrategy":
 "SUCCEED_WITH_RESPONSE_HEADER",
            "throttlingRateLimit": 500.0,
            "cacheDataEncrypted": false,
            "cachingEnabled": false,
            "throttlingBurstLimit": 1000,
            "requireAuthorizationForCacheControl": true
        },
        "~1resource/GET": {
            "cacheTtlInSeconds": 300,
            "loggingLevel": "INFO",
            "dataTraceEnabled": false,
            "metricsEnabled": true,
            "unauthorizedCacheControlHeaderStrategy":
 "SUCCEED_WITH_RESPONSE_HEADER",
            "throttlingRateLimit": 500.0,
            "cacheDataEncrypted": false,
            "cachingEnabled": false,
            "throttlingBurstLimit": 1000,
            "requireAuthorizationForCacheControl": true
        }
    }
}
```

- Para obtener información sobre la API, consulte GetStage en la Referencia de comandos de la AWS CLI.

`get-stages`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-stages`.

AWS CLI

Para obtener una lista de etapas de una API de REST

Comando:

```
aws apigateway get-stages --rest-api-id 1234123412
```

Salida:

```
{
    "item": [
        {
            "stageName": "dev",
            "cacheClusterSize": "0.5",
            "cacheClusterEnabled": true,
            "cacheClusterStatus": "AVAILABLE",
            "deploymentId": "123h64",
            "lastUpdatedDate": 1456185138,
            "createdDate": 1453589092,
            "methodSettings": {
                "~1resource~1subresource/POST": {
                    "cacheTtlInSeconds": 300,
                    "loggingLevel": "INFO",
                    "dataTraceEnabled": true,
                    "metricsEnabled": true,
                    "throttlingRateLimit": 500.0,
                    "cacheDataEncrypted": false,
                    "cachingEnabled": false,
                    "throttlingBurstLimit": 1000
                }
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetStages en la Referencia de comandos de la AWS CLI.

`get-usage-plan-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-usage-plan-key`.

AWS CLI

Para obtener los detalles de una clave de API asociada a un plan de uso

Comando:

```
aws apigateway get-usage-plan-key --usage-plan-id a1b2c3 --key-
id 1NbjQzMReAkeEQPNAW8r3dXsU2rDD7fc7f2Sipnu
```

- Para obtener información sobre la API, consulte GetUsagePlanKey en la Referencia de comandos de la AWS CLI.

`get-usage-plan-keys`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-usage-plan-keys`.

AWS CLI

Para obtener la lista de claves de API asociadas a un plan de uso

Comando:

```
aws apigateway get-usage-plan-keys --usage-plan-id a1b2c3
```

- Para obtener información sobre la API, consulte GetUsagePlanKeys en la Referencia de comandos de la AWS CLI.

`get-usage-plan`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-usage-plan`.

AWS CLI

Para obtener los detalles de un plan de uso

Comando:

```
aws apigateway get-usage-plan --usage-plan-id a1b2c3
```

- Para obtener información sobre la API, consulte GetUsagePlan en la Referencia de comandos de la AWS CLI.

`get-usage-plans`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-usage-plans`.

AWS CLI

Para obtener los detalles de todos los planes de uso

Comando:

```
aws apigateway get-usage-plans
```

- Para obtener información sobre la API, consulte GetUsagePlans en la Referencia de comandos de la AWS CLI.

`get-usage`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-usage`.

AWS CLI

Para obtener los detalles de uso de un plan de uso

Comando:

```
aws apigateway get-usage --usage-plan-id a1b2c3 --start-date "2016-08-16" --end-
date "2016-08-17"
```

- Para obtener información sobre la API, consulte GetUsage en la Referencia de comandos de la AWS CLI.

`import-rest-api`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-rest-api`.

AWS CLI

Importación de una plantilla Swagger y creación de una API

Comando:

```
aws apigateway import-rest-api --body 'file:///path/to/API_Swagger_template.json'
```

- Para obtener información sobre la API, consulte ImportRestApi en la Referencia de comandos de la AWS CLI.

`put-integration-response`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-integration-response`.

AWS CLI

Para crear una respuesta de integración como respuesta predeterminada con una plantilla de mapeo definida

Comando:

```
aws apigateway put-integration-response --rest-api-id 1234123412 --resource-
id a1b2c3 --http-method GET --status-code 200 --selection-pattern "" --response-
templates '{"application/json": "{\"json\": \"template\"}"}'
```

Para crear una respuesta de integración con una expresión regular de 400 y un valor de encabezado definido estáticamente

Comando:

```
aws apigateway put-integration-response --rest-api-id 1234123412 --resource-
id a1b2c3 --http-method GET --status-code 400 --selection-pattern 400 --response-
parameters '{"method.response.header.custom-header": "'"'"'custom-value'"'"'"}'
```

- Para obtener información sobre la API, consulte PutIntegrationResponse en la Referencia de comandos de la AWS CLI.

`put-integration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-integration`.

AWS CLI

Creación de una solicitud de integración MOCK

Comando:

```
aws apigateway put-integration --rest-api-id 1234123412 --resource-id a1b2c3 --http-
method GET --type MOCK --request-templates '{ "application/json": "{\"statusCode\":
 200}" }'
```

Para crear una solicitud de integración HTTP

Comando:

```
aws apigateway put-integration --rest-api-id 1234123412 --resource-id a1b2c3 --http-
method GET --type HTTP --integration-http-method GET --uri 'https://domain.tld/path'
```

Creación de una solicitud de integración AWS con un punto de conexión de función de Lambda

Comando:

```
aws apigateway put-integration --rest-api-id 1234123412 --resource-
id a1b2c3 --http-method GET --type AWS --integration-http-method POST --uri
 'arn:aws:apigateway:us-west-2:lambda:path/2015-03-31/functions/arn:aws:lambda:us-
west-2:123412341234:function:function_name/invocations'
```

- Para obtener información acerca de la API, consulte PutIntegration en la Referencia de comandos de la AWS CLI.

`put-method-response`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-method-response`.

AWS CLI

Creación de una respuesta de método en el código de estado especificado con un encabezado de respuesta de método personalizado

Comando:

```
aws apigateway put-method-response --rest-api-id 1234123412 --
resource-id a1b2c3 --http-method GET --status-code 400 --response-
parameters "method.response.header.custom-header=false"
```

- Para obtener información sobre la API, consulta PutMethodResponse en la Referencia de comandos de la AWS CLI.

put-method

En el siguiente ejemplo de código, se muestra cómo utilizar `put-method`.

AWS CLI

Para crear un método para un recurso en una API sin autorización, sin clave de API y con un encabezado de solicitud de método personalizado

Comando:

```
aws apigateway put-method --rest-api-id 1234123412 --resource-id a1b2c3 --
http-method PUT --authorization-type "NONE" --no-api-key-required --request-
parameters "method.request.header.custom-header=false"
```

- Para obtener información sobre la API, consulte PutMethod en la Referencia de comandos de la AWS CLI.

put-rest-api

En el siguiente ejemplo de código, se muestra cómo utilizar `put-rest-api`.

AWS CLI

Sobrescritura de una API existente mediante una plantilla de Swagger

Comando:

```
aws apigateway put-rest-api --rest-api-id 1234123412 --mode overwrite --body
 'fileb:///path/to/API_Swagger_template.json'
```

Combinación de una plantilla de Swagger con una API existente

Comando:

```
aws apigateway put-rest-api --rest-api-id 1234123412 --mode merge --body 'fileb:///
path/to/API_Swagger_template.json'
```

- Para obtener información sobre la API, consulte PutRestApi en la Referencia de comandos de la AWS CLI.

`reject-domain-name-access-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `reject-domain-name-access-association`.

AWS CLI

Rechazo de una asociación de acceso a nombres de dominio

En el siguiente ejemplo de `reject-domain-name-access-association`, se rechaza una asociación de acceso a un nombre de dominio entre un nombre de dominio personalizado privado y un punto de conexión de VPC.

```
aws apigateway reject-domain-name-access-association \
    --domain-name-access-association-arn arn:aws:apigateway:us-west-2:012345678910:/
domainnameaccessassociations/domainname/my.private.domain.tld/vpcesource/vpce-
abcd1234efg \
    --domain-name-arn arn:aws:apigateway:us-east-1:012345678910:/domainnames/
my.private.domain.tld+abcd1234
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Nombres de dominio personalizados para las API privadas en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte RejectDomainNameAccessAssociation en la Referencia de comandos de la AWS CLI.

`test-invoke-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `test-invoke-authorizer`.

AWS CLI

Prueba de invocación de una solicitud a un autorizador personalizado que incluya el encabezado y el valor necesarios

Comando:

```
aws apigateway test-invoke-authorizer --rest-api-id 1234123412 --authorizer-
id 5yid1t --headers Authorization='Value'
```

- Para obtener información sobre la API, consulte TestInvokeAuthorizer en la Referencia de comandos de la AWS CLI.

`test-invoke-method`

En el siguiente ejemplo de código, se muestra cómo utilizar `test-invoke-method`.

AWS CLI

Prueba de invocación del recurso raíz en una API mediante una solicitud GET

Comando:

```
aws apigateway test-invoke-method --rest-api-id 1234123412 --resource-id avl5sg8fw8
 --http-method GET --path-with-query-string '/'
```

Prueba de invocación de un subrecurso en una API mediante una solicitud GET con un valor de parámetro de ruta especificado

Comando:

```
aws apigateway test-invoke-method --rest-api-id 1234123412 --resource-id 3gapai --
http-method GET --path-with-query-string '/pets/1'
```

- Para obtener información sobre la API, consulte TestInvokeMethod en la Referencia de comandos de la AWS CLI.

`update-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-account`.

AWS CLI

Cambio del rol de IAM ARN para iniciar sesión en los registros de CloudWatch

Comando:

```
aws apigateway update-account --patch-operations op='replace',path='/
cloudwatchRoleArn',value='arn:aws:iam::123412341234:role/APIGatewayToCloudWatchLogs'
```

Salida:

```
{
    "cloudwatchRoleArn": "arn:aws:iam::123412341234:role/
APIGatewayToCloudWatchLogs",
    "throttleSettings": {
        "rateLimit": 1000.0,
        "burstLimit": 2000
    }
}
```

- Para obtener información sobre la API, consulte UpdateAccount en la Referencia de comandos de la AWS CLI.

update-api-key

En el siguiente ejemplo de código, se muestra cómo utilizar `update-api-key`.

AWS CLI

Cambio del nombre de una clave de API

Comando:

```
aws apigateway update-api-key --api-key sNvjQDMReA1eEQPNAW8r37XsU2rDD7fc7m2SiMnu --
patch-operations op='replace',path='/name',value='newName'
```

Salida:

```
{
    "description": "currentDescription",
```

```
    "enabled": true,
    "stageKeys": [
        "41t2j324r5/dev"
    ],
    "lastUpdatedDate": 1470086052,
    "createdDate": 1445460347,
    "id": "sNvjQDMReA1vEQPNzW8r3dXsU2rrD7fcjm2SiMnu",
    "name": "newName"
}
```

Deshabilitación de la clave de API

Comando:

```
aws apigateway update-api-key --api-key sNvjQDMReA1eEQPNAW8r37XsU2rDD7fc7m2SiMnu --
patch-operations op='replace',path='/enabled',value='false'
```

Salida:

```
{
    "description": "currentDescription",
    "enabled": false,
    "stageKeys": [
        "41t2j324r5/dev"
    ],
    "lastUpdatedDate": 1470086052,
    "createdDate": 1445460347,
    "id": "sNvjQDMReA1vEQPNzW8r3dXsU2rrD7fcjm2SiMnu",
    "name": "newName"
}
```

- Para obtener información sobre la API, consulte UpdateApiKey en la Referencia de comandos de la AWS CLI.

`update-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-authorizer`.

AWS CLI

Cambio del nombre del autorizador personalizado

Comando:

```
aws apigateway update-authorizer --rest-api-id 1234123412 --authorizer-id gfi4n3 --
patch-operations op='replace',path='/name',value='testAuthorizer'
```

Salida:

```
{
    "authType": "custom",
    "name": "testAuthorizer",
    "authorizerUri": "arn:aws:apigateway:us-west-2:lambda:path/2015-03-31/functions/
arn:aws:lambda:us-west-2:123412341234:function:customAuthorizer/invocations",
    "authorizerResultTtlInSeconds": 300,
    "identitySource": "method.request.header.Authorization",
    "type": "TOKEN",
    "id": "gfi4n3"
}
```

Cambio de la función de Lambda que invoca el autorizador personalizado

Comando:

```
aws apigateway update-authorizer --rest-api-id 1234123412 --authorizer-id gfi4n3 --
patch-operations op='replace',path='/authorizerUri',value='arn:aws:apigateway:us-
west-2:lambda:path/2015-03-31/functions/arn:aws:lambda:us-
west-2:123412341234:function:newAuthorizer/invocations'
```

Salida:

```
{
    "authType": "custom",
    "name": "testAuthorizer",
    "authorizerUri": "arn:aws:apigateway:us-west-2:lambda:path/2015-03-31/functions/
arn:aws:lambda:us-west-2:123412341234:function:newAuthorizer/invocations",
    "authorizerResultTtlInSeconds": 300,
    "identitySource": "method.request.header.Authorization",
    "type": "TOKEN",
    "id": "gfi4n3"
}
```

- Para obtener información sobre la API, consulte UpdateAuthorizer en la Referencia de comandos de la AWS CLI.

update-base-path-mapping

En el siguiente ejemplo de código, se muestra cómo utilizar `update-base-path-mapping`.

AWS CLI

Para cambiar la ruta base de un nombre de dominio personalizado

Comando:

```
aws apigateway update-base-path-mapping --domain-name api.domain.tld --base-
path prod --patch-operations op='replace',path='/basePath',value='v1'
```

Salida:

```
{
    "basePath": "v1",
    "restApiId": "1234123412",
    "stage": "api"
}
```

- Para obtener información sobre la API, consulte UpdateBasePathMapping en la Referencia de comandos de la AWS CLI.

update-client-certificate

En el siguiente ejemplo de código, se muestra cómo utilizar `update-client-certificate`.

AWS CLI

Actualización de la descripción de un certificado de cliente

Comando:

```
aws apigateway update-client-certificate --client-certificate-id a1b2c3 --patch-
operations op='replace',path='/description',value='My new description'
```

- Para obtener información sobre la API, consulte UpdateClientCertificate en la Referencia de comandos de la AWS CLI.

update-deployment

En el siguiente ejemplo de código, se muestra cómo utilizar `update-deployment`.

AWS CLI

Cambio de la descripción de una implementación

Comando:

```
aws apigateway update-deployment --rest-api-id 1234123412 --deployment-id ztt4m2 --
patch-operations op='replace',path='/description',value='newDescription'
```

Salida:

```
{
    "description": "newDescription",
    "id": "ztt4m2",
    "createdDate": 1455218022
}
```

- Para obtener más información sobre la API, consulte UpdateDeployment en la Referencia de comandos de la AWS CLI.

update-domain-name

En el siguiente ejemplo de código, se muestra cómo utilizar `update-domain-name`.

AWS CLI

Cambio del nombre de certificado de un dominio personalizado

En el siguiente ejemplo de `update-domain-name`, se cambia el nombre de certificado de un dominio personalizado.

```
aws apigateway update-domain-name \
    --domain-name api.domain.tld \
    --patch-operations op='replace',path='/certificateArn',value='arn:aws:acm:us-
west-2:111122223333:certificate/CERTEXAMPLE123EXAMPLE'
```

Salida:

```
{
    "domainName": "api.domain.tld",
    "distributionDomainName": "d123456789012.cloudfront.net",
    "certificateArn": "arn:aws:acm:us-west-2:111122223333:certificate/
CERTEXAMPLE123EXAMPLE",
    "certificateUploadDate": 1462565487
}
```

Para obtener más información, consulte Nombre de dominio personalizado para las API de REST en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte UpdateDomainName en la Referencia de comandos de la AWS CLI.

`update-integration-response`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-integration-response`.

AWS CLI

Cambio del encabezado de una respuesta de integración para que tenga una asignación estática de '*'

Comando:

```
aws apigateway update-integration-response --rest-api-id 1234123412 --
resource-id 3gapai --http-method GET --status-code 200 --patch-operations
 op='replace',path='/responseParameters/method.response.header.Access-Control-Allow-
Origin',value='"'"'*'"'"'
```

Salida:

```
{
    "statusCode": "200",
    "responseParameters": {
        "method.response.header.Access-Control-Allow-Origin": "'*'"
    }
}
```

Eliminación de un encabezado de respuesta de integración

Comando:

```
aws apigateway update-integration-response --rest-api-id 1234123412 --resource-
id 3gapai --http-method GET --status-code 200 --patch-operations op='remove',path='/
responseParameters/method.response.header.Access-Control-Allow-Origin'
```

- Para obtener información sobre la API, consulte UpdateIntegrationResponse en la Referencia de comandos de la AWS CLI.

`update-integration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-integration`.

AWS CLI

Adición de la plantilla de asignación Content-Type: application/json configurada con Input Passthrough

Comando:

```
aws apigateway update-integration \
    --rest-api-id a1b2c3d4e5 \
    --resource-id a1b2c3 \
    --http-method POST \
    --patch-operations "op='add',path='/requestTemplates/application~1json'"
```

Actualización (sustitución) de la plantilla de asignación Content-Type: application/json configurada con una plantilla personalizada

Comando:

```
aws apigateway update-integration \
    --rest-api-id a1b2c3d4e5 \
    --resource-id a1b2c3 \
    --http-method POST \
    --patch-operations "op='replace',path='/requestTemplates/
application~1json',value='{"example": "json"}'"
```

Actualización (sustitución) de una plantilla personalizada asociada a Content-Type: application/json con Input Passthrough

Comando:

```
aws apigateway update-integration \
    --rest-api-id a1b2c3d4e5 \
    --resource-id a1b2c3 \
    --http-method POST \
    --patch-operations "op='replace',path='requestTemplates/application~1json'"
```

Eliminación de la plantilla de asignación Content-Type: application/json

Comando:

```
aws apigateway update-integration \
    --rest-api-id a1b2c3d4e5 \
    --resource-id a1b2c3 \
    --http-method POST \
    --patch-operations "op='remove',path='/requestTemplates/application~1json'"
```

- Para obtener información sobre la API, consulte UpdateIntegration en la Referencia de comandos de la AWS CLI.

update-method-response

En el siguiente ejemplo de código, se muestra cómo utilizar `update-method-response`.

AWS CLI

Creación de un nuevo encabezado de respuesta de método para la respuesta 200 en un método y definición como no obligatorio (predeterminado)

Comando:

```
aws apigateway update-method-response --rest-api-id 1234123412 --resource-
id a1b2c3 --http-method GET --status-code 200 --patch-operations op="add",path="/
responseParameters/method.response.header.custom-header",value="false"
```

Eliminación de un modelo de respuesta de la respuesta 200 en un método

Comando:

```
aws apigateway update-method-response --rest-api-id 1234123412 --resource-id a1b2c3
 --http-method GET --status-code 200 --patch-operations op="remove",path="/
responseModels/application~1json"
```

- Para obtener información sobre la API, consulte UpdateMethodResponse en la Referencia de comandos de la AWS CLI.

`update-method`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-method`.

AWS CLI

Ejemplo 1: cómo modificar un método para que exija una clave de API

En el siguiente ejemplo de `update-method`, se modifica el método para que exija una clave de API.

```
aws apigateway update-method \
    --rest-api-id 1234123412 \
    --resource-id a1b2c3 \
    --http-method GET \
    --patch-operations op="replace",path="/apiKeyRequired",value="true"
```

Salida:

```
{
    "httpMethod": "GET",
    "authorizationType": "NONE",
    "apiKeyRequired": true,
    "methodResponses": {
        "200": {
            "statusCode": "200",
            "responseModels": {}
        }
    },
    "methodIntegration": {
        "type": "AWS",
        "httpMethod": "POST",
        "uri": "arn:aws:apigateway:us-east-1:lambda:path/2015-03-31/functions/
arn:aws:lambda:us-east-1:123456789111:function:hello-world/invocations",
        "passthroughBehavior": "WHEN_NO_MATCH",
        "contentHandling": "CONVERT_TO_TEXT",
        "timeoutInMillis": 29000,
        "cacheNamespace": "h7i8j9",
        "cacheKeyParameters": [],
```

```
        "integrationResponses": {
            "200": {
                "statusCode": "200",
                "responseTemplates": {}
            }
        }
    }
}
```

Ejemplo 2: cómo modificar un método para que exija una autorización de IAM

En el siguiente ejemplo de `update-method`, se modifica el método para que exija una autorización de IAM.

```
aws apigateway update-method \
    --rest-api-id 1234123412 \
    --resource-id a1b2c3 \
    --http-method GET \
    --patch-operations op="replace",path="/authorizationType",value="AWS_IAM"
```

Salida:

```
 {
    "httpMethod": "GET",
    "authorizationType": "AWS_IAM",
    "apiKeyRequired": false,
    "methodResponses": {
        "200": {
            "statusCode": "200",
            "responseModels": {}
        }
    },
    "methodIntegration": {
        "type": "AWS",
        "httpMethod": "POST",
        "uri": "arn:aws:apigateway:us-east-1:lambda:path/2015-03-31/functions/
arn:aws:lambda:us-east-1:123456789111:function:hello-world/invocations",
        "passthroughBehavior": "WHEN_NO_MATCH",
        "contentHandling": "CONVERT_TO_TEXT",
        "timeoutInMillis": 29000,
        "cacheNamespace": "h7i8j9",
        "cacheKeyParameters": [],
        "integrationResponses": {
```

```
            "200": {
                "statusCode": "200",
                "responseTemplates": {}
            }
        }
    }
}
```

Ejemplo 3: cómo modificar un método para que exija una autorización de Lambda

En el siguiente ejemplo de `update-method`, se modifica el método para que exija una autorización de Lambda.

```
aws apigateway update-method --rest-api-id 1234123412 \
    --resource-id a1b2c3 \
    --http-method GET \
    --patch-operations op="replace",path="/authorizationType",value="CUSTOM"
 op="replace",path="/authorizerId",value="e4f5g6"
```

Salida:

```
 {
    "httpMethod": "GET",
    "authorizationType": "CUSTOM",
    "authorizerId" : "e4f5g6",
    "apiKeyRequired": false,
    "methodResponses": {
        "200": {
            "statusCode": "200",
            "responseModels": {}
        }
    },
    "methodIntegration": {
        "type": "AWS",
        "httpMethod": "POST",
        "uri": "arn:aws:apigateway:us-east-1:lambda:path/2015-03-31/functions/
arn:aws:lambda:us-east-1:123456789111:function:hello-world/invocations",
        "passthroughBehavior": "WHEN_NO_MATCH",
        "contentHandling": "CONVERT_TO_TEXT",
        "timeoutInMillis": 29000,
        "cacheNamespace": "h7i8j9",
        "cacheKeyParameters": [],
        "integrationResponses": {
```

```
            "200": {
                "statusCode": "200",
                "responseTemplates": {}
            }
        }
    }
}
```

Para obtener más información, consulte Creación, configuración y prueba de planes de uso con la CLI y la API de REST de API Gateway y Control y administración del acceso a las API de REST en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte UpdateMethod en la Referencia de comandos de la AWS CLI.

`update-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-model`.

AWS CLI

Cambio de la descripción de un modelo en una API

Comando:

```
aws apigateway update-model --rest-api-id 1234123412 --model-name 'Empty' --patch-operations op=replace,path=/description,value='New Description'
```

Cambio del esquema de un modelo en una API

Comando:

```
aws apigateway update-model --rest-api-id 1234123412 --model-name 'Empty' --patch-operations op=replace,path=/schema,value='"{ \"$schema\": \"http://json-schema.org/draft-04/schema#\", \"title\" : \"Empty Schema\", \"type\" : \"object\" }"'
```

- Para obtener información sobre la API, consulte UpdateModel en la Referencia de comandos de la AWS CLI.

`update-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-resource`.

AWS CLI

Desplazamiento y colocación de un recurso en un recurso principal distinto de una API

Comando:

```
aws apigateway update-resource --rest-api-id 1234123412 --resource-id 1a2b3c --
patch-operations op=replace,path=/parentId,value='3c2b1a'
```

Salida:

```
{
    "path": "/resource",
    "pathPart": "resource",
    "id": "1a2b3c",
    "parentId": "3c2b1a"
}
```

Cambio del nombre de un recurso (pathPart) en una API

Comando:

```
aws apigateway update-resource --rest-api-id 1234123412 --resource-id 1a2b3c --
patch-operations op=replace,path=/pathPart,value=newresourcename
```

Salida:

```
{
    "path": "/newresourcename",
    "pathPart": "newresourcename",
    "id": "1a2b3c",
    "parentId": "3c2b1a"
}
```

- Para obtener información sobre la API, consulte UpdateResource en la Referencia de comandos de la AWS CLI.

`update-rest-api`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-rest-api`.

AWS CLI

Cambio del nombre de una API

Comando:

```
aws apigateway update-rest-api --rest-api-id 1234123412 --patch-operations
 op=replace,path=/name,value='New Name'
```

Cambio de la descripción de una API

Comando:

```
aws apigateway update-rest-api --rest-api-id 1234123412 --patch-operations
 op=replace,path=/description,value='New Description'
```

- Para obtener información sobre la API, consulte UpdateRestApi en la Referencia de comandos de la AWS CLI.

`update-stage`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-stage`.

AWS CLI

Ejemplo 1: cómo anular la configuración de etapa de un recurso y un método

En el siguiente ejemplo de `update-stage`, se anula la configuración de etapa y se desactiva el registro completo de solicitudes y respuestas de un recurso y un método específicos.

```
aws apigateway update-stage \
    --rest-api-id 1234123412 \
    --stage-name 'dev' \
    --patch-operations op=replace,path=/~1resourceName/GET/logging/
dataTrace,value=false
```

Salida:

```
{
    "deploymentId": "5ubd17",
    "stageName": "dev",
    "cacheClusterEnabled": false,
```

```
    "cacheClusterStatus": "NOT_AVAILABLE",
    "methodSettings": {
        "~1resourceName/GET": {
            "metricsEnabled": false,
            "dataTraceEnabled": false,
            "throttlingBurstLimit": 5000,
            "throttlingRateLimit": 10000.0,
            "cachingEnabled": false,
            "cacheTtlInSeconds": 300,
            "cacheDataEncrypted": false,
            "requireAuthorizationForCacheControl": true,
            "unauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER"
        }
    },
    "tracingEnabled": false,
    "createdDate": "2022-07-18T10:11:18-07:00",
    "lastUpdatedDate": "2022-07-18T10:19:04-07:00"
}
```

Para obtener más información, consulte Configuración de una etapa para una API de REST en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

Ejemplo 2: cómo actualizar la configuración de etapa de todos los recursos y métodos de una etapa de API

En el siguiente ejemplo de `update-stage`, se activa el registro completo de solicitudes y respuestas de todos los recursos y métodos de una etapa de API.

```
aws apigateway update-stage \
    --rest-api-id 1234123412 \
    --stage-name 'dev' \
    --patch-operations 'op=replace,path=/*/*/logging/dataTrace,value=true'
```

Salida:

```
{
    "deploymentId": "5ubd17",
    "stageName": "dev",
    "cacheClusterEnabled": false,
    "cacheClusterStatus": "NOT_AVAILABLE",
    "methodSettings": {
        "*/*": {
            "metricsEnabled": false,
```

```
            "dataTraceEnabled": true,
            "throttlingBurstLimit": 5000,
            "throttlingRateLimit": 10000.0,
            "cachingEnabled": false,
            "cacheTtlInSeconds": 300,
            "cacheDataEncrypted": false,
            "requireAuthorizationForCacheControl": true,
            "unauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER"
        }
    },
    "tracingEnabled": false,
    "createdDate": "2022-07-18T10:11:18-07:00",
    "lastUpdatedDate": "2022-07-18T10:31:04-07:00"
}
```

Para obtener más información, consulte Configuración de una etapa para una API de REST en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener más información sobre la API, consulte UpdateStage en la Referencia de comandos de la AWS CLI.

`update-usage-plan`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-usage-plan`.

AWS CLI

Cambio del período definido en un plan de uso

Comando:

```
aws apigateway update-usage-plan --usage-plan-id a1b2c3 --patch-operations
 op="replace",path="/quota/period",value="MONTH"
```

Cambio del límite de cuota definido en un plan de uso

Comando:

```
aws apigateway update-usage-plan --usage-plan-id a1b2c3 --patch-operations
 op="replace",path="/quota/limit",value="500"
```

Cambio del límite de tasa de limitación definido en un plan de uso

Comando:

```
aws apigateway update-usage-plan --usage-plan-id a1b2c3 --patch-operations
 op="replace",path="/throttle/rateLimit",value="10"
```

Cambio del límite de ráfaga de limitación definido en un plan de uso

Comando:

```
aws apigateway update-usage-plan --usage-plan-id a1b2c3 --patch-operations
 op="replace",path="/throttle/burstLimit",value="20"
```

- Para obtener más información sobre la API, consulte UpdateUsagePlan en la Referencia de comandos de la AWS CLI.

update-usage

En el siguiente ejemplo de código, se muestra cómo utilizar `update-usage`.

AWS CLI

Modificación temporal de la cuota de una clave de API durante el período actual definido en el plan de uso

Comando:

```
aws apigateway update-usage --usage-plan-id a1b2c3 --key-
id 1NbjQzMReAkeEQPNAW8r3dXsU2rDD7fc7f2Sipnu --patch-operations op="replace",path="/
remaining",value="50"
```

- Para obtener información sobre la API, consulte UpdateUsage en la Referencia de comandos de la AWS CLI.

update-vpc-link

En el siguiente ejemplo de código, se muestra cómo utilizar `update-vpc-link`.

AWS CLI

Ejemplo 1: Para actualizar el nombre de un enlace de VPC existente

En el ejemplo de `update-vpc-link` siguiente, se actualiza el nombre del enlace de la VPC especificado.

```
aws apigateway update-vpc-link  \
    --vpc-link-id ab3de6 \
    --patch-operations op=replace,path=/name,value=my-vpc-link
```

Salida:

```
{
    "id": "ab3de6",
    "name": "my-vpc-link",
    "targetArns": [
        "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/my-
lb/12a456s89aaa12345"
    ],
    "status": "AVAILABLE",
    "statusMessage": "Your vpc link is ready for use",
    "tags": {}
}
```

Para obtener más información, consulte Actualización del enlace de la VPC existente en la Referencia de comandos de la CLI de AWS.

Ejemplo 2: Para actualizar el nombre y la descripción de un enlace de VPC existente

En el ejemplo de `update-vpc-link` siguiente, se actualiza el nombre del enlace de la VPC especificado.

```
aws apigateway update-vpc-link  \
    --vpc-link-id ab3de6 \
    --patch-operations op=replace,path=/name,value=my-vpc-link op=replace,path=/
description,value="My custom description"
```

Salida:

```
{
    "id": "ab3de6",
    "name": "my-vpc-link",
    "description": "My custom description",
    "targetArns": [
```

```
        "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/my-
lb/12a456s89aaa12345"
    ],
    "status": "AVAILABLE",
    "statusMessage": "Your vpc link is ready for use",
    "tags": {}
}
```

Para obtener más información, consulte Actualización del enlace de la VPC existente en la Referencia de comandos de la CLI de AWS.

- Para obtener información sobre la API, consulte UpdateVpcLink en la Referencia de comandos de la AWS CLI.

Ejemplos de API de WebSocket y HTTP de API Gateway que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar situaciones comunes mediante AWS Command Line Interface con API de WebSocket y HTTP de API Gateway.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-api-mapping`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-api-mapping`.

AWS CLI

Creación de una asignación de API para una API

En el siguiente ejemplo de `create-api-mapping`, se asigna la etapa `test` de una API a la ruta `/myApi` del nombre de dominio personalizado `regional.example.com`.

```
aws apigatewayv2 create-api-mapping \
    --domain-name regional.example.com \
    --api-mapping-key myApi \
    --api-id a1b2c3d4 \
    --stage test
```

Salida:

```
{
    "ApiId": "a1b2c3d4",
    "ApiMappingId": "0qzs2sy7bh",
    "ApiMappingKey": "myApi"
    "Stage": "test"
}
```

Para obtener más información, consulte Configuración de un nombre de dominio personalizado regional en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte CreateApiMapping en la Referencia de comandos de la AWS CLI.

`create-api`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-api`.

AWS CLI

Cómo crear una API de HTTP

En el siguiente ejemplo de `create-api`, se crea una API de HTTP mediante la creación rápida. Puede utilizar la creación rápida para crear una API con una integración de AWS Lambda o HTTP, una ruta de método catch-all predeterminada y una etapa predeterminada configurada para implementar automáticamente los cambios. El siguiente comando utiliza la creación rápida para crear una API de HTTP que se integra con una función de Lambda.

```
aws apigatewayv2 create-api \
    --name my-http-api \
```

```
    --protocol-type HTTP \
    --target arn:aws:lambda:us-west-2:123456789012:function:my-lambda-function
```

Salida:

```
{
    "ApiEndpoint": "https://a1b2c3d4.execute-api.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "CreatedDate": "2020-04-08T19:05:45+00:00",
    "Name": "my-http-api",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path"
}
```

Para obtener más información, consulte Desarrollo de las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

Creación de una API de WebSocket

En el siguiente ejemplo de `create-api`, se crea una API de WebSocket con el nombre especificado.

```
aws apigatewayv2 create-api \
    --name "myWebSocketApi" \
    --protocol-type WEBSOCKET \
    --route-selection-expression '$request.body.action'
```

Salida:

```
{
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "Name": "myWebSocketApi",
    "CreatedDate": "2018-11-15T06:23:51Z",
    "ProtocolType": "WEBSOCKET",
    "RouteSelectionExpression": "'$request.body.action'",
    "ApiId": "aabbccddee"
}
```

Para obtener más información, consulte Creación de las API de WebSocket en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte CreateApi en la Referencia de comandos de la AWS CLI.

`create-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-authorizer`.

AWS CLI

Creación de un autorizador de JWT para una API de HTTP

En el siguiente ejemplo de `create-authorizer`, se crea un autorizador de JWT que utiliza Amazon Cognito como un proveedor de identidades.

```
aws apigatewayv2 create-authorizer \
    --name my-jwt-authorizer \
    --api-id a1b2c3d4 \
    --authorizer-type JWT \
    --identity-source '$request.header.Authorization' \
    --jwt-configuration Audience=123456abc,Issuer=https://cognito-idp.us-
west-2.amazonaws.com/us-west-2_abc123
```

Salida:

```
{
    "AuthorizerId": "a1b2c3",
    "AuthorizerType": "JWT",
    "IdentitySource": [
        "$request.header.Authorization"
    ],
    "JwtConfiguration": {
        "Audience": [
            "123456abc"
        ],
        "Issuer": "https://cognito-idp.us-west-2.amazonaws.com/us-west-2_abc123"
    },
    "Name": "my-jwt-authorizer"
}
```

Para obtener más información, consulte Control del acceso a las API de HTTP con autorizadores de JWT en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte CreateAuthorizer en la Referencia de comandos de la AWS CLI.

`create-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-deployment`.

AWS CLI

Creación de una implementación para una API

En el siguiente ejemplo de `create-deployment`, se crea una implementación para una API y se asocia dicha implementación con la etapa `dev` de la API.

```
aws apigatewayv2 create-deployment \
    --api-id a1b2c3d4 \
    --stage-name dev
```

Salida:

```
{
    "AutoDeployed": false,
    "CreatedDate": "2020-04-06T23:38:08Z",
    "DeploymentId": "53lz9l",
    "DeploymentStatus": "DEPLOYED"
}
```

Para obtener más información, consulte Implementación de API en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte CreateDeployment en la Referencia de comandos de la AWS CLI.

`create-domain-name`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-domain-name`.

AWS CLI

Creación de un nombre de dominio personalizado

En el siguiente ejemplo de `create-domain-name`, se crea un nombre de dominio personalizado regional para una API.

```
aws apigatewayv2 create-domain-name \
    --domain-name regional.example.com \
    --domain-name-configurations CertificateArn=arn:aws:acm:us-
west-2:123456789012:certificate/123456789012-1234-1234-1234-12345678
```

Salida:

```
{
    "ApiMappingSelectionExpression": "$request.basepath",
    "DomainName": "regional.example.com",
    "DomainNameConfigurations": [
        {
            "ApiGatewayDomainName": "d-id.execute-api.us-west-2.amazonaws.com",
            "CertificateArn": "arn:aws:acm:us-
west-2:123456789012:certificate/123456789012-1234-1234-1234-12345678",
            "EndpointType": "REGIONAL",
            "HostedZoneId": "123456789111",
            "SecurityPolicy": "TLS_1_2",
            "DomainNameStatus": "AVAILABLE"
        }
    ]
}
```

Para obtener más información, consulte Configuración de un nombre de dominio personalizado regional en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte CreateDomainName en la Referencia de comandos de la AWS CLI.

`create-integration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-integration`.

AWS CLI

Creación de una integración de API de WebSocket

En el siguiente ejemplo de `create-integration`, se crea una integración simulada para una API de WebSocket.

```
aws apigatewayv2 create-integration \
    --api-id aabbccddee \
    --passthrough-behavior WHEN_NO_MATCH \
    --timeout-in-millis 29000 \
    --connection-type INTERNET \
    --integration-type MOCK
```

Salida:

```
{
    "ConnectionType": "INTERNET",
    "IntegrationId": "0abcdef",
    "IntegrationResponseSelectionExpression": "${integration.response.statuscode}",
    "IntegrationType": "MOCK",
    "PassthroughBehavior": "WHEN_NO_MATCH",
    "PayloadFormatVersion": "1.0",
    "TimeoutInMillis": 29000
}
```

Para obtener más información, consulte Configuración de una solicitud de integración de API de WebSocket en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

Creación de una integración de API de HTTP

En el siguiente ejemplo de `create-integration`, se crea una integración de AWS Lambda para una API de HTTP.

```
aws apigatewayv2 create-integration \
    --api-id a1b2c3d4 \
    --integration-type AWS_PROXY \
    --integration-uri arn:aws:lambda:us-west-2:123456789012:function:my-function \
    --payload-format-version 2.0
```

Salida:

```
{
    "ConnectionType": "INTERNET",
    "IntegrationId": "0abcdef",
    "IntegrationMethod": "POST",
    "IntegrationType": "AWS_PROXY",
    "IntegrationUri": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
```

```
    "PayloadFormatVersion": "2.0",
    "TimeoutInMillis": 30000
}
```

Para obtener más información, consulte Creación de integraciones para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte CreateIntegration en la Referencia de comandos de la AWS CLI.

`create-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-route`.

AWS CLI

Creación de una ruta $default para una API de WebSocket o HTTP

En el siguiente ejemplo de `create-route`, se crea una ruta `$default` para una API de WebSocket o HTTP.

```
aws apigatewayv2 create-route \
    --api-id aabbccddee \
    --route-key '$default'
```

Salida:

```
{
    "ApiKeyRequired": false,
    "AuthorizationType": "NONE",
    "RouteKey": "$default",
    "RouteId": "1122334"
}
```

Para obtener más información, consulte Creación de rutas para las API de WebSocket en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

Creación de una ruta para una API de HTTP

En el siguiente ejemplo de `create-route`, se crea una ruta con el nombre `signup` que acepta solicitudes POST.

```
aws apigatewayv2 create-route \
    --api-id aabbccddee \
    --route-key 'POST /signup'
```

Salida:

```
{
    "ApiKeyRequired": false,
    "AuthorizationType": "NONE",
    "RouteKey": "POST /signup",
    "RouteId": "1122334"
}
```

Para obtener más información, consulte Creación de rutas para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte CreateRoute en la Referencia de comandos de la AWS CLI.

`create-routing-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-routing-rule`.

AWS CLI

Creación de una regla de enrutamiento

El siguiente ejemplo de `create-routing-rule` crea una regla de enrutamiento con una prioridad de `50`.

```
aws apigatewayv2 create-routing-rule \
    --domain-name 'regional.example.com' \
    --priority 50 \
    --conditions '[ \
        { \
            "MatchBasePaths": { \
                "AnyOf": [ \
                    "PetStoreShopper" \
                ] \
            } \
        } \
```

```
    ]' \
    --actions '[ \
        { \
            "InvokeApi": { \
                "ApiId": "abcd1234", \
                "Stage": "prod" \
            } \
        } \
    ]'
```

Salida:

```
{
    "Actions": [
        {
            "InvokeApi": {
                "ApiId": "abcd1234",
                "Stage": "prod",
                "StripBasePath": false
            }
        }
    ],
    "Conditions": [
        {
            "MatchBasePaths": {
                "AnyOf": [
                    "PetStoreShopper"
                ]
            }
        }
    ],
    "Priority": 50,
    "RoutingRuleArn": "arn:aws:apigateway:us-east-2:123456789012:/domainnames/
regional.example.com/routingrules/aaa111",
    "RoutingRuleId": "aaa111"
}
```

Para obtener más información, consulte Reglas de enrutamiento para conectar etapas de la API a un nombre de dominio personalizado para las API de REST en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte CreateRoutingRule en la Referencia de comandos de la AWS CLI.

`create-stage`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-stage`.

AWS CLI

Creación de una etapa

En el siguiente ejemplo de `create-stage`, se crea una etapa denominada dev para una API.

```
aws apigatewayv2 create-stage \
    --api-id a1b2c3d4 \
    --stage-name dev
```

Salida:

```
{
    "CreatedDate": "2020-04-06T23:23:46Z",
    "DefaultRouteSettings": {
        "DetailedMetricsEnabled": false
    },
    "LastUpdatedDate": "2020-04-06T23:23:46Z",
    "RouteSettings": {},
    "StageName": "dev",
    "StageVariables": {},
    "Tags": {}
}
```

Para obtener más información, consulte Etapas para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte CreateStage en la Referencia de comandos de la AWS CLI.

`create-vpc-link`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-vpc-link`.

AWS CLI

Creación de un enlace de VPC para una API de HTTP

En el siguiente ejemplo de `create-vpc-link`, se crea un enlace de VPC para API de HTTP.

```
aws apigatewayv2 create-vpc-link \
    --name MyVpcLink \
    --subnet-ids subnet-aaaa subnet-bbbb \
    --security-group-ids sg1234 sg5678
```

Salida:

```
{
    "CreatedDate": "2020-04-07T00:11:46Z",
    "Name": "MyVpcLink",
    "SecurityGroupIds": [
        "sg1234",
        "sg5678"
    ],
    "SubnetIds": [
        "subnet-aaaa",
        "subnet-bbbb"
    ],
    "Tags": {},
    "VpcLinkId": "abcd123",
    "VpcLinkStatus": "PENDING",
    "VpcLinkStatusMessage": "VPC link is provisioning ENIs",
    "VpcLinkVersion": "V2"
}
```

Para obtener más información, consulte Configuración de enlaces de VPC para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte CreateVpcLink en la Referencia de comandos de la AWS CLI.

`delete-access-log-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-access-log-settings`.

AWS CLI

Deshabiltación del registro de acceso de una API

En el siguiente ejemplo de `delete-access-log-settings`, se elimina la configuración de registro de acceso de la etapa `$default` de una API. Para deshabilitar el registro de acceso de una etapa, elimine su configuración de registro de acceso.

```
aws apigatewayv2 delete-access-log-settings \
    --api-id a1b2c3d4 \
    --stage-name '$default'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración del registro de las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte DeleteAccessLogSettings en la Referencia de comandos de la AWS CLI.

`delete-api-mapping`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-api-mapping`.

AWS CLI

Eliminación de una asignación de API

En el siguiente ejemplo de `delete-api-mapping`, se elimina una asignación de API del nombre de dominio personalizado `api.example.com`.

```
aws apigatewayv2 delete-api-mapping \
    --api-mapping-id a1b2c3 \
    --domain-name api.example.com
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de un nombre de dominio personalizado regional en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte DeleteApiMapping en la Referencia de comandos de la AWS CLI.

`delete-api`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-api`.

AWS CLI

Eliminación de una API

En el siguiente ejemplo de `delete-api`, se elimina una API.

```
aws apigatewayv2 delete-api \
    --api-id a1b2c3d4
```

Este comando no genera ninguna salida.

Para obtener más información, consulte API de HTTP de API Gateway y API de WebSocket de API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte DeleteApi en la Referencia de comandos de la AWS CLI.

`delete-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-authorizer`.

AWS CLI

Eliminación de un autorizador

En el siguiente ejemplo de `delete-authorizer`, se elimina un autorizador.

```
aws apigatewayv2 delete-authorizer \
    --api-id a1b2c3d4 \
    --authorizer-id a1b2c3
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Control del acceso a las API de HTTP con autorizadores de JWT en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener detalles sobre la API, consulte DeleteAuthorizer en la Referencia de comandos de la AWS CLI.

`delete-cors-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-cors-configuration`.

AWS CLI

Eliminación de la configuración de CORS para una API de HTTP

En el siguiente ejemplo de `delete-cors-configuration`, se deshabilita CORS para una API de HTTP mediante la eliminación de su configuración de CORS.

```
aws apigatewayv2 delete-cors-configuration \
    --api-id a1b2c3d4
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de CORS de las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte DeleteCorsConfiguration en la Referencia de comandos de la AWS CLI.

`delete-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-deployment`.

AWS CLI

Eliminación de una implementación

En el siguiente ejemplo de `delete-deployment`, se elimina una implementación de una API.

```
aws apigatewayv2 delete-deployment \
    --api-id a1b2c3d4 \
    --deployment-id a1b2c3
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Implementación de API en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte DeleteDeployment en la Referencia de comandos de la AWS CLI.

`delete-domain-name`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-domain-name`.

AWS CLI

Eliminación de un nombre de dominio personalizado

En el siguiente ejemplo de `delete-domain-name`, se elimina un nombre de dominio personalizado.

```
aws apigatewayv2 delete-domain-name \
    --domain-name api.example.com
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de un nombre de dominio personalizado regional en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte DeleteDomainName en la Referencia de comandos de la AWS CLI.

`delete-integration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-integration`.

AWS CLI

Eliminación de una integración

En el siguiente ejemplo de `delete-integration`, se elimina una integración de API.

```
aws apigatewayv2 delete-integration \
    --api-id a1b2c3d4 \
    --integration-id a1b2c3
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación de integraciones para las API de HTTP en API Gateway e Integraciones de API de WebSocket en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte DeleteIntegration en la Referencia de comandos de la AWS CLI.

`delete-route-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-route-settings`.

AWS CLI

Eliminación de una configuración de ruta

En el siguiente ejemplo de `delete-route-settings`, se elimina la configuración de la ruta especificada.

```
aws apigatewayv2 delete-route-settings \
    --api-id a1b2c3d4 \
    --stage-name dev \
    --route-key 'GET /pets'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación de rutas para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte DeleteRouteSettings en la Referencia de comandos de la AWS CLI.

`delete-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-route`.

AWS CLI

Para eliminar una ruta

En el siguiente ejemplo de `delete-route`, se elimina una ruta de API.

```
aws apigatewayv2 delete-route \
    --api-id a1b2c3d4 \
    --route-id a1b2c3
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación de rutas para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte DeleteRoute en la Referencia de comandos de la AWS CLI.

`delete-routing-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-routing-rule`.

AWS CLI

Eliminación de una regla de enrutamiento

En el siguiente ejemplo de `delete-routing-rule`, se elimina una regla de enrutamiento para un nombre de dominio personalizado.

```
aws apigatewayv2 delete-routing-rule \
    --domain-name 'regional.example.com' \
    --routing-rule-id aaa111
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Reglas de enrutamiento para conectar etapas de la API a un nombre de dominio personalizado para las API de REST en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte DeleteRoutingRule en la Referencia de comandos de la AWS CLI.

`delete-stage`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-stage`.

AWS CLI

Para eliminar un escenario

En el siguiente ejemplo de `delete-stage`, se elimina la etapa `test` de una API.

```
aws apigatewayv2 delete-stage \
    --api-id a1b2c3d4 \
    --stage-name test
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etapas para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte DeleteStage en la Referencia de comandos de la AWS CLI.

`delete-vpc-link`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-vpc-link`.

AWS CLI

Eliminación de un enlace de VPC para una API de HTTP

En el siguiente ejemplo de `delete-vpc-link` se elimina un enlace de VPC.

```
aws apigatewayv2 delete-vpc-link \
    --vpc-link-id abcd123
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de enlaces de VPC para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte DeleteVpcLink en la Referencia de comandos de la AWS CLI.

`export-api`

En el siguiente ejemplo de código, se muestra cómo utilizar `export-api`.

AWS CLI

Exportación de una definición de OpenAPI de una API de HTTP

En el siguiente ejemplo de `export-api`, se exporta una definición de OpenAPI 3.0 de una etapa de API denominada `prod` a un archivo YAML denominado `stage-definition.yaml`. El archivo de definición exportado incluye extensiones de API Gateway de forma predeterminada.

```
aws apigatewayv2 export-api \
    --api-id a1b2c3d4 \
    --output-type YAML \
```

```
    --specification OAS30 \
    --stage-name prod \
    stage-definition.yaml
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Exportación de las API de HTTP desde API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte ExportApi en la Referencia de comandos de la AWS CLI.

`get-api-mapping`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-api-mapping`.

AWS CLI

Para obtener información acerca de una asignación de API de un nombre de dominio personalizado

En el siguiente ejemplo de `get-api-mapping`, se muestra información sobre una asignación de API del nombre de dominio personalizado `api.example.com`.

```
aws apigatewayv2 get-api-mapping \
    --api-mapping-id a1b2c3 \
    --domain-name api.example.com
```

Salida:

```
{
    "ApiId": "a1b2c3d4",
    "ApiMappingId": "a1b2c3d5",
    "ApiMappingKey": "myTestApi"
    "Stage": "test"
}
```

Para obtener más información, consulte Configuración de un nombre de dominio personalizado regional en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetApiMapping en la Referencia de comandos de la AWS CLI.

get-api-mappings

En el siguiente ejemplo de código, se muestra cómo utilizar `get-api-mappings`.

AWS CLI

Para obtener las asignaciones de API de un nombre de dominio personalizado

En el siguiente ejemplo de `get-api-mappings`, se muestra una lista de todas las asignaciones de API del nombre de dominio personalizado `api.example.com`.

```
aws apigatewayv2 get-api-mappings \
    --domain-name api.example.com
```

Salida:

```
{
    "Items": [
        {
            "ApiId": "a1b2c3d4",
            "ApiMappingId": "a1b2c3d5",
            "ApiMappingKey": "myTestApi"
            "Stage": "test"
        },
        {
            "ApiId": "a5b6c7d8",
            "ApiMappingId": "a1b2c3d6",
            "ApiMappingKey": "myDevApi"
            "Stage": "dev"
        },
    ]
}
```

Para obtener más información, consulte Configuración de un nombre de dominio personalizado regional en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetApiMappings en la Referencia de comandos de la AWS CLI.

get-api

En el siguiente ejemplo de código, se muestra cómo utilizar `get-api`.

AWS CLI

Recuperación de información sobre una API

En el siguiente ejemplo de `get-api`, se muestra información acerca de una API.

```
aws apigatewayv2 get-api \
    --api-id a1b2c3d4
```

Salida:

```
{
    "ApiEndpoint": "https://a1b2c3d4.execute-api.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "CreatedDate": "2020-03-28T00:32:37Z",
    "Name": "my-api",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
    "Tags": {
        "department": "finance"
    }
}
```

- Para obtener información sobre la API, consulte GetApi en la Referencia de comandos de la AWS CLI.

get-apis

En el siguiente ejemplo de código, se muestra cómo utilizar `get-apis`.

AWS CLI

Recuperación de una lista de API

En el siguiente ejemplo de `get-apis`, se genera una lista de las API del usuario actual.

```
aws apigatewayv2 get-apis
```

Salida:

```
{
    "Items": [
        {
            "ApiEndpoint": "wss://a1b2c3d4.execute-api.us-west-2.amazonaws.com",
            "ApiId": "a1b2c3d4",
            "ApiKeySelectionExpression": "$request.header.x-api-key",
            "CreatedDate": "2020-04-07T20:21:59Z",
            "Name": "my-websocket-api",
            "ProtocolType": "WEBSOCKET",
            "RouteSelectionExpression": "$request.body.message",
            "Tags": {}
        },
        {
            "ApiEndpoint": "https://a1b2c3d5.execute-api.us-west-2.amazonaws.com",
            "ApiId": "a1b2c3d5",
            "ApiKeySelectionExpression": "$request.header.x-api-key",
            "CreatedDate": "2020-04-07T20:23:50Z",
            "Name": "my-http-api",
            "ProtocolType": "HTTP",
            "RouteSelectionExpression": "$request.method $request.path",
            "Tags": {}
        }
    ]
}
```

Para obtener más información, consulte API de HTTP de API Gateway y API de WebSocket de API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetApis en la Referencia de comandos de la AWS CLI.

`get-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-authorizer`.

AWS CLI

Recuperación de información sobre un autorizador

En el siguiente ejemplo de `get-authorizer`, se muestra información acerca de un autorizador.

```
aws apigatewayv2 get-authorizer \
    --api-id a1b2c3d4 \
```

```
    --authorizer-id a1b2c3
```

Salida:

```
{
    "AuthorizerId": "a1b2c3",
    "AuthorizerType": "JWT",
    "IdentitySource": [
        "$request.header.Authorization"
    ],
    "JwtConfiguration": {
        "Audience": [
            "123456abc"
        ],
        "Issuer": "https://cognito-idp.us-west-2.amazonaws.com/us-west-2_abc123"
    },
    "Name": "my-jwt-authorizer"
}
```

Para obtener más información, consulte Control del acceso a las API de HTTP con autorizadores de JWT en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetAuthorizer en la Referencia de comandos de la AWS CLI.

`get-authorizers`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-authorizers`.

AWS CLI

Recuperación de una lista de autorizadores de una API

En el siguiente ejemplo de `get-authorizers`, se muestra una lista de todos los autorizadores de una API.

```
aws apigatewayv2 get-authorizers \
    --api-id a1b2c3d4
```

Salida:

```
{
```

```
    "Items": [
        {
            "AuthorizerId": "a1b2c3",
            "AuthorizerType": "JWT",
            "IdentitySource": [
                "$request.header.Authorization"
            ],
            "JwtConfiguration": {
                "Audience": [
                    "123456abc"
                ],
                "Issuer": "https://cognito-idp.us-west-2.amazonaws.com/us-
west-2_abc123"
            },
            "Name": "my-jwt-authorizer"
        },
        {
            "AuthorizerId": "a1b2c4",
            "AuthorizerType": "JWT",
            "IdentitySource": [
                "$request.header.Authorization"
            ],
            "JwtConfiguration": {
                "Audience": [
                    "6789abcde"
                ],
                "Issuer": "https://cognito-idp.us-west-2.amazonaws.com/us-
west-2_abc234"
            },
            "Name": "new-jwt-authorizer"
        }
    ]
}
```

Para obtener más información, consulte Control del acceso a las API de HTTP con autorizadores de JWT en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetAuthorizers en la Referencia de comandos de la AWS CLI.

`get-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-deployment`.

AWS CLI

Recuperación de información acerca de una implementación

En el siguiente ejemplo de `get-deployment`, se muestra información acerca de una implementación.

```
aws apigatewayv2 get-deployment \
    --api-id a1b2c3d4 \
    --deployment-id abcdef
```

Salida:

```
{
    "AutoDeployed": true,
    "CreatedDate": "2020-04-07T23:58:40Z",
    "DeploymentId": "abcdef",
    "DeploymentStatus": "DEPLOYED",
    "Description": "Automatic deployment triggered by changes to the Api
 configuration"
}
```

Para obtener más información, consulte Implementación de API en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetDeployment en la Referencia de comandos de la AWS CLI.

`get-deployments`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-deployments`.

AWS CLI

Recuperación de una lista de implementaciones

En el siguiente ejemplo de `get-deployments`, se muestra una lista de todas las implementaciones de una API.

```
aws apigatewayv2 get-deployments \
```

```
    --api-id a1b2c3d4
```

Salida:

```
{
    "Items": [
        {
            "AutoDeployed": true,
            "CreatedDate": "2020-04-07T23:58:40Z",
            "DeploymentId": "abcdef",
            "DeploymentStatus": "DEPLOYED",
            "Description": "Automatic deployment triggered by changes to the Api
 configuration"
        },
        {
            "AutoDeployed": true,
            "CreatedDate": "2020-04-06T00:33:00Z",
            "DeploymentId": "bcdefg",
            "DeploymentStatus": "DEPLOYED",
            "Description": "Automatic deployment triggered by changes to the Api
 configuration"
        }
    ]
}
```

Para obtener más información, consulte Implementación de API en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetDeployments en la Referencia de comandos de la AWS CLI.

`get-domain-name`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-domain-name`.

AWS CLI

Recuperación de información acerca de un nombre de dominio personalizado

En el siguiente ejemplo de `get-domain-name`, se muestra información sobre un nombre de dominio personalizado.

```
aws apigatewayv2 get-domain-name \
```

```
    --domain-name api.example.com
```

Salida:

```
{
    "ApiMappingSelectionExpression": "$request.basepath",
    "DomainName": "api.example.com",
    "DomainNameConfigurations": [
        {
            "ApiGatewayDomainName": "d-1234.execute-api.us-west-2.amazonaws.com",
            "CertificateArn": "arn:aws:acm:us-
west-2:123456789012:certificate/123456789012-1234-1234-1234-12345678",
            "EndpointType": "REGIONAL",
            "HostedZoneId": "123456789111",
            "SecurityPolicy": "TLS_1_2",
            "DomainNameStatus": "AVAILABLE"
        }
    ],
    "Tags": {}
}
```

Para obtener más información, consulte Configuración de un nombre de dominio personalizado regional en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetDomainName en la Referencia de comandos de la AWS CLI.

`get-domain-names`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-domain-names`.

AWS CLI

Recuperación de una lista de nombres de dominio personalizados

En el siguiente ejemplo de `get-domain-names`, se muestra una lista de todos los nombres de dominio personalizados del usuario actual.

```
aws apigatewayv2 get-domain-names
```

Salida:

```
{
    "Items": [
        {
            "ApiMappingSelectionExpression": "$request.basepath",
            "DomainName": "api.example.com",
            "DomainNameConfigurations": [
                {
                    "ApiGatewayDomainName": "d-1234.execute-api.us-
west-2.amazonaws.com",
                    "CertificateArn": "arn:aws:acm:us-
west-2:123456789012:certificate/123456789012-1234-1234-1234-12345678",
                    "EndpointType": "REGIONAL",
                    "HostedZoneId": "123456789111",
                    "SecurityPolicy": "TLS_1_2",
                    "DomainNameStatus": "AVAILABLE"
                }
            ]
        },
        {
            "ApiMappingSelectionExpression": "$request.basepath",
            "DomainName": "newApi.example.com",
            "DomainNameConfigurations": [
                {
                    "ApiGatewayDomainName": "d-5678.execute-api.us-
west-2.amazonaws.com",
                    "CertificateArn": "arn:aws:acm:us-
west-2:123456789012:certificate/123456789012-1234-1234-1234-12345678",
                    "EndpointType": "REGIONAL",
                    "HostedZoneId": "123456789222",
                    "SecurityPolicy": "TLS_1_2",
                    "DomainNameStatus": "AVAILABLE"
                }
            ]
        }
    ]
}
```


Para obtener más información, consulte Configuración de un nombre de dominio personalizado regional en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetDomainNames en la Referencia de comandos de la AWS CLI.

`get-integration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-integration`.

AWS CLI

Recuperación de información acerca de una integración

En el siguiente ejemplo de `get-integration`, se muestra información acerca de una integración.

```
aws apigatewayv2 get-integration \
    --api-id a1b2c3d4 \
    --integration-id a1b2c3
```

Salida:

```
{
    "ApiGatewayManaged": true,
    "ConnectionType": "INTERNET",
    "IntegrationId": "a1b2c3",
    "IntegrationMethod": "POST",
    "IntegrationType": "AWS_PROXY",
    "IntegrationUri": "arn:aws:lambda:us-west-2:12356789012:function:hello12",
    "PayloadFormatVersion": "2.0",
    "TimeoutInMillis": 30000
}
```

Para obtener más información, consulte Creación de integraciones para las API de HTTP en API Gateway e Integraciones de API de WebSocket en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetIntegration en la Referencia de comandos de la AWS CLI.

`get-integrations`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-integrations`.

AWS CLI

Recuperación de una lista de integraciones

En el siguiente ejemplo de `get-integrations`, se muestra una lista de todas las integraciones de una API.

```
aws apigatewayv2 get-integrations \
    --api-id a1b2c3d4
```

Salida:

```
{
    "Items": [
        {
            "ApiGatewayManaged": true,
            "ConnectionType": "INTERNET",
            "IntegrationId": "a1b2c3",
            "IntegrationMethod": "POST",
            "IntegrationType": "AWS_PROXY",
            "IntegrationUri": "arn:aws:lambda:us-west-2:123456789012:function:my-
function",
            "PayloadFormatVersion": "2.0",
            "TimeoutInMillis": 30000
        },
        {
            "ConnectionType": "INTERNET",
            "IntegrationId": "a1b2c4",
            "IntegrationMethod": "ANY",
            "IntegrationType": "HTTP_PROXY",
            "IntegrationUri": "https://www.example.com",
            "PayloadFormatVersion": "1.0",
            "TimeoutInMillis": 30000
        }
    ]
}
```

Para obtener más información, consulte Creación de integraciones para las API de HTTP en API Gateway e Integraciones de API de WebSocket en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetIntegrations en la Referencia de comandos de la AWS CLI.

`get-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-route`.

AWS CLI

Recuperación de información sobre una ruta

En el siguiente ejemplo de `get-route`, se muestra información acerca de una ruta.

```
aws apigatewayv2 get-route \
    --api-id a1b2c3d4 \
    --route-id 72jz1wk
```

Salida:

```
{
    "ApiKeyRequired": false,
    "AuthorizationType": "NONE",
    "RouteId": "72jz1wk",
    "RouteKey": "ANY /pets",
    "Target": "integrations/a1b2c3"
}
```

Para obtener más información, consulte Creación de rutas para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetRoute en la Referencia de comandos de la AWS CLI.

`get-routes`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-routes`.

AWS CLI

Recuperación de una lista de rutas

En el siguiente ejemplo de `get-routes`, se muestra una lista de todas las rutas de una API.

```
aws apigatewayv2 get-routes \
    --api-id a1b2c3d4
```

Salida:

```
{
    "Items": [
        {
            "ApiKeyRequired": false,
            "AuthorizationType": "NONE",
            "RouteId": "72jz1wk",
            "RouteKey": "ANY /admin",
            "Target": "integrations/a1b2c3"
        },
        {
            "ApiGatewayManaged": true,
            "ApiKeyRequired": false,
            "AuthorizationType": "NONE",
            "RouteId": "go65gqi",
            "RouteKey": "$default",
            "Target": "integrations/a1b2c4"
        }
    ]
}
```

Para obtener más información, consulte Creación de rutas para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetRoutes en la Referencia de comandos de la AWS CLI.

`get-routing-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-routing-rule`.

AWS CLI

Obtención de una regla de enrutamiento

En el siguiente ejemplo de `get-routing-rule`, se obtiene una regla de enrutamiento para un nombre de dominio.

```
aws apigatewayv2 get-routing-rule \
    --domain-name 'regional.example.com' \
    --routing-rule-id aaa111
```

Salida:

```
{
    "Actions": [
        {
            "InvokeApi": {
                "ApiId": "abcd1234",
                "Stage": "prod",
                "StripBasePath": false
            }
        }
    ],
    "Conditions": [
        {
            "MatchBasePaths": {
                "AnyOf": [
                    "PetStoreShopper"
                ]
            }
        }
    ],
    "Priority": 50,
    "RoutingRuleArn": "arn:aws:apigateway:us-east-2:123456789012:/domainnames/
regional.example.com/routingrules/aaa111",
    "RoutingRuleId": "aaa111"
}
```

Para obtener más información, consulte Reglas de enrutamiento para conectar etapas de la API a un nombre de dominio personalizado para las API de REST en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetRoutingRule en la Referencia de comandos de la AWS CLI.

`get-stage`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-stage`.

AWS CLI

Recuperación de información sobre una etapa

En el siguiente ejemplo de `get-stage`, se muestra información acerca de la etapa `prod` de una API.

```
aws apigatewayv2 get-stage \
    --api-id a1b2c3d4 \
    --stage-name prod
```

Salida:

```
{
    "CreatedDate": "2020-04-08T00:36:05Z",
    "DefaultRouteSettings": {
        "DetailedMetricsEnabled": false
    },
    "DeploymentId": "x1zwyv",
    "LastUpdatedDate": "2020-04-08T00:36:13Z",
    "RouteSettings": {},
    "StageName": "prod",
    "StageVariables": {
        "function": "my-prod-function"
    },
    "Tags": {}
}
```

Para obtener más información, consulte Etapas para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetStage en la Referencia de comandos de la AWS CLI.

`get-stages`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-stages`.

AWS CLI

Recuperación de una lista de etapas

En el siguiente ejemplo de `get-stages`, se genera una lista de todas las etapas de una API.

```
aws apigatewayv2 get-stages \
    --api-id a1b2c3d4
```

Salida:


```
{
    "Items": [
        {
            "ApiGatewayManaged": true,
            "AutoDeploy": true,
            "CreatedDate": "2020-04-08T00:08:44Z",
            "DefaultRouteSettings": {
                "DetailedMetricsEnabled": false
            },
            "DeploymentId": "dty748",
            "LastDeploymentStatusMessage": "Successfully deployed stage with
 deployment ID 'dty748'",
            "LastUpdatedDate": "2020-04-08T00:09:49Z",
            "RouteSettings": {},
            "StageName": "$default",
            "StageVariables": {},
            "Tags": {}
        },
        {
            "AutoDeploy": true,
            "CreatedDate": "2020-04-08T00:35:06Z",
            "DefaultRouteSettings": {
                "DetailedMetricsEnabled": false
            },
            "LastUpdatedDate": "2020-04-08T00:35:48Z",
            "RouteSettings": {},
            "StageName": "dev",
            "StageVariables": {
                "function": "my-dev-function"
            },
            "Tags": {}
        },
        {
            "CreatedDate": "2020-04-08T00:36:05Z",
            "DefaultRouteSettings": {
                "DetailedMetricsEnabled": false
            },
            "DeploymentId": "x1zwyv",
            "LastUpdatedDate": "2020-04-08T00:36:13Z",
            "RouteSettings": {},
            "StageName": "prod",
            "StageVariables": {
```

```
                "function": "my-prod-function"
            },
            "Tags": {}
        }
    ]
}
```

Para obtener más información, consulte Etapas para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetStages en la Referencia de comandos de la AWS CLI.

`get-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-tags`.

AWS CLI

Pare recuperar una lista de etiquetas para un recurso

En el siguiente ejemplo de `get-tags`, se genera una lista de todas las etiquetas de una API.

```
aws apigatewayv2 get-tags \
    --resource-arn arn:aws:apigateway:us-west-2::/apis/a1b2c3d4
```

Salida:

```
{
    "Tags": {
        "owner": "dev-team",
        "environment": "prod"
    }
}
```

Para obtener más información, consulte Etiquetado de recursos de API Gateway la Guía para desarrolladores de Amazon API Gateway.

- Para obtener detalles sobre la API, consulte GetTags en la Referencia de comandos de la AWS CLI.

get-vpc-link

En el siguiente ejemplo de código, se muestra cómo utilizar `get-vpc-link`.

AWS CLI

Recuperación de información sobre un enlace de VPC

En el siguiente ejemplo de `get-vpc-link`, se muestra información acerca de un enlace de VPC.

```
aws apigatewayv2 get-vpc-link \
    --vpc-link-id abcd123
```

Salida:

```
{
    "CreatedDate": "2020-04-07T00:27:47Z",
    "Name": "MyVpcLink",
    "SecurityGroupIds": [
        "sg1234",
        "sg5678"
    ],
    "SubnetIds": [
        "subnet-aaaa",
        "subnet-bbbb"
    ],
    "Tags": {},
    "VpcLinkId": "abcd123",
    "VpcLinkStatus": "AVAILABLE",
    "VpcLinkStatusMessage": "VPC link is ready to route traffic",
    "VpcLinkVersion": "V2"
}
```

Para obtener más información, consulte Configuración de enlaces de VPC para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetVpcLink en la Referencia de comandos de la AWS CLI.

get-vpc-links

En el siguiente ejemplo de código, se muestra cómo utilizar `get-vpc-links`.

AWS CLI

Recuperación de una lista de enlaces de VPC

En el siguiente ejemplo de `get-vpc-links`, se muestra una lista de todos los enlaces de VPC del usuario actual.

```
aws apigatewayv2 get-vpc-links
```

Salida:

```
{
    "Items": [
        {
            "CreatedDate": "2020-04-07T00:27:47Z",
            "Name": "MyVpcLink",
            "SecurityGroupIds": [
                "sg1234",
                "sg5678"
            ],
            "SubnetIds": [
                "subnet-aaaa",
                "subnet-bbbb"
            ],
            "Tags": {},
            "VpcLinkId": "abcd123",
            "VpcLinkStatus": "AVAILABLE",
            "VpcLinkStatusMessage": "VPC link is ready to route traffic",
            "VpcLinkVersion": "V2"
        }
        {
            "CreatedDate": "2020-04-07T00:27:47Z",
            "Name": "MyOtherVpcLink",
            "SecurityGroupIds": [
                "sg1234",
                "sg5678"
            ],
            "SubnetIds": [
                "subnet-aaaa",
                "subnet-bbbb"
            ],
            "Tags": {},
            "VpcLinkId": "abcd456",
```

```
            "VpcLinkStatus": "AVAILABLE",
            "VpcLinkStatusMessage": "VPC link is ready to route traffic",
            "VpcLinkVersion": "V2"
        }
    ]
}
```

Para obtener más información, consulte Configuración de enlaces de VPC para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte GetVpcLinks en la Referencia de comandos de la AWS CLI.

`import-api`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-api`.

AWS CLI

Importación de una API de HTTP

En el siguiente ejemplo de `import-api`, se crea una API de HTTP a partir de un archivo de definición de OpenAPI 3.0 denominado `api-definition.yaml`.

```
aws apigatewayv2 import-api \
    --body file://api-definition.yaml
```

Contenido de `api-definition.yaml`:

```
openapi: 3.0.1
info:
    title: My Lambda API
    version: v1.0
paths:
    /hello:
        x-amazon-apigateway-any-method:
            x-amazon-apigateway-integration:
                payloadFormatVersion: 2.0
                type: aws_proxy
                httpMethod: POST
                uri: arn:aws:apigateway:us-west-2:lambda:path/2015-03-31/functions/
arn:aws:lambda:us-west-2:123456789012:function:hello/invocations
```

```
                connectionType: INTERNET
```

Salida:

```
{
    "ApiEndpoint": "https://a1b2c3d4.execute-api.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "CreatedDate": "2020-04-08T17:19:38+00:00",
    "Name": "My Lambda API",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
    "Tags": {},
    "Version": "v1.0"
}
```

Para obtener más información, consulte Uso de definiciones de OpenAPI para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte ImportApi en la Referencia de comandos de la AWS CLI.

`list-routing-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-routing-rules`.

AWS CLI

Muestra de las reglas de enrutamiento

En el siguiente ejemplo de `list-routing-rules`, se muestran las reglas de enrutamiento de un nombre de dominio.

```
aws apigatewayv2 list-routing-rules \
    --domain-name 'regional.example.com'
```

Salida:

```
{
    "RoutingRules": [
        {
```

```
            "Actions": [
                {
                    "InvokeApi": {
                        "ApiId": "abcd1234",
                        "Stage": "prod",
                        "StripBasePath": false
                    }
                }
            ],
            "Conditions": [
                {
                    "MatchBasePaths": {
                        "AnyOf": [
                            "PetStoreShopper"
                        ]
                    }
                }
            ],
            "Priority": 150,
            "RoutingRuleArn": "arn:aws:apigateway:us-east-1:123456789012:/
domainnames/regional.example.com/routingrules/aaa111",
            "RoutingRuleId": "aaa111"
        }
    ]
}
```

Para obtener más información, consulte Reglas de enrutamiento para conectar etapas de la API a un nombre de dominio personalizado para las API de REST en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte ListRoutingRules en la Referencia de comandos de la AWS CLI.

`put-routing-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-routing-rule`.

AWS CLI

Actualización de una regla de enrutamiento

En el siguiente ejemplo de `put-routing-rule`, se actualiza la prioridad de una regla de enrutamiento.

```
aws apigatewayv2 put-routing-rule \
    --domain-name 'regional.example.com' \
    --priority 150 \
    --conditions '[ \
        { \
            "MatchBasePaths": { \
                "AnyOf": [ \
                    "PetStoreShopper" \
                ] \
            } \
        } \
    ]' \
    --actions '[ \
        { \
            "InvokeApi": { \
                "ApiId": "abcd1234", \
                "Stage": "prod" \
            } \
        } \
    ]'
```

Salida:

```
{
    "Actions": [
        {
            "InvokeApi": {
                "ApiId": "abcd1234",
                "Stage": "prod",
                "StripBasePath": false
            }
        }
    ],
    "Conditions": [
        {
            "MatchBasePaths": {
                "AnyOf": [
                    "PetStoreShopper"
                ]
            }
        }
    ],
    "Priority": 150,
```

```
    "RoutingRuleArn": "arn:aws:apigateway:us-east-2:123456789012:/domainnames/
regional.example.com/routingrules/aaa111",
    "RoutingRuleId": "aaa111"
}
```

Para obtener más información, consulte Reglas de enrutamiento para conectar etapas de la API a un nombre de dominio personalizado para las API de REST en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información acerca de la API, consulte PutRoutingRule en la Referencia de comandos de la AWS CLI.

`reimport-api`

En el siguiente ejemplo de código, se muestra cómo utilizar `reimport-api`.

AWS CLI

Reimportación de una API de HTTP

En el siguiente ejemplo de `reimport-api`, se actualiza una API de HTTP existente para utilizar la definición de OpenAPI 3.0 especificada en `api-definition.yaml`.

```
aws apigatewayv2 reimport-api \
    --body file://api-definition.yaml \
    --api-id a1b2c3d4
```

Contenido de `api-definition.yaml`:

```
openapi: 3.0.1
info:
    title: My Lambda API
    version: v1.0
paths:
    /hello:
        x-amazon-apigateway-any-method:
            x-amazon-apigateway-integration:
                payloadFormatVersion: 2.0
                type: aws_proxy
                httpMethod: POST
                uri: arn:aws:apigateway:us-west-2:lambda:path/2015-03-31/functions/
arn:aws:lambda:us-west-2:12356789012:function:hello/invocations
```

```
                connectionType: INTERNET
```

Salida:

```
{
    "ApiEndpoint": "https://a1b2c3d4.execute-api.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "CreatedDate": "2020-04-08T17:19:38+00:00",
    "Name": "My Lambda API",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
    "Tags": {},
    "Version": "v1.0"
}
```

Para obtener más información, consulte Uso de definiciones de OpenAPI para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte ReimportApi en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para etiquetar un recurso

En el siguiente ejemplo de `tag-resource`, se añade una etiqueta con el nombre de clave `Department` y un valor de `Accounting` a la API especificada.

```
aws apigatewayv2 tag-resource \
    --resource-arn arn:aws:apigateway:us-west-2::/apis/a1b2c3d4 \
    --tags Department=Accounting
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de API Gateway la Guía para desarrolladores de Amazon API Gateway.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar etiquetas de un recurso

En el siguiente ejemplo de `untag-resource`, se eliminan las etiquetas con los nombres de clave `Project` y `Owner` de la API especificada.

```
aws apigatewayv2 untag-resource \
    --resource-arn arn:aws:apigateway:us-west-2::/apis/a1b2c3d4 \
    --tag-keys Project Owner
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de API Gateway la Guía para desarrolladores de Amazon API Gateway.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-api-mapping`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-api-mapping`.

AWS CLI

Actualización de una asignación de API

En el siguiente ejemplo de `update-api-mapping`, se cambia una asignación de API de un nombre de dominio personalizado. Como resultado, la URL base que utiliza el nombre de dominio personalizado para la API especificada y la etapa se convierte en `https://api.example.com/dev`.

```
aws apigatewayv2 update-api-mapping \
    --api-id a1b2c3d4 \
```

```
    --stage dev \
    --domain-name api.example.com \
    --api-mapping-id 0qzs2sy7bh \
    --api-mapping-key dev
```

Salida:

```
{
    "ApiId": "a1b2c3d4",
    "ApiMappingId": "0qzs2sy7bh",
    "ApiMappingKey": "dev"
    "Stage": "dev"
}
```

Para obtener más información, consulte Configuración de un nombre de dominio personalizado regional en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte UpdateApiMapping en la Referencia de comandos de la AWS CLI.

`update-api`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-api`.

AWS CLI

Habilitación de CORS para una API de HTTP

En el siguiente ejemplo de `update-api`, se actualiza la configuración CORS de la API especificada para admitir solicitudes de `https://www.example.com`.

```
aws apigatewayv2 update-api \
    --api-id a1b2c3d4 \
    --cors-configuration AllowOrigins=https://www.example.com
```

Salida:

```
{
    "ApiEndpoint": "https://a1b2c3d4.execute-api.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "CorsConfiguration": {
```

```
        "AllowCredentials": false,
        "AllowHeaders": [
            "header1",
            "header2"
        ],
        "AllowMethods": [
            "GET",
            "OPTIONS"
        ],
        "AllowOrigins": [
            "https://www.example.com"
        ]
    },
    "CreatedDate": "2020-04-08T18:39:37+00:00",
    "Name": "my-http-api",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
    "Tags": {},
    "Version": "v1.0"
}
```

Para obtener más información, consulte Configuración de CORS de las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte UpdateApi en la Referencia de comandos de la AWS CLI.

`update-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-authorizer`.

AWS CLI

Actualización de un autorizador

En el siguiente ejemplo de `update-authorizer`, se cambia una fuente de identidad del autorizador de JWT por un encabezado denominado `Authorization`.

```
aws apigatewayv2 update-authorizer \
    --api-id a1b2c3d4 \
    --authorizer-id a1b2c3 \
    --identity-source '$request.header.Authorization'
```

Salida:

```
{
    "AuthorizerId": "a1b2c3",
    "AuthorizerType": "JWT",
    "IdentitySource": [
        "$request.header.Authorization"
    ],
    "JwtConfiguration": {
        "Audience": [
            "123456abc"
        ],
        "Issuer": "https://cognito-idp.us-west-2.amazonaws.com/us-west-2_abc123"
    },
    "Name": "my-jwt-authorizer"
}
```

Para obtener más información, consulte Control del acceso a las API de HTTP con autorizadores de JWT en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte UpdateAuthorizer en la Referencia de comandos de la AWS CLI.

`update-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-deployment`.

AWS CLI

Cambio de la descripción de una implementación

En el siguiente ejemplo de `update-deployment`, se actualiza la descripción de una implementación.

```
aws apigatewayv2 update-deployment \
    --api-id a1b2c3d4 \
    --deployment-id abcdef \
    --description 'Manual deployment to fix integration test failures.'
```

Salida:

```
{
```

```
    "AutoDeployed": false,
    "CreatedDate": "2020-02-05T16:21:48+00:00",
    "DeploymentId": "abcdef",
    "DeploymentStatus": "DEPLOYED",
    "Description": "Manual deployment to fix integration test failures."
}
```

Para obtener más información, consulte Desarrollo de las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener más información sobre la API, consulte UpdateDeployment en la Referencia de comandos de la AWS CLI.

`update-domain-name`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-domain-name`.

AWS CLI

Actualización de un nombre de dominio personalizado

En el siguiente ejemplo de `update-domain-name`, se especifica un nuevo certificado de ACM para el nombre de dominio personalizado `api.example.com`.

```
aws apigatewayv2 update-domain-name \
    --domain-name api.example.com \
    --domain-name-configurations CertificateArn=arn:aws:acm:us-
west-2:123456789012:certificate/123456789012-1234-1234-1234-12345678
```

Salida:

```
{
    "ApiMappingSelectionExpression": "$request.basepath",
    "DomainName": "regional.example.com",
    "DomainNameConfigurations": [
        {
            "ApiGatewayDomainName": "d-id.execute-api.us-west-2.amazonaws.com",
            "CertificateArn": "arn:aws:acm:us-
west-2:123456789012:certificate/123456789012-1234-1234-1234-12345678",
            "EndpointType": "REGIONAL",
            "HostedZoneId": "123456789111",
            "SecurityPolicy": "TLS_1_2",
```

```
            "DomainNameStatus": "AVAILABLE"
        }
    ]
}
```

Para obtener más información, consulte Configuración de un nombre de dominio personalizado regional en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte UpdateDomainName en la Referencia de comandos de la AWS CLI.

`update-integration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-integration`.

AWS CLI

Actualización de una integración de Lambda

En el siguiente ejemplo de `update-integration`, se actualiza una integración de AWS Lambda existente para utilizar la función de Lambda especificada.

```
aws apigatewayv2 update-integration \
    --api-id a1b2c3d4 \
    --integration-id a1b2c3 \
    --integration-uri arn:aws:apigateway:us-west-2:lambda:path/2015-03-31/functions/
arn:aws:lambda:us-west-2:123456789012:function:my-new-function/invocations
```

Salida:

```
{
    "ConnectionType": "INTERNET",
    "IntegrationId": "a1b2c3",
    "IntegrationMethod": "POST",
    "IntegrationType": "AWS_PROXY",
    "IntegrationUri": "arn:aws:apigateway:us-west-2:lambda:path/2015-03-31/
functions/arn:aws:lambda:us-west-2:123456789012:function:my-new-function/
invocations",
    "PayloadFormatVersion": "2.0",
    "TimeoutInMillis": 5000
}
```

Para obtener más información, consulte Creación de integraciones para las API de HTTP en API Gateway e Integraciones de API de WebSocket en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte UpdateIntegration en la Referencia de comandos de la AWS CLI.

`update-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-route`.

AWS CLI

Ejemplo 1: cómo actualizar la integración de una ruta

En el siguiente ejemplo de `update-route`, se actualiza la integración de una ruta especificada.

```
aws apigatewayv2 update-route \
    --api-id a1b2c3d4 \
    --route-id a1b2c3 \
    --target integrations/a1b2c6
```

Salida:

```
{
    "ApiKeyRequired": false,
    "AuthorizationType": "NONE",
    "RouteId": "a1b2c3",
    "RouteKey": "ANY /pets",
    "Target": "integrations/a1b2c6"
}
```

Ejemplo 2: cómo añadir un autorizador a una ruta

En el siguiente ejemplo de `update-route`, se actualiza la ruta especificada para que utilice un autorizador de JWT.

```
aws apigatewayv2 update-route \
    --api-id a1b2c3d4  \
    --route-id a1b2c3  \
    --authorization-type JWT \
    --authorizer-id a1b2c5 \
```

```
    --authorization-scopes user.id user.email
```

Salida:

```
{
    "ApiKeyRequired": false,
    "AuthorizationScopes": [
        "user.id",
        "user.email"
    ],
    "AuthorizationType": "JWT",
    "AuthorizerId": "a1b2c5",
    "OperationName": "GET HTTP",
    "RequestParameters": {},
    "RouteId": "a1b2c3",
    "RouteKey": "GET /pets",
    "Target": "integrations/a1b2c6"
}
```

Para obtener más información, consulte Control del acceso a las API de HTTP con autorizadores de JWT en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener más información sobre la API, consulte UpdateRoute en la Referencia de comandos de la AWS CLI.

`update-stage`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-stage`.

AWS CLI

Configuración de una limitación personalizada

En el siguiente ejemplo de `update-stage`, se configura la limitación personalizada de la etapa y la ruta especificadas de una API.

```
aws apigatewayv2 update-stage \
    --api-id a1b2c3d4 \
    --stage-name dev \
    --route-settings '{"GET /pets":
{"ThrottlingBurstLimit":100,"ThrottlingRateLimit":2000}}'
```

Salida:

```
{
    "CreatedDate": "2020-04-05T16:21:16+00:00",
    "DefaultRouteSettings": {
        "DetailedMetricsEnabled": false
    },
    "DeploymentId": "shktxb",
    "LastUpdatedDate": "2020-04-08T22:23:17+00:00",
    "RouteSettings": {
        "GET /pets": {
            "ThrottlingBurstLimit": 100,
            "ThrottlingRateLimit": 2000.0
        }
    },
    "StageName": "dev",
    "StageVariables": {},
    "Tags": {}
}
```

Para obtener más información, consulte Protección de sus API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener más información sobre la API, consulte UpdateStage en la Referencia de comandos de la AWS CLI.

`update-vpc-link`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-vpc-link`.

AWS CLI

Actualización de un enlace de VPC

En el siguiente ejemplo de `update-vpc-link`, se actualiza el nombre de un enlace de VPC. Después de crear un enlace de VPC, no puede cambiar sus subredes ni grupos de seguridad.

```
aws apigatewayv2 update-vpc-link \
    --vpc-link-id abcd123 \
    --name MyUpdatedVpcLink
```

Salida:

```
{
    "CreatedDate": "2020-04-07T00:27:47Z",
    "Name": "MyUpdatedVpcLink",
    "SecurityGroupIds": [
        "sg1234",
        "sg5678"
    ],
    "SubnetIds": [
        "subnet-aaaa",
        "subnet-bbbb"
    ],
    "Tags": {},
    "VpcLinkId": "abcd123",
    "VpcLinkStatus": "AVAILABLE",
    "VpcLinkStatusMessage": "VPC link is ready to route traffic",
    "VpcLinkVersion": "V2"
}
```

Para obtener más información, consulte Configuración de enlaces de VPC para las API de HTTP en API Gateway en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte UpdateVpcLink en la Referencia de comandos de la AWS CLI.

Ejemplos de API de administración de puertas de enlace de API que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo llevar a cabo acciones e implementar situaciones comunes mediante la AWS Command Line Interface con una API de administración de puertas de enlace de API.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`delete-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-connection`.

AWS CLI

Eliminación de una conexión WebSocket

En el siguiente ejemplo de `delete-connection`, se desconecta un cliente de la API de WebSocket especificada.

```
aws apigatewaymanagementapi delete-connection \
    --connection-id L0SM9cOFvHcCIhw= \
    --endpoint-url https://aabbccddee.execute-api.us-west-2.amazonaws.com/prod
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de comandos @connections en el servicio de backend en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener detalles sobre la API, consulte DeleteConnection en la Referencia de comandos de la AWS CLI.

`get-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-connection`.

AWS CLI

Para obtener información sobre una conexión WebSocket

En el siguiente ejemplo de `get-connection`, se describe una conexión a la API de WebSocket especificada.

```
aws apigatewaymanagementapi get-connection \
    --connection-id L0SM9cOFvHcCIhw= \
    --endpoint-url https://aabbccddee.execute-api.us-west-2.amazonaws.com/prod
```

Salida:

```
{
```

```
    "ConnectedAt": "2020-04-30T20:10:33.236Z",
    "Identity": {
        "SourceIp": "192.0.2.1"
    },
    "LastActiveAt": "2020-04-30T20:10:42.997Z"
}
```

Para obtener más información, consulte Uso de comandos @connections en el servicio de backend en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener detalles sobre la API, consulte GetConnection en la Referencia de comandos de la AWS CLI.

`post-to-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `post-to-connection`.

AWS CLI

Para enviar datos a una conexión WebSocket

En el siguiente ejemplo `post-to-connection` se envía un mensaje a un cliente que está conectado a la API de WebSocket especificada.

```
aws apigatewaymanagementapi post-to-connection \
    --connection-id L0SM9cOFvHcCIhw= \
    --data "Hello from API Gateway!" \
    --endpoint-url https://aabbccddee.execute-api.us-west-2.amazonaws.com/prod
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de comandos @connections en el servicio de backend en la Guía para desarrolladores de Amazon API Gateway.

- Para obtener información sobre la API, consulte PostToConnection en la Referencia de comandos de la AWS CLI.

Ejemplos de App Mesh que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar situaciones comunes usando la AWS Command Line Interface con App Mesh.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-mesh`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-mesh`.

AWS CLI

Ejemplo 1: cómo crear una nueva malla de servicios

En el siguiente ejemplo de `create-mesh`, se crea una malla de servicios.

```
aws appmesh create-mesh \
    --mesh-name app1
```

Salida:

```
{
    "mesh":{
        "meshName":"app1",
        "metadata":{
            "arn":"arn:aws:appmesh:us-east-1:123456789012:mesh/app1",
            "createdAt":1563809909.282,
            "lastUpdatedAt":1563809909.282,
            "uid":"a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version":1
        },
        "spec":{},
        "status":{
            "status":"ACTIVE"
        }
    }
```

```
}
```

Ejemplo 2: cómo crear una nueva malla de servicios con varias etiquetas

En el siguiente ejemplo de `create-mesh`, se crea una malla de servicios con varias etiquetas.

```
aws appmesh create-mesh \
    --mesh-name app2 \
    --tags key=key1,value=value1 key=key2,value=value2 key=key3,value=value3
```

Salida:

```
{
    "mesh":{
        "meshName":"app2",
        "metadata":{
            "arn":"arn:aws:appmesh:us-east-1:123456789012:mesh/app2",
            "createdAt":1563822121.877,
            "lastUpdatedAt":1563822121.877,
            "uid":"a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version":1
        },
        "spec":{},
        "status":{
            "status":"ACTIVE"
        }
    }
}
```

Para obtener más información, consulte Service Meshes en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte CreateMesh en la Referencia de comandos de la AWS CLI.

`create-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-route`.

AWS CLI

Creación de una nueva ruta gRPC

En el siguiente ejemplo de `create-route`, se usa un archivo de entrada JSON para crear una ruta gRPC. El tráfico de GRPC que tiene metadatos que comienzan por 123 se enruta a un nodo virtual denominado serviceBgrpc. Si hay errores específicos de gRPC, HTTP o TCP, al intentar comunicarse con el destino de la ruta, se vuelve a intentar la ruta tres veces. Hay un retraso de 15 segundos entre cada reintento.

```
aws appmesh create-route \
    --cli-input-json file://create-route-grpc.json
```

Contenido de `create-route-grpc.json`:

```
{
    "meshName" : "apps",
    "routeName" : "grpcRoute",
    "spec" : {
       "grpcRoute" : {
          "action" : {
             "weightedTargets" : [
                {
                   "virtualNode" : "serviceBgrpc",
                   "weight" : 100
                }
             ]
          },
          "match" : {
             "metadata" : [
                {
                   "invert" : false,
                   "match" : {
                      "prefix" : "123"
                   },
                   "name" : "myMetadata"
                }
             ],
             "methodName" : "GetColor",
             "serviceName" : "com.amazonaws.services.ColorService"
          },
          "retryPolicy" : {
             "grpcRetryEvents" : [ "deadline-exceeded" ],
             "httpRetryEvents" : [ "server-error", "gateway-error" ],
             "maxRetries" : 3,
             "perRetryTimeout" : {
```

```
                "unit" : "s",
                "value" : 15
             },
             "tcpRetryEvents" : [ "connection-error" ]
          }
       },
       "priority" : 100
    },
    "virtualRouterName" : "serviceBgrpc"
}
```

Salida:

```
{
    "route": {
        "meshName": "apps",
        "metadata": {
            "arn": "arn:aws:appmesh:us-west-2:123456789012:mesh/apps/virtualRouter/
serviceBgrpc/route/grpcRoute",
            "createdAt": 1572010806.008,
            "lastUpdatedAt": 1572010806.008,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 1
        },
        "routeName": "grpcRoute",
        "spec": {
            "grpcRoute": {
                "action": {
                    "weightedTargets": [
                        {
                            "virtualNode": "serviceBgrpc",
                            "weight": 100
                        }
                    ]
                },
                "match": {
                    "metadata": [
                        {
                            "invert": false,
                            "match": {
                                "prefix": "123"
                            },
                            "name": "mymetadata"
```

```
                        }
                    ],
                    "methodName": "GetColor",
                    "serviceName": "com.amazonaws.services.ColorService"
                },
                "retryPolicy": {
                    "grpcRetryEvents": [
                        "deadline-exceeded"
                    ],
                    "httpRetryEvents": [
                        "server-error",
                        "gateway-error"
                    ],
                    "maxRetries": 3,
                    "perRetryTimeout": {
                        "unit": "s",
                        "value": 15
                    },
                    "tcpRetryEvents": [
                        "connection-error"
                    ]
                }
            },
            "priority": 100
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualRouterName": "serviceBgrpc"
    }
}
```

Creación de una nueva ruta HTTP o HTTP/2

En el siguiente ejemplo de `create-route`, se usa un archivo de entrada JSON para crear una ruta HTTP/2. Para crear una ruta HTTP, sustituya http2Route por httpRoute según las especificaciones. Todo el tráfico HTTP/2 dirigido a cualquier prefijo de URL que tenga un valor de encabezado que comience por 123 se enruta a un nodo virtual denominado serviceBhttp2. Si hay errores específicos de HTTP o TCP al intentar comunicarse con el destino de la ruta, se vuelve a intentar la ruta tres veces. Hay un retraso de 15 segundos entre cada reintento.

```
aws appmesh create-route \
```

```
    --cli-input-json file://create-route-http2.json
```

Contenido de `create-route-http2.json`:

```
{
    "meshName": "apps",
    "routeName": "http2Route",
    "spec": {
        "http2Route": {
            "action": {
                "weightedTargets": [
                    {
                        "virtualNode": "serviceBhttp2",
                        "weight": 100
                    }
                ]
            },
            "match": {
                "headers": [
                    {
                        "invert": false,
                        "match": {
                            "prefix": "123"
                        },
                        "name": "clientRequestId"
                    }
                ],
                "method": "POST",
                "prefix": "/",
                "scheme": "http"
            },
            "retryPolicy": {
                "httpRetryEvents": [
                    "server-error",
                    "gateway-error"
                ],
                "maxRetries": 3,
                "perRetryTimeout": {
                    "unit": "s",
                    "value": 15
                },
                "tcpRetryEvents": [
                    "connection-error"
```

```
                ]
            }
        },
        "priority": 200
    },
    "virtualRouterName": "serviceBhttp2"
}
```

Salida:

```
{
    "route": {
        "meshName": "apps",
        "metadata": {
            "arn": "arn:aws:appmesh:us-west-2:123456789012:mesh/apps/virtualRouter/
serviceBhttp2/route/http2Route",
            "createdAt": 1572011008.352,
            "lastUpdatedAt": 1572011008.352,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 1
        },
        "routeName": "http2Route",
        "spec": {
            "http2Route": {
                "action": {
                    "weightedTargets": [
                        {
                            "virtualNode": "serviceBhttp2",
                            "weight": 100
                        }
                    ]
                },
                "match": {
                    "headers": [
                        {
                            "invert": false,
                            "match": {
                                "prefix": "123"
                            },
                            "name": "clientRequestId"
                        }
                    ],
                    "method": "POST",
```

```
                    "prefix": "/",
                    "scheme": "http"
                },
                "retryPolicy": {
                    "httpRetryEvents": [
                        "server-error",
                        "gateway-error"
                    ],
                    "maxRetries": 3,
                    "perRetryTimeout": {
                        "unit": "s",
                        "value": 15
                    },
                    "tcpRetryEvents": [
                        "connection-error"
                    ]
                }
            },
            "priority": 200
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualRouterName": "serviceBhttp2"
    }
}
```

Creación de una nueva ruta de TCP

En el siguiente ejemplo de `create-route`, se utiliza un archivo de entrada JSON para crear una ruta de TCP. El 75 % del tráfico se enruta a un nodo virtual denominado serviceBtcp y el 25 % del tráfico se enruta a un nodo virtual denominado serviceBv2tcp. Especificar diferentes ponderaciones para distintos destinos es una forma eficaz de implementar una nueva versión de una aplicación. Puede ajustar las ponderaciones para que, en última instancia, el cien por cien de todo el tráfico se enrute a un destino que tenga la nueva versión de una aplicación.

```
aws appmesh create-route \
    --cli-input-json file://create-route-tcp.json
```

Contenido de create-route-tcp.json:

```
{
```

```
    "meshName": "apps",
    "routeName": "tcpRoute",
    "spec": {
        "priority": 300,
        "tcpRoute": {
            "action": {
                "weightedTargets": [
                    {
                        "virtualNode": "serviceBtcp",
                        "weight": 75
                    },
                    {
                        "virtualNode": "serviceBv2tcp",
                        "weight": 25
                    }
                ]
            }
        }
    },
    "virtualRouterName": "serviceBtcp"
}
```

Salida:

```
{
    "route": {
        "meshName": "apps",
        "metadata": {
            "arn": "arn:aws:appmesh:us-west-2:123456789012:mesh/apps/virtualRouter/
serviceBtcp/route/tcpRoute",
            "createdAt": 1572011436.26,
            "lastUpdatedAt": 1572011436.26,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 1
        },
        "routeName": "tcpRoute",
        "spec": {
            "priority": 300,
            "tcpRoute": {
                "action": {
                    "weightedTargets": [
                        {
                            "virtualNode": "serviceBtcp",
```

```
                            "weight": 75
                        },
                        {
                            "virtualNode": "serviceBv2tcp",
                            "weight": 25
                        }
                    ]
                }
            }
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualRouterName": "serviceBtcp"
    }
}
```

Para obtener más información, consulte Routes en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte CreateRoute en la Referencia de comandos de la AWS CLI.

`create-virtual-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-virtual-gateway`.

AWS CLI

Creación de una nueva puerta de enlace virtual

El siguiente ejemplo de `create-virtual-gateway`, se utiliza un archivo de entrada JSON para crear una puerta de enlace virtual con un oyente para HTTP mediante el puerto 9080.

```
aws appmesh create-virtual-gateway \
    --mesh-name meshName \
    --virtual-gateway-name virtualGatewayName \
    --cli-input-json file://create-virtual-gateway.json
```

Contenido de `create-virtual-gateway.json`:

```
{
```

```
    "spec": {
      "listeners": [
        {
          "portMapping": {
            "port": 9080,
            "protocol": "http"
          }
        }
      ]
    }
}
```

Salida:

```
{
    "virtualGateway": {
        "meshName": "meshName",
        "metadata": {
            "arn": "arn:aws:appmesh:us-west-2:123456789012:mesh/meshName/
virtualGateway/virtualGatewayName",
            "createdAt": "2022-04-06T10:42:42.015000-05:00",
            "lastUpdatedAt": "2022-04-06T10:42:42.015000-05:00",
            "meshOwner": "123456789012",
            "resourceOwner": "123456789012",
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 1
        },
        "spec": {
            "listeners": [
                {
                    "portMapping": {
                        "port": 9080,
                        "protocol": "http"
                    }
                }
            ]
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualGatewayName": "virtualGatewayName"
    }
}
```

Para obtener más información, consulte Virtual Gateways en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte CreateVirtualGateway en la Referencia de comandos de la AWS CLI.

`create-virtual-node`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-virtual-node`.

AWS CLI

Ejemplo 1: cómo crear un nuevo nodo virtual que utilice DNS para la detección

En el siguiente ejemplo de `create-virtual-node`, se usa un archivo de entrada JSON para crear un nodo virtual que utilice DNS para la detección de servicios.

```
aws appmesh create-virtual-node \
    --cli-input-json file://create-virtual-node-dns.json
```

Contenido de `create-virtual-node-dns.json`:

```
{
    "meshName": "app1",
    "spec": {
        "listeners": [
            {
                "portMapping": {
                    "port": 80,
                    "protocol": "http"
                }
            }
        ],
        "serviceDiscovery": {
            "dns": {
                "hostname": "serviceBv1.svc.cluster.local"
            }
        }
    },
    "virtualNodeName": "vnServiceBv1"
}
```

Salida:

```
{
    "virtualNode": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualNode/
vnServiceBv1",
            "createdAt": 1563810019.874,
            "lastUpdatedAt": 1563810019.874,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 1
        },
        "spec": {
            "listeners": [
                {
                    "portMapping": {
                        "port": 80,
                        "protocol": "http"
                    }
                }
            ],
            "serviceDiscovery": {
                "dns": {
                    "hostname": "serviceBv1.svc.cluster.local"
                }
            }
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualNodeName": "vnServiceBv1"
    }
}
```

Ejemplo 2: cómo crear un nuevo nodo virtual que utilice AWS Cloud Map para la detección

En el siguiente ejemplo de `create-virtual-node`, se usa un archivo de entrada JSON para crear un nodo virtual que utilice AWS Cloud Map para la detección de servicios.

```
aws appmesh create-virtual-node \
    --cli-input-json file://create-virtual-node-cloud-map.json
```

Contenido de `create-virtual-node-cloud-map.json`:

```
{
    "meshName": "app1",
    "spec": {
        "backends": [
            {
                "virtualService": {
                    "virtualServiceName": "serviceA.svc.cluster.local"
                }
            }
        ],
        "listeners": [
            {
                "portMapping": {
                    "port": 80,
                    "protocol": "http"
                }
            }
        ],
        "serviceDiscovery": {
            "awsCloudMap": {
                "attributes": [
                    {
                        "key": "Environment",
                        "value": "Testing"
                    }
                ],
                "namespaceName": "namespace1",
                "serviceName": "serviceA"
            }
        }
    },
    "virtualNodeName": "vnServiceA"
}
```

Salida:

```
{
    "virtualNode": {
        "meshName": "app1",
        "metadata": {
```

```
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualNode/
vnServiceA",
            "createdAt": 1563810859.465,
            "lastUpdatedAt": 1563810859.465,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 1
        },
        "spec": {
            "backends": [
                {
                    "virtualService": {
                        "virtualServiceName": "serviceA.svc.cluster.local"
                    }
                }
            ],
            "listeners": [
                {
                    "portMapping": {
                        "port": 80,
                        "protocol": "http"
                    }
                }
            ],
            "serviceDiscovery": {
                "awsCloudMap": {
                    "attributes": [
                        {
                            "key": "Environment",
                            "value": "Testing"
                        }
                    ],
                    "namespaceName": "namespace1",
                    "serviceName": "serviceA"
                }
            }
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualNodeName": "vnServiceA"
    }
}
```

Para obtener más información, consulte Virtual Nodes en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte CreateVirtualNode en la Referencia de comandos de la AWS CLI.

`create-virtual-router`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-virtual-router`.

AWS CLI

Creación de un nuevo enrutador virtual

El siguiente ejemplo de `create-virtual-router`, se utiliza un archivo de entrada JSON para crear un enrutador virtual con un oyente para HTTP mediante el puerto 80.

```
aws appmesh create-virtual-router \
    --cli-input-json file://create-virtual-router.json
```

Contenido de `create-virtual-router.json`:

```
{
    "meshName": "app1",
    "spec": {
        "listeners": [
            {
                "portMapping": {
                    "port": 80,
                    "protocol": "http"
                }
            }
        ]
    },
    "virtualRouterName": "vrServiceB"
}
```

Salida:

```
{
    "virtualRouter": {
        "meshName": "app1",
```

```
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualRouter/
vrServiceB",
            "createdAt": 1563810546.59,
            "lastUpdatedAt": 1563810546.59,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 1
        },
        "spec": {
            "listeners": [
                {
                    "portMapping": {
                        "port": 80,
                        "protocol": "http"
                    }
                }
            ]
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualRouterName": "vrServiceB"
    }
}
```

Para obtener más información, consulte Virtual Routers en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte CreateVirtualRouter en la Referencia de comandos de la AWS CLI.

`create-virtual-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-virtual-service`.

AWS CLI

Ejemplo 1: cómo crear un nuevo servicio virtual con un proveedor de nodos virtuales

En el siguiente ejemplo de `create-virtual-service`, se usa un archivo de entrada JSON para crear un servicio virtual con un proveedor de nodos virtuales.

```
aws appmesh create-virtual-service \
```

```
    --cli-input-json file://create-virtual-service-virtual-node.json
```

Contenido de `create-virtual-service-virtual-node.json`:

```
{
    "meshName": "app1",
    "spec": {
        "provider": {
            "virtualNode": {
                "virtualNodeName": "vnServiceA"
            }
        }
    },
    "virtualServiceName": "serviceA.svc.cluster.local"
}
```

Salida:

```
{
    "virtualService": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualService/
serviceA.svc.cluster.local",
            "createdAt": 1563810859.474,
            "lastUpdatedAt": 1563810967.179,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 2
        },
        "spec": {
            "provider": {
                "virtualNode": {
                    "virtualNodeName": "vnServiceA"
                }
            }
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualServiceName": "serviceA.svc.cluster.local"
    }
}
```

Para obtener más información, consulte Virtual Node en la Guía del usuario de AWS App Mesh.

Ejemplo 2: cómo crear un nuevo servicio virtual con un proveedor de enrutadores virtuales

En el siguiente ejemplo de `create-virtual-service`, se usa un archivo de entrada JSON para crear un servicio virtual con un proveedor de enrutadores virtuales.

```
aws appmesh create-virtual-service \
    --cli-input-json file://create-virtual-service-virtual-router.json
```

Contenido de `create-virtual-service-virtual-router.json`:

```
{
    "meshName": "app1",
    "spec": {
        "provider": {
            "virtualRouter": {
                "virtualRouterName": "vrServiceB"
            }
        }
    },
    "virtualServiceName": "serviceB.svc.cluster.local"
}
```

Salida:

```
{
    "virtualService": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualService/
serviceB.svc.cluster.local",
            "createdAt": 1563908363.999,
            "lastUpdatedAt": 1563908363.999,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 1
        },
        "spec": {
            "provider": {
                "virtualRouter": {
                    "virtualRouterName": "vrServiceB"
                }
            }
```

```
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualServiceName": "serviceB.svc.cluster.local"
    }
}
```

Para obtener más información, consulte Virtual Services<https://docs.aws.amazon.com/app-mesh/latest/userguide/virtual_services.html> en la Guía del usuario de AWS App Mesh

- Para obtener información sobre la API, consulte CreateVirtualService en la Referencia de comandos de la AWS CLI.

`delete-mesh`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-mesh`.

AWS CLI

Eliminación de una malla de servicios

En el siguiente ejemplo de `delete-mesh`, se elimina la malla de servicios especificada.

```
aws appmesh delete-mesh \
    --mesh-name app1
```

Salida:

```
{
    "mesh": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1",
            "createdAt": 1563809909.282,
            "lastUpdatedAt": 1563824981.248,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 2
        },
        "spec": {
            "egressFilter": {
                "type": "ALLOW_ALL"
```

```
            }
        },
        "status": {
            "status": "DELETED"
        }
    }
}
```

Para obtener más información, consulte Service Meshes en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte DeleteMesh en la Referencia de comandos de la AWS CLI.

`delete-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-route`.

AWS CLI

Para eliminar una ruta

En el siguiente ejemplo de `delete-route`, se elimina la ruta especificada.

```
aws appmesh delete-route \
    --mesh-name app1 \
    --virtual-router-name vrServiceB \
    --route-name toVnServiceB-weighted
```

Salida:

```
{
    "route": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualRouter/
vrServiceB/route/toVnServiceB-weighted",
            "createdAt": 1563811384.015,
            "lastUpdatedAt": 1563823915.936,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 3
        },
```

```
        "routeName": "toVnServiceB-weighted",
        "spec": {
            "httpRoute": {
                "action": {
                    "weightedTargets": [
                        {
                            "virtualNode": "vnServiceBv1",
                            "weight": 80
                        },
                        {
                            "virtualNode": "vnServiceBv2",
                            "weight": 20
                        }
                    ]
                },
                "match": {
                    "prefix": "/"
                }
            }
        },
        "status": {
            "status": "DELETED"
        },
        "virtualRouterName": "vrServiceB"
    }
}
```

Para obtener más información, consulte Routes en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte DeleteRoute en la Referencia de comandos de la AWS CLI.

`delete-virtual-node`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-virtual-node`.

AWS CLI

Eliminación de un nodo virtual

En el siguiente ejemplo de `delete-virtual-node`, se elimina el nodo virtual especificado.

```
aws appmesh delete-virtual-node \
```

```
    --mesh-name app1 \
    --virtual-node-name vnServiceBv2
```

Salida:

```
{
    "virtualNode": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualNode/
vnServiceBv2",
            "createdAt": 1563810117.297,
            "lastUpdatedAt": 1563824700.678,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 2
        },
        "spec": {
            "backends": [],
            "listeners": [
                {
                    "portMapping": {
                        "port": 80,
                        "protocol": "http"
                    }
                }
            ],
            "serviceDiscovery": {
                "dns": {
                    "hostname": "serviceBv2.svc.cluster.local"
                }
            }
        },
        "status": {
            "status": "DELETED"
        },
        "virtualNodeName": "vnServiceBv2"
    }
}
```

Para obtener más información, consulte Virtual Nodes en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte DeleteVirtualNode en la Referencia de comandos de la AWS CLI.

delete-virtual-router

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-virtual-router`.

AWS CLI

Eliminación de un enrutador virtual

En el siguiente ejemplo de `delete-virtual-router`, se elimina el enrutador virtual especificado.

```
aws appmesh delete-virtual-router \
    --mesh-name app1 \
    --virtual-router-name vrServiceB
```

Salida:

```
{
    "virtualRouter": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualRouter/
vrServiceB",
            "createdAt": 1563810546.59,
            "lastUpdatedAt": 1563824253.467,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 3
        },
        "spec": {
            "listeners": [
                {
                    "portMapping": {
                        "port": 80,
                        "protocol": "http"
                    }
                }
            ]
        },
        "status": {
            "status": "DELETED"
        },
        "virtualRouterName": "vrServiceB"
    }
```

```
}
```

Para obtener más información, consulte Virtual Routers en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte DeleteVirtualRouter en la Referencia de comandos de la AWS CLI.

`delete-virtual-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-virtual-service`.

AWS CLI

Eliminación de un servicio virtual

En el siguiente ejemplo de `delete-virtual-service`, se elimina el servicio virtual especificado.

```
aws appmesh delete-virtual-service \
    --mesh-name app1 \
    --virtual-service-name serviceB.svc.cluster.local
```

Salida:

```
{
    "virtualService": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualService/
serviceB.svc.cluster.local",
            "createdAt": 1563908363.999,
            "lastUpdatedAt": 1563913940.866,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 3
        },
        "spec": {},
        "status": {
            "status": "DELETED"
        },
        "virtualServiceName": "serviceB.svc.cluster.local"
    }
```

```
}
```

Para obtener más información, consulte Virtual Service en la Guía del usuario de AWS.

- Para obtener información sobre la API, consulte DeleteVirtualService en la Referencia de comandos de la AWS CLI.

`describe-mesh`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-mesh`.

AWS CLI

Para describir una malla de servicios

En el siguiente ejemplo de `describe-mesh`, se ofrecen detalles sobre la malla de servicios especificada.

```
aws appmesh describe-mesh \
    --mesh-name app1
```

Salida:

```
{
    "mesh": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1",
            "createdAt": 1563809909.282,
            "lastUpdatedAt": 1563809909.282,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 1
        },
        "spec": {},
        "status": {
            "status": "ACTIVE"
        }
    }
}
```

Para obtener más información, consulte Service Meshes en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte DescribeMesh en la Referencia de comandos de la AWS CLI.

`describe-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-route`.

AWS CLI

Descripción de una ruta

En el siguiente ejemplo de `describe-route`, se ofrecen detalles sobre la ruta especificada.

```
aws appmesh describe-route \
    --mesh-name app1 \
    --virtual-router-name vrServiceB \
    --route-name toVnServiceB-weighted
```

Salida:

```
{
    "route": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualRouter/
vrServiceB/route/toVnServiceB-weighted",
            "createdAt": 1563811384.015,
            "lastUpdatedAt": 1563811384.015,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 1
        },
        "routeName": "toVnServiceB-weighted",
        "spec": {
            "httpRoute": {
                "action": {
                    "weightedTargets": [
                        {
                            "virtualNode": "vnServiceBv1",
                            "weight": 90
                        },
                        {
                            "virtualNode": "vnServiceBv2",
```

```
                            "weight": 10
                        }
                    ]
                },
                "match": {
                    "prefix": "/"
                }
            }
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualRouterName": "vrServiceB"
    }
}
```

Para obtener más información, consulte Routes en la Guía del usuario de AWS App Mesh.

- Para obtener más información sobre la API, consulte DescribeRoute en la Referencia de comandos de la AWS CLI.

`describe-virtual-node`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-virtual-node`.

AWS CLI

Descripción de un nodo virtual

En el siguiente ejemplo de `describe-virtual-node`, se ofrecen detalles sobre el nodo virtual especificado.

```
aws appmesh describe-virtual-node \
    --mesh-name app1 \
    --virtual-node-name vnServiceBv1
```

Salida:

```
{
    "virtualNode": {
        "meshName": "app1",
```

```
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualNode/
vnServiceBv1",
            "createdAt": 1563810019.874,
            "lastUpdatedAt": 1563810019.874,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 1
        },
        "spec": {
            "backends": [],
            "listeners": [
                {
                    "portMapping": {
                        "port": 80,
                        "protocol": "http"
                    }
                }
            ],
            "serviceDiscovery": {
                "dns": {
                    "hostname": "serviceBv1.svc.cluster.local"
                }
            }
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualNodeName": "vnServiceBv1"
    }
}
```

Para obtener más información, consulte Virtual Nodes en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte DescribeVirtualNode en la Referencia de comandos de la AWS CLI.

`describe-virtual-router`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-virtual-router`.

AWS CLI

Descripción de un enrutador virtual

En el siguiente ejemplo de `describe-virtual-router`, se ofrecen detalles sobre el enrutador virtual especificado.

```
aws appmesh describe-virtual-router \
    --mesh-name app1 \
    --virtual-router-name vrServiceB
```

Salida:

```
{
    "virtualRouter": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualRouter/
vrServiceB",
            "createdAt": 1563810546.59,
            "lastUpdatedAt": 1563810546.59,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 1
        },
        "spec": {
            "listeners": [
                {
                    "portMapping": {
                        "port": 80,
                        "protocol": "http"
                    }
                }
            ]
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualRouterName": "vrServiceB"
    }
}
```

Para obtener más información, consulte Virtual Routers en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte DescribeVirtualRouter en la Referencia de comandos de la AWS CLI.

describe-virtual-service

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-virtual-service`.

AWS CLI

Descripción de un servicio virtual

En el siguiente ejemplo de `describe-virtual-service`, se ofrecen detalles sobre el servicio virtual especificado.

```
aws appmesh describe-virtual-service \
    --mesh-name app1 \
    --virtual-service-name serviceB.svc.cluster.local
```

Salida:

```
{
    "virtualService": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualService/
serviceB.svc.cluster.local",
            "createdAt": 1563908363.999,
            "lastUpdatedAt": 1563908363.999,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 1
        },
        "spec": {
            "provider": {
                "virtualRouter": {
                    "virtualRouterName": "vrServiceB"
                }
            }
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualServiceName": "serviceB.svc.cluster.local"
    }
}
```

Para obtener más información, consulte Virtual Services en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte DescribeVirtualService en la Referencia de comandos de la AWS CLI.

`list-meshes`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-meshes`.

AWS CLI

Generación de una lista de mallas de servicio

En el siguiente ejemplo de `list-meshes`, se genera una lista de todas las mallas de servicio de la región de AWS actual.

```
aws appmesh list-meshes
```

Salida:

```
{
    "meshes": [
        {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1",
            "meshName": "app1"
        }
    ]
}
```

Para obtener más información, consulte Service Meshes en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte ListMeshes en la Referencia de comandos de la AWS CLI.

`list-routes`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-routes`.

AWS CLI

Generación de una lista de las rutas

En el siguiente `list-routes` ejemplo, se genera una lista de todas las rutas del enrutador virtual especificado.

```
aws appmesh list-routes \
    --mesh-name app1 \
    --virtual-router-name vrServiceB
```

Salida:

```
{
    "routes": [
        {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualRouter/
vrServiceB/route/toVnServiceB",
            "meshName": "app1",
            "routeName": "toVnServiceB-weighted",
            "virtualRouterName": "vrServiceB"
        }
    ]
}
```

Para obtener más información, consulte Routes en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte ListRoutes en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se genera una lista de todas las etiquetas asignadas al recurso especificado.

```
aws appmesh list-tags-for-resource \
```

```
    --resource-arn arn:aws:appmesh:us-east-1:123456789012:mesh/app1
```

Salida:

```
{
    "tags": [
        {
            "key": "key1",
            "value": "value1"
        },
        {
            "key": "key2",
            "value": "value2"
        },
        {
            "key": "key3",
            "value": "value3"
        }
    ]
}
```

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-virtual-nodes`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-virtual-nodes`.

AWS CLI

Generación de una lista de nodos virtuales

En el siguiente ejemplo de `list-virtual-nodes`, se genera una lista de todos los nodos virtuales de la malla de servicios especificada.

```
aws appmesh list-virtual-nodes \
    --mesh-name app1
```

Salida:

```
{
```

```
    "virtualNodes": [
        {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualNode/
vnServiceBv1",
            "meshName": "app1",
            "virtualNodeName": "vnServiceBv1"
        },
        {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualNode/
vnServiceBv2",
            "meshName": "app1",
            "virtualNodeName": "vnServiceBv2"
        }
    ]
}
```

Para obtener más información, consulte Virtual Nodes en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte ListVirtualNodes en la Referencia de comandos de la AWS CLI.

`list-virtual-routers`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-virtual-routers`.

AWS CLI

Generación de una lista de enrutadores virtuales

En el siguiente ejemplo de `list-virtual-routers`, se genera una lista de todos los enrutadores virtuales de la malla de servicios especificada.

```
aws appmesh list-virtual-routers \
    --mesh-name app1
```

Salida:

```
{
    "virtualRouters": [
        {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualRouter/
vrServiceB",
```

```
            "meshName": "app1",
            "virtualRouterName": "vrServiceB"
        }
    ]
}
```

Para obtener más información, consulte Virtual Routers en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte ListVirtualRouters en la Referencia de comandos de la AWS CLI.

`list-virtual-services`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-virtual-services`.

AWS CLI

Generación de una lista de servicios virtuales

En el siguiente ejemplo de `list-virtual-services`, se genera una lista de todos los servicios virtuales de la malla de servicios especificada.

```
aws appmesh list-virtual-services \
    --mesh-name app1
```

Salida:

```
{
    "virtualServices": [
        {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualService/
serviceA.svc.cluster.local",
            "meshName": "app1",
            "virtualServiceName": "serviceA.svc.cluster.local"
        },
        {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualService/
serviceB.svc.cluster.local",
            "meshName": "app1",
            "virtualServiceName": "serviceB.svc.cluster.local"
        }
```

```
    ]
}
```

Para obtener más información, consulte Virtual Services en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte ListVirtualServices en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para etiquetar un recurso

En el siguiente ejemplo de `tag-resource`, se añade la etiqueta `key1` con el valor `value1` al recurso especificado.

```
aws appmesh tag-resource \
    --resource-arn arn:aws:appmesh:us-east-1:123456789012:mesh/app1 \
    --tags key=key1,value=value1
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para retirar la etiqueta de un recurso

En el siguiente ejemplo de `untag-resource`, se elimina una etiqueta con la clave `key1` del recurso especificado.

```
aws appmesh untag-resource \
```

```
    --resource-arn arn:aws:appmesh:us-east-1:123456789012:mesh/app1 \
    --tag-keys key1
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-mesh`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-mesh`.

AWS CLI

Actualización de una malla de servicios

En el siguiente ejemplo de `update-mesh`, se utiliza un archivo de entrada JSON para actualizar una malla de servicios y permitir que todo el tráfico de salida externo se reenvíe intacto a través del proxy de Envoy.

```
aws appmesh update-mesh \
    --cli-input-json file://update-mesh.json
```

Contenido de `update-mesh.json`:

```
{
    "meshName": "app1",
    "spec": {
        "egressFilter": {
            "type": "ALLOW_ALL"
        }
    }
}
```

Salida:

```
{
    "mesh": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1",
```

```
            "createdAt": 1563809909.282,
            "lastUpdatedAt": 1563812829.687,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 2
        },
        "spec": {
            "egressFilter": {
                "type": "ALLOW_ALL"
            }
        },
        "status": {
            "status": "ACTIVE"
        }
    }
}
```

Para obtener más información, consulte Service Meshes en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte UpdateMesh en la Referencia de comandos de la AWS CLI.

`update-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-route`.

AWS CLI

Actualización de una ruta

En el siguiente ejemplo de `update-route`, se utiliza un archivo de entrada JSON para actualizar las ponderaciones de una ruta.

```
aws appmesh update-route \
    --cli-input-json file://update-route-weighted.json
```

Contenido de `update-route-weighted.json`:

```
{
    "meshName": "app1",
    "routeName": "toVnServiceB-weighted",
    "spec": {
```

```
        "httpRoute": {
            "action": {
                "weightedTargets": [
                    {
                        "virtualNode": "vnServiceBv1",
                        "weight": 80
                    },
                    {
                        "virtualNode": "vnServiceBv2",
                        "weight": 20
                    }
                ]
            },
            "match": {
                "prefix": "/"
            }
        }
    },
    "virtualRouterName": "vrServiceB"
}
```

Salida:

```
{
    "route": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualRouter/
vrServiceB/route/toVnServiceB-weighted",
            "createdAt": 1563811384.015,
            "lastUpdatedAt": 1563819600.022,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 2
        },
        "routeName": "toVnServiceB-weighted",
        "spec": {
            "httpRoute": {
                "action": {
                    "weightedTargets": [
                        {
                            "virtualNode": "vnServiceBv1",
                            "weight": 80
                        },
```

```
                        {
                            "virtualNode": "vnServiceBv2",
                            "weight": 20
                        }
                    ]
                },
                "match": {
                    "prefix": "/"
                }
            }
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualRouterName": "vrServiceB"
    }
}
```

Para obtener más información, consulte Routes en la Guía del usuario de AWS App Mesh.

- Para obtener más información sobre la API, consulte UpdateRoute en la Referencia de comandos de la AWS CLI.

`update-virtual-node`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-virtual-node`.

AWS CLI

Actualización de un nodo virtual

En el siguiente ejemplo de `update-virtual-node`, se utiliza un archivo de entrada JSON para añadir una comprobación de estado a un nodo virtual.

```
aws appmesh update-virtual-node \
    --cli-input-json file://update-virtual-node.json
```

Contenido de `update-virtual-node.json`:

```
{
    "clientToken": "500",
    "meshName": "app1",
```

```
    "spec": {
        "listeners": [
            {
                "healthCheck": {
                    "healthyThreshold": 5,
                    "intervalMillis": 10000,
                    "path": "/",
                    "port": 80,
                    "protocol": "http",
                    "timeoutMillis": 3000,
                    "unhealthyThreshold": 3
                },
                "portMapping": {
                    "port": 80,
                    "protocol": "http"
                }
            }
        ],
        "serviceDiscovery": {
            "dns": {
                "hostname": "serviceBv1.svc.cluster.local"
            }
        }
    },
    "virtualNodeName": "vnServiceBv1"
}
```

Salida:

```
{
    "virtualNode": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualNode/
vnServiceBv1",
            "createdAt": 1563810019.874,
            "lastUpdatedAt": 1563819234.825,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 2
        },
        "spec": {
            "listeners": [
                {
```

```
                    "healthCheck": {
                        "healthyThreshold": 5,
                        "intervalMillis": 10000,
                        "path": "/",
                        "port": 80,
                        "protocol": "http",
                        "timeoutMillis": 3000,
                        "unhealthyThreshold": 3
                    },
                    "portMapping": {
                        "port": 80,
                        "protocol": "http"
                    }
                }
            ],
            "serviceDiscovery": {
                "dns": {
                    "hostname": "serviceBv1.svc.cluster.local"
                }
            }
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualNodeName": "vnServiceBv1"
    }
}
```

Para obtener más información, consulte Virtual Nodes en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte UpdateVirtualNode en la Referencia de comandos de la AWS CLI.

`update-virtual-router`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-virtual-router`.

AWS CLI

Actualización de un enrutador virtual

El siguiente ejemplo de `update-virtual-router`, se utiliza un archivo de entrada JSON para actualizar un puerto de oyente de enrutador virtual.

```
aws appmesh update-virtual-router \
    --cli-input-json file://update-virtual-router.json
```

Contenido de `update-virtual-router.json`:

```
{
    "meshName": "app1",
    "spec": {
        "listeners": [
            {
                "portMapping": {
                    "port": 8080,
                    "protocol": "http"
                }
            }
        ]
    },
    "virtualRouterName": "vrServiceB"
}
```

Salida:

```
{
    "virtualRouter": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualRouter/
vrServiceB",
            "createdAt": 1563810546.59,
            "lastUpdatedAt": 1563819431.352,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 2
        },
        "spec": {
            "listeners": [
                {
                    "portMapping": {
                        "port": 8080,
                        "protocol": "http"
                    }
                }
            ]
```

```
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualRouterName": "vrServiceB"
    }
}
```

Para obtener más información, consulte Virtual Routers en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte UpdateVirtualRouter en la Referencia de comandos de la AWS CLI.

`update-virtual-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-virtual-service`.

AWS CLI

Actualización de un servicio virtual

En el siguiente ejemplo de `update-virtual-service`, se usa un archivo de entrada JSON para actualizar un servicio virtual de manera que utilice un proveedor de enrutadores virtuales.

```
aws appmesh update-virtual-service \
    --cli-input-json file://update-virtual-service.json
```

Contenido de `update-virtual-service.json`:

```
{
    "meshName": "app1",
    "spec": {
        "provider": {
            "virtualRouter": {
                "virtualRouterName": "vrServiceA"
            }
        }
    },
    "virtualServiceName": "serviceA.svc.cluster.local"
}
```

Salida:

```
{
    "virtualService": {
        "meshName": "app1",
        "metadata": {
            "arn": "arn:aws:appmesh:us-east-1:123456789012:mesh/app1/virtualService/
serviceA.svc.cluster.local",
            "createdAt": 1563810859.474,
            "lastUpdatedAt": 1563820257.411,
            "uid": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "version": 3
        },
        "spec": {
            "provider": {
                "virtualRouter": {
                    "virtualRouterName": "vrServiceA"
                }
            }
        },
        "status": {
            "status": "ACTIVE"
        },
        "virtualServiceName": "serviceA.svc.cluster.local"
    }
}
```

Para obtener más información, consulte Virtual Services en la Guía del usuario de AWS App Mesh.

- Para obtener información sobre la API, consulte UpdateVirtualService en la Referencia de comandos de la AWS CLI.

Ejemplos de App Runner que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar situaciones comunes usando la AWS Command Line Interface con App Runner.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-custom-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-custom-domain`.

AWS CLI

Asociación de un nombre de dominio y del subdominio www a un servicio

En el siguiente ejemplo de `associate-custom-domain`, se asocia un nombre de dominio personalizado que se controla con un servicio de App Runner. El nombre de dominio es el dominio raíz `example.com`, incluido el caso especial de subdominio `www.example.com`.

```
aws apprunner associate-custom-domain \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
    "DomainName": "example.com",
    "EnableWWWSubdomain": true
}
```

Salida:

```
{
    "CustomDomain": {
        "CertificateValidationRecords": [
            {
                "Name": "_70d3f50a94f7c72dc28784cf55db2f6b.example.com",
                "Status": "PENDING_VALIDATION",
                "Type": "CNAME",
```

```
                "Value": "_1270c137383c6307b6832db02504c4b0.bsgbmzkfwj.acm-
validations.aws."
            },
            {
                "Name": "_287870d3f50a94f7c72dc4cf55db2f6b.www.example.com",
                "Status": "PENDING_VALIDATION",
                "Type": "CNAME",
                "Value": "_832db01270c137383c6307b62504c4b0.mzkbsgbfwj.acm-
validations.aws."
            }
        ],
        "DomainName": "example.com",
        "EnableWWWSubdomain": true,
        "Status": "CREATING"
    },
    "DNSTarget": "psbqam834h.us-east-1.awsapprunner.com",
    "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa"
}
```

- Para obtener información sobre la API, consulte AssociateCustomDomain en la Referencia de comandos de la AWS CLI.

`create-auto-scaling-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-auto-scaling-configuration`.

AWS CLI

Creación de una configuración de escalado automático de alta disponibilidad

En el siguiente ejemplo de `create-auto-scaling-configuration`, se crea una configuración de escalado automático optimizada para alta disponibilidad estableciendo `MinSize` en un valor de 5. Con esta configuración, App Runner intenta distribuir las instancias de servicio en el mayor número posible de zonas de disponibilidad, hasta cinco, según la región de AWS.

Con la llamada se obtiene un objeto `AutoScalingConfiguration` y el resto de la configuración se establece en los valores predeterminados. En el ejemplo, esta es la primera llamada para crear una configuración denominada `high-availability`. La revisión se establece en 1 y se trata de la revisión más reciente.

```
aws apprunner create-auto-scaling-configuration \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "AutoScalingConfigurationName": "high-availability",
    "MinSize": 5
}
```

Salida:

```
{
    "AutoScalingConfiguration": {
        "AutoScalingConfigurationArn": "arn:aws:apprunner:us-
east-1:123456789012:autoscalingconfiguration/high-
availability/1/2f50e7656d7819fead0f59672e68042e",
        "AutoScalingConfigurationName": "high-availability",
        "AutoScalingConfigurationRevision": 1,
        "CreatedAt": "2020-11-03T00:29:17Z",
        "Latest": true,
        "Status": "ACTIVE",
        "MaxConcurrency": 100,
        "MaxSize": 50,
        "MinSize": 5
    }
}
```

- Para obtener información sobre la API, consulte CreateAutoScalingConfiguration en la Referencia de comandos de la AWS CLI.

`create-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-connection`.

AWS CLI

Creación de una conexión GitHub

En el siguiente ejemplo de `create-connection`, se crea una conexión a un repositorio de código de GitHub privado. El estado de la conexión después de una llamada correcta es

PENDING_HANDSHAKE. El motivo es que aún no ha tenido lugar un protocolo de enlace de autenticación con el proveedor. Se completa el protocolo de enlace con la consola de App Runner.

```
aws apprunner create-connection \
    --cli-input-json file://input.json
```

Contenido de input.json:

```
{
    "ConnectionName": "my-github-connection",
    "ProviderType": "GITHUB"
}
```

Salida:

```
{
    "Connection": {
        "ConnectionArn": "arn:aws:apprunner:us-east-1:123456789012:connection/my-
github-connection",
        "ConnectionName": "my-github-connection",
        "Status": "PENDING_HANDSHAKE",
        "CreatedAt": "2020-11-03T00:32:51Z",
        "ProviderType": "GITHUB"
    }
}
```

Para obtener más información, consulte Managing App Runner connections en la Guía para desarrolladores de AWS App Runner.

- Para obtener más información sobre la API, consulte CreateConnection en la Referencia de comandos de la AWS CLI.

create-service

En el siguiente ejemplo de código, se muestra cómo utilizar create-service.

AWS CLI

Ejemplo 1: cómo crear un servicio de repositorio de código fuente

En el siguiente ejemplo de `create-service`, se crea un servicio de App Runner basado en un repositorio de código fuente de Python.

```
aws apprunner create-service \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ServiceName": "python-app",
    "SourceConfiguration": {
        "AuthenticationConfiguration": {
            "ConnectionArn": "arn:aws:apprunner:us-east-1:123456789012:connection/
my-github-connection/e7656250f67242d7819feade6800f59e"
        },
        "AutoDeploymentsEnabled": true,
        "CodeRepository": {
            "RepositoryUrl": "https://github.com/my-account/python-hello",
            "SourceCodeVersion": {
                "Type": "BRANCH",
                "Value": "main"
            },
            "CodeConfiguration": {
                "ConfigurationSource": "API",
                "CodeConfigurationValues": {
                    "Runtime": "PYTHON_3",
                    "BuildCommand": "pip install -r requirements.txt",
                    "StartCommand": "python server.py",
                    "Port": "8080",
                    "RuntimeEnvironmentVariables": [
                        {
                            "NAME": "Jane"
                        }
                    ]
                }
            }
        }
    },
    "InstanceConfiguration": {
        "CPU": "1 vCPU",
        "Memory": "3 GB"
    }
```

```
}
```

Salida:

```
{
    "OperationId": "17fe9f55-7e91-4097-b243-fcabbb69a4cf",
    "Service": {
        "CreatedAt": "2020-11-20T19:05:25Z",
        "UpdatedAt": "2020-11-20T19:05:25Z",
        "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
        "ServiceId": "8fe1e10304f84fd2b0df550fe98a71fa",
        "ServiceName": "python-app",
        "ServiceUrl": "psbqam834h.us-east-1.awsapprunner.com",
        "SourceConfiguration": {
            "AuthenticationConfiguration": {
                "ConnectionArn": "arn:aws:apprunner:us-
east-1:123456789012:connection/my-github-connection/
e7656250f67242d7819feade6800f59e"
            },
            "AutoDeploymentsEnabled": true,
            "CodeRepository": {
                "CodeConfiguration": {
                    "CodeConfigurationValues": {
                        "BuildCommand": "pip install -r requirements.txt",
                        "Port": "8080",
                        "Runtime": "PYTHON_3",
                        "RuntimeEnvironmentVariables": [
                            {
                                "NAME": "Jane"
                            }
                        ],
                        "StartCommand": "python server.py"
                    },
                    "ConfigurationSource": "Api"
                },
                "RepositoryUrl": "https://github.com/my-account/python-hello",
                "SourceCodeVersion": {
                    "Type": "BRANCH",
                    "Value": "main"
                }
            }
        },
```

```
        "Status": "OPERATION_IN_PROGRESS",
        "InstanceConfiguration": {
            "CPU": "1 vCPU",
            "Memory": "3 GB"
        }
    }
}
```

Ejemplo 2: cómo crear un servicio de repositorio de código fuente

En el siguiente ejemplo de `create-service`, se crea un servicio de App Runner basado en un repositorio de código fuente de Python.

```
aws apprunner create-service \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ServiceName": "python-app",
    "SourceConfiguration": {
        "AuthenticationConfiguration": {
            "ConnectionArn": "arn:aws:apprunner:us-east-1:123456789012:connection/
my-github-connection/e7656250f67242d7819feade6800f59e"
        },
        "AutoDeploymentsEnabled": true,
        "CodeRepository": {
            "RepositoryUrl": "https://github.com/my-account/python-hello",
            "SourceCodeVersion": {
                "Type": "BRANCH",
                "Value": "main"
            },
            "CodeConfiguration": {
                "ConfigurationSource": "API",
                "CodeConfigurationValues": {
                    "Runtime": "PYTHON_3",
                    "BuildCommand": "pip install -r requirements.txt",
                    "StartCommand": "python server.py",
                    "Port": "8080",
                    "RuntimeEnvironmentVariables": [
                        {
                            "NAME": "Jane"
                        }
```

```
                    ]
                }
            }
        }
    },
    "InstanceConfiguration": {
        "CPU": "1 vCPU",
        "Memory": "3 GB"
    }
}
```

Salida:

```
{
    "OperationId": "17fe9f55-7e91-4097-b243-fcabbb69a4cf",
    "Service": {
        "CreatedAt": "2020-11-20T19:05:25Z",
        "UpdatedAt": "2020-11-20T19:05:25Z",
        "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
        "ServiceId": "8fe1e10304f84fd2b0df550fe98a71fa",
        "ServiceName": "python-app",
        "ServiceUrl": "psbqam834h.us-east-1.awsapprunner.com",
        "SourceConfiguration": {
            "AuthenticationConfiguration": {
                "ConnectionArn": "arn:aws:apprunner:us-
east-1:123456789012:connection/my-github-connection/
e7656250f67242d7819feade6800f59e"
            },
            "AutoDeploymentsEnabled": true,
            "CodeRepository": {
                "CodeConfiguration": {
                    "CodeConfigurationValues": {
                        "BuildCommand": "pip install -r requirements.txt",
                        "Port": "8080",
                        "Runtime": "PYTHON_3",
                        "RuntimeEnvironmentVariables": [
                            {
                                "NAME": "Jane"
                            }
                        ],
                        "StartCommand": "python server.py"
                    },
```

```
                    "ConfigurationSource": "Api"
                },
                "RepositoryUrl": "https://github.com/my-account/python-hello",
                "SourceCodeVersion": {
                    "Type": "BRANCH",
                    "Value": "main"
                }
            }
        },
        "Status": "OPERATION_IN_PROGRESS",
        "InstanceConfiguration": {
            "CPU": "1 vCPU",
            "Memory": "3 GB"
        }
    }
}
```

Ejemplo 3: cómo crear un servicio de repositorio de imagen de origen

En el siguiente ejemplo de `create-service`, se crea un servicio de App Runner basado en una imagen almacenada en Elastic Container Registry (ECR).

```
aws apprunner create-service \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ServiceName": "golang-container-app",
    "SourceConfiguration": {
        "AuthenticationConfiguration": {
            "AccessRoleArn": "arn:aws:iam::123456789012:role/my-ecr-role"
        },
        "AutoDeploymentsEnabled": true,
        "ImageRepository": {
            "ImageIdentifier": "123456789012.dkr.ecr.us-east-1.amazonaws.com/golang-
app:latest",
            "ImageConfiguration": {
                "Port": "8080",
                "RuntimeEnvironmentVariables": [
                    {
                        "NAME": "Jane"
                    }
```

```
                ]
            },
            "ImageRepositoryType": "ECR"
        }
    },
    "InstanceConfiguration": {
        "CPU": "1 vCPU",
        "Memory": "3 GB"
    }
}
```

Salida:

```
{
    "OperationId": "17fe9f55-7e91-4097-b243-fcabbb69a4cf",
    "Service": {
        "CreatedAt": "2020-11-06T23:15:30Z",
        "UpdatedAt": "2020-11-06T23:15:30Z",
        "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/golang-
container-app/51728f8a20ce46d39b25398a6c8e9d1a",
        "ServiceId": "51728f8a20ce46d39b25398a6c8e9d1a",
        "ServiceName": "golang-container-app",
        "ServiceUrl": "psbqam834h.us-east-1.awsapprunner.com",
        "SourceConfiguration": {
            "AuthenticationConfiguration": {
                "AccessRoleArn": "arn:aws:iam::123456789012:role/my-ecr-role"
            },
            "AutoDeploymentsEnabled": true,
            "ImageRepository": {
                "ImageIdentifier": "123456789012.dkr.ecr.us-east-1.amazonaws.com/
golang-app:latest",
                "ImageConfiguration": {
                    "Port": "8080",
                    "RuntimeEnvironmentVariables": [
                        {
                            "NAME": "Jane"
                        }
                    ]
                },
                "ImageRepositoryType": "ECR"
            }
        },
        "Status": "OPERATION_IN_PROGRESS",
```

```
        "InstanceConfiguration": {
            "CPU": "1 vCPU",
            "Memory": "3 GB"
        }
    }
}
```

- Para obtener información sobre la API, consulte CreateService en la Referencia de comandos de la AWS CLI.

`delete-auto-scaling-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-auto-scaling-configuration`.

AWS CLI

Ejemplo 1: cómo eliminar la última revisión activa de una configuración de escalado automático

En el siguiente ejemplo de `delete-auto-scaling-configuration`, se elimina la última revisión activa de una configuración de escalado automático de App Runner. Para eliminar la última revisión activa, especifique un nombre de recurso de Amazon (ARN) que termine con el nombre de la configuración, sin el componente de revisión.

En el ejemplo, existen dos revisiones antes de esta acción. Por lo tanto, se elimina la revisión 2 (la más reciente). Sin embargo, ahora se muestra `"Latest": false`, ya que, tras ser eliminada, ya no es la última revisión activa.

```
aws apprunner delete-auto-scaling-configuration \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "AutoScalingConfigurationArn": "arn:aws:apprunner:us-
east-1:123456789012:autoscalingconfiguration/high-availability"
}
```

Salida:

```
{
```

```
    "AutoScalingConfiguration": {
        "AutoScalingConfigurationArn": "arn:aws:apprunner:us-
east-1:123456789012:autoscalingconfiguration/high-availability/2/
e76562f50d78042e819fead0f59672e6",
        "AutoScalingConfigurationName": "high-availability",
        "AutoScalingConfigurationRevision": 2,
        "CreatedAt": "2021-02-25T17:42:59Z",
        "DeletedAt": "2021-03-02T08:07:06Z",
        "Latest": false,
        "Status": "INACTIVE",
        "MaxConcurrency": 30,
        "MaxSize": 90,
        "MinSize": 5
    }
}
```

Ejemplo 2: cómo eliminar una revisión específica de una configuración de escalado automático

En el siguiente ejemplo de `delete-auto-scaling-configuration`, se elimina una revisión específica de una configuración de escalado automático de App Runner. Para eliminar una revisión específica, especifique un ARN que incluya el número de revisión.

En el ejemplo, existen varias revisiones antes de esta acción. La acción elimina la revisión 1.

```
aws apprunner delete-auto-scaling-configuration \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "AutoScalingConfigurationArn": "arn:aws:apprunner:us-
east-1:123456789012:autoscalingconfiguration/high-availability/1"
}
```

Salida:

```
{
    "AutoScalingConfiguration": {
        "AutoScalingConfigurationArn": "arn:aws:apprunner:us-
east-1:123456789012:autoscalingconfiguration/high-
availability/1/2f50e7656d7819fead0f59672e68042e",
```

```
        "AutoScalingConfigurationName": "high-availability",
        "AutoScalingConfigurationRevision": 1,
        "CreatedAt": "2020-11-03T00:29:17Z",
        "DeletedAt": "2021-03-02T08:07:06Z",
        "Latest": false,
        "Status": "INACTIVE",
        "MaxConcurrency": 100,
        "MaxSize": 50,
        "MinSize": 5
    }
}
```

- Para obtener información sobre la API, consulte DeleteAutoScalingConfiguration en la Referencia de comandos de la AWS CLI.

`delete-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-connection`.

AWS CLI

Para eliminar una conexión

En el siguiente ejemplo de `delete-connection`, se elimina una conexión de App Runner. El estado de la conexión después de una llamada correcta es `DELETED`. El motivo es que la conexión ya no está disponible.

```
aws apprunner delete-connection \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ConnectionArn": "arn:aws:apprunner:us-east-1:123456789012:connection/my-github-
connection"
}
```

Salida:

```
{
    "Connection": {
```

```
        "ConnectionArn": "arn:aws:apprunner:us-east-1:123456789012:connection/my-
github-connection",
        "ConnectionName": "my-github-connection",
        "Status": "DELETED",
        "CreatedAt": "2020-11-03T00:32:51Z",
        "ProviderType": "GITHUB"
    }
}
```

- Para obtener detalles sobre la API, consulte DeleteConnection en la Referencia de comandos de la AWS CLI.

`delete-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-service`.

AWS CLI

Para eliminar un servicio

En el siguiente ejemplo de `delete-service`, se elimina un servicio de App Runner.

```
aws apprunner delete-service \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa"
}
```

Salida:

```
{
    "OperationId": "17fe9f55-7e91-4097-b243-fcabbb69a4cf",
    "Service": {
        "CreatedAt": "2020-11-20T19:05:25Z",
        "UpdatedAt": "2020-11-20T19:05:25Z",
        "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
```

```
        "ServiceId": "8fe1e10304f84fd2b0df550fe98a71fa",
        "ServiceName": "python-app",
        "ServiceUrl": "psbqam834h.us-east-1.awsapprunner.com",
        "SourceConfiguration": {
            "AuthenticationConfiguration": {
                "ConnectionArn": "arn:aws:apprunner:us-
east-1:123456789012:connection/my-github-connection/
e7656250f67242d7819feade6800f59e"
            },
            "AutoDeploymentsEnabled": true,
            "CodeRepository": {
                "CodeConfiguration": {
                    "CodeConfigurationValues": {
                        "BuildCommand": "pip install -r requirements.txt",
                        "Port": "8080",
                        "Runtime": "PYTHON_3",
                        "RuntimeEnvironmentVariables": [
                            {
                                "NAME": "Jane"
                            }
                        ],
                        "StartCommand": "python server.py"
                    },
                    "ConfigurationSource": "Api"
                },
                "RepositoryUrl": "https://github.com/my-account/python-hello",
                "SourceCodeVersion": {
                    "Type": "BRANCH",
                    "Value": "main"
                }
            }
        },
        "Status": "OPERATION_IN_PROGRESS",
        "InstanceConfiguration": {
            "CPU": "1 vCPU",
            "Memory": "3 GB"
        }
    }
}
```

- Para obtener información sobre la API, consulte DeleteService en la Referencia de comandos de la AWS CLI.

`describe-auto-scaling-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-auto-scaling-configuration`.

AWS CLI

Ejemplo 1: cómo describir la última revisión activa de una configuración de escalado automático

En el siguiente ejemplo de `describe-auto-scaling-configuration`, se obtiene una descripción de la última revisión activa de una configuración de escalado automático de App Runner. Para eliminar la última revisión activa, especifique un ARN que termine con el nombre de la configuración, sin el componente de revisión.

En el ejemplo, existen dos revisiones. Por lo tanto, se elimina la revisión 2 (la más reciente). El objeto resultante muestra `"Latest": true`.

```
aws apprunner describe-auto-scaling-configuration \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "AutoScalingConfigurationArn": "arn:aws:apprunner:us-
east-1:123456789012:autoscalingconfiguration/high-availability"
}
```

Salida:

```
{
    "AutoScalingConfiguration": {
        "AutoScalingConfigurationArn": "arn:aws:apprunner:us-
east-1:123456789012:autoscalingconfiguration/high-availability/2/
e76562f50d78042e819fead0f59672e6",
        "AutoScalingConfigurationName": "high-availability",
        "AutoScalingConfigurationRevision": 2,
        "CreatedAt": "2021-02-25T17:42:59Z",
        "Latest": true,
        "Status": "ACTIVE",
        "MaxConcurrency": 30,
        "MaxSize": 90,
```

```
        "MinSize": 5
    }
}
```

Ejemplo 2: cómo describir una revisión específica de una configuración de escalado automático

En el siguiente ejemplo de `describe-auto-scaling-configuration`, se obtiene una descripción de una revisión específica de una configuración de escalado automático de App Runner. Para describir una revisión específica, especifique un ARN que incluya el número de revisión.

En el ejemplo, existen varias revisiones y se consulta la revisión 1. El objeto resultante muestra `"Latest": false`.

```
aws apprunner describe-auto-scaling-configuration \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "AutoScalingConfigurationArn": "arn:aws:apprunner:us-
east-1:123456789012:autoscalingconfiguration/high-availability/1"
}
```

Salida:

```
{
    "AutoScalingConfiguration": {
        "AutoScalingConfigurationArn": "arn:aws:apprunner:us-
east-1:123456789012:autoscalingconfiguration/high-
availability/1/2f50e7656d7819fead0f59672e68042e",
        "AutoScalingConfigurationName": "high-availability",
        "AutoScalingConfigurationRevision": 1,
        "CreatedAt": "2020-11-03T00:29:17Z",
        "Latest": false,
        "Status": "ACTIVE",
        "MaxConcurrency": 100,
        "MaxSize": 50,
        "MinSize": 5
    }
}
```

- Para obtener información sobre la API, consulte DescribeAutoScalingConfiguration en la Referencia de comandos de la AWS CLI.

`describe-custom-domains`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-custom-domains`.

AWS CLI

Para obtener descripciones de nombres de dominio personalizados y asociados a un servicio

En el siguiente ejemplo de `describe-custom-domains`, se muestran descripciones y el estado de los nombres de dominio personalizados y asociados a un servicio de App Runner.

```
aws apprunner describe-custom-domains \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
    "DomainName": "example.com",
    "EnableWWWSubdomain": true
}
```

Salida:

```
{
    "CustomDomains": [
        {
            "CertificateValidationRecords": [
                {
                    "Name": "_70d3f50a94f7c72dc28784cf55db2f6b.example.com",
                    "Status": "PENDING_VALIDATION",
                    "Type": "CNAME",
                    "Value": "_1270c137383c6307b6832db02504c4b0.bsgbmzkfwj.acm-
validations.aws."
                },
                {
                    "Name": "_287870d3f50a94f7c72dc4cf55db2f6b.www.example.com",
```

```
                    "Status": "PENDING_VALIDATION",
                    "Type": "CNAME",
                    "Value": "_832db01270c137383c6307b62504c4b0.mzkbsgbfwj.acm-
validations.aws."
                }
            ],
            "DomainName": "example.com",
            "EnableWWWSubdomain": true,
            "Status": "PENDING_CERTIFICATE_DNS_VALIDATION"
        },
        {
            "CertificateValidationRecords": [
                {
                    "Name": "_a94f784c70d3f507c72dc28f55db2f6b.deals.example.com",
                    "Status": "SUCCESS",
                    "Type": "CNAME",
                    "Value": "_2db02504c1270c137383c6307b6834b0.bsgbmzkfwj.acm-
validations.aws."
                }
            ],
            "DomainName": "deals.example.com",
            "EnableWWWSubdomain": false,
            "Status": "ACTIVE"
        }
    ],
    "DNSTarget": "psbqam834h.us-east-1.awsapprunner.com",
    "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa"
}
```

- Para obtener información sobre la API, consulte DescribeCustomDomains en la Referencia de comandos de la AWS CLI.

`describe-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-service`.

AWS CLI

Para describir un servicio

En el siguiente ejemplo de `describe-service`, se obtiene una descripción de un servicio de App Runner.

```
aws apprunner describe-service \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa"
}
```

Salida:

```
{
    "Service": {
        "CreatedAt": "2020-11-20T19:05:25Z",
        "UpdatedAt": "2020-11-20T19:05:25Z",
        "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
        "ServiceId": "8fe1e10304f84fd2b0df550fe98a71fa",
        "ServiceName": "python-app",
        "ServiceUrl": "psbqam834h.us-east-1.awsapprunner.com",
        "SourceConfiguration": {
            "AuthenticationConfiguration": {
                "ConnectionArn": "arn:aws:apprunner:us-
east-1:123456789012:connection/my-github-connection/
e7656250f67242d7819feade6800f59e"
            },
            "AutoDeploymentsEnabled": true,
            "CodeRepository": {
                "CodeConfiguration": {
                    "CodeConfigurationValues": {
                        "BuildCommand": "pip install -r requirements.txt",
                        "Port": "8080",
                        "Runtime": "PYTHON_3",
                        "RuntimeEnvironmentVariables": [
                            {
                                "NAME": "Jane"
                            }
                        ],
                        "StartCommand": "python server.py"
                    },
                    "ConfigurationSource": "Api"
```

```
                },
                "RepositoryUrl": "https://github.com/my-account/python-hello",
                "SourceCodeVersion": {
                    "Type": "BRANCH",
                    "Value": "main"
                }
            }
        },
        "Status": "RUNNING",
        "InstanceConfiguration": {
            "CPU": "1 vCPU",
            "Memory": "3 GB"
        }
    }
}
```

- Para obtener información sobre la API, consulte DescribeService en la Referencia de comandos de la AWS CLI.

`disassociate-custom-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-custom-domain`.

AWS CLI

Desasociación de un nombre de dominio de un servicio

En el siguiente ejemplo de `disassociate-custom-domain`, se desasocia el dominio `example.com` de un servicio de App Runner. La llamada también desasocia el subdominio `www.example.com` que estaba asociado al dominio raíz.

```
aws apprunner disassociate-custom-domain \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
    "DomainName": "example.com"
}
```

Salida:

```
{
    "CustomDomain": {
        "CertificateValidationRecords": [
            {
                "Name": "_70d3f50a94f7c72dc28784cf55db2f6b.example.com",
                "Status": "PENDING_VALIDATION",
                "Type": "CNAME",
                "Value": "_1270c137383c6307b6832db02504c4b0.bsgbmzkfwj.acm-
validations.aws."
            },
            {
                "Name": "_287870d3f50a94f7c72dc4cf55db2f6b.www.example.com",
                "Status": "PENDING_VALIDATION",
                "Type": "CNAME",
                "Value": "_832db01270c137383c6307b62504c4b0.mzkbsgbfwj.acm-
validations.aws."
            }
        ],
        "DomainName": "example.com",
        "EnableWWWSubdomain": true,
        "Status": "DELETING"
    },
    "DNSTarget": "psbqam834h.us-east-1.awsapprunner.com",
    "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa"
}
```

- Para obtener información sobre la API, consulte DisassociateCustomDomain en la Referencia de comandos de la AWS CLI.

`list-auto-scaling-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-auto-scaling-configurations`.

AWS CLI

Generación de una lista paginada de las configuraciones de escalado automático de App Runner

En el siguiente ejemplo de `list-auto-scaling-configurations`, se genera una lista de todas las configuraciones de escalado automático de App Runner de la cuenta de AWS. En cada respuesta se indican hasta cinco configuraciones de escalado automático. `AutoScalingConfigurationName` y `LatestOnly` no se especifican. Los valores predeterminados hacen que aparezca la última revisión de todas las configuraciones activas.

En este ejemplo, la respuesta incluye dos resultados y no hay otros adicionales, por lo que no se obtiene ningún `NextToken`.

```
aws apprunner list-auto-scaling-configurations \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "MaxResults": 5
}
```

Salida:

```
{
    "AutoScalingConfigurationSummaryList": [
        {
            "AutoScalingConfigurationArn": "arn:aws:apprunner:us-
east-1:123456789012:autoscalingconfiguration/high-availability/2/
e76562f50d78042e819fead0f59672e6",
            "AutoScalingConfigurationName": "high-availability",
            "AutoScalingConfigurationRevision": 2
        },
        {
            "AutoScalingConfigurationArn": "arn:aws:apprunner:us-
east-1:123456789012:autoscalingconfiguration/low-
cost/1/50d7804e7656fead0f59672e62f2e819",
            "AutoScalingConfigurationName": "low-cost",
            "AutoScalingConfigurationRevision": 1
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte ListAutoScalingConfigurations en la Referencia de comandos de la AWS CLI.

`list-connections`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-connections`.

AWS CLI

Ejemplo 1: cómo generar una lista de todas las conexiones

En el siguiente ejemplo de `list-connections`, se genera una lista de todas las conexiones de App Runner de la cuenta de AWS.

```
aws apprunner list-connections
```

Salida:

```
{
    "ConnectionSummaryList": [
        {
            "ConnectionArn": "arn:aws:apprunner:us-east-1:123456789012:connection/
my-github-connection",
            "ConnectionName": "my-github-connection",
            "Status": "AVAILABLE",
            "CreatedAt": "2020-11-03T00:32:51Z",
            "ProviderType": "GITHUB"
        },
        {
            "ConnectionArn": "arn:aws:apprunner:us-east-1:123456789012:connection/
my-github-org-connection",
            "ConnectionName": "my-github-org-connection",
            "Status": "AVAILABLE",
            "CreatedAt": "2020-11-03T02:54:17Z",
            "ProviderType": "GITHUB"
        }
    ]
}
```

Ejemplo 2: cómo indicar una conexión por el nombre

En el siguiente ejemplo de `list-connections`, se indica una conexión por el nombre.

```
aws apprunner list-connections \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ConnectionName": "my-github-org-connection"
}
```

Salida:

```
{
    "ConnectionSummaryList": [
        {
            "ConnectionArn": "arn:aws:apprunner:us-east-1:123456789012:connection/
my-github-org-connection",
            "ConnectionName": "my-github-org-connection",
            "Status": "AVAILABLE",
            "CreatedAt": "2020-11-03T02:54:17Z",
            "ProviderType": "GITHUB"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte ListConnections en la Referencia de comandos de la AWS CLI.

`list-operations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-operations`.

AWS CLI

Generación de una lista de las operaciones realizadas en un servicio

En el siguiente ejemplo de `list-operations`, se genera una lista de todas las operaciones que se han realizado en un servicio de App Runner hasta el momento. En este ejemplo, el servicio es nuevo y solo se ha realizado una operación del tipo `CREATE_SERVICE`.

```
aws apprunner list-operations \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa"
}
```

Salida:

```
{
    "OperationSummaryList": [
        {
            "EndedAt": 1606156217,
            "Id": "17fe9f55-7e91-4097-b243-fcabbb69a4cf",
            "StartedAt": 1606156014,
            "Status": "SUCCEEDED",
            "TargetArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
            "Type": "CREATE_SERVICE",
            "UpdatedAt": 1606156217
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListOperations en la Referencia de comandos de la AWS CLI.

`list-services`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-services`.

AWS CLI

Generación de una lista paginada de los servicios de App Runner

En el siguiente ejemplo de `list-services`, se genera una lista de todas las conexiones de App Runner de la cuenta de AWS. En cada respuesta se muestran hasta dos servicios. En este ejemplo, se muestra la primera solicitud. La respuesta incluye dos resultados y un token que se puede usar en la siguiente solicitud. Cuando una respuesta posterior no incluye un token, se muestran todos los servicios.

```
aws apprunner list-services \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "MaxResults": 2
}
```

Salida:

```
{
    "NextToken":
 "eyJDdXN0b21lckFjY291bnRJZCI6IjI3MDIwNTQwMjg0NSIsIlNlcnZpY2VTdGF0dXNDb2RlIjoiUFJPVklTU9OU
    "ServiceSummaryList": [
        {
            "CreatedAt": "2020-11-20T19:05:25Z",
            "UpdatedAt": "2020-11-23T12:41:37Z",
            "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
            "ServiceId": "8fe1e10304f84fd2b0df550fe98a71fa",
            "ServiceName": "python-app",
            "ServiceUrl": "psbqam834h.us-east-1.awsapprunner.com",
            "Status": "RUNNING"
        },
        {
            "CreatedAt": "2020-11-06T23:15:30Z",
            "UpdatedAt": "2020-11-23T13:21:22Z",
            "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/golang-
container-app/ab8f94cfe29a460fb8760afd2ee87555",
            "ServiceId": "ab8f94cfe29a460fb8760afd2ee87555",
            "ServiceName": "golang-container-app",
            "ServiceUrl": "e2m8rrrx33.us-east-1.awsapprunner.com",
            "Status": "RUNNING"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListServices en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Generación de una lista de las etiquetas asociadas a un servicio de App Runner

En el siguiente ejemplo de `list-tags-for-resource`, se muestran todas las etiquetas asociadas con un servicio de App Runner.

```
aws apprunner list-tags-for-resource \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ResourceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa"
}
```

Salida:

```
{
    "Tags": [
        {
            "Key": "Department",
            "Value": "Retail"
        },
        {
            "Key": "CustomerId",
            "Value": "56439872357912"
        }
    ]
}
```

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`pause-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `pause-service`.

AWS CLI

Pausa de un servicio

En el siguiente ejemplo de `pause-service`, se pausa un servicio de App Runner.

```
aws apprunner pause-service \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa"
}
```

Salida:

```
{
    "OperationId": "17fe9f55-7e91-4097-b243-fcabbb69a4cf",
    "Service": {
        "CreatedAt": "2020-11-20T19:05:25Z",
        "UpdatedAt": "2020-11-23T12:41:37Z",
        "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
        "ServiceId": "8fe1e10304f84fd2b0df550fe98a71fa",
        "ServiceName": "python-app",
        "ServiceUrl": "psbqam834h.us-east-1.awsapprunner.com",
        "SourceConfiguration": {
            "AuthenticationConfiguration": {
                "ConnectionArn": "arn:aws:apprunner:us-
east-1:123456789012:connection/my-github-connection/
e7656250f67242d7819feade6800f59e"
            },
            "AutoDeploymentsEnabled": true,
            "CodeRepository": {
                "CodeConfiguration": {
                    "CodeConfigurationValues": {
                        "BuildCommand": "pip install -r requirements.txt",
                        "Port": "8080",
                        "Runtime": "PYTHON_3",
                        "RuntimeEnvironmentVariables": [
                            {
                                "NAME": "Jane"
                            }
                        ],
```

```
                    "StartCommand": "python server.py"
                },
                "ConfigurationSource": "Api"
            },
            "RepositoryUrl": "https://github.com/my-account/python-hello",
            "SourceCodeVersion": {
                "Type": "BRANCH",
                "Value": "main"
            }
        }
    },
    "Status": "OPERATION_IN_PROGRESS",
    "InstanceConfiguration": {
        "CPU": "1 vCPU",
        "Memory": "3 GB"
    }
}
}
```

- Para obtener información sobre la API, consulte PauseService en la Referencia de comandos de la AWS CLI.

`resume-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `resume-service`.

AWS CLI

Reanudación de un servicio

En el siguiente ejemplo de `resume-service`, se reanuda un servicio de App Runner.

```
aws apprunner resume-service \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa"
}
```

Salida:

```
{
    "OperationId": "17fe9f55-7e91-4097-b243-fcabbb69a4cf",
    "Service": {
        "CreatedAt": "2020-11-20T19:05:25Z",
        "UpdatedAt": "2020-11-23T12:41:37Z",
        "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
        "ServiceId": "8fe1e10304f84fd2b0df550fe98a71fa",
        "ServiceName": "python-app",
        "ServiceUrl": "psbqam834h.us-east-1.awsapprunner.com",
        "SourceConfiguration": {
            "AuthenticationConfiguration": {
                "ConnectionArn": "arn:aws:apprunner:us-
east-1:123456789012:connection/my-github-connection/
e7656250f67242d7819feade6800f59e"
            },
            "AutoDeploymentsEnabled": true,
            "CodeRepository": {
                "CodeConfiguration": {
                    "CodeConfigurationValues": {
                        "BuildCommand": "pip install -r requirements.txt",
                        "Port": "8080",
                        "Runtime": "PYTHON_3",
                        "RuntimeEnvironmentVariables": [
                            {
                                "NAME": "Jane"
                            }
                        ],
                        "StartCommand": "python server.py"
                    },
                    "ConfigurationSource": "Api"
                },
                "RepositoryUrl": "https://github.com/my-account/python-hello",
                "SourceCodeVersion": {
                    "Type": "BRANCH",
                    "Value": "main"
                }
            }
        },
        "Status": "OPERATION_IN_PROGRESS",
        "InstanceConfiguration": {
            "CPU": "1 vCPU",
```

```
            "Memory": "3 GB"
        }
    }
}
```

- Para obtener información sobre la API, consulte ResumeService en la Referencia de comandos de la AWS CLI.

`start-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-deployment`.

AWS CLI

Inicio de una implementación manual

En el siguiente ejemplo de `start-deployment`, se realiza una implementación manual en un servicio de App Runner.

```
aws apprunner start-deployment \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa"
}
```

Salida:

```
{
    "OperationId": "853a7d5b-fc9f-4730-831b-fd8037ab832a"
}
```

- Para obtener información sobre la API, consulte StartDeployment en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Adición de etiquetas a un servicio de App Runner

En el siguiente ejemplo de `tag-resource`, se añaden dos etiquetas a un servicio de App Runner.

```
aws apprunner tag-resource \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ResourceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
    "Tags": [
        {
            "Key": "Department",
            "Value": "Retail"
        },
        {
            "Key": "CustomerId",
            "Value": "56439872357912"
        }
    ]
}
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de etiquetas de un servicio de App Runner

En el siguiente ejemplo de `untag-resource`, se eliminan dos etiquetas de un servicio de App Runner.

```
aws apprunner untag-resource \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ResourceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
    "TagKeys": [
        "Department",
        "CustomerId"
    ]
}
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-service`.

AWS CLI

Actualización del tamaño de memoria

En el siguiente ejemplo de `update-service`, se actualiza a 2048 MiB el tamaño de memoria de las instancias (unidades de escalado) de un servicio de App Runner.

Cuando la llamada se realiza correctamente, App Runner inicia un proceso de actualización asíncrono. La estructura de `Service` que devuelve la llamada refleja el nuevo valor de memoria que aplica esta llamada.

```
aws apprunner update-service \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
```

```
    "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
    "InstanceConfiguration": {
        "Memory": "4 GB"
    }
}
```

Salida:

```
{
    "OperationId": "17fe9f55-7e91-4097-b243-fcabbb69a4cf",
    "Service": {
        "CreatedAt": "2020-11-20T19:05:25Z",
        "UpdatedAt": "2020-11-23T12:41:37Z",
        "ServiceArn": "arn:aws:apprunner:us-east-1:123456789012:service/python-
app/8fe1e10304f84fd2b0df550fe98a71fa",
        "ServiceId": "8fe1e10304f84fd2b0df550fe98a71fa",
        "ServiceName": "python-app",
        "ServiceUrl": "psbqam834h.us-east-1.awsapprunner.com",
        "SourceConfiguration": {
            "AuthenticationConfiguration": {
                "ConnectionArn": "arn:aws:apprunner:us-
east-1:123456789012:connection/my-github-connection/
e7656250f67242d7819feade6800f59e"
            },
            "AutoDeploymentsEnabled": true,
            "CodeRepository": {
                "CodeConfiguration": {
                    "CodeConfigurationValues": {
                        "BuildCommand": "pip install -r requirements.txt",
                        "Port": "8080",
                        "Runtime": "PYTHON_3",
                        "RuntimeEnvironmentVariables": [
                            {
                                "NAME": "Jane"
                            }
                        ],
                        "StartCommand": "python server.py"
                    },
                    "ConfigurationSource": "Api"
                },
                "RepositoryUrl": "https://github.com/my-account/python-hello",
                "SourceCodeVersion": {
```

```
                    "Type": "BRANCH",
                    "Value": "main"
                }
            }
        },
        "Status": "OPERATION_IN_PROGRESS",
        "InstanceConfiguration": {
            "CPU": "1 vCPU",
            "Memory": "4 GB"
        }
    }
}
```

- Para obtener información sobre la API, consulte UpdateService en la Referencia de comandos de la AWS CLI.

AWS AppConfig Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS AppConfig.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-application`.

AWS CLI

Para crear una aplicación

En el siguiente ejemplo de `create-application`, se crea una aplicación en AWS AppConfig.

```
aws appconfig create-application \
    --name "example-application" \
    --description "An application used for creating an example."
```

Salida:

```
{
    "Description": "An application used for creating an example.",
    "Id": "339ohji",
    "Name": "example-application"
}
```

Para obtener más información, consulte Step 1: Creating an AWS AppConfig application en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte CreateApplication en la Referencia de comandos de la AWS CLI.

`create-configuration-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-configuration-profile`.

AWS CLI

Para crear un perfil de configuración

En el siguiente ejemplo de `create-configuration-profile`, se crea un perfil de configuración mediante una configuración almacenada en Parameter Store, una funcionalidad de Systems Manager.

```
aws appconfig create-configuration-profile \
    --application-id "339ohji" \
    --name "Example-Configuration-Profile" \
    --location-uri "ssm-parameter://Example-Parameter" \
    --retrieval-role-arn "arn:aws:iam::111122223333:role/Example-App-Config-Role"
```

Salida:

```
{
```

```
    "ApplicationId": "339ohji",
    "Description": null,
    "Id": "ur8hx2f",
    "LocationUri": "ssm-parameter://Example-Parameter",
    "Name": "Example-Configuration-Profile",
    "RetrievalRoleArn": "arn:aws:iam::111122223333:role/Example-App-Config-Role",
    "Type": null,
    "Validators": null
}
```

Para obtener más información, consulte Step 3: Creating a configuration and a configuration profile en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte CreateConfigurationProfile en la Referencia de comandos de la AWS CLI.

`create-environment`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-environment`.

AWS CLI

Para crear un entorno

En el siguiente ejemplo de `create-environment`, se crea un entorno de AWS AppConfig denominado Example-Environment con la aplicación creada con create-application.

```
aws appconfig create-environment \
    --application-id "339ohji" \
    --name "Example-Environment"
```

Salida:

```
{
    "ApplicationId": "339ohji",
    "Description": null,
    "Id": "54j1r29",
    "Monitors": null,
    "Name": "Example-Environment",
    "State": "ReadyForDeployment"
}
```

Para obtener más información, consulte Step 2: Creating an environment en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte CreateEnvironment en la Referencia de comandos de la AWS CLI.

`create-extension-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-extension-association`.

AWS CLI

Para crear una asociación de extensiones

En el siguiente ejemplo de `create-extension-association`, se crea una nueva asociación de extensiones en AWS AppConfig.

```
aws appconfig create-extension-association \
    --region us-west-2 \
    --extension-identifier S3-backup-extension \
    --resource-identifier "arn:aws:appconfig:us-west-2:123456789012:application/
Finance" \
    --parameters S3bucket=FinanceConfigurationBackup
```

Salida:

```
{
  "Id": "a1b2c3d4",
  "ExtensionArn": "arn:aws:appconfig:us-west-2:123456789012:extension/S3-backup-
extension/1",
  "ResourceArn": "arn:aws:appconfig:us-west-2:123456789012:application/Finance",
  "Parameters": {
    "S3bucket": "FinanceConfigurationBackup"
  },
  "ExtensionVersionNumber": 1
}
```

Para obtener más información, consulte Working with AWS AppConfig extensions en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte CreateExtensionAssociation en la Referencia de comandos de la AWS CLI.

`create-extension`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-extension`.

AWS CLI

Para crear una extensión

En el siguiente ejemplo de `create-extension`, se crea una nueva extensión en AWS AppConfig.

```
aws appconfig create-extension \
    --region us-west-2 \
    --name S3-backup-extension \
    --
actions PRE_CREATE_HOSTED_CONFIGURATION_VERSION=[{Name=S3backup,Uri=arn:aws:lambda:us-
west-2:123456789012:function:s3backupfunction,RoleArn=arn:aws:iam::123456789012:role/
appconfigextensionrole}] \
    --parameters S3bucket={Required=true}
```

Salida:

```
{
    "Id": "1A2B3C4D",
    "Name": "S3-backup-extension",
    "VersionNumber": 1,
    "Arn": "arn:aws:appconfig:us-west-2:123456789012:extension/1A2B3C4D/1",
    "Actions": {
        "PRE_CREATE_HOSTED_CONFIGURATION_VERSION": [
            {
                "Name": "S3backup",
                "Uri": "arn:aws:lambda:us-
west-2:123456789012:function:s3backupfunction",
                "RoleArn": "arn:aws:iam::123456789012:role/appconfigextensionrole"
            }
        ]
    },
    "Parameters": {
        "S3bucket": {
            "Required": true
        }
    }
}
```

Para obtener más información, consulte Working with AWS AppConfig extensions en la Guía del usuario de AWS AppConfig.

- Para obtener más información sobre la API, consulte CreateExtension en la Referencia de comandos de la AWS CLI.

`create-hosted-configuration-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-hosted-configuration-version`.

AWS CLI

Para crear una versión de configuración alojada

En el siguiente ejemplo de `create-hosted-configuration-version`, se crea una nueva configuración en el almacén de configuración alojado de AWS AppConfig. El contenido de la configuración debe convertirse primero a base64.

```
aws appconfig create-hosted-configuration-version \
    --application-id "339ohji" \
    --configuration-profile-id "ur8hx2f" \
    --
content eyAiTmFtZSI6ICJFeGFtcGxlQXBwbGljYXRpb24iLCAiSWQiOiBFeGFtcGxlSUQsICJSYW5rIjogNyB9
 \
    --content-type "application/json" \
    configuration_version_output_file
```

Contenido de `configuration_version_output_file`:

```
{ "Name": "ExampleApplication", "Id": ExampleID, "Rank": 7 }
```

Salida:

```
{
    "ApplicationId": "339ohji",
    "ConfigurationProfileId": "ur8hx2f",
    "VersionNumber": "1",
    "ContentType": "application/json"
}
```

Para obtener más información, consulte About the AWS AppConfig hosted configuration store en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte CreateHostedConfigurationVersion en la Referencia de comandos de la AWS CLI.

`delete-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-application`.

AWS CLI

Para eliminar una aplicación de

En el siguiente ejemplo de `delete-application`, se elimina la aplicación especificada.

```
aws appconfig delete-application \
--application-id 339ohji
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Step 1: Creating an AWS AppConfig application en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte DeleteApplication en la Referencia de comandos de la AWS CLI.

`delete-configuration-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-configuration-profile`.

AWS CLI

Para eliminar un perfil de configuración

En el siguiente ejemplo de `delete-configuration-profile`, se elimina el perfil de configuración especificado.

```
aws appconfig delete-configuration-profile \
    --application-id 339ohji \
    --configuration-profile-id ur8hx2f
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Step 3: Creating a configuration and a configuration profile en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte DeleteConfigurationProfile en la Referencia de comandos de la AWS CLI.

`delete-deployment-strategy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-deployment-strategy`.

AWS CLI

Para eliminar una estrategia de implementación

En el siguiente ejemplo de `delete-deployment-strategy`, se elimina la estrategia de implementación especificada.

```
aws appconfig delete-deployment-strategy \
    --deployment-strategy-id 1225qzk
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Step 4: Creating a deployment strategy en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte DeleteDeploymentStrategy en la Referencia de comandos de la AWS CLI.

`delete-environment`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-environment`.

AWS CLI

Para eliminar un entorno

En el siguiente ejemplo de `delete-environment`, se elimina el entorno de aplicación especificado.

```
aws appconfig delete-environment \
```

```
    --application-id 339ohji \
    --environment-id 54j1r29
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Step 2: Creating an environment en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte DeleteEnvironment en la Referencia de comandos de la AWS CLI.

`delete-extension-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-extension-association`.

AWS CLI

Para eliminar una asociación de extensiones

En el siguiente ejemplo de `delete-extension-association`, se elimina una asociación de extensiones de AWS AppConfig.

```
aws appconfig delete-extension-association \
    --region us-west-2 \
    --extension-association-id a1b2c3d4
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with AWS AppConfig extensions en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte DeleteExtensionAssociation en la Referencia de comandos de la AWS CLI.

`delete-extension`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-extension`.

AWS CLI

Para eliminar una extensión

En el siguiente ejemplo de `delete-extension`, se elimina una extensión de AWS AppConfig.

```
aws appconfig delete-extension \
    --region us-west-2 \
    --extension-identifier S3-backup-extension
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with AWS AppConfig extensions en la Guía del usuario de AWS AppConfig.

- Para obtener más información sobre la API, consulte DeleteExtension en la Referencia de comandos de la AWS CLI.

`delete-hosted-configuration-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-hosted-configuration-version`.

AWS CLI

Para eliminar una versión de configuración alojada

En el siguiente ejemplo de `delete-hosted-configuration-version`, se elimina una versión de configuración alojada del almacén de configuración alojado de AWS AppConfig.

```
aws appconfig delete-hosted-configuration-version \
    --application-id 339ohji \
    --configuration-profile-id ur8hx2f \
    --version-number 1
```

Salida: este comando no genera ninguna salida.

Para obtener más información, consulte Step 3: Creating a configuration and a configuration profile en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte DeleteHostedConfigurationVersion en la Referencia de comandos de la AWS CLI.

`get-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-application`.

AWS CLI

Para generar una lista de detalles de una aplicación

En el siguiente ejemplo de `get-application`, se genera una lista de detalles de la aplicación especificada.

```
aws appconfig get-application \
    --application-id 339ohji
```

Salida:

```
{
    "Description": "An application used for creating an example.",
    "Id": "339ohji",
    "Name": "example-application"
}
```

Para obtener más información, consulte How AWS AppConfig works en la Guía del usuario de AWS AppConfig.

- Para obtener más información sobre la API, consulte GetApplication en la Referencia de comandos de la AWS CLI.

`get-configuration-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-configuration-profile`.

AWS CLI

Para recuperar los detalles del perfil de configuración

En el siguiente ejemplo de `get-configuration-profile`, se ofrecen los detalles del perfil de configuración especificado.

```
aws appconfig get-configuration-profile \
    --application-id 339ohji \
    --configuration-profile-id ur8hx2f
```

Salida:

```
{
```

```
    "ApplicationId": "339ohji",
    "Id": "ur8hx2f",
    "Name": "Example-Configuration-Profile",
    "LocationUri": "ssm-parameter://Example-Parameter",
    "RetrievalRoleArn": "arn:aws:iam::111122223333:role/Example-App-Config-Role"
}
```

Para obtener más información, consulte Step 3: Creating a configuration and a configuration profile en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte GetConfigurationProfile en la Referencia de comandos de la AWS CLI.

`get-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-configuration`.

AWS CLI

Para recuperar los detalles de configuración

En el siguiente ejemplo de `get-configuration`, se ofrecen los detalles de configuración de la aplicación de ejemplo. En llamadas posteriores a get-configuration, utilice el parámetro `client-configuration-version` para actualizar la configuración de la aplicación únicamente si la versión ha cambiado. Al actualizar la configuración solo cuando la versión ha cambiado, se evitan los cargos excesivos que se generen al llamar a get-configuration.

```
aws appconfig get-configuration \
    --application "example-application" \
    --environment "Example-Environment" \
    --configuration "Example-Configuration-Profile" \
    --client-id "test-id" \
    configuration-output-file
```

Contenido de `configuration-output-file`:

```
{ "Name": "ExampleApplication", "Id": ExampleID, "Rank": 7 }
```

Salida:

```
{
```

```
    "ConfigurationVersion": "1",
    "ContentType": "application/json"
}
```

Para obtener más información, consulte Step 6: Receiving the configuration en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte GetConfiguration en la Referencia de comandos de la AWS CLI.

`get-deployment-strategy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-deployment-strategy`.

AWS CLI

Para recuperar los detalles de una estrategia de implementación

En el siguiente ejemplo de `get-deployment-strategy`, se genera una lista de los detalles de la estrategia de implementación especificada.

```
aws appconfig get-deployment-strategy \
    --deployment-strategy-id 1225qzk
```

Salida:

```
{
    "Id": "1225qzk",
    "Name": "Example-Deployment",
    "DeploymentDurationInMinutes": 15,
    "GrowthType": "LINEAR",
    "GrowthFactor": 25.0,
    "FinalBakeTimeInMinutes": 0,
    "ReplicateTo": "SSM_DOCUMENT"
}
```

Para obtener más información, consulte Step 4: Creating a deployment strategy en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte GetDeploymentStrategy en la Referencia de comandos de la AWS CLI.

get-deployment

En el siguiente ejemplo de código, se muestra cómo utilizar `get-deployment`.

AWS CLI

Recuperación de los detalles de la implementación

En el siguiente ejemplo de `get-deployment`, se genera una lista de los detalles de la implementación en la aplicación en el entorno y la implementación especificados.

```
aws appconfig get-deployment \
    --application-id 339ohji \
    --environment-id 54j1r29 \
    --deployment-number 1
```

Salida:

```
{
    "ApplicationId": "339ohji",
    "EnvironmentId": "54j1r29",
    "DeploymentStrategyId": "1225qzk",
    "ConfigurationProfileId": "ur8hx2f",
    "DeploymentNumber": 1,
    "ConfigurationName": "Example-Configuration-Profile",
    "ConfigurationLocationUri": "ssm-parameter://Example-Parameter",
    "ConfigurationVersion": "1",
    "DeploymentDurationInMinutes": 15,
    "GrowthType": "LINEAR",
    "GrowthFactor": 25.0,
    "FinalBakeTimeInMinutes": 0,
    "State": "COMPLETE",
    "EventLog": [
        {
            "EventType": "DEPLOYMENT_COMPLETED",
            "TriggeredBy": "APPCONFIG",
            "Description": "Deployment completed",
            "OccurredAt": "2021-09-17T21:59:03.888000+00:00"
        },
        {
            "EventType": "BAKE_TIME_STARTED",
            "TriggeredBy": "APPCONFIG",
            "Description": "Deployment bake time started",
```

```
            "OccurredAt": "2021-09-17T21:58:57.722000+00:00"
        },
        {
            "EventType": "PERCENTAGE_UPDATED",
            "TriggeredBy": "APPCONFIG",
            "Description": "Configuration available to 100.00% of clients",
            "OccurredAt": "2021-09-17T21:55:56.816000+00:00"
        },
        {
            "EventType": "PERCENTAGE_UPDATED",
            "TriggeredBy": "APPCONFIG",
            "Description": "Configuration available to 75.00% of clients",
            "OccurredAt": "2021-09-17T21:52:56.567000+00:00"
        },
        {
            "EventType": "PERCENTAGE_UPDATED",
            "TriggeredBy": "APPCONFIG",
            "Description": "Configuration available to 50.00% of clients",
            "OccurredAt": "2021-09-17T21:49:55.737000+00:00"
        },
        {
            "EventType": "PERCENTAGE_UPDATED",
            "TriggeredBy": "APPCONFIG",
            "Description": "Configuration available to 25.00% of clients",
            "OccurredAt": "2021-09-17T21:46:55.187000+00:00"
        },
        {
            "EventType": "DEPLOYMENT_STARTED",
            "TriggeredBy": "USER",
            "Description": "Deployment started",
            "OccurredAt": "2021-09-17T21:43:54.205000+00:00"
        }
    ],
    "PercentageComplete": 100.0,
    "StartedAt": "2021-09-17T21:43:54.205000+00:00",
    "CompletedAt": "2021-09-17T21:59:03.888000+00:00"
}
```

Para obtener más información, consulte Step 5: Deploying a configuration en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte GetDeployment en la Referencia de comandos de la AWS CLI.

`get-environment`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-environment`.

AWS CLI

Recuperación de los detalles del entorno

En el siguiente ejemplo de `get-environment`, se recuperan los detalles y el estado del entorno especificado.

```
aws appconfig get-environment \
    --application-id 339ohji \
    --environment-id 54j1r29
```

Salida:

```
{
    "ApplicationId": "339ohji",
    "Id": "54j1r29",
    "Name": "Example-Environment",
    "State": "ReadyForDeployment"
}
```

Para obtener más información, consulte Step 2: Creating an environment en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte GetEnvironment en la Referencia de comandos de la AWS CLI.

`get-extension-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-extension-association`.

AWS CLI

Para obtener detalles de una asociación de extensiones

En el siguiente ejemplo de `get-extension-association`, se muestra información acerca de una asociación de extensiones.

```
aws appconfig get-extension-association \
```

```
    --region us-west-2 \
    --extension-association-id a1b2c3d4
```

Salida:

```
{
    "Id": "a1b2c3d4",
    "ExtensionArn": "arn:aws:appconfig:us-west-2:123456789012:extension/S3-backup-
extension/1",
    "ResourceArn": "arn:aws:appconfig:us-west-2:123456789012:application/Finance",
    "Parameters": {
        "S3bucket": "FinanceConfigurationBackup"
    },
    "ExtensionVersionNumber": 1
}
```

Para obtener más información, consulte Working with AWS AppConfig extensions en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte GetExtensionAssociation en la Referencia de comandos de la AWS CLI.

`get-extension`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-extension`.

AWS CLI

Para obtener detalles de una extensión

En el siguiente ejemplo de `get-extension`, se muestra información acerca de una extensión.

```
aws appconfig get-extension \
    --region us-west-2 \
    --extension-identifier S3-backup-extension
```

Salida:

```
{
    "Id": "1A2B3C4D",
    "Name": "S3-backup-extension",
    "VersionNumber": 1,
```

```
    "Arn": "arn:aws:appconfig:us-west-2:123456789012:extension/S3-backup-
extension/1",
    "Actions": {
        "PRE_CREATE_HOSTED_CONFIGURATION_VERSION": [
            {
                "Name": "S3backup",
                "Uri": "arn:aws:lambda:us-
west-2:123456789012:function:S3backupfunction",
                "RoleArn": "arn:aws:iam::123456789012:role/appconfigextensionrole"
            }
        ]
    },
    "Parameters": {
        "S3bucket": {
            "Required": true
        }
    }
}
```

Para obtener más información, consulte Working with AWS AppConfig extensions en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte GetExtension en la Referencia de comandos de la AWS CLI.

`get-hosted-configuration-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-hosted-configuration-version`.

AWS CLI

Recuperación de detalles de la configuración alojada

En el siguiente ejemplo de `get-hosted-configuration-version`, se recuperan los detalles de configuración de la configuración alojada de AWS AppConfig.

```
aws appconfig get-hosted-configuration-version \
    --application-id 339ohji \
    --configuration-profile-id ur8hx2f \
    --version-number 1 \
    hosted-configuration-version-output
```

Contenido de `hosted-configuration-version-output`:

```
{ "Name": "ExampleApplication", "Id": ExampleID, "Rank": 7 }
```

Salida:

```
{
    "ApplicationId": "339ohji",
    "ConfigurationProfileId": "ur8hx2f",
    "VersionNumber": "1",
    "ContentType": "application/json"
}
```

Para obtener más información, consulte About the AWS AppConfig hosted configuration store en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte GetHostedConfigurationVersion en la Referencia de comandos de la AWS CLI.

`list-applications`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-applications`.

AWS CLI

Generación de una lista de las aplicaciones disponibles

En el siguiente ejemplo de `list-applications`, se genera una lista de las aplicaciones disponibles en la cuenta de AWS.

```
aws appconfig list-applications
```

Salida:

```
{
    "Items": [
        {
            "Id": "339ohji",
            "Name": "test-application",
            "Description": "An application used for creating an example."
        },
```

```
        {
            "Id": "rwalwu7",
            "Name": "Test-Application"
        }
    ]
}
```

Para obtener más información, consulte Step 1: Creating an AWS AppConfig application en la Guía del usuario de AWS AppConfig.

- Para obtener más información sobre la API, consulte ListApplications en la Referencia de comandos de la AWS CLI.

`list-configuration-profiles`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-configuration-profiles`.

AWS CLI

Generación de una lista de los perfiles de configuración disponibles

En el siguiente ejemplo de `list-configuration-profiles`, se genera una lista de los perfiles de configuración disponibles para la aplicación especificada.

```
aws appconfig list-configuration-profiles \
    --application-id 339ohji
```

Salida:

```
{
    "Items": [
        {
            "ApplicationId": "339ohji",
            "Id": "ur8hx2f",
            "Name": "Example-Configuration-Profile",
            "LocationUri": "ssm-parameter://Example-Parameter"
        }
    ]
}
```

Para obtener más información, consulte Step 3: Creating a configuration and a configuration profile en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte ListConfigurationProfiles en la Referencia de comandos de la AWS CLI.

`list-deployment-strategies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-deployment-strategies`.

AWS CLI

Generación de una lista de las estrategias de implementación disponibles

En el siguiente ejemplo de `list-deployment-strategies`, se genera una lista de las estrategias de implementación disponibles en la cuenta de AWS.

```
aws appconfig list-deployment-strategies
```

Salida:

```
{
    "Items": [
        {
            "Id": "1225qzk",
            "Name": "Example-Deployment",
            "DeploymentDurationInMinutes": 15,
            "GrowthType": "LINEAR",
            "GrowthFactor": 25.0,
            "FinalBakeTimeInMinutes": 0,
            "ReplicateTo": "SSM_DOCUMENT"
        },
        {
            "Id": "AppConfig.AllAtOnce",
            "Name": "AppConfig.AllAtOnce",
            "Description": "Quick",
            "DeploymentDurationInMinutes": 0,
            "GrowthType": "LINEAR",
            "GrowthFactor": 100.0,
            "FinalBakeTimeInMinutes": 10,
            "ReplicateTo": "NONE"
        },
        {
            "Id": "AppConfig.Linear50PercentEvery30Seconds",
            "Name": "AppConfig.Linear50PercentEvery30Seconds",
```

```
            "Description": "Test/Demo",
            "DeploymentDurationInMinutes": 1,
            "GrowthType": "LINEAR",
            "GrowthFactor": 50.0,
            "FinalBakeTimeInMinutes": 1,
            "ReplicateTo": "NONE"
        },
        {
            "Id": "AppConfig.Canary10Percent20Minutes",
            "Name": "AppConfig.Canary10Percent20Minutes",
            "Description": "AWS Recommended",
            "DeploymentDurationInMinutes": 20,
            "GrowthType": "EXPONENTIAL",
            "GrowthFactor": 10.0,
            "FinalBakeTimeInMinutes": 10,
            "ReplicateTo": "NONE"
        }
    ]
}
```

Para obtener más información, consulte Step 4: Creating a deployment strategy en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte ListDeploymentStrategies en la Referencia de comandos de la AWS CLI.

`list-deployments`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-deployments`.

AWS CLI

Generación de una lista de las implementaciones disponibles

En el siguiente ejemplo de `list-deployments`, se genera una lista de las implementaciones disponibles en la cuenta de AWS para la aplicación y el entorno especificados.

```
aws appconfig list-deployments \
    --application-id 339ohji \
    --environment-id 54j1r29
```

Salida:

```
{
    "Items": [
        {
            "DeploymentNumber": 1,
            "ConfigurationName": "Example-Configuration-Profile",
            "ConfigurationVersion": "1",
            "DeploymentDurationInMinutes": 15,
            "GrowthType": "LINEAR",
            "GrowthFactor": 25.0,
            "FinalBakeTimeInMinutes": 0,
            "State": "COMPLETE",
            "PercentageComplete": 100.0,
            "StartedAt": "2021-09-17T21:43:54.205000+00:00",
            "CompletedAt": "2021-09-17T21:59:03.888000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Step 5: Deploying a configuration en la Guía del usuario de AWS AppConfig.

- Para obtener más información sobre la API, consulte ListDeployments en Referencia de comandos de la AWS CLI.

`list-environments`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-environments`.

AWS CLI

Generación de una lista de los entornos disponibles

En el siguiente ejemplo de `list-environments`, se genera una lista de los entornos disponibles en la cuenta de AWS para la aplicación especificada.

```
aws appconfig list-environments \
    --application-id 339ohji
```

Salida:

```
{
```

```
    "Items": [
        {
            "ApplicationId": "339ohji",
            "Id": "54j1r29",
            "Name": "Example-Environment",
            "State": "ReadyForDeployment"
        }
    ]
}
```

Para obtener más información, consulte Step 2: Creating an environment en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte ListEnvironments en la Referencia de comandos de la AWS CLI.

`list-extension-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-extension-associations`.

AWS CLI

Generación de una lista de todas las asociaciones de extensiones de AWS AppConfig de la cuenta de AWS para una región de AWS

En el siguiente ejemplo de `list-extension-associations`, se genera una lista de todas las asociaciones de extensiones de AWS AppConfig para la cuenta de AWS actual en una región de AWS específica.

```
aws appconfig list-extension-associations \
    --region us-west-2
```

Salida:

```
{
    "Items": [
        {
            "Id": "a1b2c3d4",
            "ExtensionArn": "arn:aws:appconfig:us-west-2:123456789012:extension/S3-
backup-extension/1",
            "ResourceArn": "arn:aws:appconfig:us-west-2:123456789012:application/
Finance"
```

```
        }
    ]
}
```

Para obtener más información, consulte Working with AWS AppConfig extensions en la Guía del usuario de AWS AppConfig.

- Para obtener más información sobre la API, consulte ListExtensionAssociations en la Referencia de comandos de la AWS CLI.

`list-extensions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-extensions`.

AWS CLI

Generación de una lista de todas las extensiones de AWS AppConfig en la cuenta de AWS para una región de AWS

En el siguiente ejemplo de `list-extensions`, se genera una lista de todas las extensiones de AWS AppConfig para la cuenta de AWS actual en una región de AWS específica. Con el comando se obtienen las extensiones personalizadas y creadas por AWS.

```
aws appconfig list-extensions \
    --region us-west-2
```

Salida:

```
{
    "Items": [
        {
            "Id": "1A2B3C4D",
            "Name": "S3-backup-extension",
            "VersionNumber": 1,
            "Arn": "arn:aws:appconfig:us-west-2:123456789012:extension/1A2B3C4D/1"
        },
        {
            "Id": "AWS.AppConfig.FeatureFlags",
            "Name": "AppConfig Feature Flags Helper",
            "VersionNumber": 1,
            "Arn": "arn:aws:appconfig:us-west-2::extension/
AWS.AppConfig.FeatureFlags/1",
```

```
            "Description": "Validates AppConfig feature flag data automatically
 against a JSON schema that includes structure and constraints. Also transforms
 feature flag data prior to sending to the client. This extension is automatically
 associated to configuration profiles with type \"AWS.AppConfig.FeatureFlags\"."
        },
        {
            "Id": "AWS.AppConfig.JiraIntegration",
            "Name": "AppConfig integration with Atlassian Jira",
            "VersionNumber": 1,
            "Arn": "arn:aws:appconfig:us-west-2::extension/
AWS.AppConfig.JiraIntegration/1",
            "Description": "Exports feature flag data from AWS AppConfig into
 Jira. The lifecycle of each feature flag in AppConfig is tracked in Jira as an
 individual issue. Customers can see in Jira when flags are updated, turned on or
 off. Works in conjunction with the AppConfig app in the Atlassian Marketplace and
 is automatically associated to configuration profiles configured within that app."
        },
        {
            "Id": "AWS.AppConfig.DeploymentNotificationsToEventBridge",
            "Name": "AppConfig deployment events to Amazon EventBridge",
            "VersionNumber": 1,
            "Arn": "arn:aws:appconfig:us-west-2::extension/
AWS.AppConfig.DeploymentNotificationsToEventBridge/1",
            "Description": "Sends events to Amazon EventBridge when a deployment
 of configuration data in AppConfig is started, completed, or rolled back. Can
 be associated to the following resources in AppConfig: Application, Environment,
 Configuration Profile."
        },
        {
            "Id": "AWS.AppConfig.DeploymentNotificationsToSqs",
            "Name": "AppConfig deployment events to Amazon SQS",
            "VersionNumber": 1,
            "Arn": "arn:aws:appconfig:us-west-2::extension/
AWS.AppConfig.DeploymentNotificationsToSqs/1",
            "Description": "Sends messages to the configured Amazon SQS queue when
 a deployment of configuration data in AppConfig is started, completed, or rolled
 back. Can be associated to the following resources in AppConfig: Application,
 Environment, Configuration Profile."
        },
        {
            "Id": "AWS.AppConfig.DeploymentNotificationsToSns",
            "Name": "AppConfig deployment events to Amazon SNS",
            "VersionNumber": 1,
```

```
            "Description": "Sends events to the configured Amazon SNS topic when
 a deployment of configuration data in AppConfig is started, completed, or rolled
 back. Can be associated to the following resources in AppConfig: Application,
 Environment, Configuration Profile."
        }
    ]
}
```

Para obtener más información, consulte Working with AWS AppConfig extensions en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte ListExtensions en la Referencia de comandos de la AWS CLI.

`list-hosted-configuration-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-hosted-configuration-versions`.

AWS CLI

Generación de una lista de las versiones de configuración alojadas disponibles

En el ejemplo siguiente de `list-hosted-configuration-versions`, se genera una lista de las versiones de configuración alojadas en el almacén de configuración alojado de AWS AppConfig para la aplicación y el perfil de configuración especificados.

```
aws appconfig list-hosted-configuration-versions \
    --application-id 339ohji \
    --configuration-profile-id ur8hx2f
```

Salida:

```
{
    "Items": [
        {
            "ApplicationId": "339ohji",
            "ConfigurationProfileId": "ur8hx2f",
            "VersionNumber": 1,
            "ContentType": "application/json"
        }
```

```
    ]
}
```

Para obtener más información, consulte About the AWS AppConfig hosted configuration store en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte ListHostedConfigurationVersions en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Generación de una lista de las etiquetas de una aplicación

En el siguiente ejemplo de `list-tags-for-resource`, se genera una lista de las etiquetas de la aplicación especificada.

```
aws appconfig list-tags-for-resource \
    --resource-arn arn:aws:appconfig:us-east-1:682428703967:application/339ohji
```

Salida:

```
{
    "Tags": {
        "group1": "1"
    }
}
```

Para obtener más información, consulte Step 1: Creating an AWS AppConfig application en la Guía del usuario de AWS AppConfig.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`start-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-deployment`.

AWS CLI

Inicio de una implementación de configuración

En el siguiente ejemplo de `start-deployment`, se inicia una implementación en la aplicación con el entorno, la estrategia de implementación y el perfil de configuración especificados.

```
aws appconfig start-deployment \
    --application-id 339ohji \
    --environment-id 54j1r29 \
    --deployment-strategy-id 1225qzk \
    --configuration-profile-id ur8hx2f \
    --configuration-version 1
```

Salida:

```
{
    "ApplicationId": "339ohji",
    "EnvironmentId": "54j1r29",
    "DeploymentStrategyId": "1225qzk",
    "ConfigurationProfileId": "ur8hx2f",
    "DeploymentNumber": 1,
    "ConfigurationName": "Example-Configuration-Profile",
    "ConfigurationLocationUri": "ssm-parameter://Example-Parameter",
    "ConfigurationVersion": "1",
    "DeploymentDurationInMinutes": 15,
    "GrowthType": "LINEAR",
    "GrowthFactor": 25.0,
    "FinalBakeTimeInMinutes": 0,
    "State": "DEPLOYING",
    "EventLog": [
        {
            "EventType": "DEPLOYMENT_STARTED",
            "TriggeredBy": "USER",
            "Description": "Deployment started",
            "OccurredAt": "2021-09-17T21:43:54.205000+00:00"
        }
    ],
    "PercentageComplete": 0.0,
    "StartedAt": "2021-09-17T21:43:54.205000+00:00"
}
```

Para obtener más información, consulte Step 5: Deploying a configuration en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte StartDeployment en la Referencia de comandos de la AWS CLI.

`stop-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-deployment`.

AWS CLI

Detención de una implementación de configuración

En el siguiente ejemplo de `stop-deployment`, se detiene la implementación en una configuración de aplicación en el entorno especificado.

```
aws appconfig stop-deployment \
    --application-id 339ohji \
    --environment-id 54j1r29 \
    --deployment-number 2
```

Salida:

```
{
    "DeploymentNumber": 0,
    "DeploymentDurationInMinutes": 0,
    "GrowthFactor": 0.0,
    "FinalBakeTimeInMinutes": 0,
    "PercentageComplete": 0.0
}
```

Para obtener más información, consulte Step 5: Deploying a configuration en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte StopDeployment en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Etiquetado de una aplicación

En el siguiente ejemplo de `tag-resource`, se etiqueta un recurso de aplicación.

```
aws appconfig tag-resource \
    --resource-arn arn:aws:appconfig:us-east-1:682428703967:application/339ohji \
    --tags '{"group1" : "1"}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Step 1: Creating an AWS AppConfig application en la Guía del usuario de AWS AppConfig.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de una etiqueta de una aplicación

En el siguiente ejemplo de `untag-resource`, se elimina la etiqueta group1 de la aplicación especificada.

```
aws appconfig untag-resource \
    --resource-arn arn:aws:appconfig:us-east-1:111122223333:application/339ohji \
    --tag-keys '["group1"]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Step 1: Creating an AWS AppConfig application en la Guía del usuario de AWS AppConfig.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-application

En el siguiente ejemplo de código, se muestra cómo utilizar `update-application`.

AWS CLI

Para actualizar una aplicación

En el siguiente ejemplo de `update-application`, se actualiza el nombre de la aplicación especificada.

```
aws appconfig update-application \
    --application-id 339ohji \
    --name "Example-Application"
```

Salida:

```
{
    "Id": "339ohji",
    "Name": "Example-Application",
    "Description": "An application used for creating an example."
}
```

Para obtener más información, consulte Step 1: Creating an AWS AppConfig application en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte UpdateApplication en la Referencia de comandos de la AWS CLI.

update-configuration-profile

En el siguiente ejemplo de código, se muestra cómo utilizar `update-configuration-profile`.

AWS CLI

Actualización de un perfil de configuración

En el siguiente ejemplo de `update-configuration-profile`, se actualiza la descripción del perfil de configuración especificado.

```
aws appconfig update-configuration-profile \
```

```
    --application-id 339ohji \
    --configuration-profile-id ur8hx2f \
    --description "Configuration profile used for examples."
```

Salida:

```
{
    "ApplicationId": "339ohji",
    "Id": "ur8hx2f",
    "Name": "Example-Configuration-Profile",
    "Description": "Configuration profile used for examples.",
    "LocationUri": "ssm-parameter://Example-Parameter",
    "RetrievalRoleArn": "arn:aws:iam::111122223333:role/Example-App-Config-Role"
}
```

Para obtener más información, consulte Step 3: Creating a configuration and a configuration profile en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte UpdateConfigurationProfile en la Referencia de comandos de la AWS CLI.

`update-deployment-strategy`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-deployment-strategy`.

AWS CLI

Actualización de una estrategia de implementación

En el siguiente ejemplo de `update-deployment-strategy`, se actualiza el tiempo de incorporación final a 20 minutos en la estrategia de implementación especificada.

```
aws appconfig update-deployment-strategy \
    --deployment-strategy-id 1225qzk \
    --final-bake-time-in-minutes 20
```

Salida:

```
{
    "Id": "1225qzk",
```

```
    "Name": "Example-Deployment",
    "DeploymentDurationInMinutes": 15,
    "GrowthType": "LINEAR",
    "GrowthFactor": 25.0,
    "FinalBakeTimeInMinutes": 20,
    "ReplicateTo": "SSM_DOCUMENT"
}
```

Para obtener más información, consulte Step 4: Creating a deployment strategy en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte UpdateDeploymentStrategy en la Referencia de comandos de la AWS CLI.

`update-environment`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-environment`.

AWS CLI

Actualización de un entorno

En el siguiente ejemplo de `update-environment`, se actualiza la descripción de un entorno.

```
aws appconfig update-environment \
    --application-id 339ohji \
    --environment-id 54j1r29 \
    --description "An environment for examples."
```

Salida:

```
{
    "ApplicationId": "339ohji",
    "Id": "54j1r29",
    "Name": "Example-Environment",
    "Description": "An environment for examples.",
    "State": "RolledBack"
}
```

Para obtener más información, consulte Step 2: Creating an environment en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte UpdateEnvironment en la Referencia de comandos de la AWS CLI.

`update-extension-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-extension-association`.

AWS CLI

Actualización de una asociación de extensiones de AWS AppConfig

En el siguiente ejemplo de `update-extension-association`, se agrega un nuevo valor de parámetros a una asociación de extensiones en AWS AppConfig.

```
aws appconfig update-extension-association \
    --region us-west-2 \
    --extension-association-id a1b2c3d4 \
    --parameters S3bucket=FinanceMobileApp
```

Salida:

```
{
    "Id": "a1b2c3d4",
    "ExtensionArn": "arn:aws:appconfig:us-west-2:123456789012:extension/S3-backup-
extension/1",
    "ResourceArn": "arn:aws:appconfig:us-west-2:123456789012:application/Finance",
    "Parameters": {
        "S3bucket": "FinanceMobileApp"
    },
    "ExtensionVersionNumber": 1
}
```

Para obtener más información, consulte Working with AWS AppConfig extensions en la Guía del usuario de AWS AppConfig.

- Para obtener información acerca de la API, consulte UpdateExtensionAssociation en la Referencia de comandos de la AWS CLI.

`update-extension`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-extension`.

AWS CLI

Actualización de una extensión de AWS AppConfig

En el siguiente ejemplo de `update-extension`, se agrega un parámetro adicional Key a una extensión en AWS AppConfig.

```
aws appconfig update-extension \
    --region us-west-2 \
    --extension-identifier S3-backup-extension \
    --parameters S3bucket={Required=true},CampaignID={Required=false}
```

Salida:

```
{
    "Id": "1A2B3C4D",
    "Name": "S3-backup-extension",
    "VersionNumber": 1,
    "Arn": "arn:aws:appconfig:us-west-2:123456789012:extension/1A2B3C4D/1",
    "Actions": {
        "PRE_CREATE_HOSTED_CONFIGURATION_VERSION": [
            {
                "Name": "S3backup",
                "Uri": "arn:aws:lambda:us-
west-2:123456789012:function:S3backupfunction",
                "RoleArn": "arn:aws:iam::123456789012:role/appconfigextensionrole"
            }
        ]
    },
    "Parameters": {
        "CampaignID": {
            "Required": false
        },
        "S3bucket": {
            "Required": true
        }
    }
}
```

Para obtener más información, consulte Working with AWS AppConfig extensions en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte UpdateExtension en la Referencia de comandos de la AWS CLI.

`validate-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `validate-configuration`.

AWS CLI

Validación de una configuración

En el siguiente ejemplo de `validate-configuration`, se utilizan los validadores en un perfil de configuración para validar una configuración.

```
aws appconfig validate-configuration \
    --application-id abc1234 \
    --configuration-profile-id ur8hx2f \
    --configuration-version 1
```

El comando no genera ninguna salida.

Para obtener más información, consulte Step 3: Creating a configuration and a configuration profile en la Guía del usuario de AWS AppConfig.

- Para obtener información sobre la API, consulte ValidateConfiguration en la Referencia de comandos de la AWS CLI.

Ejemplos de Auto Scaling de aplicaciones que utilizan la AWS CLI

Los siguientes ejemplos de código le muestran cómo realizar acciones e implementar situaciones comunes utilizando la AWS Command Line Interface con el escalado automático de aplicaciones.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`delete-scaling-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-scaling-policy`.

AWS CLI

Eliminación de una política de escalado

En este ejemplo, se elimina una política de escalado del servicio de Amazon ECS denominado web-app que se ejecuta en el clúster predeterminado.

Comando:

```
aws application-autoscaling delete-scaling-policy --policy-name web-app-cpu-lt-25 --
scalable-dimension ecs:service:DesiredCount --resource-id service/default/web-app --
service-namespace ecs
```

- Para obtener información sobre la API, consulte DeleteScalingPolicy en la Referencia de comandos de AWS CLI.

`delete-scheduled-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-scheduled-action`.

AWS CLI

Para eliminar una acción programada

En el siguiente ejemplo de `delete-scheduled-action`, se elimina la acción programada especificada de la flota de Amazon AppStream 2.0 especificada:

```
aws application-autoscaling delete-scheduled-action \
    --service-namespace appstream \
    --scalable-dimension appstream:fleet:DesiredCapacity \
    --resource-id fleet/sample-fleet \
    --scheduled-action-name my-recurring-action
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Scheduled Scaling en la Guía del usuario de Auto Scaling de aplicaciones.

- Para obtener información sobre la API, consulte DeleteScheduledAction en la Referencia de comandos de la AWS CLI.

`deregister-scalable-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-scalable-target`.

AWS CLI

Anulación del registro de un destino escalable

En este ejemplo, se anula el registro de un destino escalable para un servicio de Amazon ECS denominado web-app que se ejecuta en el clúster predeterminado.

Comando:

```
aws application-autoscaling deregister-scalable-target --service-namespace ecs --
scalable-dimension ecs:service:DesiredCount --resource-id service/default/web-app
```

En este ejemplo se anula el registro de un destino escalable para un recurso personalizado. El archivo custom-resource-id.txt contiene una cadena que identifica el ID de recurso, que, para un recurso personalizado, es la ruta al recurso personalizado a través de su punto de conexión de Amazon API Gateway.

Comando:

```
aws application-autoscaling deregister-scalable-target --service-namespace custom-
resource --scalable-dimension custom-resource:ResourceType:Property --resource-
id file://~/custom-resource-id.txt
```

Contenido del archivo custom-resource-id.txt:

```
https://example.execute-api.us-west-2.amazonaws.com/prod/
scalableTargetDimensions/1-23456789
```

- Para obtener información sobre la API, consulte DeregisterScalableTarget en la Referencia de comandos de la AWS CLI.

`describe-scalable-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-scalable-targets`.

AWS CLI

Descripción de destinos escalables

En el siguiente ejemplo de `describe-scalable-targets`, se describen los destinos escalables del espacio de nombres del servicio de `ecs`.

```
aws application-autoscaling describe-scalable-targets \
    --service-namespace ecs
```

Salida:

```
{
    "ScalableTargets": [
        {
            "ServiceNamespace": "ecs",
            "ScalableDimension": "ecs:service:DesiredCount",
            "ResourceId": "service/default/web-app",
            "MinCapacity": 1,
            "MaxCapacity": 10,
            "RoleARN": "arn:aws:iam::123456789012:role/
aws-service-role/ecs.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_ECSService",
            "CreationTime": 1462558906.199,
            "SuspendedState": {
                "DynamicScalingOutSuspended": false,
                "ScheduledScalingSuspended": false,
                "DynamicScalingInSuspended": false
            },
            "ScalableTargetARN": "arn:aws:application-autoscaling:us-
west-2:123456789012:scalable-target/1234abcd56ab78cd901ef1234567890ab123"
        }
    ]
}
```

Para obtener más información, consulte AWS services that you can use with Application Auto Scaling en la Guía del usuario de Auto Scaling de aplicaciones.

- Para obtener información sobre la API, consulte DescribeScalableTargets en la Referencia de comandos de la AWS CLI.

`describe-scaling-activities`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-scaling-activities`.

AWS CLI

Ejemplo 1: cómo describir las actividades de escalado para el servicio de Amazon ECS especificado

En el siguiente ejemplo de `describe-scaling-activities`, se describen las actividades de escalado de un servicio de Amazon ECS denominado `web-app` que se ejecuta en el clúster `default`. El resultado muestra una actividad de escalado iniciada por una política de escalado.

```
aws application-autoscaling describe-scaling-activities \
    --service-namespace ecs \
    --resource-id service/default/web-app
```

Salida:

```
{
    "ScalingActivities": [
        {
            "ScalableDimension": "ecs:service:DesiredCount",
            "Description": "Setting desired count to 1.",
            "ResourceId": "service/default/web-app",
            "ActivityId": "e6c5f7d1-dbbb-4a3f-89b2-51f33e766399",
            "StartTime": 1462575838.171,
            "ServiceNamespace": "ecs",
            "EndTime": 1462575872.111,
            "Cause": "monitor alarm web-app-cpu-lt-25 in state ALARM triggered
 policy web-app-cpu-lt-25",
            "StatusMessage": "Successfully set desired count to 1. Change
 successfully fulfilled by ecs.",
            "StatusCode": "Successful"
        }
```

```
    ]
}
```

Para obtener más información, consulte Scaling activities for Application Auto Scaling en la Guía del usuario de Auto Scaling de aplicaciones.

Ejemplo 2: cómo describir las actividades de escalado para la tabla de DynamoDB especificada

En el siguiente ejemplo de `describe-scaling-activities`, se describen las actividades de escalado de una tabla de DynamoDB denominada `TestTable`. El resultado muestra las actividades de escalado iniciadas por dos acciones programadas diferentes.

```
aws application-autoscaling describe-scaling-activities \
    --service-namespace dynamodb \
    --resource-id table/TestTable
```

Salida:

```
{
    "ScalingActivities": [
        {
            "ScalableDimension": "dynamodb:table:WriteCapacityUnits",
            "Description": "Setting write capacity units to 10.",
            "ResourceId": "table/my-table",
            "ActivityId": "4d1308c0-bbcf-4514-a673-b0220ae38547",
            "StartTime": 1561574415.086,
            "ServiceNamespace": "dynamodb",
            "EndTime": 1561574449.51,
            "Cause": "maximum capacity was set to 10",
            "StatusMessage": "Successfully set write capacity units to 10. Change
 successfully fulfilled by dynamodb.",
            "StatusCode": "Successful"
        },
        {
            "ScalableDimension": "dynamodb:table:WriteCapacityUnits",
            "Description": "Setting min capacity to 5 and max capacity to 10",
            "ResourceId": "table/my-table",
            "ActivityId": "f2b7847b-721d-4e01-8ef0-0c8d3bacc1c7",
            "StartTime": 1561574414.644,
            "ServiceNamespace": "dynamodb",
            "Cause": "scheduled action name my-second-scheduled-action was
 triggered",
```

```
            "StatusMessage": "Successfully set min capacity to 5 and max capacity to
 10",
            "StatusCode": "Successful"
        },
        {
            "ScalableDimension": "dynamodb:table:WriteCapacityUnits",
            "Description": "Setting write capacity units to 15.",
            "ResourceId": "table/my-table",
            "ActivityId": "d8ea4de6-9eaa-499f-b466-2cc5e681ba8b",
            "StartTime": 1561574108.904,
            "ServiceNamespace": "dynamodb",
            "EndTime": 1561574140.255,
            "Cause": "minimum capacity was set to 15",
            "StatusMessage": "Successfully set write capacity units to 15. Change
 successfully fulfilled by dynamodb.",
            "StatusCode": "Successful"
        },
        {
            "ScalableDimension": "dynamodb:table:WriteCapacityUnits",
            "Description": "Setting min capacity to 15 and max capacity to 20",
            "ResourceId": "table/my-table",
            "ActivityId": "3250fd06-6940-4e8e-bb1f-d494db7554d2",
            "StartTime": 1561574108.512,
            "ServiceNamespace": "dynamodb",
            "Cause": "scheduled action name my-first-scheduled-action was
 triggered",
            "StatusMessage": "Successfully set min capacity to 15 and max capacity
 to 20",
            "StatusCode": "Successful"
        }
    ]
}
```

Para obtener más información, consulte Scaling activities for Application Auto Scaling en la Guía del usuario de Auto Scaling de aplicaciones.

- Para obtener información sobre la API, consulte DescribeScalingActivities en la Referencia de comandos de la AWS CLI.

`describe-scaling-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-scaling-policies`.

AWS CLI

Descripción de políticas de escalado

En este comando de ejemplo se describen las políticas de escalado del espacio de nombres del servicio de ecs.

Comando:

```
aws application-autoscaling describe-scaling-policies --service-namespace ecs
```

Salida:

```
{
    "ScalingPolicies": [
        {
            "PolicyName": "web-app-cpu-gt-75",
            "ScalableDimension": "ecs:service:DesiredCount",
            "ResourceId": "service/default/web-app",
            "CreationTime": 1462561899.23,
            "StepScalingPolicyConfiguration": {
                "Cooldown": 60,
                "StepAdjustments": [
                    {
                        "ScalingAdjustment": 200,
                        "MetricIntervalLowerBound": 0.0
                    }
                ],
                "AdjustmentType": "PercentChangeInCapacity"
            },
            "PolicyARN": "arn:aws:autoscaling:us-
west-2:012345678910:scalingPolicy:6d8972f3-efc8-437c-92d1-6270f29a66e7:resource/ecs/
service/default/web-app:policyName/web-app-cpu-gt-75",
            "PolicyType": "StepScaling",
            "Alarms": [
                {
                    "AlarmName": "web-app-cpu-gt-75",
                    "AlarmARN": "arn:aws:cloudwatch:us-
west-2:012345678910:alarm:web-app-cpu-gt-75"
                }
            ],
            "ServiceNamespace": "ecs"
        },
```

```
        {
            "PolicyName": "web-app-cpu-lt-25",
            "ScalableDimension": "ecs:service:DesiredCount",
            "ResourceId": "service/default/web-app",
            "CreationTime": 1462562575.099,
            "StepScalingPolicyConfiguration": {
                "Cooldown": 1,
                "StepAdjustments": [
                    {
                        "ScalingAdjustment": -50,
                        "MetricIntervalUpperBound": 0.0
                    }
                ],
                "AdjustmentType": "PercentChangeInCapacity"
            },
            "PolicyARN": "arn:aws:autoscaling:us-
west-2:012345678910:scalingPolicy:6d8972f3-efc8-437c-92d1-6270f29a66e7:resource/ecs/
service/default/web-app:policyName/web-app-cpu-lt-25",
            "PolicyType": "StepScaling",
            "Alarms": [
                {
                    "AlarmName": "web-app-cpu-lt-25",
                    "AlarmARN": "arn:aws:cloudwatch:us-
west-2:012345678910:alarm:web-app-cpu-lt-25"
                }
            ],
            "ServiceNamespace": "ecs"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeScalingPolicies en la Referencia de comandos de la AWS CLI.

`describe-scheduled-actions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-scheduled-actions`.

AWS CLI

Para describir acciones programadas

En el siguiente ejemplo de `describe-scheduled-actions`, se muestran los detalles de las acciones programadas para el espacio de nombres del servicio especificado:

```
aws application-autoscaling describe-scheduled-actions \
    --service-namespace dynamodb
```

Salida:

```
{
    "ScheduledActions": [
        {
            "ScalableDimension": "dynamodb:table:WriteCapacityUnits",
            "Schedule": "at(2019-05-20T18:35:00)",
            "ResourceId": "table/my-table",
            "CreationTime": 1561571888.361,
            "ScheduledActionARN": "arn:aws:autoscaling:us-
west-2:123456789012:scheduledAction:2d36aa3b-cdf9-4565-b290-81db519b227d:resource/
dynamodb/table/my-table:scheduledActionName/my-first-scheduled-action",
            "ScalableTargetAction": {
                "MinCapacity": 15,
                "MaxCapacity": 20
            },
            "ScheduledActionName": "my-first-scheduled-action",
            "ServiceNamespace": "dynamodb"
        },
        {
            "ScalableDimension": "dynamodb:table:WriteCapacityUnits",
            "Schedule": "at(2019-05-20T18:40:00)",
            "ResourceId": "table/my-table",
            "CreationTime": 1561571946.021,
            "ScheduledActionARN": "arn:aws:autoscaling:us-
west-2:123456789012:scheduledAction:2d36aa3b-cdf9-4565-b290-81db519b227d:resource/
dynamodb/table/my-table:scheduledActionName/my-second-scheduled-action",
            "ScalableTargetAction": {
                "MinCapacity": 5,
                "MaxCapacity": 10
            },
            "ScheduledActionName": "my-second-scheduled-action",
            "ServiceNamespace": "dynamodb"
        }
    ]
}
```

Para obtener más información, consulte Scheduled Scaling en la Guía del usuario de Auto Scaling de aplicaciones.

- Para obtener información sobre la API, consulte DescribeScheduledActions en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Generación de una lista de etiquetas de un destino escalable

En el siguiente ejemplo de `list-tags-for-resource`, se genera una lista de los nombres de clave y valores de las etiquetas que se adjuntan al destino escalable especificado por el ARN.

```
aws application-autoscaling list-tags-for-resource \
    --resource-arn arn:aws:application-autoscaling:us-west-2:123456789012:scalable-target/1234abcd56ab78cd901ef1234567890ab123
```

Salida:

```
{
    "Tags": {
        "environment": "production"
    }
}
```

Para obtener más información, consulte Tagging support for Application Auto Scaling en la Guía del usuario de Auto Scaling de aplicaciones.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-scaling-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-scaling-policy`.

AWS CLI

Ejemplo 1: aplicar una política de escalado de seguimiento de destino con una especificación de métrica predefinida

En el siguiente ejemplo de `put-scaling-policy`, se aplica una política de escalado de seguimiento de destino con una especificación de métricas predefinida para un servicio de Amazon ECS denominado web-app en el clúster predeterminado. La política mantiene la utilización media de la CPU del servicio en un 75 %, con períodos de recuperación de escalado horizontal y reducción horizontal de 60 segundos. La salida contiene los ARN y nombres de las dos alarmas de CloudWatch creadas en su nombre.

```
aws application-autoscaling put-scaling-policy --service-namespace ecs \
--scalable-dimension ecs:service:DesiredCount \
--resource-id service/default/web-app \
--policy-name cpu75-target-tracking-scaling-policy --policy-
type TargetTrackingScaling \
--target-tracking-scaling-policy-configuration file://config.json
```

En este ejemplo se supone que tiene un archivo config.json en el directorio actual con el siguiente contenido:

```
{
     "TargetValue": 75.0,
     "PredefinedMetricSpecification": {
         "PredefinedMetricType": "ECSServiceAverageCPUUtilization"
     },
     "ScaleOutCooldown": 60,
    "ScaleInCooldown": 60
}
```

Salida:

```
{
    "PolicyARN": "arn:aws:autoscaling:us-west-2:012345678910:scalingPolicy:6d8972f3-
efc8-437c-92d1-6270f29a66e7:resource/ecs/service/default/web-app:policyName/cpu75-
target-tracking-scaling-policy",
    "Alarms": [
        {
            "AlarmARN": "arn:aws:cloudwatch:us-
west-2:012345678910:alarm:TargetTracking-service/default/web-app-AlarmHigh-d4f0770c-
b46e-434a-a60f-3b36d653feca",
```

```
            "AlarmName": "TargetTracking-service/default/web-app-AlarmHigh-d4f0770c-
b46e-434a-a60f-3b36d653feca"
        },
        {
            "AlarmARN": "arn:aws:cloudwatch:us-
west-2:012345678910:alarm:TargetTracking-service/default/web-app-AlarmLow-1b437334-
d19b-4a63-a812-6c67aaf2910d",
            "AlarmName": "TargetTracking-service/default/web-app-AlarmLow-1b437334-
d19b-4a63-a812-6c67aaf2910d"
        }
    ]
}
```

Ejemplo 2: aplicar una política de escalado de seguimiento de destino con una especificación de métrica personalizada

En el siguiente ejemplo de `put-scaling-policy`, se aplica una política de escalado de seguimiento de destino con una especificación de métricas personalizada para un servicio de Amazon ECS denominado web-app en el clúster predeterminado. La política mantiene la utilización media del servicio en un 75 %, con períodos de recuperación de escalado horizontal y reducción horizontal de 60 segundos. La salida contiene los ARN y nombres de las dos alarmas de CloudWatch creadas en su nombre.

```
aws application-autoscaling put-scaling-policy --service-namespace ecs \
--scalable-dimension ecs:service:DesiredCount \
--resource-id service/default/web-app \
--policy-name cms75-target-tracking-scaling-policy
--policy-type TargetTrackingScaling \
--target-tracking-scaling-policy-configuration file://config.json
```

En este ejemplo se supone que tiene un archivo config.json en el directorio actual con el siguiente contenido:

```
{
    "TargetValue":75.0,
    "CustomizedMetricSpecification":{
        "MetricName":"MyUtilizationMetric",
        "Namespace":"MyNamespace",
        "Dimensions": [
            {
                "Name":"MyOptionalMetricDimensionName",
```

```
                "Value":"MyOptionalMetricDimensionValue"
            }
        ],
        "Statistic":"Average",
        "Unit":"Percent"
    },
    "ScaleOutCooldown": 60,
    "ScaleInCooldown": 60
}
```

Salida:

```
{
    "PolicyARN": "arn:aws:autoscaling:us-west-2:012345678910:scalingPolicy:
 8784a896-b2ba-47a1-b08c-27301cc499a1:resource/ecs/service/default/web-
app:policyName/cms75-target-tracking-scaling-policy",
    "Alarms": [
        {
            "AlarmARN": "arn:aws:cloudwatch:us-
west-2:012345678910:alarm:TargetTracking-service/default/web-app-
AlarmHigh-9bc77b56-0571-4276-ba0f-d4178882e0a0",
            "AlarmName": "TargetTracking-service/default/web-app-
AlarmHigh-9bc77b56-0571-4276-ba0f-d4178882e0a0"
        },
        {
            "AlarmARN": "arn:aws:cloudwatch:us-
west-2:012345678910:alarm:TargetTracking-service/default/web-app-
AlarmLow-9b6ad934-6d37-438e-9e05-02836ddcbdc4",
            "AlarmName": "TargetTracking-service/default/web-app-
AlarmLow-9b6ad934-6d37-438e-9e05-02836ddcbdc4"
        }
    ]
}
```

Ejemplo 3: aplicar una política de escalado de seguimiento de destino solo para el escalado ascendente

En el siguiente ejemplo de `put-scaling-policy`, se aplica una política de escalado de seguimiento de destino a un servicio de Amazon ECS denominado `web-app` en el clúster predeterminado. La política se usa para escalar horizontalmente el servicio de ECS cuando la métrica `RequestCountPerTarget` del equilibrador de carga de aplicación supera el umbral. El resultado contiene el ARN y el nombre de la alarma de CloudWatch creada en su nombre.

```
aws application-autoscaling put-scaling-policy \
    --service-namespace ecs \
    --scalable-dimension ecs:service:DesiredCount \
    --resource-id service/default/web-app \
    --policy-name alb-scale-out-target-tracking-scaling-policy \
    --policy-type TargetTrackingScaling \
    --target-tracking-scaling-policy-configuration file://config.json
```

Contenido de `config.json`:

```
{
     "TargetValue": 1000.0,
     "PredefinedMetricSpecification": {
         "PredefinedMetricType": "ALBRequestCountPerTarget",
         "ResourceLabel": "app/EC2Co-EcsEl-1TKLTMITMM0EO/f37c06a68c1748aa/
targetgroup/EC2Co-Defau-LDNM7Q3ZH1ZN/6d4ea56ca2d6a18d"
     },
     "ScaleOutCooldown": 60,
    "ScaleInCooldown": 60,
    "DisableScaleIn": true
}
```

Salida:

```
{
    "PolicyARN": "arn:aws:autoscaling:us-west-2:123456789012:scalingPolicy:6d8972f3-
efc8-437c-92d1-6270f29a66e7:resource/ecs/service/default/web-app:policyName/alb-
scale-out-target-tracking-scaling-policy",
    "Alarms": [
        {
            "AlarmName": "TargetTracking-service/default/web-app-AlarmHigh-d4f0770c-
b46e-434a-a60f-3b36d653feca",
            "AlarmARN": "arn:aws:cloudwatch:us-
west-2:123456789012:alarm:TargetTracking-service/default/web-app-AlarmHigh-d4f0770c-
b46e-434a-a60f-3b36d653feca"
        }
    ]
}
```

Para obtener más información, consulte Target Tracking Scaling Policies for Application Auto Scaling en la Guía del usuario de AWS Auto Scaling de aplicaciones.

- Para obtener información sobre la API, consulte PutScalingPolicy en la Referencia de comandos de la AWS CLI.

`put-scheduled-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-scheduled-action`.

AWS CLI

Adición de una acción programada a una tabla de DynamoDB

En este ejemplo, se añade una acción programada a una tabla de DynamoDB denominada TestTable para escalarla horizontalmente con una programación periódica. En el horario especificado (todos los días a las 12:15 p. m. UTC), si la capacidad actual está por debajo del valor especificado para MinCapacity, el escalado automático de aplicaciones escala horizontalmente al valor especificado por MinCapacity.

Comando:

```
aws application-autoscaling put-scheduled-action --service-namespace dynamodb
 --scheduled-action-name my-recurring-action --schedule "cron(15 12 * * ? *)" --
resource-id table/TestTable --scalable-dimension dynamodb:table:WriteCapacityUnits
 --scalable-target-action MinCapacity=6
```

Para obtener más información, consulte Scheduled Scaling en la Guía del usuario de Auto Scaling de aplicaciones.

- Para obtener información sobre la API, consulte PutScheduledAction en la Referencia de comandos de la AWS CLI.

`register-scalable-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-scalable-target`.

AWS CLI

Ejemplo 1: cómo registrar un servicio de ECS como un destino escalable

En el siguiente ejemplo de `register-scalable-target`, se registra un servicio de Amazon ECS con el escalado automático de aplicaciones. También añade una etiqueta con el nombre de clave `environment` y el valor `production` al destino escalable.

```
aws application-autoscaling register-scalable-target \
    --service-namespace ecs \
    --scalable-dimension ecs:service:DesiredCount \
    --resource-id service/default/web-app \
    --min-capacity 1 --max-capacity 10 \
    --tags environment=production
```

Salida:

```
{
    "ScalableTargetARN": "arn:aws:application-autoscaling:us-
west-2:123456789012:scalable-target/1234abcd56ab78cd901ef1234567890ab123"
}
```

Para ver ejemplos de otros servicios de y recursos personalizados de AWS, consulte los temas en AWS services that you can use with Application Auto Scaling en la Guía del usuario de Auto Scaling de aplicaciones.

Ejemplo 2: cómo suspender las actividades de escalado de un destino escalable

En el siguiente ejemplo de `register-scalable-target`, se suspenden las actividades de escalado de un destino escalable existente.

```
aws application-autoscaling register-scalable-target \
    --service-namespace dynamodb \
    --scalable-dimension dynamodb:table:ReadCapacityUnits \
    --resource-id table/my-table \
    --suspended-
state DynamicScalingInSuspended=true,DynamicScalingOutSuspended=true,ScheduledScalingSuspend
```

Salida:

```
{
    "ScalableTargetARN": "arn:aws:application-autoscaling:us-
west-2:123456789012:scalable-target/1234abcd56ab78cd901ef1234567890ab123"
}
```

Para obtener más información, consulte Suspending and resuming scaling for Application Auto Scaling en la Guía del usuario de Auto Scaling de aplicaciones.

Ejemplo 3: cómo reanudar las actividades de escalado de un destino escalable

En el siguiente ejemplo de `register-scalable-target`, se reanudan las actividades de escalado de un destino escalable existente.

```
aws application-autoscaling register-scalable-target \
    --service-namespace dynamodb \
    --scalable-dimension dynamodb:table:ReadCapacityUnits \
    --resource-id table/my-table \
    --suspended-
state DynamicScalingInSuspended=false,DynamicScalingOutSuspended=false,ScheduledScalingSuspe
```

Salida:

```
{
    "ScalableTargetARN": "arn:aws:application-autoscaling:us-
west-2:123456789012:scalable-target/1234abcd56ab78cd901ef1234567890ab123"
}
```

Para obtener más información, consulte Suspending and resuming scaling for Application Auto Scaling en la Guía del usuario de Auto Scaling de aplicaciones.

- Para obtener información sobre la API, consulte RegisterScalableTarget en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Adición de una etiqueta a un destino escalable

En el siguiente ejemplo de `tag-resource`, se agrega una etiqueta con el nombre de clave `environment` y el valor `production` al destino escalable especificado por su ARN.

```
aws application-autoscaling tag-resource \
    --resource-arn arn:aws:application-autoscaling:us-west-2:123456789012:scalable-
target/1234abcd56ab78cd901ef1234567890ab123 \
    --tags environment=production
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging support for Application Auto Scaling en la Guía del usuario de Auto Scaling de aplicaciones.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de una etiqueta de un destino escalable

En el siguiente ejemplo de `untag-resource`, se elimina un par de etiquetas con el nombre de clave `environment` del destino escalable especificado por su ARN.

```
aws application-autoscaling untag-resource \
    --resource-arn arn:aws:application-autoscaling:us-west-2:123456789012:scalable-target/1234abcd56ab78cd901ef1234567890ab123 \
    --tag-keys "environment"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging support for Application Auto Scaling en la Guía del usuario de Auto Scaling de aplicaciones.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

Ejemplos de Application Discovery Service que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar situaciones comunes utilizando la AWS Command Line Interface con Application Discovery Service.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`describe-agents`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-agents`.

AWS CLI

Descripción de los agentes con estados de collectionStatus específicos

En este comando de ejemplo se describen los agentes recopiladores con el estado de recopilación STARTED o STOPPED.

Comando:

```
aws discovery describe-agents --filters
 name="collectionStatus",values="STARTED","STOPPED",condition="EQUALS" --max-
results 3
```

Salida:

```
{
       "Snapshots": [
      {
            "version": "1.0.40.0",
            "agentType": "EC2",
            "hostName": "ip-172-31-40-234",
            "collectionStatus": "STOPPED",
            "agentNetworkInfoList": [
                {
                    "macAddress": "06:b5:97:14:fc:0d",
                    "ipAddress": "172.31.40.234"
                }
            ],
            "health": "UNKNOWN",
```

```
            "agentId": "i-003305c02a776e883",
            "registeredTime": "2016-12-09T19:05:06Z",
            "lastHealthPingTime": "2016-12-09T19:05:10Z"
        },
        {
            "version": "1.0.40.0",
            "agentType": "EC2",
            "hostName": "ip-172-31-39-64",
            "collectionStatus": "STARTED",
            "agentNetworkInfoList": [
                {
                    "macAddress": "06:a1:0e:c7:b2:73",
                    "ipAddress": "172.31.39.64"
                }
            ],
            "health": "SHUTDOWN",
            "agentId": "i-003a5e5e2b36cf8bd",
            "registeredTime": "2016-11-16T16:36:25Z",
            "lastHealthPingTime": "2016-11-16T16:47:37Z"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeAgents en la Referencia de comandos de la AWS CLI.

`describe-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-configurations`.

AWS CLI

Descripción de las configuraciones de activos seleccionadas

En este comando de ejemplo se describen las configuraciones de dos servidores específicos. La acción detecta el tipo de activo a partir del ID de configuración. Solo se permite un tipo de activo por comando.

Comando:

```
aws discovery describe-configurations --configuration-ids "d-
server-099385097ef9fbcfb" "d-server-0c4f2dd1fee22c6c1"
```

Salida:


```
{
    "configurations": [
        {
                "server.performance.maxCpuUsagePct": "0.0",
                "server.performance.maxDiskReadIOPS": "0.0",
                "server.performance.avgCpuUsagePct": "0.0",
                "server.type": "EC2",
                "server.performance.maxNetworkReadsPerSecondInKB": "0.19140625",
                "server.hostName": "ip-172-31-35-152",
                "server.configurationId": "d-server-0c4f2dd1fee22c6c1",
                "server.tags.hasMoreValues": "false",
                "server.performance.minFreeRAMInKB": "1543496.0",
                "server.osVersion": "3.14.48-33.39.amzn1.x86_64",
                "server.performance.maxDiskReadsPerSecondInKB": "0.0",
                "server.applications": "[]",
                "server.performance.numDisks": "1",
                "server.performance.numCpus": "1",
                "server.performance.numCores": "1",
                "server.performance.maxDiskWriteIOPS": "0.0",
                "server.performance.maxNetworkWritesPerSecondInKB": "0.82421875",
                "server.performance.avgDiskWritesPerSecondInKB": "0.0",
                "server.networkInterfaceInfo": "[{\"name\":\"eth0\",
\"macAddress\":\"06:A7:7D:3F:54:57\",\"ipAddress\":\"172.31.35.152\",\"netMask\":
\"255.255.240.0\"},{\"name\":\"lo\",\"macAddress\":\"00:00:00:00:00:00\",\"ipAddress
\":\"127.0.0.1\",\"netMask\":\"255.0.0.0\"},{\"name\":\"eth0\",\"macAddress\":
\"06:A7:7D:3F:54:57\",\"ipAddress\":\"fe80::4a7:7dff:fe3f:5457\"},{\"name\":\"lo\",
\"macAddress\":\"00:00:00:00:00:00\",\"ipAddress\":\"::1\"}]",
                "server.performance.avgNetworkReadsPerSecondInKB":
 "0.04915364583333333",
                "server.tags": "[]",
                "server.applications.hasMoreValues": "false",
                "server.timeOfCreation": "2016-10-28 23:44:00.0",
                "server.agentId": "i-4447bc1b",
                "server.performance.maxDiskWritesPerSecondInKB": "0.0",
                "server.performance.avgDiskReadIOPS": "0.0",
                "server.performance.avgFreeRAMInKB": "1547210.1333333333",
                "server.performance.avgDiskReadsPerSecondInKB": "0.0",
                "server.performance.avgDiskWriteIOPS": "0.0",
                "server.performance.numNetworkCards": "2",
                "server.hypervisor": "xen",
                "server.networkInterfaceInfo.hasMoreValues": "false",
                "server.performance.avgNetworkWritesPerSecondInKB": "0.1380859375",
```

```
                "server.osName": "Linux - Amazon Linux AMI release 2015.03",
                "server.performance.totalRAMInKB": "1694732.0",
                "server.cpuType": "x64"
        },
        {
                "server.performance.maxCpuUsagePct": "100.0",
                "server.performance.maxDiskReadIOPS": "0.0",
                "server.performance.avgCpuUsagePct": "14.733333333333338",
                "server.type": "EC2",
                "server.performance.maxNetworkReadsPerSecondInKB": "13.400390625",
                "server.hostName": "ip-172-31-42-208",
                "server.configurationId": "d-server-099385097ef9fbcfb",
                "server.tags.hasMoreValues": "false",
                "server.performance.minFreeRAMInKB": "1531104.0",
                "server.osVersion": "3.14.48-33.39.amzn1.x86_64",
                "server.performance.maxDiskReadsPerSecondInKB": "0.0",
                "server.applications": "[]",
                "server.performance.numDisks": "1",
                "server.performance.numCpus": "1",
                "server.performance.numCores": "1",
                "server.performance.maxDiskWriteIOPS": "1.0",
                "server.performance.maxNetworkWritesPerSecondInKB": "12.271484375",
                "server.performance.avgDiskWritesPerSecondInKB":
 "0.5333333333333334",
                "server.networkInterfaceInfo": "[{\"name\":\"eth0\",
\"macAddress\":\"06:4A:79:60:75:61\",\"ipAddress\":\"172.31.42.208\",\"netMask
\":\"255.255.240.0\"},{\"name\":\"eth0\",\"macAddress\":\"06:4A:79:60:75:61\",
\"ipAddress\":\"fe80::44a:79ff:fe60:7561\"},{\"name\":\"lo\",\"macAddress\":
\"00:00:00:00:00:00\",\"ipAddress\":\"::1\"},{\"name\":\"lo\",\"macAddress\":
\"00:00:00:00:00:00\",\"ipAddress\":\"127.0.0.1\",\"netMask\":\"255.0.0.0\"}]",
                "server.performance.avgNetworkReadsPerSecondInKB":
 "2.8720052083333334",
                "server.tags": "[]",
                "server.applications.hasMoreValues": "false",
                "server.timeOfCreation": "2016-10-28 23:44:30.0",
                "server.agentId": "i-c142b99e",
                "server.performance.maxDiskWritesPerSecondInKB": "4.0",
                "server.performance.avgDiskReadIOPS": "0.0",
                "server.performance.avgFreeRAMInKB": "1534946.4",
                "server.performance.avgDiskReadsPerSecondInKB": "0.0",
                "server.performance.avgDiskWriteIOPS": "0.13333333333333336",
                "server.performance.numNetworkCards": "2",
                "server.hypervisor": "xen",
                "server.networkInterfaceInfo.hasMoreValues": "false",
```

```
                "server.performance.avgNetworkWritesPerSecondInKB":
 "1.7977864583333332",
                "server.osName": "Linux - Amazon Linux AMI release 2015.03",
                "server.performance.totalRAMInKB": "1694732.0",
                "server.cpuType": "x64"
        }
    ]
}
```

Descripción de las configuraciones de activos seleccionadas

En este comando de ejemplo se describen las configuraciones de dos aplicaciones específicas. La acción detecta el tipo de activo a partir del ID de configuración. Solo se permite un tipo de activo por comando.

Comando:

```
aws discovery describe-configurations --configuration-ids "d-
application-0ac39bc0e4fad0e42" "d-application-02444a45288013764q"
```

Salida:

```
{
    "configurations": [
        {
                "application.serverCount": "0",
                "application.name": "Application-12345",
                "application.lastModifiedTime": "2016-12-13 23:53:27.0",
                "application.description": "",
                "application.timeOfCreation": "2016-12-13 23:53:27.0",
                "application.configurationId": "d-application-0ac39bc0e4fad0e42"
        },
        {
                "application.serverCount": "0",
                "application.name": "Application-67890",
                "application.lastModifiedTime": "2016-12-13 23:53:33.0",
                "application.description": "",
                "application.timeOfCreation": "2016-12-13 23:53:33.0",
                "application.configurationId": "d-application-02444a45288013764"
         }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeConfigurations en la Referencia de comandos de la AWS CLI.

`list-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-configurations`.

AWS CLI

Generación de una lista de todos los servidores detectados que cumplen un conjunto de condiciones de filtrado

En este comando de ejemplo se muestran los servidores detectados que coinciden con uno de los dos patrones de nombres de host y que no ejecutan Ubuntu.

Comando:

```
aws discovery list-configurations --configuration-type SERVER --filters
 name="server.hostName",values="172-31-35","172-31-42",condition="CONTAINS"
 name="server.osName",values="Ubuntu",condition="NOT_CONTAINS"
```

Salida:

```
{
    "configurations": [
      {
            "server.osVersion": "3.14.48-33.39.amzn1.x86_64",
            "server.type": "EC2",
            "server.hostName": "ip-172-31-42-208",
            "server.timeOfCreation": "2016-10-28 23:44:30.0",
            "server.configurationId": "d-server-099385097ef9fbcfb",
            "server.osName": "Linux - Amazon Linux AMI release 2015.03",
            "server.agentId": "i-c142b99e"
        },
        {
            "server.osVersion": "3.14.48-33.39.amzn1.x86_64",
            "server.type": "EC2",
            "server.hostName": "ip-172-31-35-152",
            "server.timeOfCreation": "2016-10-28 23:44:00.0",
            "server.configurationId": "d-server-0c4f2dd1fee22c6c1",
            "server.osName": "Linux - Amazon Linux AMI release 2015.03",
            "server.agentId": "i-4447bc1b"
```

```
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListConfigurations en la Referencia de comandos de la AWS CLI.

Ejemplos de señales de aplicación que utilizan AWS CLI

En los ejemplos de código siguientes, se muestra cómo realizar acciones e implementar situaciones comunes mediante la AWS Command Line Interface con señales de aplicaciones.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`batch-get-service-level-objective-budget-report`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-service-level-objective-budget-report`.

AWS CLI

Para recuperar uno o más informes de presupuesto de objetivos de nivel de servicio (SLO).

En el ejemplo de `batch-get-service-level-objective-budget-report` siguiente, se recuperan uno o más informes de presupuesto de objetivos de nivel de servicio (SLO).

```
aws application-signals batch-get-service-level-objective-budget-report \
--timestamp 1735059869 \
--slo-ids "arn:aws:application-signals:us-east-1:123456789101:slo/
SLOName1" "arn:aws:application-signals:us-east-1:123456789101:slo/SLOName2"
```

Salida:

```
{
    "Timestamp": "2024-12-24T22:34:29+05:30",
    "Reports": [{
            "Arn": "arn:aws:application-signals:us-east-1:123456789101:slo/
SLOName1",
            "Name": "Your SLO Name",
            "EvaluationType": "PeriodBased",
            "BudgetStatus": "OK",
            "Attainment": 100.0,
            "TotalBudgetSeconds": 6048,
            "BudgetSecondsRemaining": 6048,
            "Sli": {
                "SliMetric": {
                    "MetricDataQueries": [{
                        "Id": "m1",
                        "MetricStat": {
                            "Metric": {
                                "Namespace": "AWS/EC2",
                                "MetricName": "CPUUtilization",
                                "Dimensions": [{
                                    "Name": "InstanceId",
                                    "Value": "i-0e098765432522"
                                }]
                            },
                            "Period": 60,
                            "Stat": "Average"
                        },
                        "ReturnData": true
                    }]
                },
                "MetricThreshold": 200.0,
                "ComparisonOperator": "LessThanOrEqualTo"
            },
            "Goal": {
                "Interval": {
                    "RollingInterval": {
                        "DurationUnit": "DAY",
                        "Duration": 7
                    }
                },
                "AttainmentGoal": 99.0,
                "WarningThreshold": 50.0
```

```
            }
        },
        {
            "Arn": "arn:aws:application-signals:us-east-1:123456789101:slo/
SLOName2",
            "Name": "test",
            "EvaluationType": "PeriodBased",
            "BudgetStatus": "BREACHED",
            "Attainment": 97.39583275,
            "TotalBudgetSeconds": 86,
            "BudgetSecondsRemaining": -2154,
            "Sli": {
                "SliMetric": {
                    "MetricDataQueries": [{
                        "Id": "cwMetric",
                        "MetricStat": {
                            "Metric": {
                                "Namespace": "AWS/EC2",
                                "MetricName": "CPUUtilization",
                                "Dimensions": [{
                                    "Name": "InstanceId",
                                    "Value": "i-0e12345678922"
                                }]
                            },
                            "Period": 300,
                            "Stat": "Average"
                        },
                        "ReturnData": true
                    }]
                },
                "MetricThreshold": 5.0,
                "ComparisonOperator": "GreaterThan"
            },
            "Goal": {
                "Interval": {
                    "RollingInterval": {
                        "DurationUnit": "DAY",
                        "Duration": 1
                    }
                },
                "AttainmentGoal": 99.9,
                "WarningThreshold": 30.0
            }
        }
```

```
    ],
    "Errors": []
}
```

Para obtener más información, consulte Señales de aplicaciones en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte BatchGetServiceLevelObjectiveBudgetReport en la Referencia de comandos de la AWS CLI.

`create-service-level-objective`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-service-level-objective`.

AWS CLI

Creación de un objetivo de nivel de servicio (SLO)

En el ejemplo de `create-service-level-objective` siguiente, se crea un objetivo de nivel de servicio (SLO), que puede ayudarlo a garantizar que las operaciones empresariales críticas cumplan con las expectativas de los clientes.

```
aws application-signals create-service-level-objective \
    --name "SLOName" \
    --description "Description of your SLO" \
    --sli-config file://sli-config.json
```

Contenido de `sli-config.json`:

```
{
    "SliMetricConfig": {
        "MetricDataQueries": [
            {
                "Id": "m1",
                "MetricStat": {
                    "Metric": {
                        "Namespace": "AWS/EC2",
                        "MetricName": "CPUUtilization",
                        "Dimensions": [
                            {
                                "Name": "InstanceId",
                                "Value": "i-0e5a1234561522"
```

```
                            }
                        ]
                    },
                    "Period": 60,
                    "Stat": "Average"
                },
                "ReturnData": true
            }
        ]
    },
    "MetricThreshold": 200,
    "ComparisonOperator": "LessThanOrEqualTo"
}
```

Salida:

```
{
    "Slo": {
    "Arn": "arn:aws:application-signals:us-east-1:123456789101:slo/SLOName",
    "Name": "SLOName",
    "Description": "Description of your SLO",
    "CreatedTime": "2024-12-27T08:16:09.032000+05:30",
    "LastUpdatedTime": "2024-12-27T08:16:09.032000+05:30",
    "Sli": {
        "SliMetric": {
            "MetricDataQueries": [
                {
                    "Id": "m1",
                    "MetricStat": {
                        "Metric": {
                            "Namespace": "AWS/EC2",
                            "MetricName": "CPUUtilization",
                            "Dimensions": [
                                {
                                    "Name": "InstanceId",
                                    "Value": "i-0e59876543234522"
                                }
                            ]
                        },
                        "Period": 60,
                        "Stat": "Average"
                    },
                    "ReturnData": true
```

```
                }
            ]
        },
        "MetricThreshold": 200.0,
        "ComparisonOperator": "LessThanOrEqualTo"
    },
    "EvaluationType": "PeriodBased",
    "Goal": {
        "Interval": {
            "RollingInterval": {
                "DurationUnit": "DAY",
                "Duration": 7
            }
        },
        "AttainmentGoal": 99.0,
        "WarningThreshold": 50.0
      }
    }
}
```

Para obtener más información, consulte Señales de aplicaciones en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte CreateServiceLevelObjective en la Referencia de comandos de la AWS CLI.

`delete-service-level-objective`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-service-level-objective`.

AWS CLI

Para eliminar el objetivo de nivel de servicio especificado.

En el ejemplo de `delete-service-level-objective` siguiente, se elimina el objetivo de nivel de servicio especificado.

```
aws application-signals delete-service-level-objective \
    --id "arn:aws:application-signals:us-east-1:123456789101:slo/SLOName"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Señales de aplicaciones en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DeleteServiceLevelObjective en la Referencia de comandos de la AWS CLI.

`get-service-level-objective`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-level-objective`.

AWS CLI

Devolución de información sobre un SLO creado en la cuenta

En el ejemplo de `get-service-level-objective` siguiente, se devuelve información sobre un SLO creado en la cuenta.

```
aws application-signals get-service-level-objective \
    --id "arn:aws:application-signals:us-east-1:123456789101:slo/SLOName"
```

Salida:

```
{
    "Slo": {
        "Arn": "arn:aws:application-signals:us-east-1:123456789101:slo/SLOName",
        "Name": "SLOName",
        "Description": "Description of your SLO",
        "CreatedTime": "2024-12-24T22:19:18.624000+05:30",
        "LastUpdatedTime": "2024-12-24T22:19:55.280000+05:30",
        "Sli": {
            "SliMetric": {
                "MetricDataQueries": [{
                    "Id": "m1",
                    "MetricStat": {
                        "Metric": {
                            "Namespace": "AWS/EC2",
                            "MetricName": "CPUUtilization",
                            "Dimensions": [{
                                "Name": "InstanceId",
                                "Value": "i-0e0987654321522"
                            }]
                        },
```

```
                        "Period": 60,
                        "Stat": "Average"
                    },
                    "ReturnData": true
                }]
            },
            "MetricThreshold": 200.0,
            "ComparisonOperator": "LessThanOrEqualTo"
        },
        "EvaluationType": "PeriodBased",
        "Goal": {
            "Interval": {
                "RollingInterval": {
                    "DurationUnit": "DAY",
                    "Duration": 7
                }
            },
            "AttainmentGoal": 99.0,
            "WarningThreshold": 50.0
        }
    }
}
```

Para obtener más información, consulte Señales de aplicaciones en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetServiceLevelObjective en la Referencia de comandos de la AWS CLI.

`get-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service`.

AWS CLI

Recuperación de información sobre un servicio detectado por señales de aplicaciones

En el ejemplo de `get-service` siguiente, se devuelve información sobre un servicio detectado por señales de aplicaciones.

```
aws application-signals get-service \
    --start-time 1732704000 \
    --end-time 1732714500 \
```

```
    --key-attributes Environment=lambda:default,Name=hello-world-python,Type=Service
```

Salida:

```
{
    "Service": {
        "KeyAttributes": {
            "Environment": "lambda:default",
            "Name": "hello-world-python",
            "Type": "Service"
        },
        "AttributeMaps": [{
            "Lambda.Function.Name": "hello-world-python",
            "PlatformType": "AWS::Lambda"
        }],
        "MetricReferences": [{
            "Namespace": "ApplicationSignals",
            "MetricType": "LATENCY",
            "Dimensions": [{
                "Name": "Environment",
                "Value": "lambda:default"
            }, {
                "Name": "Service",
                "Value": "hello-world-python"
            }],
            "MetricName": "Latency"
        }, {
            "Namespace": "ApplicationSignals",
            "MetricType": "FAULT",
            "Dimensions": [{
                "Name": "Environment",
                "Value": "lambda:default"
            }, {
                "Name": "Service",
                "Value": "hello-world-python"
            }],
            "MetricName": "Fault"
        }, {
            "Namespace": "ApplicationSignals",
            "MetricType": "ERROR",
            "Dimensions": [{
                "Name": "Environment",
                "Value": "lambda:default"
```

```
            }, {
                "Name": "Service",
                "Value": "hello-world-python"
            }],
            "MetricName": "Error"
        }],
        "LogGroupReferences": [{
            "Identifier": "/aws/lambda/hello-world-python",
            "ResourceType": "AWS::Logs::LogGroup",
            "Type": "AWS::Resource"
        }]
    },
    "StartTime": "2024-11-27T10:00:00+00:00",
    "EndTime": "2024-11-27T14:00:01+00:00",
    "LogGroupReferences": [{
        "Identifier": "/aws/lambda/hello-world-python",
        "ResourceType": "AWS::Logs::LogGroup",
        "Type": "AWS::Resource"
    }]
}
```

Para obtener más información, consulte Señales de aplicaciones en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetService en la Referencia de comandos de la AWS CLI.

`list-service-dependencies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-service-dependencies`.

AWS CLI

Devolución de una lista de las dependencias del servicio que se especifique

En el ejemplo de `list-service-dependencies` siguiente, se devuelve una lista de dependencias del servicio que se especifique.

```
aws application-signals list-service-dependencies \
    --start-time 1732021200 \
    --end-time 1732107600 \
```

```
    --key-attributes Environment=api-
gateway:prod, Name=PetAdoptionStatusUpdater,Type=Service
```

Salida:

```
{
    "ServiceDependencies": [{
        "OperationName": "PUT /prod",
        "DependencyKeyAttributes": {
            "Environment": "lambda:default",
            "Name": "Services-name",
            "Type": "Service"
        },
        "DependencyOperationName": "Invoke",
        "MetricReferences": [{
            "Namespace": "ApplicationSignals",
            "MetricType": "LATENCY",
            "Dimensions": [{
                "Name": "Environment",
                "Value": "api-gateway:prod"
            }, {
                "Name": "Operation",
                "Value": "PUT /prod"
            }, {
                "Name": "RemoteEnvironment",
                "Value": "lambda:default"
            }, {
                "Name": "RemoteOperation",
                "Value": "Invoke"
            }, {
                "Name": "RemoteService",
                "Value": "Services-name"
            }, {
                "Name": "Service",
                "Value": "PetAdoptionStatusUpdater"
            }],
            "MetricName": "Latency"
        }, {
            "Namespace": "ApplicationSignals",
            "MetricType": "FAULT",
            "Dimensions": [{
                "Name": "Environment",
                "Value": "api-gateway:prod"
```

```
            }, {
                "Name": "Operation",
                "Value": "PUT /prod"
            }, {
                "Name": "RemoteEnvironment",
                "Value": "lambda:default"
            }, {
                "Name": "RemoteOperation",
                "Value": "Invoke"
            }, {
                "Name": "RemoteService",
                "Value": "Services-name"
            }, {
                "Name": "Service",
                "Value": "PetAdoptionStatusUpdater"
            }],
            "MetricName": "Fault"
        }, {
            "Namespace": "ApplicationSignals",
            "MetricType": "ERROR",
            "Dimensions": [{
                "Name": "Environment",
                "Value": "api-gateway:prod"
            }, {
                "Name": "Operation",
                "Value": "PUT /prod"
            }, {
                "Name": "RemoteEnvironment",
                "Value": "lambda:default"
            }, {
                "Name": "RemoteOperation",
                "Value": "Invoke"
            }, {
                "Name": "RemoteService",
                "Value": "Services-name"
            }, {
                "Name": "Service",
                "Value": "PetAdoptionStatusUpdater"
            }],
            "MetricName": "Error"
        }]
    }],
    "StartTime": "2024-11-19T13:00:00+00:00",
    "EndTime": "2024-11-20T13:00:01+00:00"
```

```
}
```

Para obtener más información, consulte Señales de aplicaciones en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListServiceDependencies en la Referencia de comandos de la AWS CLI.

`list-service-dependents`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-service-dependents`.

AWS CLI

Devolución de la lista de dependientes que invocaron el servicio especificado durante el intervalo de tiempo proporcionado

En el ejemplo de `list-service-dependents` siguiente, se devuelve la lista de dependientes que invocaron el servicio especificado durante el intervalo de tiempo proporcionado.

```
aws application-signals list-service-dependents \
    --start-time 1732021200 \
    --end-time 1732107600 \
    --key-attributes Environment=generic:default,Name=PetSite,Type=Service
```

Salida:

```
{
    "ServiceDependents": [{
        "OperationName": "",
        "DependentKeyAttributes": {
            "Identifier": "pet-api-canary-hao",
            "ResourceType": "AWS::Synthetics::Canary",
            "Type": "AWS::Resource"
        },
        "DependentOperationName": "",
        "MetricReferences": []
    }, {
        "OperationName": "",
        "DependentKeyAttributes": {
            "Identifier": "PetSite",
```

```
            "ResourceType": "AWS::Synthetics::Canary",
            "Type": "AWS::Resource"
        },
        "DependentOperationName": "",
        "MetricReferences": []
    }],
    "StartTime": "2024-12-24T05:00:00+00:00",
    "EndTime": "2024-12-25T06:00:01+00:00"
}
```

Para obtener más información, consulte Señales de aplicaciones en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListServiceDependents en la Referencia de comandos de la AWS CLI.

`list-service-level-objectives`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-service-level-objectives`.

AWS CLI

Para devolver una lista de los SLO creados en esta cuenta.

En el ejemplo de `list-service-level-objectives` siguiente, se devuelve una lista de los SLO creada en esta cuenta.

```
aws application-signals list-service-level-objectives
```

Salida:

```
{
    "SloSummaries": [{
        "Arn": "arn:aws:application-signals:us-east-1:123456789101:slo/test",
        "Name": "test",
        "CreatedTime": "2024-12-24T22:01:21.116000+05:30"
    }]
}
```

Para obtener más información, consulte Señales de aplicaciones en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListServiceLevelObjectives en la Referencia de comandos de la AWS CLI.

`list-service-operations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-service-operations`.

AWS CLI

Devolución de una lista de las operaciones de este servicio descubiertas por señales de aplicaciones

En el ejemplo de `list-service-operations` siguiente, se devuelve una lista de las operaciones de este servicio descubiertas por señales de aplicaciones.

```
aws application-signals list-service-operations \
    --start-time 1735017423 \
    --end-time 1735103823 \
    --key-attributes Environment=generic:default,Name=payforadoption,Type=Service
```

Salida:

```
{
    "ServiceOperations": [{
        "Name": "POST /api",
        "MetricReferences": [{
            "Namespace": "ApplicationSignals",
            "MetricType": "LATENCY",
            "Dimensions": [{
                "Name": "Environment",
                "Value": "generic:default"
            }, {
                "Name": "Operation",
                "Value": "POST /api"
            }, {
                "Name": "Service",
                "Value": "payforadoption"
            }],
            "MetricName": "Latency"
        }, {
            "Namespace": "ApplicationSignals",
```

```
            "MetricType": "FAULT",
            "Dimensions": [{
                "Name": "Environment",
                "Value": "generic:default"
            }, {
                "Name": "Operation",
                "Value": "POST /api"
            }, {
                "Name": "Service",
                "Value": "payforadoption"
            }],
            "MetricName": "Fault"
        }, {
            "Namespace": "ApplicationSignals",
            "MetricType": "ERROR",
            "Dimensions": [{
                "Name": "Environment",
                "Value": "generic:default"
            }, {
                "Name": "Operation",
                "Value": "POST /api"
            }, {
                "Name": "Service",
                "Value": "payforadoption"
            }],
            "MetricName": "Error"
        }]
    }],
    "StartTime": "2024-12-24T05:00:00+00:00",
    "EndTime": "2024-12-25T06:00:01+00:00"
}
```

Para obtener más información, consulte Señales de aplicaciones en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListServiceOperations en la Referencia de comandos de la AWS CLI.

`list-services`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-services`.

AWS CLI

Devolución de una lista de los servicios descubiertos por señales de aplicaciones

En el ejemplo de `list-services` siguiente, se devuelve una lista de servicios detectados por señales de aplicaciones.

```
aws application-signals list-services \
    --start-time 1734918791 \
    --end-time 1734965591
```

Salida:

```
{
    "ServiceSummaries": [{
        "KeyAttributes": {
            "Environment": "lambda:default",
            "Name": "hello-world-python",
            "Type": "Service"
        },
        "AttributeMaps": [{
            "Lambda.Function.Name": "hello-world-python",
            "PlatformType": "AWS::Lambda"
        }],
        "MetricReferences": [{
            "Namespace": "ApplicationSignals",
            "MetricType": "LATENCY",
            "Dimensions": [{
                "Name": "Environment",
                "Value": "lambda:default"
            }, {
                "Name": "Service",
                "Value": "hello-world-python"
            }],
            "MetricName": "Latency"
        }, {
            "Namespace": "ApplicationSignals",
            "MetricType": "FAULT",
            "Dimensions": [{
                "Name": "Environment",
                "Value": "lambda:default"
            }, {
                "Name": "Service",
```

```
                "Value": "hello-world-python"
            }],
            "MetricName": "Fault"
        }, {
            "Namespace": "ApplicationSignals",
            "MetricType": "ERROR",
            "Dimensions": [{
                "Name": "Environment",
                "Value": "lambda:default"
            }, {
                "Name": "Service",
                "Value": "hello-world-python"
            }],
            "MetricName": "Error"
        }]
    }],
    "StartTime": "2024-11-27T10:00:00+00:00",
    "EndTime": "2024-11-27T14:00:01+00:00"
}
```

Para obtener más información, consulte Señales de aplicaciones en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListServices en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Muestra de las etiquetas asociadas a un recurso de CloudWatch

En el ejemplo de `list-tags-for-resource` siguiente, se muestran las etiquetas asociadas con un recurso de CloudWatch.

```
aws application-signals list-tags-for-resource \
    --resource-arn "arn:aws:application-signals:us-east-1:123456789101:slo/SLOName"
```

Salida:

```
{
```

```
    "Tags": [{
        "Key": "test",
        "Value": "value"
    }]
}
```

Para obtener más información, consulte Señales de aplicaciones en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`start-discovery`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-discovery`.

AWS CLI

Permiso para que esta cuenta de Amazon Web Services pueda utilizar señales de aplicaciones de CloudWatch

En el ejemplo de `start-discovery` siguiente, se permite que esta cuenta de Amazon Web Services pueda utilizar señales de aplicaciones de CloudWatch mediante la creación del rol vinculado al servicio AWSServiceRoleForCloudWatchApplicationSignals.

```
aws application-signals start-discovery
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Señales de aplicaciones en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte StartDiscovery en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Asignación de una o más etiquetas (pares clave-valor) al recurso de CloudWatch especificado, como un objetivo de nivel de servicio

En el ejemplo de `tag-resource` siguiente, se asignan una o más etiquetas (pares clave-valor) al recurso de CloudWatch especificado, como un objetivo de nivel de servicio.

```
aws application-signals tag-resource \
    --resource-arn "arn:aws:application-signals:us-east-1:123456789101:slo/SLOName"
 \
    --tags '{"Key":"test","Value":"value"}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Señales de aplicaciones en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de una o varias etiquetas del recurso especificado

En el ejemplo de `untag-resource` siguiente, se eliminan una o más etiquetas del recurso especificado.

```
aws application-signals untag-resource \
    --resource-arn "arn:aws:application-signals:us-east-1:123456789101:slo/SLOName"
 \
    --tag-keys "test"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Señales de aplicaciones en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-service-level-objective`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-service-level-objective`.

AWS CLI

Actualización de un objetivo de nivel de servicio (SLO) existente

En el ejemplo de `update-service-level-objective` siguiente, se actualiza un objetivo de nivel de servicio (SLO) existente.

```
aws application-signals update-service-level-objective \
--cli-input-json file://update-slo.json
```

Contenido de `update-slo.json`:

```
{
    "id": "arn:aws:application-signals:us-east-1:123456789101:slo/SLOName",
    "goal": {
        "Interval": {
            "RollingInterval": {
                "DurationUnit": "DAY",
                "Duration": 7
            }
        },
        "AttainmentGoal": 90.0,
        "WarningThreshold": 50.0
    }
}
```

Salida:

```
{
    "Slo": {
        "Arn": "arn:aws:application-signals:us-east-1:123456789101:slo/SLOName",
        "Name": "SLOName",
        "Description": "Description of your SLO",
```

```
        "CreatedTime": "2024-12-24T22:19:18.624000+05:30",
        "LastUpdatedTime": "2024-12-27T08:51:38.278000+05:30",
        "Sli": {
            "SliMetric": {
                "MetricDataQueries": [{
                    "Id": "m1",
                    "MetricStat": {
                        "Metric": {
                            "Namespace": "AWS/EC2",
                            "MetricName": "CPUUtilization",
                            "Dimensions": [{
                                "Name": "InstanceId",
                                "Value": "i-00987654345222"
                            }]
                        },
                        "Period": 60,
                        "Stat": "Average"
                    },
                    "ReturnData": true
                }]
            },
            "MetricThreshold": 200.0,
            "ComparisonOperator": "LessThanOrEqualTo"
        },
        "EvaluationType": "PeriodBased",
        "Goal": {
            "Interval": {
                "RollingInterval": {
                    "DurationUnit": "DAY",
                    "Duration": 7
                }
            },
            "AttainmentGoal": 90.0,
            "WarningThreshold": 50.0
        }
    }
}
```

Para obtener más información, consulte Señales de aplicaciones en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte UpdateServiceLevelObjective en la Referencia de comandos de la AWS CLI.

Ejemplos de AppRegistry que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar situaciones comunes usando la AWS Command Line Interface con AppRegistry.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-attribute-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-attribute-group`.

AWS CLI

Para asociar un grupo de atributos

En el siguiente ejemplo de `associate-attribute-group`, se asocia un grupo de atributos específico de su cuenta de AWS a una aplicación determinada de su cuenta de AWS.

```
aws servicecatalog-appregistry associate-attribute-group \
    --application "ExampleApplication" \
    --attribute-group "ExampleAttributeGroup"
```

Salida:

```
{
    "applicationArn": "arn:aws:servicecatalog:us-west-2:813737243517:/
applications/0ars38r6btoohvpvd9gqrptt9l",
    "attributeGroupArn": "arn:aws:servicecatalog:us-west-2:813737243517:/attribute-
groups/01sj5xdwhbw54kejwnt09fnpcl"
```

```
}
```

Para obtener más información, consulte Associating and disassociating attribute groups en la Guía para administradores de AWS Service Catalog AppRegistry.

- Para obtener información sobre la API, consulte AssociateAttributeGroup en la Referencia de comandos de la AWS CLI.

`create-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-application`.

AWS CLI

Para crear una aplicación

En el siguiente ejemplo de `create-application`, se crea una aplicación nueva en su cuenta de AWS.

```
aws servicecatalog-appregistry create-application \
    --name "ExampleApplication"
```

Salida:

```
{
    "application": {
        "id": "0ars38r6btoohvpvd9gqrptt9l",
        "arn": "arn:aws:servicecatalog:us-west-2:813737243517:/
applications/0ars38r6btoohvpvd9gqrptt9l",
        "name": "ExampleApplication",
        "creationTime": "2023-02-28T21:10:10.820000+00:00",
        "lastUpdateTime": "2023-02-28T21:10:10.820000+00:00",
        "tags": {}
    }
}
```

Para obtener más información, consulte Creating applications en la Guía para administradores de AWS Service Catalog AppRegistry.

- Para obtener información sobre la API, consulte CreateApplication en la Referencia de comandos de la AWS CLI.

`create-attribute-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-attribute-group`.

AWS CLI

Para crear un grupo de atributos

En el siguiente ejemplo de `create-attribute-group`, se crea un grupo de atributos nuevo en su cuenta de AWS.

```
aws servicecatalog-appregistry create-attribute-group \
    --name "ExampleAttributeGroup" \
    --attributes '{"SomeKey1":"SomeValue1","SomeKey2":"SomeValue2"}'
```

Salida:

```
{
    "attributeGroup": {
        "id": "01sj5xdwhbw54kejwnt09fnpcl",
        "arn": "arn:aws:servicecatalog:us-west-2:813737243517:/attribute-
groups/01sj5xdwhbw54kejwnt09fnpcl",
        "name": "ExampleAttributeGroup",
        "creationTime": "2023-02-28T20:38:01.389000+00:00",
        "lastUpdateTime": "2023-02-28T20:38:01.389000+00:00",
        "tags": {}
    }
}
```

Para obtener más información, consulte Creating attribute groups en la Guía para administradores de AWS Service Catalog AppRegistry.

- Para obtener información sobre la API, consulte CreateAttributeGroup en la Referencia de comandos de la AWS CLI.

`delete-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-application`.

AWS CLI

Para eliminar una aplicación de

En el siguiente ejemplo de `delete-application`, se elimina una aplicación específica de su cuenta de AWS.

```
aws servicecatalog-appregistry delete-application \
    --application "ExampleApplication3"
```

Salida:

```
{
    "application": {
        "id": "055gw7aynr1i5mbv7kjwzx5945",
        "arn": "arn:aws:servicecatalog:us-west-2:813737243517:/
applications/055gw7aynr1i5mbv7kjwzx5945",
        "name": "ExampleApplication3",
        "creationTime": "2023-02-28T22:06:28.228000+00:00",
        "lastUpdateTime": "2023-02-28T22:06:28.228000+00:00"
    }
}
```

Para obtener más información, consulte Deleting applications en la Guía para administradores de AWS Service Catalog AppRegistry.

- Para obtener información sobre la API, consulte DeleteApplication en la Referencia de comandos de la AWS CLI.

`delete-attribute-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-attribute-group`.

AWS CLI

Ejemplo 8: eliminación de un grupo de atributos

En el siguiente ejemplo de `delete-attribute-group`, se elimina un atributo específico de su cuenta de AWS.

```
aws servicecatalog-appregistry delete-attribute-group \
    --attribute-group "ExampleAttributeGroup3"
```

Salida:

```
{
    "attributeGroup": {
        "id": "011ge6y3emyjijt8dw8jn6r0hv",
        "arn": "arn:aws:servicecatalog:us-west-2:813737243517:/attribute-
groups/011ge6y3emyjijt8dw8jn6r0hv",
        "name": "ExampleAttributeGroup3",
        "creationTime": "2023-02-28T22:05:35.224000+00:00",
        "lastUpdateTime": "2023-02-28T22:05:35.224000+00:00"
    }
}
```

Para obtener más información, consulte Deleting attribute groups en la Guía para administradores de AWS Service Catalog AppRegistry.

- Para obtener información sobre la API, consulte DeleteAttributeGroup en la Referencia de comandos de la AWS CLI.

`get-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-application`.

AWS CLI

Para obtener una aplicación

En el siguiente ejemplo de `get-application`, se recupera información de metadatos de una aplicación específica en la cuenta de AWS.

```
aws servicecatalog-appregistry get-application \
    --application "ExampleApplication"
```

Salida:

```
{
    "id": "0ars38r6btoohvpvd9gqrptt9l",
    "arn": "arn:aws:servicecatalog:us-west-2:813737243517:/
applications/0ars38r6btoohvpvd9gqrptt9l",
    "name": "ExampleApplication",
    "creationTime": "2023-02-28T21:10:10.820000+00:00",
    "lastUpdateTime": "2023-02-28T21:10:10.820000+00:00",
    "associatedResourceCount": 0,
```

```
    "tags": {
        "aws:servicecatalog:applicationName": "ExampleApplication"
    },
    "integrations": {
        "resourceGroup": {
            "state": "CREATE_COMPLETE",
            "arn": "arn:aws:resource-groups:us-west-2:813737243517:group/
AWS_AppRegistry_Application-ExampleApplication"
        }
    }
}
```

Para obtener más información, consulte Using Application details en la Guía para administradores de AWS Service Catalog AppRegistry.

- Para obtener más información sobre la API, consulte GetApplication en la Referencia de comandos de la AWS CLI.

`get-attribute-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-attribute-group`.

AWS CLI

Para obtener un grupo de atributos

En el siguiente ejemplo de `get-attribute-group`, se recupera un grupo de atributos específico de su cuenta de AWS.

```
aws servicecatalog-appregistry get-attribute-group \
    --attribute-group "ExampleAttributeGroup"
```

Salida:

```
{
    "id": "01sj5xdwhbw54kejwnt09fnpcl",
    "arn": "arn:aws:servicecatalog:us-west-2:813737243517:/attribute-
groups/01sj5xdwhbw54kejwnt09fnpcl",
    "name": "ExampleAttributeGroup",
    "attributes": "{\"SomeKey1\":\"SomeValue1\",\"SomeKey2\":\"SomeValue2\"}",
    "creationTime": "2023-02-28T20:38:01.389000+00:00",
    "lastUpdateTime": "2023-02-28T20:38:01.389000+00:00",
```

```
    "tags": {
        "aws:servicecatalog:attributeGroupName": "ExampleAttributeGroup"
    }
}
```

Para obtener más información, consulte Managing metadata for attribute groups en la Guía para administradores de AWS Service Catalog AppRegistry.

- Para obtener información sobre la API, consulte GetAttributeGroup en la Referencia de comandos de la AWS CLI.

`list-applications`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-applications`.

AWS CLI

Para enumerar aplicaciones

En el siguiente ejemplo de `list-applications`, se recupera una lista de todas las aplicaciones de su cuenta de AWS.

```
aws servicecatalog-appregistry list-applications
```

Salida:

```
{
    "applications": [
        {
            "id": "03axw94pjfj3uan00tcgbrxnkw",
            "arn": "arn:aws:servicecatalog:us-west-2:813737243517:/
applications/03axw94pjfj3uan00tcgbrxnkw",
            "name": "ExampleApplication2",
            "creationTime": "2023-02-28T21:59:34.094000+00:00",
            "lastUpdateTime": "2023-02-28T21:59:34.094000+00:00"
        },
        {
            "id": "055gw7aynr1i5mbv7kjwzx5945",
            "arn": "arn:aws:servicecatalog:us-west-2:813737243517:/
applications/055gw7aynr1i5mbv7kjwzx5945",
            "name": "ExampleApplication3",
            "creationTime": "2023-02-28T22:06:28.228000+00:00",
```

```
            "lastUpdateTime": "2023-02-28T22:06:28.228000+00:00"
        },
        {
            "id": "0ars38r6btoohvpvd9gqrptt9l",
            "arn": "arn:aws:servicecatalog:us-west-2:813737243517:/
applications/0ars38r6btoohvpvd9gqrptt9l",
            "name": "ExampleApplication",
            "description": "This is an example application",
            "creationTime": "2023-02-28T21:10:10.820000+00:00",
            "lastUpdateTime": "2023-02-28T21:24:19.729000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Viewing application details en la Guía para administradores de AWS Service Catalog AppRegistry.

- Para obtener más información sobre la API, consulte ListApplications en la Referencia de comandos de la AWS CLI.

`list-associated-attribute-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-associated-attribute-groups`.

AWS CLI

Para enumerar los grupos de atributos asociados

En el siguiente ejemplo de `list-associated-attribute-groups`, se recupera una lista de todos los grupos de atributos de su cuenta de AWS que están asociados a una aplicación específica de su cuenta de AWS.

```
aws servicecatalog-appregistry list-associated-attribute-groups \
    --application "ExampleApplication"
```

Salida:

```
{
    "attributeGroups": [
        "01sj5xdwhbw54kejwnt09fnpcl"
```

```
    ]
}
```

Para obtener más información, consulte Associating and disassociating attribute groups en la Guía para administradores de AWS Service Catalog AppRegistry.

- Para obtener información sobre la API, consulte ListAssociatedAttributeGroups en la Referencia de comandos de la AWS CLI.

`list-attribute-groups-for-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-attribute-groups-for-application`.

AWS CLI

Para enumerar los grupos de atributos de una aplicación

En el siguiente ejemplo de `list-attribute-groups-for-application`, se enumeran los detalles de todos los grupos de atributos de su cuenta de AWS que están asociados a una aplicación específica de su cuenta de AWS.

```
aws servicecatalog-appregistry list-attribute-groups-for-application \
    --application "ExampleApplication"
```

Salida:

```
{
    "attributeGroupsDetails": [
        {
            "id": "01sj5xdwhbw54kejwnt09fnpcl",
            "arn": "arn:aws:servicecatalog:us-west-2:813737243517:/attribute-
groups/01sj5xdwhbw54kejwnt09fnpcl",
            "name": "ExampleAttributeGroup"
        }
    ]
}
```

Para obtener más información, consulte Viewing attribute group details en la Guía para administradores de AWS Service Catalog AppRegistry.

- Para obtener información sobre la API, consulte ListAttributeGroupsForApplication en la Referencia de comandos de la AWS CLI.

`list-attribute-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-attribute-groups`.

AWS CLI

Para enumerar grupos de atributos

En el siguiente ejemplo de `list-attribute-groups`, se recupera una lista de todos los grupos de atributos de su cuenta de AWS.

```
aws servicecatalog-appregistry list-attribute-groups
```

Salida:

```
{
    "attributeGroups": [
        {
            "id": "011ge6y3emyjijt8dw8jn6r0hv",
            "arn": "arn:aws:servicecatalog:us-west-2:813737243517:/attribute-
groups/011ge6y3emyjijt8dw8jn6r0hv",
            "name": "ExampleAttributeGroup3",
            "creationTime": "2023-02-28T22:05:35.224000+00:00",
            "lastUpdateTime": "2023-02-28T22:05:35.224000+00:00"
        },
        {
            "id": "01sj5xdwhbw54kejwnt09fnpcl",
            "arn": "arn:aws:servicecatalog:us-west-2:813737243517:/attribute-
groups/01sj5xdwhbw54kejwnt09fnpcl",
            "name": "ExampleAttributeGroup",
            "description": "This is an example attribute group",
            "creationTime": "2023-02-28T20:38:01.389000+00:00",
            "lastUpdateTime": "2023-02-28T21:02:04.559000+00:00"
        },
        {
            "id": "03n1yffgq6d18vwrzxf0c70nm3",
            "arn": "arn:aws:servicecatalog:us-west-2:813737243517:/attribute-
groups/03n1yffgq6d18vwrzxf0c70nm3",
            "name": "ExampleAttributeGroup2",
```

```
            "creationTime": "2023-02-28T21:57:30.687000+00:00",
            "lastUpdateTime": "2023-02-28T21:57:30.687000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Viewing attribute group details en la Guía para administradores de AWS Service Catalog AppRegistry.

- Para obtener información sobre la API, consulte ListAttributeGroups en la Referencia de comandos de la AWS CLI.

`update-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-application`.

AWS CLI

Para actualizar una aplicación

En el siguiente ejemplo de `update-application`, se actualiza una aplicación específica de su cuenta de AWS para incluir una descripción.

```
aws servicecatalog-appregistry update-application \
    --application "ExampleApplication" \
    --description "This is an example application"
```

Salida:

```
{
    "application": {
        "id": "0ars38r6btoohvpvd9gqrptt9l",
        "arn": "arn:aws:servicecatalog:us-west-2:813737243517:/
applications/0ars38r6btoohvpvd9gqrptt9l",
        "name": "ExampleApplication",
        "description": "This is an example application",
        "creationTime": "2023-02-28T21:10:10.820000+00:00",
        "lastUpdateTime": "2023-02-28T21:24:19.729000+00:00",
        "tags": {
            "aws:servicecatalog:applicationName": "ExampleApplication"
        }
    }
```

```
}
```

Para obtener más información, consulte Editing applications en la Guía para administradores de AWS Service Catalog AppRegistry.

- Para obtener información sobre la API, consulte UpdateApplication en la Referencia de comandos de la AWS CLI.

`update-attribute-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-attribute-group`.

AWS CLI

Para actualizar un grupo de atributos

En el siguiente ejemplo de `update-attribute-group`, se actualiza un grupo de atributos específico de su cuenta de AWS para incluir una descripción.

```
aws servicecatalog-appregistry update-attribute-group \
    --attribute-group "ExampleAttributeGroup" \
    --description "This is an example attribute group"
```

Salida:

```
{
    "attributeGroup": {
        "id": "01sj5xdwhbw54kejwnt09fnpcl",
        "arn": "arn:aws:servicecatalog:us-west-2:813737243517:/attribute-
groups/01sj5xdwhbw54kejwnt09fnpcl",
        "name": "ExampleAttributeGroup",
        "description": "This is an example attribute group",
        "creationTime": "2023-02-28T20:38:01.389000+00:00",
        "lastUpdateTime": "2023-02-28T21:02:04.559000+00:00",
        "tags": {
            "aws:servicecatalog:attributeGroupName": "ExampleAttributeGroup"
        }
    }
}
```

Para obtener más información, consulte Editing attribute groups en la Guía para administradores de AWS Service Catalog AppRegistry.

- Para obtener información sobre la API, consulte UpdateAttributeGroup en la Referencia de comandos de AWS CLI.

Ejemplos de Athena que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar situaciones comunes usando la AWS Command Line Interface con Athena.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`batch-get-named-query`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-named-query`.

AWS CLI

Para obtener información sobre más de una consulta

En el siguiente ejemplo de `batch-get-named-query`, se ofrece información sobre las consultas con nombre que tienen los ID especificados.

```
aws athena batch-get-named-query \
    --named-query-ids a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 a1b2c3d4-5678-90ab-cdef-EXAMPLE33333
```

Salida:

```
{
    "NamedQueries": [
```

```
        {
            "Name": "Flights Select Query",
            "Description": "Sample query to get the top 10 airports with the most
 number of departures since 2000",
            "Database": "sampledb",
            "QueryString": "SELECT origin, count(*) AS total_departures\nFROM
\nflights_parquet\nWHERE year >= '2000'\nGROUP BY origin\nORDER BY total_departures
 DESC\nLIMIT 10;",
            "NamedQueryId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "WorkGroup": "primary"
        },
        {
            "Name": "Load flights table partitions",
            "Description": "Sample query to load flights table partitions using MSCK
 REPAIR TABLE statement",
            "Database": "sampledb",
            "QueryString": "MSCK REPAIR TABLE flights_parquet;",
            "NamedQueryId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "WorkGroup": "primary"
        },
        {
            "Name": "CloudFront Select Query",
            "Description": "Sample query to view requests per operating system
 during a particular time frame",
            "Database": "sampledb",
            "QueryString": "SELECT os, COUNT(*) count FROM cloudfront_logs WHERE
 date BETWEEN date '2014-07-05' AND date '2014-08-05' GROUP BY os;",
            "NamedQueryId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "WorkGroup": "primary"
        }
    ],
    "UnprocessedNamedQueryIds": []
}
```

Si desea obtener más información, consulte Ejecución de consultas SQL mediante Amazon Athena en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte BatchGetNamedQuery en la Referencia de comandos de la AWS CLI.

`batch-get-query-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-query-execution`.

AWS CLI

Para obtener información sobre una o más ejecuciones de consulta

En el siguiente ejemplo de `batch-get-query-execution`, se ofrece información de la ejecución de las consultas que tienen los ID de consulta especificados.

```
aws athena batch-get-query-execution \
    --query-execution-ids a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

Salida:

```
{
    "QueryExecutions": [
        {
            "QueryExecutionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "Query": "create database if not exists webdata",
            "StatementType": "DDL",
            "ResultConfiguration": {
                "OutputLocation": "s3://amzn-s3-demo-bucket/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111.txt"
            },
            "QueryExecutionContext": {},
            "Status": {
                "State": "SUCCEEDED",
                "SubmissionDateTime": 1593470720.592,
                "CompletionDateTime": 1593470720.902
            },
            "Statistics": {
                "EngineExecutionTimeInMillis": 232,
                "DataScannedInBytes": 0,
                "TotalExecutionTimeInMillis": 310,
            "ResultConfiguration": {

                "QueryQueueTimeInMillis": 50,
                "ServiceProcessingTimeInMillis": 28
            },
            "WorkGroup": "AthenaAdmin"
        },
        {
            "QueryExecutionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
```

```
            "Query": "select date, location, browser, uri, status from
 cloudfront_logs where method = 'GET' and status = 200 and location like 'SFO%'
 limit 10",
            "StatementType": "DML",
            "ResultConfiguration": {
                "OutputLocation": "s3://amzn-s3-demo-bucket/a1b2c3d4-5678-90ab-cdef-
EXAMPLE22222.csv"
            },
            "QueryExecutionContext": {
                "Database": "mydatabase",
                "Catalog": "awsdatacatalog"
            },
            "Status": {
                "State": "SUCCEEDED",
                "SubmissionDateTime": 1593469842.665,
                "CompletionDateTime": 1593469846.486
            },
            "Statistics": {
                "EngineExecutionTimeInMillis": 3600,
                "DataScannedInBytes": 203089,
                "TotalExecutionTimeInMillis": 3821,
                "QueryQueueTimeInMillis": 267,
                "QueryPlanningTimeInMillis": 1175
            },
            "WorkGroup": "AthenaAdmin"
        }
    ],
    "UnprocessedQueryExecutionIds": []
}
```

Si desea obtener más información, consulte Ejecución de consultas SQL mediante Amazon Athena en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte BatchGetQueryExecution en la Referencia de comandos de la AWS CLI.

`create-data-catalog`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-data-catalog`.

AWS CLI

Creación de un catálogo de datos

En el siguiente ejemplo de `create-data-catalog`, se crea el catálogo de datos `dynamo_db_catalog`.

```
aws athena create-data-catalog \
    --name dynamo_db_catalog \
    --type LAMBDA \
    --description "DynamoDB Catalog" \
    --parameters function=arn:aws:lambda:us-
west-2:111122223333:function:dynamo_db_lambda
```

Este comando no genera ninguna salida. Para ver el resultado, utilice `aws athena get-data-catalog --name dynamo_db_catalog`.

Para obtener más información, consulte Registro de un catálogo: create-data-catalog en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte CreateDataCatalog en la Referencia de comandos de la AWS CLI.

`create-named-query`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-named-query`.

AWS CLI

Creación de una consulta con nombre

En el siguiente ejemplo de `create-named-query`, se crea una consulta guardada en el grupo de trabajo `AthenaAdmin` que consulta la tabla `flights_parquet` sobre los vuelos de Seattle a Nueva York en enero de 2016 cuya salida y llegada se retrasaron más de diez minutos. Como los valores de los códigos de aeropuerto de la tabla son cadenas que incluyen comillas dobles (por ejemplo, SEA), aparecen separados por barras diagonales invertidas y entre comillas simples.

```
aws athena create-named-query \
    --name "SEA to JFK delayed flights Jan 2016" \
    --description "Both arrival and departure delayed more than 10 minutes." \
    --database sampledb \
    --query-string "SELECT flightdate, carrier, flightnum, origin, dest,
 depdelayminutes, arrdelayminutes FROM sampledb.flights_parquet WHERE yr = 2016 AND
 month = 1 AND origin = '\"SEA\"' AND dest = '\"JFK\"' AND depdelayminutes > 10 AND
 arrdelayminutes > 10" \
```

```
    --work-group AthenaAdmin
```

Salida:

```
{
    "NamedQueryId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Si desea obtener más información, consulte Ejecución de consultas SQL mediante Amazon Athena en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte CreateNamedQuery en la Referencia de comandos de la AWS CLI.

`create-work-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-work-group`.

AWS CLI

Creación de un grupo de trabajo

En el siguiente ejemplo de `create-work-group`, se crea un grupo de trabajo denominado `Data_Analyst_Group` que tiene la ubicación de salida de los resultados de la consulta `s3://amzn-s3-demo-bucket`. El comando crea un grupo de trabajo que anula los ajustes de configuración del cliente, lo que incluye la ubicación de salida de los resultados de la consulta. El comando también habilita las métricas de CloudWatch y añade tres pares de etiquetas clave-valor al grupo de trabajo para distinguirlo de otros grupos de trabajo. Tenga en cuenta que el argumento `--configuration` no tiene espacios antes de las comas que separan sus opciones.

```
aws athena create-work-group \
    --name Data_Analyst_Group \
    --configuration ResultConfiguration={OutputLocation="s3://amzn-s3-demo-
bucket"},EnforceWorkGroupConfiguration="true",PublishCloudWatchMetricsEnabled="true"
 \
    --description "Workgroup for data analysts" \
    --tags Key=Division,Value=West Key=Location,Value=Seattle Key=Team,Value="Big
 Data"
```

Este comando no genera ninguna salida. Para ver los resultados, utilice `aws athena get-work-group --work-group Data_Analyst_Group`.

Para obtener más información, consulte Administración de los grupos de trabajo en la Guía del usuario de Amazon Athena.

- Para obtener más información sobre la API, consulte CreateWorkGroup en la Referencia de comandos de la AWS CLI.

`delete-data-catalog`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-data-catalog`.

AWS CLI

Eliminación de un catálogo de datos

En el siguiente ejemplo de `delete-data-catalog`, se elimina el catálogo de datos `UnusedDataCatalog`.

```
aws athena delete-data-catalog \
    --name UnusedDataCatalog
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de un catálogo: delete-data-catalog en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte DeleteDataCatalog en la Referencia de comandos de la AWS CLI.

`delete-named-query`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-named-query`.

AWS CLI

Eliminación de una consulta con nombre

En el siguiente ejemplo de `delete-named-query`, se elimina la consulta con nombre que tiene el ID especificado.

```
aws athena delete-named-query \
    --named-query-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Este comando no genera ninguna salida.

Si desea obtener más información, consulte Ejecución de consultas SQL mediante Amazon Athena en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte DeleteNamedQuery en la Referencia de comandos de la AWS CLI.

`delete-work-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-work-group`.

AWS CLI

Eliminación de un grupo de trabajo

En el siguiente ejemplo de `delete-work-group`, se elimina el grupo de trabajo `TeamB`.

```
aws athena delete-work-group \
    --work-group TeamB
```

Este comando no genera ninguna salida. Para confirmar la eliminación, utilice `aws athena list-work-groups`.

Para obtener más información, consulte Administración de los grupos de trabajo en la Guía del usuario de Amazon Athena.

- Para obtener más información sobre la API, consulte DeleteWorkGroup en la Referencia de comandos de la AWS CLI.

`get-data-catalog`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-data-catalog`.

AWS CLI

Para obtener información sobre un catálogo de datos

En el siguiente ejemplo de `get-data-catalog`, se obtiene información sobre el catálogo de datos `dynamo_db_catalog`.

```
aws athena get-data-catalog \
```

```
    --name dynamo_db_catalog
```

Salida:

```
{
    "DataCatalog": {
        "Name": "dynamo_db_catalog",
        "Description": "DynamoDB Catalog",
        "Type": "LAMBDA",
        "Parameters": {
            "catalog": "dynamo_db_catalog",
            "metadata-function": "arn:aws:lambda:us-
west-2:111122223333:function:dynamo_db_lambda",
            "record-function": "arn:aws:lambda:us-
west-2:111122223333:function:dynamo_db_lambda"
        }
    }
}
```

Para obtener más información, consulte Visualización de los detalles del catálogo: get-data-catalog en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte GetDataCatalog en la Referencia de comandos de la AWS CLI.

`get-database`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-database`.

AWS CLI

Para obtener información sobre una base de datos en un catálogo de datos

El siguiente ejemplo de `get-database`, se obtiene información sobre la base de datos `sampledb` del catálogo de datos `AwsDataCatalog`.

```
aws athena get-database \
    --catalog-name AwsDataCatalog \
    --database-name sampledb
```

Salida:

```
{
    "Database": {
        "Name": "sampledb",
        "Description": "Sample database",
        "Parameters": {
            "CreatedBy": "Athena",
            "EXTERNAL": "TRUE"
        }
    }
}
```

Para obtener más información, consulte Visualización de los detalles del catálogo: get-data-catalog en la Guía del usuario de Amazon Athena.

- Para obtener más información sobre la API, consulte GetDatabase en la Referencia de comandos de la AWS CLI.

`get-named-query`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-named-query`.

AWS CLI

Devolución de una consulta con nombre

En el siguiente ejemplo de `get-named-query`, se ofrece información sobre la consulta con el ID especificado.

```
aws athena get-named-query \
    --named-query-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "NamedQuery": {
        "Name": "CloudFront Logs - SFO",
        "Description": "Shows successful GET request data for SFO",
        "Database": "default",
        "QueryString": "select date, location, browser, uri, status from
 cloudfront_logs where method = 'GET' and status = 200 and location like 'SFO%'
 limit 10",
        "NamedQueryId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
        "WorkGroup": "AthenaAdmin"
    }
}
```

Si desea obtener más información, consulte Ejecución de consultas SQL mediante Amazon Athena en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte GetNamedQuery en la Referencia de comandos de la AWS CLI.

`get-query-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-query-execution`.

AWS CLI

Para obtener información sobre una ejecución de consulta

En el siguiente ejemplo de `get-query-execution`, se ofrece información sobre la consulta con el ID de consulta especificado.

```
aws athena get-query-execution \
    --query-execution-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "QueryExecution": {
        "QueryExecutionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "Query": "select date, location, browser, uri, status from cloudfront_logs
 where method = 'GET
' and status = 200 and location like 'SFO%' limit 10",
        "StatementType": "DML",
        "ResultConfiguration": {
            "OutputLocation": "s3://amzn-s3-demo-bucket/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111.csv"
        },
        "QueryExecutionContext": {
            "Database": "mydatabase",
            "Catalog": "awsdatacatalog"
        },
        "Status": {
            "State": "SUCCEEDED",
```

```
            "SubmissionDateTime": 1593469842.665,
            "CompletionDateTime": 1593469846.486
        },
        "Statistics": {
            "EngineExecutionTimeInMillis": 3600,
            "DataScannedInBytes": 203089,
            "TotalExecutionTimeInMillis": 3821,
            "QueryQueueTimeInMillis": 267,
            "QueryPlanningTimeInMillis": 1175
        },
        "WorkGroup": "AthenaAdmin"
    }
}
```

Si desea obtener más información, consulte Ejecución de consultas SQL mediante Amazon Athena en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte GetQueryExecution en la Referencia de comandos de la AWS CLI.

`get-query-results`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-query-results`.

AWS CLI

Para obtener los resultados de una consulta

En el siguiente ejemplo de `get-query-results`, se ofrecen los resultados de la consulta con el ID de consulta especificado.

```
aws athena get-query-results \
    --query-execution-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "ResultSet": {
        "Rows": [
            {
                "Data": [
                    {
                        "VarCharValue": "date"
```

```
                    },
                    {
                        "VarCharValue": "location"
                    },
                    {
                        "VarCharValue": "browser"
                    },
                    {
                        "VarCharValue": "uri"
                    },
                    {
                        "VarCharValue": "status"
                    }
                ]
            },
            {
                "Data": [
                    {
                        "VarCharValue": "2014-07-05"
                    },
                    {
                        "VarCharValue": "SFO4"
                    },
                    {
                        "VarCharValue": "Safari"
                    },
                    {
                        "VarCharValue": "/test-image-2.jpeg"
                    },
                    {
                        "VarCharValue": "200"
                    }
                ]
            },
            {
                "Data": [
                    {
                        "VarCharValue": "2014-07-05"
                    },
                    {
                        "VarCharValue": "SFO4"
                    },
                    {
                        "VarCharValue": "Opera"
```

```
                    },
                    {
                        "VarCharValue": "/test-image-2.jpeg"
                    },
                    {
                        "VarCharValue": "200"
                    }
                ]
            },
            {
                "Data": [
                    {
                        "VarCharValue": "2014-07-05"
                    },
                    {
                        "VarCharValue": "SFO4"
                    },
                    {
                        "VarCharValue": "Firefox"
                    },
                    {
                        "VarCharValue": "/test-image-3.jpeg"
                    },
                    {
                        "VarCharValue": "200"
                    }
                ]
            },
            {
                "Data": [
                    {
                        "VarCharValue": "2014-07-05"
                    },
                    {
                        "VarCharValue": "SFO4"
                    },
                    {
                        "VarCharValue": "Lynx"
                    },
                    {
                        "VarCharValue": "/test-image-3.jpeg"
                    },
                    {
                        "VarCharValue": "200"
```

```
                    }
                ]
            },
            {
                "Data": [
                    {
                        "VarCharValue": "2014-07-05"
                    },
                    {
                        "VarCharValue": "SFO4"
                    },
                    {
                        "VarCharValue": "IE"
                    },
                    {
                        "VarCharValue": "/test-image-2.jpeg"
                    },
                    {
                        "VarCharValue": "200"
                    }
                ]
            },
            {
                "Data": [
                    {
                        "VarCharValue": "2014-07-05"
                    },
                    {
                        "VarCharValue": "SFO4"
                    },
                    {
                        "VarCharValue": "Opera"
                    },
                    {
                        "VarCharValue": "/test-image-1.jpeg"
                    },
                    {
                        "VarCharValue": "200"
                    }
                ]
            },
            {
                "Data": [
                    {
```

```
                    "VarCharValue": "2014-07-05"
                },
                {
                    "VarCharValue": "SFO4"
                },
                {
                    "VarCharValue": "Chrome"
                },
                {
                    "VarCharValue": "/test-image-3.jpeg"
                },
                {
                    "VarCharValue": "200"
                }
            ]
        },
        {
            "Data": [
                {
                    "VarCharValue": "2014-07-05"
                },
                {
                    "VarCharValue": "SFO4"
                },
                {
                    "VarCharValue": "Firefox"
                },
                {
                    "VarCharValue": "/test-image-2.jpeg"
                },
                {
                    "VarCharValue": "200"
                }
            ]
        },
        {
            "Data": [
                {
                    "VarCharValue": "2014-07-05"
                },
                {
                    "VarCharValue": "SFO4"
                },
                {
```

```
                    "VarCharValue": "Chrome"
                },
                {
                    "VarCharValue": "/test-image-3.jpeg"
                },
                {
                    "VarCharValue": "200"
                }
            ]
        },
        {
            "Data": [
                {
                    "VarCharValue": "2014-07-05"
                },
                {
                    "VarCharValue": "SFO4"
                },
                {
                    "VarCharValue": "IE"
                },
                {
                    "VarCharValue": "/test-image-2.jpeg"
                },
                {
                    "VarCharValue": "200"
                }
            ]
        }
    ],
    "ResultSetMetadata": {
        "ColumnInfo": [
            {
                "CatalogName": "hive",
                "SchemaName": "",
                "TableName": "",
                "Name": "date",
                "Label": "date",
                "Type": "date",
                "Precision": 0,
                "Scale": 0,
                "Nullable": "UNKNOWN",
                "CaseSensitive": false
            },
```

```
                {
                    "CatalogName": "hive",
                    "SchemaName": "",
                    "TableName": "",
                    "Name": "location",
                    "Label": "location",
                    "Type": "varchar",
                    "Precision": 2147483647,
                "Data": [

                    "Scale": 0,
                    "Nullable": "UNKNOWN",
                    "CaseSensitive": true
                },
                {
                    "CatalogName": "hive",
                    "SchemaName": "",
                    "TableName": "",
                    "Name": "browser",
                    "Label": "browser",
                    "Type": "varchar",
                    "Precision": 2147483647,
                    "Scale": 0,
                    "Nullable": "UNKNOWN",
                    "CaseSensitive": true
                },
                {
                    "CatalogName": "hive",
                    "SchemaName": "",
                    "TableName": "",
                    "Name": "uri",
                    "Label": "uri",
                    "Type": "varchar",
                    "Precision": 2147483647,
                    "Scale": 0,
                    "Nullable": "UNKNOWN",
                    "CaseSensitive": true
                },
                {
                    "CatalogName": "hive",
                    "SchemaName": "",
                    "TableName": "",
                    "Name": "status",
                    "Label": "status",
```

```
                    "Type": "integer",
                    "Precision": 10,
                    "Scale": 0,
                    "Nullable": "UNKNOWN",
                    "CaseSensitive": false
                }
            ]
        }
    },
    "UpdateCount": 0
}
```

Para obtener más información, consulte Trabajo con resultados de la consulta y consultas recientes en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte GetQueryResults en la Referencia de comandos de la AWS CLI.

`get-table-metadata`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-table-metadata`.

AWS CLI

Para obtener información de metadatos sobre una tabla

En el siguiente ejemplo de `get-table-metadata`, se obtiene información de metadatos sobre la tabla `counties`, incluidos los nombres de las columnas y sus tipos de datos, de la base de datos `sampledb` del catálogo de datos `AwsDataCatalog`.

```
aws athena get-table-metadata \
    --catalog-name AwsDataCatalog \
    --database-name sampledb \
    --table-name counties
```

Salida:

```
{
    "TableMetadata": {
        "Name": "counties",
        "CreateTime": 1593559968.0,
```

```
        "LastAccessTime": 0.0,
        "TableType": "EXTERNAL_TABLE",
        "Columns": [
            {
                "Name": "name",
                "Type": "string",
                "Comment": "from deserializer"
            },
            {
                "Name": "boundaryshape",
                "Type": "binary",
                "Comment": "from deserializer"
            },
            {
                "Name": "motto",
                "Type": "string",
                "Comment": "from deserializer"
            },
            {
                "Name": "population",
                "Type": "int",
                "Comment": "from deserializer"
            }
        ],
        "PartitionKeys": [],
        "Parameters": {
            "EXTERNAL": "TRUE",
            "inputformat": "com.esri.json.hadoop.EnclosedJsonInputFormat",
            "location": "s3://amzn-s3-demo-bucket/json",
            "outputformat":
 "org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat",
            "serde.param.serialization.format": "1",
            "serde.serialization.lib": "com.esri.hadoop.hive.serde.JsonSerde",
            "transient_lastDdlTime": "1593559968"
        }
    }
}
```

Para obtener más información, consulte Visualización de los detalles de la tabla: get-table-metadata en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte GetTableMetadata en la Referencia de comandos de la AWS CLI.

`get-work-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-work-group`.

AWS CLI

Para obtener información sobre un grupo de trabajo

En el siguiente ejemplo de `get-work-group`, se obtiene información sobre el grupo de trabajo `AthenaAdmin`.

```
aws athena get-work-group \
    --work-group AthenaAdmin
```

Salida:

```
{
    "WorkGroup": {
        "Name": "AthenaAdmin",
        "State": "ENABLED",
        "Configuration": {
            "ResultConfiguration": {
                "OutputLocation": "s3://amzn-s3-demo-bucket/"
            },
            "EnforceWorkGroupConfiguration": false,
            "PublishCloudWatchMetricsEnabled": true,
            "RequesterPaysEnabled": false
        },
        "Description": "Workgroup for Athena administrators",
        "CreationTime": 1573677174.105
    }
}
```

Para obtener más información, consulte Administración de los grupos de trabajo en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte GetWorkGroup en la Referencia de comandos de la AWS CLI.

`list-data-catalogs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-data-catalogs`.

AWS CLI

Generación de una lista de catálogos de datos registrados en Athena

En el siguiente ejemplo de `list-data-catalogs`, se genera una lista de los catálogos de datos registrados en Athena.

```
aws athena list-data-catalogs
```

Salida:

```
{
    "DataCatalogsSummary": [
        {
            "CatalogName": "AwsDataCatalog",
            "Type": "GLUE"
        },
        {
            "CatalogName": "cw_logs_catalog",
            "Type": "LAMBDA"
        },
        {
            "CatalogName": "cw_metrics_catalog",
            "Type": "LAMBDA"
        }
    ]
}
```

Para obtener más información, consulte Enumeración de los catálogos registrados: list-data-catalogs en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte ListDataCatalogs en la Referencia de comandos de la AWS CLI.

`list-databases`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-databases`.

AWS CLI

Generación de una lista de bases de datos en un catálogo de datos

En el siguiente ejemplo de `list-databases`, se genera una lista de las bases de datos en el catálogo de datos `AwsDataCatalog`.

```
aws athena list-databases \
    --catalog-name AwsDataCatalog
```

Salida:

```
{
    "DatabaseList": [
        {
            "Name": "default"
        },
        {
            "Name": "mydatabase"
        },
        {
            "Name": "newdb"
        },
        {
            "Name": "sampledb",
            "Description": "Sample database",
            "Parameters": {
                "CreatedBy": "Athena",
                "EXTERNAL": "TRUE"
            }
        },
        {
            "Name": "webdata"
        }
    ]
}
```

Para obtener más información, consulte Enumeración de las bases de datos de un catálogo: list-databases en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte ListDatabases en la Referencia de comandos de la AWS CLI.

`list-named-queries`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-named-queries`.

AWS CLI

Generación de una lista de consultas con nombre de un grupo de trabajo

En el siguiente ejemplo de `list-named-queries`, se genera una lista de las consultas con nombre del grupo de trabajo `AthenaAdmin`.

```
aws athena list-named-queries \
    --work-group AthenaAdmin
```

Salida:

```
{
    "NamedQueryIds": [
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333"
    ]
}
```

Si desea obtener más información, consulte Ejecución de consultas SQL mediante Amazon Athena en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte ListNamedQueries en la Referencia de comandos de la AWS CLI.

`list-query-executions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-query-executions`.

AWS CLI

Generación de una lista de ID de consulta de las consultas de un grupo de trabajo especificado

En el siguiente ejemplo de `list-query-executions`, se genera una lista de un máximo de diez ID de consulta en el grupo de trabajo `AthenaAdmin`.

```
aws athena list-query-executions \
    --work-group AthenaAdmin \
    --max-items 10
```

Salida:

```
{
    "QueryExecutionIds": [
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE11110",
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE11114",
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE11115",
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE11116",
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE11117",
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE11118",
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE11119"
    ],
    "NextToken": "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxMH0="
}
```

Para obtener más información, consulte Trabajo con resultados de la consulta y consultas recientes en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte ListQueryExecutions en la Referencia de comandos de la AWS CLI.

`list-table-metadata`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-table-metadata`.

AWS CLI

Generación de una lista de los metadatos de las tablas de la base de datos especificada de un catálogo de datos

En el siguiente ejemplo de `list-table-metadata`; se obtiene información de metadatos de un máximo de dos tablas en la base de datos `geography` del catálogo de datos `AwsDataCatalog`.

```
aws athena list-table-metadata \
    --catalog-name AwsDataCatalog \
    --database-name geography \
    --max-items 2
```

Salida:

```
{
```

```
    "TableMetadataList": [
        {
            "Name": "country_codes",
            "CreateTime": 1586553454.0,
            "TableType": "EXTERNAL_TABLE",
            "Columns": [
                {
                    "Name": "country",
                    "Type": "string",
                    "Comment": "geo id"
                },
                {
                    "Name": "alpha-2 code",
                    "Type": "string",
                    "Comment": "geo id2"
                },
                {
                    "Name": "alpha-3 code",
                    "Type": "string",
                    "Comment": "state name"
                },
                {
                    "Name": "numeric code",
                    "Type": "bigint",
                    "Comment": ""
                },
                {
                    "Name": "latitude",
                    "Type": "bigint",
                    "Comment": "location (latitude)"
                },
                {
                    "Name": "longitude",
                    "Type": "bigint",
                    "Comment": "location (longitude)"
                }
            ],
            "Parameters": {
                "areColumnsQuoted": "false",
                "classification": "csv",
                "columnsOrdered": "true",
                "delimiter": ",",
                "has_encrypted_data": "false",
                "inputformat": "org.apache.hadoop.mapred.TextInputFormat",
```

```
                "location": "s3://amzn-s3-demo-bucket/csv/countrycode",
                "outputformat":
"org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat",
                "serde.param.field.delim": ",",
                "serde.serialization.lib":
"org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe",
                "skip.header.line.count": "1",
                "typeOfData": "file"
            }
        },
        {
            "Name": "county_populations",
            "CreateTime": 1586553446.0,
            "TableType": "EXTERNAL_TABLE",
            "Columns": [
                {
                    "Name": "id",
                    "Type": "string",
                    "Comment": "geo id"
                },
                {
                    "Name": "country",

                    "Name": "id2",
                    "Type": "string",
                    "Comment": "geo id2"
                },
                {
                    "Name": "county",
                    "Type": "string",
                    "Comment": "county name"
                },
                {
                    "Name": "state",
                    "Type": "string",
                    "Comment": "state name"
                },
                {
                    "Name": "population estimate 2018",
                    "Type": "string",
                    "Comment": ""
                }
            ],
            "Parameters": {
```

```
                "areColumnsQuoted": "false",
                "classification": "csv",
                "columnsOrdered": "true",
                "delimiter": ",",
                "has_encrypted_data": "false",
                "inputformat": "org.apache.hadoop.mapred.TextInputFormat",
                "location": "s3://amzn-s3-demo-bucket/csv/CountyPopulation",
                "outputformat":
 "org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat",
                "serde.param.field.delim": ",",
                "serde.serialization.lib":
 "org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe",
                "skip.header.line.count": "1",
                "typeOfData": "file"
            }
        }
    ],
    "NextToken": "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAyfQ=="
}
```

Para obtener más información, consulte Visualización de los metadatos de todas las tablas de una base de datos: list-table-metadata en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte ListTableMetadata en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Ejemplo 1: cómo generar una lista de las etiquetas de un grupo de trabajo

En el siguiente ejemplo de `list-tags-for-resource`, se genera una lista de las etiquetas del grupo de trabajo `Data_Analyst_Group`.

```
aws athena list-tags-for-resource \
    --resource-arn arn:aws:athena:us-west-2:111122223333:workgroup/
Data_Analyst_Group
```

Salida:

```
{
    "Tags": [
        {
            "Key": "Division",
            "Value": "West"
        },
        {
            "Key": "Team",
            "Value": "Big Data"
        },
        {
            "Key": "Location",
            "Value": "Seattle"
        }
    ]
}
```

Ejemplo 2: cómo generar una lista de las etiquetas de un catálogo de datos

En el ejemplo siguiente de `list-tags-for-resource`, se genera una lista de las etiquetas del catálogo de datos `dynamo_db_catalog`.

```
aws athena list-tags-for-resource \
    --resource-arn arn:aws:athena:us-west-2:111122223333:datacatalog/
dynamo_db_catalog
```

Salida:

```
{
    "Tags": [
        {
            "Key": "Division",
            "Value": "Mountain"
        },
        {
            "Key": "Organization",
            "Value": "Retail"
        },
        {
            "Key": "Product_Line",
            "Value": "Shoes"
        },
```

```
        {
            "Key": "Location",
            "Value": "Denver"
        }
    ]
}
```

Para obtener más información, consulte Descripción de las etiquetas de un recurso: list-tags-for-resource en la Guía del usuario de Amazon Athena.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-work-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-work-groups`.

AWS CLI

Generación de lista de grupos de trabajo

En el siguiente ejemplo de `list-work-groups`, se genera una lista de los grupos de trabajo en la cuenta actual.

```
aws athena list-work-groups
```

Salida:

```
{
    "WorkGroups": [
        {
            "Name": "Data_Analyst_Group",
            "State": "ENABLED",
            "Description": "",
            "CreationTime": 1578006683.016
        },
        {
            "Name": "AthenaAdmin",
            "State": "ENABLED",
            "Description": "",
            "CreationTime": 1573677174.105
```

```
        },
        {
            "Name": "primary",
            "State": "ENABLED",
            "Description": "",
            "CreationTime": 1567465222.723
        }
    ]
}
```

Para obtener más información, consulte Administración de los grupos de trabajo en la Guía del usuario de Amazon Athena.

- Para obtener detalles de la API, consulte ListWorkGroups en la Referencia de comandos de la AWS CLI.

`start-query-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-query-execution`.

AWS CLI

Ejemplo 1: cómo ejecutar una consulta en un grupo de trabajo en la tabla especificada de la base de datos y el catálogo de datos especificados

En el siguiente ejemplo de `start-query-execution`, se utiliza el grupo de trabajo `AthenaAdmin` para ejecutar una consulta en la tabla `cloudfront_logs` de la `cflogsdatabase` del catálogo de datos `AwsDataCatalog`.

```
aws athena start-query-execution \
    --query-string "select date, location, browser, uri, status from cloudfront_logs
 where method = 'GET' and status = 200 and location like 'SFO%' limit 10" \
    --work-group "AthenaAdmin" \
    --query-execution-context Database=cflogsdatabase,Catalog=AwsDataCatalog
```

Salida:

```
{
"QueryExecutionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Si desea obtener más información, consulte Ejecución de consultas SQL mediante Amazon Athena en la Guía del usuario de Amazon Athena.

Ejemplo 2: cómo ejecutar una consulta que utilice el grupo de trabajo especificado para crear una base de datos en el catálogo de datos especificado

En el siguiente ejemplo de `start-query-execution`, se utiliza el grupo de trabajo `AthenaAdmin` para crear la base de datos `newdb` en el catálogo de datos predeterminado `AwsDataCatalog`.

```
aws athena start-query-execution \
    --query-string "create database if not exists newdb" \
    --work-group "AthenaAdmin"
```

Salida:

```
{
"QueryExecutionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11112"
}
```

Si desea obtener más información, consulte Ejecución de consultas SQL mediante Amazon Athena en la Guía del usuario de Amazon Athena.

Ejemplo 3: cómo ejecutar una consulta que cree una vista en una tabla de la base de datos y el catálogo de datos especificados

En el siguiente ejemplo de `start-query-execution`, se utiliza una instrucción `SELECT` en la tabla `cloudfront_logs` de la `cflogsdatabase` para crear la vista `cf10`.

```
aws athena start-query-execution \
    --query-string  "CREATE OR REPLACE VIEW cf10 AS SELECT * FROM cloudfront_logs
 limit 10" \
    --query-execution-context Database=cflogsdatabase
```

Salida:

```
{
"QueryExecutionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11113"
}
```

Si desea obtener más información, consulte Ejecución de consultas SQL mediante Amazon Athena en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte StartQueryExecution en la Referencia de comandos de la AWS CLI.

`stop-query-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-query-execution`.

AWS CLI

Detención de una consulta en curso

En el siguiente ejemplo de `stop-query-execution`, se detiene la consulta con el ID de consulta especificado.

```
aws athena stop-query-execution \
    --query-execution-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Este comando no genera ninguna salida.

Si desea obtener más información, consulte Ejecución de consultas SQL mediante Amazon Athena en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte StopQueryExecution en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Cómo añadir una etiqueta a un recurso

En el siguiente ejemplo de `tag-resource`, se agregan tres etiquetas al catálogo de datos `dynamo_db_catalog`.

```
aws athena tag-resource \
    --resource-arn arn:aws:athena:us-west-2:111122223333:datacatalog/
dynamo_db_catalog \
```

```
    --
tags Key=Organization,Value=Retail Key=Division,Value=Mountain Key=Product_Line,Value=Shoes
```

Este comando no genera ninguna salida. Para ver el resultado, utilice `aws athena list-tags-for-resource --resource-arn arn:aws:athena:us-west-2:111122223333:datacatalog/dynamo_db_catalog`.

Para obtener más información, consulte Añadir etiquetas a un recurso: tag-resource en la Guía del usuario de Amazon Athena.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar una etiqueta de un recurso

En el ejemplo siguiente de `untag-resource`, se eliminan las claves `Specialization` y `Focus` y sus valores asociados del recurso de catálogo de datos `dynamo_db_catalog`.

```
aws athena untag-resource \
    --resource-arn arn:aws:athena:us-west-2:111122223333:datacatalog/
dynamo_db_catalog \
    --tag-keys Specialization Focus
```

Este comando no genera ninguna salida. Para ver los resultados, use el comando `list-tags-for-resource`.

Para obtener más información, consulte Eliminación de las etiquetas de un recurso: untag-resource: untag-resource en la Guía del usuario de Amazon Athena.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-data-catalog`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-data-catalog`.

AWS CLI

Actualización de un catálogo de datos

En el siguiente ejemplo de `update-data-catalog`, se actualiza la función de Lambda y la descripción del catálogo de datos `cw_logs_catalog`.

```
aws athena update-data-catalog \
    --name cw_logs_catalog \
    --type LAMBDA \
    --description "New CloudWatch Logs Catalog" \
    --function=arn:aws:lambda:us-west-2:111122223333:function:new_cw_logs_lambda
```

Este comando no genera ninguna salida. Para ver el resultado, utilice `aws athena get-data-catalog --name cw_logs_catalog`.

Para obtener más información, consulte Actualización de un catálogo: update-data-catalog en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte UpdateDataCatalog en la Referencia de comandos de la AWS CLI.

`update-work-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-work-group`.

AWS CLI

Actualización de un grupo de trabajo

En el siguiente ejemplo de `update-work-group`, se actualiza el grupo de trabajo `Data_Analyst_Group`. Los usuarios no pueden ejecutar ni crear consultas en el grupo de trabajo deshabilitado, pero sí pueden ver las métricas, los controles de los límites de uso de datos, la configuración del grupo de trabajo, el historial de consultas y las consultas guardadas.

```
aws athena update-work-group \
    --work-group Data_Analyst_Group \
    --state DISABLED
```

Este comando no genera ninguna salida. Para comprobar el cambio de estado, utilice `aws athena get-work-group --work-group Data_Analyst_Group` y compruebe la propiedad `State` en la salida.

Para obtener más información, consulte Administración de los grupos de trabajo en la Guía del usuario de Amazon Athena.

- Para obtener información sobre la API, consulte UpdateWorkGroup en la Referencia de comandos de la AWS CLI.

Ejemplos de escalado automático que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Auto Scaling.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`attach-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-instances`.

AWS CLI

Asociación de una instancia a un grupo de escalado automático

En este ejemplo, se asocia la instancia especificada al grupo de escalado automático especificado.

```
aws autoscaling attach-instances \
    --instance-ids i-061c63c5eb45f0416 \
    --auto-scaling-group-name my-asg
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte AttachInstances en la Referencia de comandos de la AWS CLI.

`attach-load-balancer-target-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-load-balancer-target-groups`.

AWS CLI

Asociación de un grupo de destino a un grupo de escalado automático

En este ejemplo, se asocia el grupo de destino especificado al grupo de escalado automático especificado.

```
aws autoscaling attach-load-balancer-target-groups \
    --auto-scaling-group-name my-asg \
    --target-group-arns arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Elastic Load Balancing y Amazon EC2 Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte AttachLoadBalancerTargetGroups en la Referencia de comandos de la AWS CLI.

`attach-load-balancers`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-load-balancers`.

AWS CLI

Asociación de un equilibrador de carga clásico al grupo de escalado automático

En este ejemplo, se asocia el equilibrador de carga clásico especificado al grupo de escalado automático especificado.

```
aws autoscaling attach-load-balancers \
```

```
    --load-balancer-names my-load-balancer \
    --auto-scaling-group-name my-asg
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Elastic Load Balancing y Amazon EC2 Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte AttachLoadBalancers en la Referencia de comandos de la AWS CLI.

`cancel-instance-refresh`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-instance-refresh`.

AWS CLI

Cómo cancelar una actualización de instancias

En el siguiente ejemplo de `cancel-instance-refresh`, se cancela una actualización de instancias en curso del grupo de escalado automático especificado.

```
aws autoscaling cancel-instance-refresh \
    --auto-scaling-group-name my-asg
```

Salida:

```
{
    "InstanceRefreshId": "08b91cf7-8fa6-48af-b6a6-d227f40f1b9b"
}
```

Para obtener más información, consulte Cancel an instance refresh en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte CancelInstanceRefresh en la Referencia de comandos de la AWS CLI.

`complete-lifecycle-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `complete-lifecycle-action`.

AWS CLI

Realización de una acción del ciclo de vida

En este ejemplo, se notifica a Amazon EC2 Auto Scaling que la acción del ciclo de vida especificada se ha completado para que pueda finalizar la inicialización o la finalización de la instancia.

```
aws autoscaling complete-lifecycle-action \
    --lifecycle-hook-name my-launch-hook \
    --auto-scaling-group-name my-asg \
    --lifecycle-action-result CONTINUE \
    --lifecycle-action-token bcd2f1b8-9a78-44d3-8a7a-4dd07d7cf635
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Enlaces de ciclo de vida de Amazon EC2 Auto Scaling en la guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte CompleteLifecycleAction en la Referencia de comandos de la AWS CLI.

`create-auto-scaling-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-auto-scaling-group`.

AWS CLI

Ejemplo 1: crear un grupo de escalado automático

En el siguiente ejemplo `create-auto-scaling-group` se crea un grupo de escalado automático en subredes de varias zonas de disponibilidad dentro de una región. Las instancias se lanzan con la versión predeterminada de la plantilla de lanzamiento especificada. Tenga en cuenta que se utilizan valores predeterminados para la mayoría de las demás configuraciones, como las políticas de terminación y la configuración de las comprobaciones de estado.

```
aws autoscaling create-auto-scaling-group \
    --auto-scaling-group-name my-asg \
    --launch-template LaunchTemplateId=lt-1234567890abcde12 \
    --min-size 1 \
    --max-size 5 \
```

```
    --vpc-zone-identifier "subnet-5ea0c127,subnet-6194ea3b,subnet-c934b782"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Grupos de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 2: asociar un equilibrador de carga de aplicación, un equilibrador de carga de red o un equilibrador de carga de puerta de enlace

En este ejemplo, se especifica el ARN de un grupo de destino para un equilibrador de carga que admite el tráfico esperado. El tipo de comprobación de estado especifica ELB para que, cuando Elastic Load Balancing informa de una instancia como en mal estado, el grupo de escalado automático reemplaza la instancia. El comando también define un período de gracia de 600 segundos para la comprobación de estado. El período de gracia ayuda a evitar la finalización prematura de las instancias recién lanzadas.

```
aws autoscaling create-auto-scaling-group \
    --auto-scaling-group-name my-asg \
    --launch-template LaunchTemplateId=lt-1234567890abcde12 \
    --target-group-arns arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/943f017f100becff \
    --health-check-type ELB \
    --health-check-grace-period 600 \
    --min-size 1 \
    --max-size 5 \
    --vpc-zone-identifier "subnet-5ea0c127,subnet-6194ea3b,subnet-c934b782"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Elastic Load Balancing y Amazon EC2 Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 3: especificación de un grupo con ubicación y utilizar la versión más reciente de la plantilla de lanzamiento

En este ejemplo, se lanzan instancias a un grupo con ubicación en una única zona de disponibilidad. Esto puede resultar útil para grupos de baja latencia con cargas de trabajo de HPC. En este ejemplo, también se especifican el tamaño mínimo, el tamaño máximo y la capacidad deseada del grupo.

```
aws autoscaling create-auto-scaling-group \
    --auto-scaling-group-name my-asg \
    --launch-template LaunchTemplateId=lt-1234567890abcde12,Version='$Latest' \
    --min-size 1 \
    --max-size 5 \
    --desired-capacity 3 \
    --placement-group my-placement-group \
    --vpc-zone-identifier "subnet-6194ea3b"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Grupos de ubicación en la Guía del usuario de Amazon EC2 para instancias Linux.

Ejemplo 4: especificación de un grupo de escalado automático de una sola instancia y utilizar una versión específica de la plantilla de lanzamiento

En este ejemplo, se crea un grupo de escalado automático con una capacidad mínima y máxima establecida en 1 para garantizar que se ejecute una instancia. El comando también especifica la v1 de una plantilla de lanzamiento en la que se especifica el ID de un ENI existente. Cuando utilice una plantilla de lanzamiento que especifique un ENI existente para eth0, debe especificar una zona de disponibilidad para el grupo de escalado automático que coincida con la interfaz de red, sin especificar también un ID de subred en la solicitud.

```
aws autoscaling create-auto-scaling-group \
    --auto-scaling-group-name my-asg-single-instance \
    --launch-template LaunchTemplateName=my-template-for-auto-scaling,Version='1' \
    --min-size 1 \
    --max-size 1 \
    --availability-zones us-west-2a
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Grupos de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 5: especificación de una política de terminación diferente

En este ejemplo, se crea un grupo de escalado automático mediante una configuración de lanzamiento y se establece la política de terminación para terminar primero las instancias más

antiguas. El comando también aplica una etiqueta al grupo y a sus instancias, con una clave de `Role` y un valor de `WebServer`.

```
aws autoscaling create-auto-scaling-group \
    --auto-scaling-group-name my-asg \
    --launch-configuration-name my-lc \
    --min-size 1 \
    --max-size 5 \
    --termination-policies "OldestInstance" \
    --tags "ResourceId=my-asg,ResourceType=auto-scaling-
group,Key=Role,Value=WebServer,PropagateAtLaunch=true" \
    --vpc-zone-identifier "subnet-5ea0c127,subnet-6194ea3b,subnet-c934b782"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Utilización de políticas de terminación de Amazon EC2 Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 6: especificación de un enlace de ciclo de vida de lanzamiento

En este ejemplo, se crea un grupo de escalado automático con un enlace de ciclo de vida que admite una acción personalizada cuando se lanza una instancia.

```
aws autoscaling create-auto-scaling-group \
    --cli-input-json file://~/config.json
```

Contenido del archivo `config.json`:

```
{
    "AutoScalingGroupName": "my-asg",
    "LaunchTemplate": {
        "LaunchTemplateId": "lt-1234567890abcde12"
    },
    "LifecycleHookSpecificationList": [{
        "LifecycleHookName": "my-launch-hook",
        "LifecycleTransition": "autoscaling:EC2_INSTANCE_LAUNCHING",
        "NotificationTargetARN": "arn:aws:sqs:us-west-2:123456789012:my-sqs-queue",
        "RoleARN": "arn:aws:iam::123456789012:role/my-notification-role",
        "NotificationMetadata": "SQS message metadata",
        "HeartbeatTimeout": 4800,
        "DefaultResult": "ABANDON"
```

```
    }],
    "MinSize": 1,
    "MaxSize": 5,
    "VPCZoneIdentifier": "subnet-5ea0c127,subnet-6194ea3b,subnet-c934b782",
    "Tags": [{
        "ResourceType": "auto-scaling-group",
        "ResourceId": "my-asg",
        "PropagateAtLaunch": true,
        "Value": "test",
        "Key": "environment"
    }]
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Enlaces de ciclo de vida de Amazon EC2 Auto Scaling en la guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 7: especificación de un enlace de ciclo de vida de terminación

En este ejemplo, se crea un grupo de escalado automático con un enlace de ciclo de vida que admite una acción personalizada en la terminación de una instancia.

```
aws autoscaling create-auto-scaling-group \
    --cli-input-json file://~/config.json
```

Contenido de `config.json`:

```
{
    "AutoScalingGroupName": "my-asg",
    "LaunchTemplate": {
        "LaunchTemplateId": "lt-1234567890abcde12"
    },
    "LifecycleHookSpecificationList": [{
        "LifecycleHookName": "my-termination-hook",
        "LifecycleTransition": "autoscaling:EC2_INSTANCE_TERMINATING",
        "HeartbeatTimeout": 120,
        "DefaultResult": "CONTINUE"
    }],
    "MinSize": 1,
    "MaxSize": 5,
    "TargetGroupARNs": [
```

```
        "arn:aws:elasticloadbalancing:us-west-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067"
    ],
    "VPCZoneIdentifier": "subnet-5ea0c127,subnet-6194ea3b,subnet-c934b782"
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Enlaces de ciclo de vida de Amazon EC2 Auto Scaling en la guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 8: especificación de una política de terminación personalizada

En este ejemplo, se crea un grupo de escalado automático que especifica una política de terminación de funciones de Lambda personalizada que indica a Amazon EC2 Auto Scaling qué instancias son seguras de terminar al escalarlas horizontalmente.

```
aws autoscaling create-auto-scaling-group \
    --auto-scaling-group-name my-asg-single-instance \
    --launch-template LaunchTemplateName=my-template-for-auto-scaling \
    --min-size 1 \
    --max-size 5 \
    --termination-policies "arn:aws:lambda:us-
west-2:123456789012:function:HelloFunction:prod" \
    --vpc-zone-identifier "subnet-5ea0c127,subnet-6194ea3b,subnet-c934b782"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación de una política de terminación personalizada con Lambda en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte CreateAutoScalingGroup en la Referencia de comandos de la AWS CLI.

`create-launch-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-launch-configuration`.

AWS CLI

Ejemplo 1: crear una configuración de inicialización

En este ejemplo, se crea una configuración de inicialización sencilla.

```
aws autoscaling create-launch-configuration \
    --launch-configuration-name my-lc \
    --image-id ami-04d5cc9b88example \
    --instance-type m5.large
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Crear una configuración de lanzamiento en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 2: crear una configuración de inicialización con un grupo de seguridad, un par de claves y un script de arranque

En este ejemplo, se crea una configuración de inicialización con un grupo de seguridad, un par de claves y un script de arranque incluidos en los datos del usuario.

```
aws autoscaling create-launch-configuration \
    --launch-configuration-name my-lc \
    --image-id ami-04d5cc9b88example \
    --instance-type m5.large \
    --security-groups sg-eb2af88example \
    --key-name my-key-pair \
    --user-data file://myuserdata.txt
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Crear una configuración de lanzamiento en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 3: crear una configuración de inicialización con un rol de IAM

En este ejemplo, se crea una configuración de inicialización con el nombre del perfil de instancia de un rol de IAM.

```
aws autoscaling create-launch-configuration \
    --launch-configuration-name my-lc \
    --image-id ami-04d5cc9b88example \
    --instance-type m5.large \
```

```
    --iam-instance-profile my-autoscaling-role
```

Este comando no genera ninguna salida.

Para obtener más información, consulte el tema Rol de IAM para las aplicaciones que se ejecutan en instancias Amazon EC2 en la guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 4: cómo habilitar la configuración de inicialización con la supervisión detallada habilitada

En este ejemplo, se crea una configuración de inicialización con la supervisión detallada de EC2 habilitada, que envía las métricas de EC2 a CloudWatch en períodos de 1 minuto.

```
aws autoscaling create-launch-configuration \
    --launch-configuration-name my-lc \
    --image-id ami-04d5cc9b88example \
    --instance-type m5.large \
    --instance-monitoring Enabled=true
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración del monitoreo para instancias de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 5: cómo crear una configuración de inicialización que inicialice instancias de spot

En este ejemplo, se crea una configuración de inicialización que utiliza instancias de spot como única opción de compra.

```
aws autoscaling create-launch-configuration \
    --launch-configuration-name my-lc \
    --image-id ami-04d5cc9b88example \
    --instance-type m5.large \
    --spot-price "0.50"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Solicitud de instancias de spot en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 6: cómo crear una configuración de inicialización con una instancia de EC2

En este ejemplo, se crea una configuración de inicialización basada en los atributos de una instancia existente. Anula la tenencia de la ubicación y si se establece una dirección IP pública al incluir las opciones `--placement-tenancy` y`--no-associate-public-ip-address`.

```
aws autoscaling create-launch-configuration \
    --launch-configuration-name my-lc-from-instance \
    --instance-id i-0123a456700123456 \
    --instance-type m5.large \
    --no-associate-public-ip-address \
    --placement-tenancy dedicated
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Crear una configuración de lanzamiento con una instancia EC2 en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 7: cómo crear una configuración de inicialización con una asignación de dispositivos de bloques para un volumen de Amazon EBS

En este ejemplo, se crea una configuración de inicialización con una asignación de dispositivos de bloques para un volumen gp3 de Amazon EBS con el nombre del dispositivo `/dev/sdh` y un tamaño de volumen de 20.

```
aws autoscaling create-launch-configuration \
    --launch-configuration-name my-lc \
    --image-id ami-04d5cc9b88example \
    --instance-type m5.large \
    --block-device-mappings '[{"DeviceName":"/dev/sdh","Ebs":
{"VolumeSize":20,"VolumeType":"gp3"}}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte EBS en la Referencia de la API de Amazon EC2 Auto Scaling.

Para obtener más información acerca de la sintaxis para aplicar comillas a los valores de parámetros con formato JSON, consulte Entrecomillado de cadenas en AWS CLI en la Guía del usuario de la interfaz de la línea de comandos de AWS.

Ejemplo 8: cómo crear una configuración de inicialización con una asignación de dispositivos de bloques para un volumen de almacén de instancias

En este ejemplo, se crea una configuración de inicialización con `ephemeral1` como un volumen de almacén de instancias con el nombre de dispositivo `/dev/sdc`.

```
aws autoscaling create-launch-configuration \
    --launch-configuration-name my-lc \
    --image-id ami-04d5cc9b88example \
    --instance-type m5.large \
    --block-device-mappings '[{"DeviceName":"/dev/sdc","VirtualName":"ephemeral1"}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte BlockDeviceMapping en la Referencia de la API de Amazon EC2 Auto Scaling.

Para obtener más información acerca de la sintaxis para aplicar comillas a los valores de parámetros con formato JSON, consulte Entrecomillado de cadenas en AWS CLI en la Guía del usuario de la interfaz de la línea de comandos de AWS.

Ejemplo 9: cómo crear una configuración de inicialización y suprimir un dispositivo de bloques se conecte en el momento de la inicialización

En este ejemplo, se crea una configuración de inicialización que suprime un dispositivo de bloques especificado por la asignación de dispositivos de bloques de la AMI (por ejemplo,`/dev/sdf`).

```
aws autoscaling create-launch-configuration \
    --launch-configuration-name my-lc \
    --image-id ami-04d5cc9b88example \
    --instance-type m5.large \
    --block-device-mappings '[{"DeviceName":"/dev/sdf","NoDevice":""}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte BlockDeviceMapping en la Referencia de la API de Amazon EC2 Auto Scaling.

Para obtener más información acerca de la sintaxis para aplicar comillas a los valores de parámetros con formato JSON, consulte Entrecomillado de cadenas en AWS CLI en la Guía del usuario de la interfaz de la línea de comandos de AWS.

- Para obtener información sobre la API, consulte CreateLaunchConfiguration en la Referencia de comandos de la AWS CLI.

`create-or-update-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-or-update-tags`.

AWS CLI

Creación o modificación de etiquetas en un grupo de escalado automático

En este ejemplo, se agregan dos etiquetas al grupo de escalado automático especificado.

```
aws autoscaling create-or-update-tags \
    --tags ResourceId=my-asg,ResourceType=auto-scaling-
group,Key=Role,Value=WebServer,PropagateAtLaunch=true ResourceId=my-
asg,ResourceType=auto-scaling-group,Key=Dept,Value=Research,PropagateAtLaunch=true
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de grupos e instancias de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte CreateOrUpdateTags en la Referencia de comandos de la AWS CLI.

`delete-auto-scaling-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-auto-scaling-group`.

AWS CLI

Ejemplo 1: eliminar el grupo de escalado automático especificado

En este ejemplo, se elimina el grupo de escalado automático especificado.

```
aws autoscaling delete-auto-scaling-group \
    --auto-scaling-group-name my-asg
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de la infraestructura de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 2: para forzar la eliminación del grupo de escalado automático especificado

Para eliminar el grupo de escalado automático sin esperar a que las instancias del grupo terminen, utilice la opción `--force-delete`.

```
aws autoscaling delete-auto-scaling-group \
    --auto-scaling-group-name my-asg \
    --force-delete
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de la infraestructura de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DeleteAutoScalingGroup en la Referencia de comandos de la AWS CLI.

`delete-launch-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-launch-configuration`.

AWS CLI

Eliminación de una configuración de inicialización

En este ejemplo se elimina la configuración de inicialización especificada.

```
aws autoscaling delete-launch-configuration \
    --launch-configuration-name my-launch-config
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de la infraestructura de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DeleteLaunchConfiguration en la Referencia de comandos de la AWS CLI.

`delete-lifecycle-hook`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-lifecycle-hook`.

AWS CLI

Eliminación de un enlace de ciclo de vida

En este ejemplo se elimina el enlace de ciclo de vida especificado.

```
aws autoscaling delete-lifecycle-hook \
    --lifecycle-hook-name my-lifecycle-hook \
    --auto-scaling-group-name my-asg
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteLifecycleHook en la Referencia de comandos de la AWS CLI.

`delete-notification-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-notification-configuration`.

AWS CLI

Eliminación de una notificación de escalado automático

En este ejemplo, se elimina la notificación especificada del grupo de escalado automático especificado.

```
aws autoscaling delete-notification-configuration \
    --auto-scaling-group-name my-asg \
    --topic-arn arn:aws:sns:us-west-2:123456789012:my-sns-topic
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Delete the notification configuration en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DeleteNotificationConfiguration en la Referencia de comandos de la AWS CLI.

`delete-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-policy`.

AWS CLI

Eliminación de una política de escalado

En este ejemplo, se elimina el grupo de escalado automático especificado.

```
aws autoscaling delete-policy \
    --auto-scaling-group-name my-asg \
    --policy-name alb1000-target-tracking-scaling-policy
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeletePolicy en la Referencia de comandos de la AWS CLI.

`delete-scheduled-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-scheduled-action`.

AWS CLI

Creación de una acción programada para un grupo de escalado automático

En este ejemplo, se elimina la acción programada especificada del grupo de escalado automático especificado.

```
aws autoscaling delete-scheduled-action \
    --auto-scaling-group-name my-asg \
    --scheduled-action-name my-scheduled-action
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteScheduledAction en la Referencia de comandos de la AWS CLI.

`delete-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-tags`.

AWS CLI

Eliminación de una etiqueta de un grupo de escalado automático

En este ejemplo, se elimina la etiqueta especificada del grupo de escalado automático especificado.

```
aws autoscaling delete-tags \
    --tags ResourceId=my-asg,ResourceType=auto-scaling-group,Key=Dept,Value=Research
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de grupos e instancias de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DeleteTags en la Referencia de comandos de la AWS CLI.

`delete-warm-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-warm-pool`.

AWS CLI

Ejemplo 1: cómo eliminar un grupo de calentamiento

En el ejemplo siguiente, se elimina un grupo de calentamiento de un grupo de escalado automático.

```
aws autoscaling delete-warm-pool \
    --auto-scaling-group-name my-asg
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Grupos de calentamiento para Amazon EC2 Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 2: cómo forzar la eliminación de un grupo de calentamiento

Para eliminar el grupo de calentamiento sin esperar a que las instancias terminen, utilice la opción `--force-delete`.

```
aws autoscaling delete-warm-pool \
    --auto-scaling-group-name my-asg \
```

```
    --force-delete
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Grupos de calentamiento para Amazon EC2 Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DeleteWarmPool en la Referencia de comandos de la AWS CLI.

`describe-account-limits`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-account-limits`.

AWS CLI

Descripción de los límites de cuenta de Amazon EC2 Auto Scaling

En este ejemplo, se describen los límites de Amazon EC2 Auto Scaling para su cuenta de AWS.

```
aws autoscaling describe-account-limits
```

Salida:

```
{
    "NumberOfLaunchConfigurations": 5,
    "MaxNumberOfLaunchConfigurations": 100,
    "NumberOfAutoScalingGroups": 3,
    "MaxNumberOfAutoScalingGroups": 20
}
```

Para obtener más información, consulte Amazon EC2 Auto Scaling service quotas en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DescribeAccountLimits en la Referencia de comandos de la AWS CLI.

`describe-adjustment-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-adjustment-types`.

AWS CLI

Descripción de los tipos de ajuste de escalado disponibles

En este ejemplo se describen los tipos de ajuste disponibles.

```
aws autoscaling describe-adjustment-types
```

Salida:

```
{
    "AdjustmentTypes": [
        {
            "AdjustmentType": "ChangeInCapacity"
        },
        {
            "AdjustmentType": "ExactCapacity"
        },
        {
            "AdjustmentType": "PercentChangeInCapacity"
        }
    ]
}
```

Para obtener más información, consulte la sección sobre tipos de ajustes de de escalado en la guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DescribeAdjustmentTypes en la Referencia de comandos de la AWS CLI.

`describe-auto-scaling-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-auto-scaling-groups`.

AWS CLI

Ejemplo 1: Descripción del grupo de escalado automático especificado

En este ejemplo, se describe el grupo de escalado automático especificado.

```
aws autoscaling describe-auto-scaling-groups \
    --auto-scaling-group-names my-asg
```

Salida:

```
{
    "AutoScalingGroups": [
        {
            "AutoScalingGroupName": "my-asg",
            "AutoScalingGroupARN": "arn:aws:autoscaling:us-
west-2:123456789012:autoScalingGroup:930d940e-891e-4781-
a11a-7b0acd480f03:autoScalingGroupName/my-asg",
            "LaunchTemplate": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1",
                "LaunchTemplateId": "lt-1234567890abcde12"
            },
            "MinSize": 0,
            "MaxSize": 1,
            "DesiredCapacity": 1,
            "DefaultCooldown": 300,
            "AvailabilityZones": [
                "us-west-2a",
                "us-west-2b",
                "us-west-2c"
            ],
            "LoadBalancerNames": [],
            "TargetGroupARNs": [],
            "HealthCheckType": "EC2",
            "HealthCheckGracePeriod": 0,
            "Instances": [
                {
                    "InstanceId": "i-06905f55584de02da",
                    "InstanceType": "t2.micro",
                    "AvailabilityZone": "us-west-2a",
                    "HealthStatus": "Healthy",
                    "LifecycleState": "InService",
                    "ProtectedFromScaleIn": false,
                    "LaunchTemplate": {
                        "LaunchTemplateName": "my-launch-template",
                        "Version": "1",
                        "LaunchTemplateId": "lt-1234567890abcde12"
                    }
                }
            ],
            "CreatedTime": "2023-10-28T02:39:22.152Z",
            "SuspendedProcesses": [],
```

```
            "VPCZoneIdentifier": "subnet-5ea0c127,subnet-6194ea3b,subnet-c934b782",
            "EnabledMetrics": [],
            "Tags": [],
            "TerminationPolicies": [
                "Default"
            ],
            "NewInstancesProtectedFromScaleIn": false,
            "ServiceLinkedRoleARN":"arn",
            "TrafficSources": []
        }
    ]
}
```

Ejemplo 2: Descripción de los 100 primeros grupos de escalado automático especificados

En este ejemplo, se describen los grupos de escalado automático especificados. Le permite especificar hasta 100 nombres de grupos.

```
aws autoscaling describe-auto-scaling-groups \
    --max-items 100 \
    --auto-scaling-group-names "group1" "group2" "group3" "group4"
```

Consulte el ejemplo 1 para ver una salida de muestra.

Ejemplo 3: descripción de un grupo de escalado automático en la región especificada

En este ejemplo, se describen los grupos de escalado automático en la región especificada, hasta un máximo de 75 grupos.

```
aws autoscaling describe-auto-scaling-groups \
    --max-items 75 \
    --region us-east-1
```

Consulte el ejemplo 1 para ver una salida de muestra.

Ejemplo 4: descripción del número especificado de grupos de escalado automático

Para devolver un número específico de grupos de escalado automático, utilice la opción `--max-items`.

```
aws autoscaling describe-auto-scaling-groups \
    --max-items 1
```

Consulte el ejemplo 1 para ver una salida de muestra.

Si la salida incluye un campo `NextToken`, hay más grupos. Para obtener los grupos adicionales, utilice el valor de este campo con la opción `--starting-token` en una llamada posterior de la siguiente manera.

```
aws autoscaling describe-auto-scaling-groups \
    --starting-token Z3M3LMPEXAMPLE
```

Consulte el ejemplo 1 para ver una salida de muestra.

Ejemplo 5: cómo describir grupos de escalado automático que utilizan configuraciones de inicialización

En este ejemplo, se utiliza la opción `--query` para describir los grupos de escalado automático que utilizan configuraciones de inicialización.

```
aws autoscaling describe-auto-scaling-groups \
    --query 'AutoScalingGroups[?LaunchConfigurationName!=`null`]'
```

Salida:

```
[
    {
        "AutoScalingGroupName": "my-asg",
        "AutoScalingGroupARN": "arn:aws:autoscaling:us-
west-2:123456789012:autoScalingGroup:930d940e-891e-4781-
a11a-7b0acd480f03:autoScalingGroupName/my-asg",
        "LaunchConfigurationName": "my-lc",
        "MinSize": 0,
        "MaxSize": 1,
        "DesiredCapacity": 1,
        "DefaultCooldown": 300,
        "AvailabilityZones": [
            "us-west-2a",
            "us-west-2b",
            "us-west-2c"
        ],
        "LoadBalancerNames": [],
        "TargetGroupARNs": [],
        "HealthCheckType": "EC2",
        "HealthCheckGracePeriod": 0,
```

```
        "Instances": [
            {
                "InstanceId": "i-088c57934a6449037",
                "InstanceType": "t2.micro",
                "AvailabilityZone": "us-west-2c",
                "HealthStatus": "Healthy",
                "LifecycleState": "InService",
                "LaunchConfigurationName": "my-lc",
                "ProtectedFromScaleIn": false
            }
        ],
        "CreatedTime": "2023-10-28T02:39:22.152Z",
        "SuspendedProcesses": [],
        "VPCZoneIdentifier": "subnet-5ea0c127,subnet-6194ea3b,subnet-c934b782",
        "EnabledMetrics": [],
        "Tags": [],
        "TerminationPolicies": [
            "Default"
        ],
        "NewInstancesProtectedFromScaleIn": false,
        "ServiceLinkedRoleARN":"arn",
        "TrafficSources": []
    }
]
```

Para obtener más información, consulte Filtrar salida AWS CLI en la Guía del usuario de la interfaz de línea de comandos de AWS.

- Para obtener información sobre la API, consulte DescribeAutoScalingGroups en la Referencia de comandos de la AWS CLI.

`describe-auto-scaling-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-auto-scaling-instances`.

AWS CLI

Ejemplo 1: Descripción de una o varias instancias

En este ejemplo, se describe la instancia especificada.

```
aws autoscaling describe-auto-scaling-instances \
```

```
    --instance-ids i-06905f55584de02da
```

Salida:

```
{
    "AutoScalingInstances": [
        {
            "InstanceId": "i-06905f55584de02da",
            "InstanceType": "t2.micro",
            "AutoScalingGroupName": "my-asg",
            "AvailabilityZone": "us-west-2b",
            "LifecycleState": "InService",
            "HealthStatus": "HEALTHY",
            "ProtectedFromScaleIn": false,
            "LaunchTemplate": {
                "LaunchTemplateId": "lt-1234567890abcde12",
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            }
        }
    ]
}
```

Ejemplo 2: Descripción de una o varias instancias

En este ejemplo, se utiliza la opción `--max-items` para especificar cuántas instancias se devolverán con esta llamada.

```
aws autoscaling describe-auto-scaling-instances \
    --max-items 1
```

Si la salida incluye un campo `NextToken`, hay más instancias. Para obtener las instancias adicionales, utilice el valor de este campo con la opción `--starting-token` en una llamada posterior de la siguiente manera.

```
aws autoscaling describe-auto-scaling-instances \
    --starting-token Z3M3LMPEXAMPLE
```

Consulte el ejemplo 1 para ver una salida de muestra.

Ejemplo 3: cómo describir las instancias que utilizan configuraciones de inicialización

En este ejemplo, se usa la opción `--query` para describir las instancias que usan configuraciones de inicialización.

```
aws autoscaling describe-auto-scaling-instances \
    --query 'AutoScalingInstances[?LaunchConfigurationName!=`null`]'
```

Salida:

```
[
    {
        "InstanceId": "i-088c57934a6449037",
        "InstanceType": "t2.micro",
        "AutoScalingGroupName": "my-asg",
        "AvailabilityZone": "us-west-2c",
        "LifecycleState": "InService",
        "HealthStatus": "HEALTHY",
        "LaunchConfigurationName": "my-lc",
        "ProtectedFromScaleIn": false
    }
]
```

Para obtener más información, consulte Filter AWS CLI output en la Guía del usuario de la interfaz de línea de comandos de AWS.

- Para obtener información sobre la API, consulte DescribeAutoScalingInstances en la Referencia de comandos de la AWS CLI.

`describe-auto-scaling-notification-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-auto-scaling-notification-types`.

AWS CLI

Descripción de los tipos de notificaciones disponibles

En este ejemplo se describen los tipos de notificaciones disponibles.

```
aws autoscaling describe-auto-scaling-notification-types
```

Salida:

```
{
    "AutoScalingNotificationTypes": [
        "autoscaling:EC2_INSTANCE_LAUNCH",
        "autoscaling:EC2_INSTANCE_LAUNCH_ERROR",
        "autoscaling:EC2_INSTANCE_TERMINATE",
        "autoscaling:EC2_INSTANCE_TERMINATE_ERROR",
        "autoscaling:TEST_NOTIFICATION"
    ]
}
```

Para obtener más información, consulte Obtener notificaciones de Amazon SNS cuando su grupo de Auto Scaling escala en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DescribeAutoScalingNotificationTypes en la Referencia de comandos de la AWS CLI.

`describe-instance-refreshes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-refreshes`.

AWS CLI

Descripción de las actualizaciones de instancias

En el siguiente ejemplo de `describe-instance-refreshes`, se ofrece una descripción de todas las solicitudes de actualización de instancias del grupo de escalado automático especificado, incluido el mensaje de estado y (si está disponible) el motivo del estado.

```
aws autoscaling describe-instance-refreshes \
    --auto-scaling-group-name my-asg
```

Salida:

```
{
    "InstanceRefreshes": [
        {
            "InstanceRefreshId": "08b91cf7-8fa6-48af-b6a6-d227f40f1b9b",
            "AutoScalingGroupName": "my-asg",
            "Status": "InProgress",
            "StatusReason": "Waiting for instances to warm up before continuing. For
 example: 0e69cc3f05f825f4f is warming up.",
            "EndTime": "2023-03-23T16:42:55Z",
```

```
            "PercentageComplete": 0,
            "InstancesToUpdate": 0,
    "Preferences": {
                "MinHealthyPercentage": 100,
                "InstanceWarmup": 300,
                "CheckpointPercentages": [
                    50
                ],
                "CheckpointDelay": 3600,
                "SkipMatching": false,
                "AutoRollback": true,
                "ScaleInProtectedInstances": "Ignore",
                "StandbyInstances": "Ignore"
            }
        },
        {
            "InstanceRefreshId": "dd7728d0-5bc4-4575-96a3-1b2c52bf8bb1",
            "AutoScalingGroupName": "my-asg",
            "Status": "Successful",
            "EndTime": "2022-06-02T16:53:37Z",
            "PercentageComplete": 100,
            "InstancesToUpdate": 0,
    "Preferences": {
                "MinHealthyPercentage": 90,
                "InstanceWarmup": 300,
                "SkipMatching": true,
                "AutoRollback": true,
                "ScaleInProtectedInstances": "Ignore",
                "StandbyInstances": "Ignore"
            }
        }
    ]
}
```

Para obtener más información, consulte Check the status of an instance refresh en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DescribeInstanceRefreshes en la Referencia de comandos de la AWS CLI.

`describe-launch-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-launch-configurations`.

AWS CLI

Ejemplo 1: Cómo describir la configuración de inicialización especificada

En este ejemplo, se describe la configuración de inicialización especificada.

```
aws autoscaling describe-launch-configurations \
    --launch-configuration-names my-launch-config
```

Salida:

```
{
    "LaunchConfigurations": [
        {
            "LaunchConfigurationName": "my-launch-config",
            "LaunchConfigurationARN": "arn:aws:autoscaling:us-
west-2:123456789012:launchConfiguration:98d3b196-4cf9-4e88-8ca1-8547c24ced8b:launchConfigura
my-launch-config",
            "ImageId": "ami-0528a5175983e7f28",
            "KeyName": "my-key-pair-uswest2",
            "SecurityGroups": [
                "sg-05eaec502fcdadc2e"
            ],
            "ClassicLinkVPCSecurityGroups": [],
            "UserData": "",
            "InstanceType": "t2.micro",
            "KernelId": "",
            "RamdiskId": "",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/xvda",
                    "Ebs": {
                        "SnapshotId": "snap-06c1606ba5ca274b1",
                        "VolumeSize": 8,
                        "VolumeType": "gp2",
                        "DeleteOnTermination": true,
                        "Encrypted": false
                    }
                }
            ],
            "InstanceMonitoring": {
                "Enabled": true
            },
```

```
            "CreatedTime": "2020-10-28T02:39:22.321Z",
            "EbsOptimized": false,
            "AssociatePublicIpAddress": true,
            "MetadataOptions": {
                "HttpTokens": "required",
                "HttpPutResponseHopLimit": 1,
                "HttpEndpoint": "disabled"
            }
        }
    ]
}
```

Ejemplo 2: describir un número específico de configuraciones de inicialización

Para devolver un número específico de configuraciones de inicialización, utilice la opción `--max-items`.

```
aws autoscaling describe-launch-configurations \
    --max-items 1
```

Si la salida incluye un campo de `NextToken`, hay más configuraciones de inicialización. Para obtener las configuraciones adicionales de inicialización, utilice el valor de este campo con la opción `--starting-token` en una llamada posterior de la siguiente manera.

```
aws autoscaling describe-launch-configurations \
    --starting-token Z3M3LMPEXAMPLE
```

- Para obtener información sobre la API, consulte DescribeLaunchConfigurations en la Referencia de comandos de la AWS CLI.

`describe-lifecycle-hook-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-lifecycle-hook-types`.

AWS CLI

Descripción de los tipos disponibles de enlaces de ciclo de vida

En este ejemplo, se describen los tipos disponibles de enlaces de ciclo de vida.

```
aws autoscaling describe-lifecycle-hook-types
```

Salida:

```
{
    "LifecycleHookTypes": [
        "autoscaling:EC2_INSTANCE_LAUNCHING",
        "autoscaling:EC2_INSTANCE_TERMINATING"
    ]
}
```

- Para obtener información sobre la API, consulte DescribeLifecycleHookTypes en la Referencia de comandos de la AWS CLI.

`describe-lifecycle-hooks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-lifecycle-hooks`.

AWS CLI

Descripción de los enlaces de ciclo de vida

En este ejemplo, se describen los enlaces de ciclo de vida para el grupo de escalado automático especificado.

```
aws autoscaling describe-lifecycle-hooks \
    --auto-scaling-group-name my-asg
```

Salida:

```
{
    "LifecycleHooks": [
        {
            "GlobalTimeout": 3000,
            "HeartbeatTimeout": 30,
            "AutoScalingGroupName": "my-asg",
            "LifecycleHookName": "my-launch-hook",
            "DefaultResult": "ABANDON",
            "LifecycleTransition": "autoscaling:EC2_INSTANCE_LAUNCHING"
        },
        {
            "GlobalTimeout": 6000,
            "HeartbeatTimeout": 60,
```

```
            "AutoScalingGroupName": "my-asg",
            "LifecycleHookName": "my-termination-hook",
            "DefaultResult": "CONTINUE",
            "LifecycleTransition": "autoscaling:EC2_INSTANCE_TERMINATING"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeLifecycleHooks en la Referencia de comandos de la AWS CLI.

`describe-load-balancer-target-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-load-balancer-target-groups`.

AWS CLI

Descripción de los grupos de destino del equilibrador de carga de un grupo de escalado automático

En este ejemplo, se describe el grupo de destino del equilibrador de carga adjunto al grupo de escalado automático especificado.

```
aws autoscaling describe-load-balancer-target-groups \
    --auto-scaling-group-name my-asg
```

Salida:

```
{
    "LoadBalancerTargetGroups": [
        {
            "LoadBalancerTargetGroupARN": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067",
            "State": "Added"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeLoadBalancerTargetGroups en la Referencia de comandos de la AWS CLI.

`describe-load-balancers`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-load-balancers`.

AWS CLI

Descripción de los equilibradores de carga clásicos de un grupo de escalado automático

En este ejemplo se describen los equilibradores de carga clásicos del grupo de escalado automático especificado.

```
aws autoscaling describe-load-balancers \
    --auto-scaling-group-name my-asg
```

Salida:

```
{
    "LoadBalancers": [
        {
            "State": "Added",
            "LoadBalancerName": "my-load-balancer"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeLoadBalancers en la Referencia de comandos de la AWS CLI.

`describe-metric-collection-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-metric-collection-types`.

AWS CLI

Descripción de los tipos de recopilación de métricas disponibles

En este ejemplo, se describen los tipos de recopilación de métricas disponibles.

```
aws autoscaling describe-metric-collection-types
```

Salida:

```
{
    "Metrics": [
        {
            "Metric": "GroupMinSize"
        },
        {
            "Metric": "GroupMaxSize"
        },
        {
            "Metric": "GroupDesiredCapacity"
        },
        {
            "Metric": "GroupInServiceInstances"
        },
        {
            "Metric": "GroupInServiceCapacity"
        },
        {
            "Metric": "GroupPendingInstances"
        },
        {
            "Metric": "GroupPendingCapacity"
        },
        {
            "Metric": "GroupTerminatingInstances"
        },
        {
            "Metric": "GroupTerminatingCapacity"
        },
        {
            "Metric": "GroupStandbyInstances"
        },
        {
            "Metric": "GroupStandbyCapacity"
        },
        {
            "Metric": "GroupTotalInstances"
        },
        {
            "Metric": "GroupTotalCapacity"
        }
    ],
```

```
    "Granularities": [
        {
            "Granularity": "1Minute"
        }
    ]
}
```

Para obtener más información, consulte Métricas de grupo de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DescribeMetricCollectionTypes en la Referencia de comandos de la AWS CLI.

`describe-notification-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-notification-configurations`.

AWS CLI

Ejemplo 1: describir las configuraciones de notificación de un grupo especificado

En este ejemplo, se describen las configuraciones de notificación para el grupo de escalado automático especificado.

```
aws autoscaling describe-notification-configurations \
    --auto-scaling-group-name my-asg
```

Salida:

```
{
    "NotificationConfigurations": [
        {
            "AutoScalingGroupName": "my-asg",
            "NotificationType": "autoscaling:TEST_NOTIFICATION",
            "TopicARN": "arn:aws:sns:us-west-2:123456789012:my-sns-topic-2"
        },
        {
            "AutoScalingGroupName": "my-asg",
            "NotificationType": "autoscaling:TEST_NOTIFICATION",
            "TopicARN": "arn:aws:sns:us-west-2:123456789012:my-sns-topic"
```

```
        }
    ]
}
```

Para obtener más información, consulte Obtener notificaciones de Amazon SNS cuando su grupo de Auto Scaling escala en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 1: describir un número específico de configuraciones de notificaciones

Para devolver un número específico de configuraciones de notificación, utilice el parámetro `max-items`.

```
aws autoscaling describe-notification-configurations \
    --auto-scaling-group-name my-auto-scaling-group \
    --max-items 1
```

Salida:

```
{
    "NotificationConfigurations": [
        {
            "AutoScalingGroupName": "my-asg",
            "NotificationType": "autoscaling:TEST_NOTIFICATION",
            "TopicARN": "arn:aws:sns:us-west-2:123456789012:my-sns-topic-2"
        },
        {
            "AutoScalingGroupName": "my-asg",
            "NotificationType": "autoscaling:TEST_NOTIFICATION",
            "TopicARN": "arn:aws:sns:us-west-2:123456789012:my-sns-topic"
        }
    ]
}
```

Si la salida incluye un campo `NextToken` de, hay más configuraciones de notificación. Para obtener las configuraciones de notificación adicionales, utilice el valor de este campo con el parámetro `starting-token` en una llamada posterior de la siguiente manera.

```
aws autoscaling describe-notification-configurations \
    --auto-scaling-group-name my-asg \
    --starting-token Z3M3LMPEXAMPLE
```

Para obtener más información, consulte Obtener notificaciones de Amazon SNS cuando su grupo de Auto Scaling escala en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DescribeNotificationConfigurations en la Referencia de comandos de la AWS CLI.

`describe-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-policies`.

AWS CLI

Ejemplo 1: describir las políticas de escalado del grupo especificado

En este ejemplo, se describen las políticas de escalado para el grupo de escalado automático especificado.

```
aws autoscaling describe-policies \
    --auto-scaling-group-name my-asg
```

Salida:

```
{
    "ScalingPolicies": [
        {
            "AutoScalingGroupName": "my-asg",
            "PolicyName": "alb1000-target-tracking-scaling-policy",
            "PolicyARN": "arn:aws:autoscaling:us-
west-2:123456789012:scalingPolicy:3065d9c8-9969-4bec-
bb6a-3fbe5550fde6:autoScalingGroupName/my-asg:policyName/alb1000-target-tracking-
scaling-policy",
            "PolicyType": "TargetTrackingScaling",
            "StepAdjustments": [],
            "Alarms": [
                {
                    "AlarmName": "TargetTracking-my-asg-
AlarmHigh-924887a9-12d7-4e01-8686-6f844d13a196",
                    "AlarmARN": "arn:aws:cloudwatch:us-
west-2:123456789012:alarm:TargetTracking-my-asg-
AlarmHigh-924887a9-12d7-4e01-8686-6f844d13a196"
                },
                {
```

```
                    "AlarmName": "TargetTracking-my-asg-AlarmLow-f96f899d-b8e7-4d09-
a010-c1aaa35da296",
                    "AlarmARN": "arn:aws:cloudwatch:us-
west-2:123456789012:alarm:TargetTracking-my-asg-AlarmLow-f96f899d-b8e7-4d09-a010-
c1aaa35da296"
                }
            ],
            "TargetTrackingConfiguration": {
                "PredefinedMetricSpecification": {
                    "PredefinedMetricType": "ALBRequestCountPerTarget",
                    "ResourceLabel": "app/my-alb/778d41231b141a0f/targetgroup/my-
alb-target-group/943f017f100becff"
                },
                "TargetValue": 1000.0,
                "DisableScaleIn": false
            },
            "Enabled": true
        },
        {
            "AutoScalingGroupName": "my-asg",
            "PolicyName": "cpu40-target-tracking-scaling-policy",
            "PolicyARN": "arn:aws:autoscaling:us-
west-2:123456789012:scalingPolicy:5fd26f71-39d4-4690-82a9-
b8515c45cdde:autoScalingGroupName/my-asg:policyName/cpu40-target-tracking-scaling-
policy",
            "PolicyType": "TargetTrackingScaling",
            "StepAdjustments": [],
            "Alarms": [
                {
                    "AlarmName": "TargetTracking-my-asg-
AlarmHigh-139f9789-37b9-42ad-bea5-b5b147d7f473",
                    "AlarmARN": "arn:aws:cloudwatch:us-
west-2:123456789012:alarm:TargetTracking-my-asg-AlarmHigh-139f9789-37b9-42ad-bea5-
b5b147d7f473"
                },
                {
                    "AlarmName": "TargetTracking-my-asg-AlarmLow-bd681c67-
fc18-4c56-8468-fb8e413009c9",
                    "AlarmARN": "arn:aws:cloudwatch:us-
west-2:123456789012:alarm:TargetTracking-my-asg-AlarmLow-bd681c67-fc18-4c56-8468-
fb8e413009c9"
                }
            ],
            "TargetTrackingConfiguration": {
```

```
                "PredefinedMetricSpecification": {
                    "PredefinedMetricType": "ASGAverageCPUUtilization"
                },
                "TargetValue": 40.0,
                "DisableScaleIn": false
            },
            "Enabled": true
        }
    ]
}
```

Para obtener más información, consulte Escalado dinámico en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 2: describir las políticas de escalado de un nombre especificado

Para devolver políticas de escalado específicas, utilice la opción `--policy-names`.

```
aws autoscaling describe-policies \
    --auto-scaling-group-name my-asg \
    --policy-names cpu40-target-tracking-scaling-policy
```

Consulte el ejemplo 1 para ver una salida de muestra.

Para obtener más información, consulte Escalado dinámico en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 3: cómo describir una serie de políticas de escalado

Para devolver un número específico de políticas, utilice la opción `--max-items`.

```
aws autoscaling describe-policies \
    --auto-scaling-group-name my-asg \
    --max-items 1
```

Consulte el ejemplo 1 para ver una salida de muestra.

Si la salida incluye un campo de `NextToken`, utilice el valor de este campo con la opción `--starting-token` en una llamada posterior para obtener las políticas adicionales.

```
aws autoscaling describe-policies --auto-scaling-group-name my-asg --starting-
token Z3M3LMPEXAMPLE
```

Para obtener más información, consulte Dynamic scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DescribePolicies en la Referencia de comandos de la AWS CLI.

`describe-scaling-activities`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-scaling-activities`.

AWS CLI

Ejemplo 1: Descripción de las actividades de escalado para el grupo especificado

En este ejemplo, se describen una o varias actividades de escalado para el grupo de escalado automático especificado.

```
aws autoscaling describe-scaling-activities \
    --auto-scaling-group-name my-asg
```

Salida:

```
{
    "Activities": [
        {
            "ActivityId": "f9f2d65b-f1f2-43e7-b46d-d86756459699",
            "Description": "Launching a new EC2 instance: i-0d44425630326060f",
            "AutoScalingGroupName": "my-asg",
            "Cause": "At 2020-10-30T19:35:51Z a user request update of
 AutoScalingGroup constraints to min: 0, max: 16, desired: 16 changing the desired
 capacity from 0 to 16.  At 2020-10-30T19:36:07Z an instance was started in response
 to a difference between desired and actual capacity, increasing the capacity from 0
 to 16.",
            "StartTime": "2020-10-30T19:36:09.766Z",
            "EndTime": "2020-10-30T19:36:41Z",
            "StatusCode": "Successful",
            "Progress": 100,
            "Details": "{\"Subnet ID\":\"subnet-5ea0c127\",\"Availability Zone\":
\"us-west-2b\"}"
        }
    ]
}
```

Para obtener más información, consulte Verificar una actividad de escalado para un grupo de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 2: Descripción de las actividades de escalado de un grupo eliminado

Para describir las actividades de escalado después de que un grupo de escalado automático se haya eliminado, añada la opción `--include-deleted-groups`.

```
aws autoscaling describe-scaling-activities \
    --auto-scaling-group-name my-asg \
    --include-deleted-groups
```

Salida:

```
{
    "Activities": [
        {
            "ActivityId": "e1f5de0e-f93e-1417-34ac-092a76fba220",
            "Description": "Launching a new EC2 instance.  Status Reason: Your Spot
 request price of 0.001 is lower than the minimum required Spot request fulfillment
 price of 0.0031. Launching EC2 instance failed.",
            "AutoScalingGroupName": "my-asg",
            "Cause": "At 2021-01-13T20:47:24Z a user request update of
 AutoScalingGroup constraints to min: 1, max: 5, desired: 3 changing the desired
 capacity from 0 to 3.  At 2021-01-13T20:47:27Z an instance was started in response
 to a difference between desired and actual capacity, increasing the capacity from 0
 to 3.",
            "StartTime": "2021-01-13T20:47:30.094Z",
            "EndTime": "2021-01-13T20:47:30Z",
            "StatusCode": "Failed",
            "StatusMessage": "Your Spot request price of 0.001 is lower than the
 minimum required Spot request fulfillment price of 0.0031. Launching EC2 instance
 failed.",
            "Progress": 100,
            "Details": "{\"Subnet ID\":\"subnet-5ea0c127\",\"Availability Zone\":
\"us-west-2b\"}",
            "AutoScalingGroupState": "Deleted",
            "AutoScalingGroupARN": "arn:aws:autoscaling:us-
west-2:123456789012:autoScalingGroup:283179a2-
f3ce-423d-93f6-66bb518232f7:autoScalingGroupName/my-asg"
        }
    ]
```

```
}
```

Para obtener más información, consulte Solución de problemas para Amazon EC2 Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 3: descripción de un número específico de actividades de escalado

Para devolver un número específico de actividades, utilice la opción `--max-items`.

```
aws autoscaling describe-scaling-activities \
    --max-items 1
```

Salida:

```
{
    "Activities": [
        {
            "ActivityId": "f9f2d65b-f1f2-43e7-b46d-d86756459699",
            "Description": "Launching a new EC2 instance: i-0d44425630326060f",
            "AutoScalingGroupName": "my-asg",
            "Cause": "At 2020-10-30T19:35:51Z a user request update of
 AutoScalingGroup constraints to min: 0, max: 16, desired: 16 changing the desired
 capacity from 0 to 16.  At 2020-10-30T19:36:07Z an instance was started in response
 to a difference between desired and actual capacity, increasing the capacity from 0
 to 16.",
            "StartTime": "2020-10-30T19:36:09.766Z",
            "EndTime": "2020-10-30T19:36:41Z",
            "StatusCode": "Successful",
            "Progress": 100,
            "Details": "{\"Subnet ID\":\"subnet-5ea0c127\",\"Availability Zone\":
\"us-west-2b\"}"
        }
    ]
}
```

Si la salida incluye un campo `NextToken`, hay más actividades. Para obtener las actividades adicionales, utilice el valor de este campo con la opción `--starting-token` en una llamada posterior de la siguiente manera.

```
aws autoscaling describe-scaling-activities \
    --starting-token Z3M3LMPEXAMPLE
```

Para obtener más información, consulte Verificar una actividad de escalado para un grupo de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DescribeScalingActivities en la Referencia de comandos de la AWS CLI.

`describe-scaling-process-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-scaling-process-types`.

AWS CLI

Descripción de los tipos de procesos disponibles

En este ejemplo se describen los tipos de procesos disponibles.

```
aws autoscaling describe-scaling-process-types
```

Salida:

```
{
    "Processes": [
        {
            "ProcessName": "AZRebalance"
        },
        {
            "ProcessName": "AddToLoadBalancer"
        },
        {
            "ProcessName": "AlarmNotification"
        },
        {
            "ProcessName": "HealthCheck"
        },
        {
            "ProcessName": "InstanceRefresh"
        },
        {
            "ProcessName": "Launch"
        },
        {
            "ProcessName": "ReplaceUnhealthy"
        },
```

```
        {
            "ProcessName": "ScheduledActions"
        },
        {
            "ProcessName": "Terminate"
        }
    ]
}
```

Para obtener más información, consulte Suspending and resuming scaling processes en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DescribeScalingProcessTypes en la Referencia de comandos de la AWS CLI.

`describe-scheduled-actions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-scheduled-actions`.

AWS CLI

Ejemplo 1: Cómo describir todas las acciones programadas

En este ejemplo, se describen todas las acciones programadas.

```
aws autoscaling describe-scheduled-actions
```

Salida:

```
{
    "ScheduledUpdateGroupActions": [
        {
            "AutoScalingGroupName": "my-asg",
            "ScheduledActionName": "my-recurring-action",
            "Recurrence": "30 0 1 1,6,12 *",
            "ScheduledActionARN": "arn:aws:autoscaling:us-
west-2:123456789012:scheduledUpdateGroupAction:8e86b655-b2e6-4410-8f29-
b4f094d6871c:autoScalingGroupName/my-asg:scheduledActionName/my-recurring-action",
            "StartTime": "2023-12-01T04:00:00Z",
            "Time": "2023-12-01T04:00:00Z",
            "MinSize": 1,
            "MaxSize": 6,
```

```
            "DesiredCapacity": 4,
            "TimeZone": "America/New_York"
        }
    ]
}
```

Para obtener más información, consulte la sección sobre Escalado programado en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 2: describir las acciones programadas para el grupo especificado

Para describir las acciones programadas para un grupo de escalado automático específico, utilice la opción `--auto-scaling-group-name`.

```
aws autoscaling describe-scheduled-actions \
    --auto-scaling-group-name my-asg
```

Salida:

```
{
    "ScheduledUpdateGroupActions": [
        {
            "AutoScalingGroupName": "my-asg",
            "ScheduledActionName": "my-recurring-action",
            "Recurrence": "30 0 1 1,6,12 *",
            "ScheduledActionARN": "arn:aws:autoscaling:us-
west-2:123456789012:scheduledUpdateGroupAction:8e86b655-b2e6-4410-8f29-
b4f094d6871c:autoScalingGroupName/my-asg:scheduledActionName/my-recurring-action",
            "StartTime": "2023-12-01T04:00:00Z",
            "Time": "2023-12-01T04:00:00Z",
            "MinSize": 1,
            "MaxSize": 6,
            "DesiredCapacity": 4,
            "TimeZone": "America/New_York"
        }
    ]
}
```

Para obtener más información, consulte la sección sobre Escalado programado en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 3: cómo describir la acción programada especificada

Para describir una acción programada específica, utilice la opción `--scheduled-action-names`.

```
aws autoscaling describe-scheduled-actions \
    --scheduled-action-names my-recurring-action
```

Salida:

```
{
    "ScheduledUpdateGroupActions": [
        {
            "AutoScalingGroupName": "my-asg",
            "ScheduledActionName": "my-recurring-action",
            "Recurrence": "30 0 1 1,6,12 *",
            "ScheduledActionARN": "arn:aws:autoscaling:us-
west-2:123456789012:scheduledUpdateGroupAction:8e86b655-b2e6-4410-8f29-
b4f094d6871c:autoScalingGroupName/my-asg:scheduledActionName/my-recurring-action",
            "StartTime": "2023-12-01T04:00:00Z",
            "Time": "2023-12-01T04:00:00Z",
            "MinSize": 1,
            "MaxSize": 6,
            "DesiredCapacity": 4,
            "TimeZone": "America/New_York"
        }
    ]
}
```

Para obtener más información, consulte la sección sobre Escalado programado en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 4: cómo describir las acciones programadas con una hora de inicio especifica

Para describir las acciones programadas que comienzan a una hora específica, utilice la opción `--start-time`.

```
aws autoscaling describe-scheduled-actions \
    --start-time "2023-12-01T04:00:00Z"
```

Salida:

```
{
```

```
    "ScheduledUpdateGroupActions": [
        {
            "AutoScalingGroupName": "my-asg",
            "ScheduledActionName": "my-recurring-action",
            "Recurrence": "30 0 1 1,6,12 *",
            "ScheduledActionARN": "arn:aws:autoscaling:us-
west-2:123456789012:scheduledUpdateGroupAction:8e86b655-b2e6-4410-8f29-
b4f094d6871c:autoScalingGroupName/my-asg:scheduledActionName/my-recurring-action",
            "StartTime": "2023-12-01T04:00:00Z",
            "Time": "2023-12-01T04:00:00Z",
            "MinSize": 1,
            "MaxSize": 6,
            "DesiredCapacity": 4,
            "TimeZone": "America/New_York"
        }
    ]
}
```

Para obtener más información, consulte la sección sobre Escalado programado en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 5: cómo describir las acciones programadas que finalizan a una hora específica

Para describir las acciones programadas que finalizan a una hora específica, utilice la opción `--end-time`.

```
aws autoscaling describe-scheduled-actions \
    --end-time "2023-12-01T04:00:00Z"
```

Salida:

```
{
    "ScheduledUpdateGroupActions": [
        {
            "AutoScalingGroupName": "my-asg",
            "ScheduledActionName": "my-recurring-action",
            "Recurrence": "30 0 1 1,6,12 *",
            "ScheduledActionARN": "arn:aws:autoscaling:us-
west-2:123456789012:scheduledUpdateGroupAction:8e86b655-b2e6-4410-8f29-
b4f094d6871c:autoScalingGroupName/my-asg:scheduledActionName/my-recurring-action",
            "StartTime": "2023-12-01T04:00:00Z",
            "Time": "2023-12-01T04:00:00Z",
            "MinSize": 1,
```

```
            "MaxSize": 6,
            "DesiredCapacity": 4,
            "TimeZone": "America/New_York"
        }
    ]
}
```

Para obtener más información, consulte la sección sobre Escalado programado en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 6: cómo describir un número específico de acciones programadas

Para devolver un número específico de acciones programadas, utilice la opción `--max-items`.

```
aws autoscaling describe-scheduled-actions \
    --auto-scaling-group-name my-asg \
    --max-items 1
```

Salida:

```
{
    "ScheduledUpdateGroupActions": [
        {
            "AutoScalingGroupName": "my-asg",
            "ScheduledActionName": "my-recurring-action",
            "Recurrence": "30 0 1 1,6,12 *",
            "ScheduledActionARN": "arn:aws:autoscaling:us-
west-2:123456789012:scheduledUpdateGroupAction:8e86b655-b2e6-4410-8f29-
b4f094d6871c:autoScalingGroupName/my-asg:scheduledActionName/my-recurring-action",
            "StartTime": "2023-12-01T04:00:00Z",
            "Time": "2023-12-01T04:00:00Z",
            "MinSize": 1,
            "MaxSize": 6,
            "DesiredCapacity": 4,
            "TimeZone": "America/New_York"
        }
    ]
}
```

Si la salida incluye un campo de `NextToken`, hay más acciones programadas. Para obtener las acciones programadas adicionales, utilice el valor de este campo con la opción `--starting-token` en una llamada posterior de la siguiente manera.

```
aws autoscaling describe-scheduled-actions \
    --auto-scaling-group-name my-asg \
    --starting-token Z3M3LMPEXAMPLE
```

Para obtener más información, consulte la sección sobre Escalado programado en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DescribeScheduledActions en la Referencia de comandos de la AWS CLI.

`describe-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-tags`.

AWS CLI

Descripción de todas las etiquetas

En este ejemplo, se describen todas las etiquetas.

```
aws autoscaling describe-tags
```

Salida:

```
{
    "Tags": [
        {
            "ResourceType": "auto-scaling-group",
            "ResourceId": "my-asg",
            "PropagateAtLaunch": true,
            "Value": "Research",
            "Key": "Dept"
        },
        {
            "ResourceType": "auto-scaling-group",
            "ResourceId": "my-asg",
            "PropagateAtLaunch": true,
            "Value": "WebServer",
            "Key": "Role"
        }
    ]
```

```
}
```

Para obtener más información, consulte Etiquetado de grupos e instancias de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 2: describir las etiquetas de un grupo específico

Para describir etiquetas de un grupo de escalado automático específico, utilice la opción `--filters`.

```
aws autoscaling describe-tags --filters Name=auto-scaling-group,Values=my-asg
```

Para obtener más información, consulte Etiquetado de grupos e instancias de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 3: cómo describir el número especificado de etiquetas

Para devolver un número específico de etiquetas, utilice la opción `--max-items`.

```
aws autoscaling describe-tags \
    --max-items 1
```

Si la salida incluye un campo de `NextToken`, hay más etiquetas. Para obtener las etiquetas adicionales, utilice el valor de este campo con la opción `--starting-token` en una llamada posterior de la siguiente manera.

```
aws autoscaling describe-tags \
    --filters Name=auto-scaling-group,Values=my-asg \
    --starting-token Z3M3LMPEXAMPLE
```

Para obtener más información, consulte Etiquetado de grupos e instancias de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener detalles sobre la API, consulte DescribeTags en la Referencia de comandos de la AWS CLI.

`describe-termination-policy-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-termination-policy-types`.

AWS CLI

Descripción de los tipos de políticas de terminación disponibles

En este ejemplo se describen los tipos de políticas de terminación disponibles.

```
aws autoscaling describe-termination-policy-types
```

Salida:

```
{
    "TerminationPolicyTypes": [
        "AllocationStrategy",
        "ClosestToNextInstanceHour",
        "Default",
        "NewestInstance",
        "OldestInstance",
        "OldestLaunchConfiguration",
        "OldestLaunchTemplate"
    ]
}
```

Para obtener más información, consulte el tema Controlar las instancias que Auto Scaling termina durante el escalado descendente en la guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DescribeTerminationPolicyTypes en la Referencia de comandos de la AWS CLI.

`describe-warm-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-warm-pool`.

AWS CLI

Descripción de un grupo de calentamiento

En este ejemplo, se describe el grupo de calentamiento del grupo de escalado automático especificado.

```
aws autoscaling describe-warm-pool \
    --auto-scaling-group-name my-asg
```

Salida:

```
{
    "WarmPoolConfiguration": {
        "MinSize": 2,
        "PoolState": "Stopped"
    },
    "Instances": [
        {
            "InstanceId": "i-070a5bbc7e7f40dc5",
            "InstanceType": "t2.micro",
            "AvailabilityZone": "us-west-2c",
            "LifecycleState": "Warmed:Pending",
            "HealthStatus": "Healthy",
            "LaunchTemplate": {
                "LaunchTemplateId": "lt-00a731f6e9fa48610",
                "LaunchTemplateName": "my-template-for-auto-scaling",
                "Version": "6"
            }
        },
        {
            "InstanceId": "i-0b52f061814d3bd2d",
            "InstanceType": "t2.micro",
            "AvailabilityZone": "us-west-2b",
            "LifecycleState": "Warmed:Pending",
            "HealthStatus": "Healthy",
            "LaunchTemplate": {
                "LaunchTemplateId": "lt-00a731f6e9fa48610",
                "LaunchTemplateName": "my-template-for-auto-scaling",
                "Version": "6"
            }
        }
    ]
}
```

Para obtener más información, consulte Grupos de calentamiento para Amazon EC2 Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DescribeWarmPool en la Referencia de comandos de la AWS CLI.

`detach-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-instances`.

AWS CLI

Desasociación de una instancia de un grupo de escalado automático

En este ejemplo, se asocia la instancia especificada del grupo de escalado automático especificado.

```
aws autoscaling detach-instances \
    --instance-ids i-030017cfa84b20135 \
    --auto-scaling-group-name my-asg \
    --should-decrement-desired-capacity
```

Salida:

```
{
    "Activities": [
        {
            "ActivityId": "5091cb52-547a-47ce-a236-c9ccbc2cb2c9",
            "AutoScalingGroupName": "my-asg",
            "Description": "Detaching EC2 instance: i-030017cfa84b20135",
            "Cause": "At 2020-10-31T17:35:04Z instance i-030017cfa84b20135 was
 detached in response to a user request, shrinking the capacity from 2 to 1.",
            "StartTime": "2020-04-12T15:02:16.179Z",
            "StatusCode": "InProgress",
            "Progress": 50,
            "Details": "{\"Subnet ID\":\"subnet-6194ea3b\",\"Availability Zone\":
\"us-west-2c\"}"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DetachInstances en la Referencia de comandos de la AWS CLI.

`detach-load-balancer-target-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-load-balancer-target-groups`.

AWS CLI

Desasociación de un grupo de destino de equilibrador de carga de un grupo de escalado automático

En este ejemplo, se desasocia el grupo de destino del equilibrador de carga especificado del grupo de escalado automático especificado.

```
aws autoscaling detach-load-balancer-target-groups \
    --auto-scaling-group-name my-asg \
    --target-group-arns arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adjuntar un equilibrador de carga al grupo de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DetachLoadBalancerTargetGroups en la Referencia de comandos de la AWS CLI.

`detach-load-balancers`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-load-balancers`.

AWS CLI

Desasociación de un equilibrador de carga clásico de un grupo de escalado automático

En este ejemplo, se asocia el equilibrador de carga clásico especificado del grupo de escalado automático especificado.

```
aws autoscaling detach-load-balancers \
    --load-balancer-names my-load-balancer \
    --auto-scaling-group-name my-asg
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adjuntar un equilibrador de carga al grupo de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DetachLoadBalancers en la Referencia de comandos de la AWS CLI.

`disable-metrics-collection`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-metrics-collection`.

AWS CLI

Desactivación de la recopilación de métricas de grupo de un grupo de escalado automático

En este ejemplo, se deshabilita la recopilación de la métrica `GroupDesiredCapacity` del grupo de escalado automático especificado.

```
aws autoscaling disable-metrics-collection \
    --auto-scaling-group-name my-asg \
    --metrics GroupDesiredCapacity
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Monitorizar las métricas de CloudWatch para las instancias y los grupos de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte DisableMetricsCollection en la Referencia de la comandos de la AWS CLI.

`enable-metrics-collection`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-metrics-collection`.

AWS CLI

Ejemplo 1: Habilitación de la recopilación de métricas de un grupo de escalado automático

En este ejemplo, se habilita la recopilación de datos para el grupo de escalado automático especificado.

```
aws autoscaling enable-metrics-collection \
    --auto-scaling-group-name my-asg \
    --granularity "1Minute"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Monitorizar las métricas de CloudWatch para las instancias y los grupos de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 2: Recopilación de datos para la métrica especificada para un grupo de escalado automático

Para recopilar datos para una métrica específica, utilice la opción `--metrics`.

```
aws autoscaling enable-metrics-collection \
    --auto-scaling-group-name my-asg \
    --metrics GroupDesiredCapacity --granularity "1Minute"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Monitorizar las métricas de CloudWatch para las instancias y los grupos de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte EnableMetricsCollection en la Referencia de comandos de la AWS CLI.

`enter-standby`

En el siguiente ejemplo de código, se muestra cómo utilizar `enter-standby`.

AWS CLI

Cambio de las instancias al modo de espera

En este ejemplo, se pone la instancia especificada en modo de espera. Esto resulta útil para actualizar o solucionar problemas de una instancia que está actualmente en servicio.

```
aws autoscaling enter-standby \
    --instance-ids i-061c63c5eb45f0416 \
    --auto-scaling-group-name my-asg \
    --should-decrement-desired-capacity
```

Salida:

```
{
    "Activities": [
```

```
        {
            "ActivityId": "ffa056b4-6ed3-41ba-ae7c-249dfae6eba1",
            "AutoScalingGroupName": "my-asg",
            "Description": "Moving EC2 instance to Standby: i-061c63c5eb45f0416",
            "Cause": "At 2020-10-31T20:31:00Z instance i-061c63c5eb45f0416 was moved
 to standby in response to a user request, shrinking the capacity from 1 to 0.",
            "StartTime": "2020-10-31T20:31:00.949Z",
            "StatusCode": "InProgress",
            "Progress": 50,
            "Details": "{\"Subnet ID\":\"subnet-6194ea3b\",\"Availability Zone\":
\"us-west-2c\"}"
        }
    ]
}
```

Para obtener más información, consulte Amazon EC2 Auto Scaling instance lifecycle en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener más información sobre la API, consulte EnterStandby en la Referencia de comandos de la AWS CLI.

`execute-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `execute-policy`.

AWS CLI

Ejecución de una política de escalado

En este ejemplo, se ejecuta la política de escalado denominada `my-step-scale-out-policy` para el grupo de escalado automático especificado.

```
aws autoscaling execute-policy \
    --auto-scaling-group-name my-asg \
    --policy-name  my-step-scale-out-policy \
    --metric-value 95 \
    --breach-threshold 80
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Step and simple scaling policies en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte ExecutePolicy en la Referencia de comandos de la AWS CLI.

`exit-standby`

En el siguiente ejemplo de código, se muestra cómo utilizar `exit-standby`.

AWS CLI

Retirada de las instancias del modo de espera

En este ejemplo se sacan las instancias especificadas del modo de espera.

```
aws autoscaling exit-standby \
    --instance-ids i-061c63c5eb45f0416 \
    --auto-scaling-group-name my-asg
```

Salida:

```
{
    "Activities": [
        {
            "ActivityId": "142928e1-a2dc-453a-9b24-b85ad6735928",
            "AutoScalingGroupName": "my-asg",
            "Description": "Moving EC2 instance out of Standby:
 i-061c63c5eb45f0416",
            "Cause": "At 2020-10-31T20:32:50Z instance i-061c63c5eb45f0416 was moved
 out of standby in response to a user request, increasing the capacity from 0 to
 1.",
            "StartTime": "2020-10-31T20:32:50.222Z",
            "StatusCode": "PreInService",
            "Progress": 30,
            "Details": "{\"Subnet ID\":\"subnet-6194ea3b\",\"Availability Zone\":
\"us-west-2c\"}"
        }
    ]
}
```

Para obtener más información, consulte Eliminación temporal de instancias de su grupo de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte ExitStandby en la Referencia de comandos de la AWS CLI.

`put-lifecycle-hook`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-lifecycle-hook`.

AWS CLI

Ejemplo 1: crear un enlace de ciclo de vida

En este ejemplo, se crea un enlace de ciclo de vida que se invocará en cualquier instancia recién inicializada, con un tiempo de espera de 4800 segundos. Esto resulta útil para mantener las instancias en estado de espera hasta que finalicen los scripts de datos de usuario o para invocar una función de Lambda de AWS mediante EventBridge.

```
aws autoscaling put-lifecycle-hook \
    --auto-scaling-group-name my-asg \
    --lifecycle-hook-name my-launch-hook \
    --lifecycle-transition autoscaling:EC2_INSTANCE_LAUNCHING \
    --heartbeat-timeout 4800
```

Este comando no genera ninguna salida. Si ya existe un enlace de ciclo de vida con el mismo nombre, el nuevo enlace de ciclo de vida lo sobrescribirá.

Para obtener más información, consulte Enlaces de ciclo de vida de Amazon EC2 Auto Scaling en la guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 2: enviar un mensaje de correo electrónico de Amazon SNS para notificarle las transiciones de estado de la instancia

En este ejemplo, se crea un enlace de ciclo de vida con el tema de Amazon SNS y rol de IAM que se debe utilizar para recibir notificaciones en la inicialización de la instancia.

```
aws autoscaling put-lifecycle-hook \
    --auto-scaling-group-name my-asg \
    --lifecycle-hook-name my-launch-hook \
    --lifecycle-transition autoscaling:EC2_INSTANCE_LAUNCHING \
    --notification-target-arn arn:aws:sns:us-west-2:123456789012:my-sns-topic \
    --role-arn arn:aws:iam::123456789012:role/my-auto-scaling-role
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Enlaces de ciclo de vida de Amazon EC2 Auto Scaling en la guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 3: cómo publicar un mensaje en una cola de Amazon SQS

En este ejemplo, se crea un enlace de ciclo de vida que publica un mensaje con metadatos en la cola de Amazon SQS especificada.

```
aws autoscaling put-lifecycle-hook \
    --auto-scaling-group-name my-asg \
    --lifecycle-hook-name my-launch-hook \
    --lifecycle-transition autoscaling:EC2_INSTANCE_LAUNCHING \
    --notification-target-arn arn:aws:sqs:us-west-2:123456789012:my-sqs-queue \
    --role-arn arn:aws:iam::123456789012:role/my-notification-role \
    --notification-metadata "SQS message metadata"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Enlaces de ciclo de vida de Amazon EC2 Auto Scaling en la guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte PutLifecycleHook en la Referencia de comandos de la AWS CLI.

`put-notification-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-notification-configuration`.

AWS CLI

Adición de una nueva notificación

En este ejemplo, se añade la notificación especificada al grupo de escalado automático especificado.

```
aws autoscaling put-notification-configuration \
    --auto-scaling-group-name my-asg \
    --topic-arn arn:aws:sns:us-west-2:123456789012:my-sns-topic \
    --notification-type autoscaling:TEST_NOTIFICATION
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Obtener notificaciones de Amazon SNS cuando su grupo de Auto Scaling escala en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte PutNotificationConfiguration en la Referencia de Cmdlet de AWS CLI.

`put-scaling-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-scaling-policy`.

AWS CLI

Adición de una política de escalado de seguimiento de destino a un grupo de escalado automático

El siguiente ejemplo de `put-scaling-policy` aplica una política de escalado de seguimiento de destino al grupo de escalado automático especificado. La salida contiene los ARN y nombres de las dos alarmas de CloudWatch creadas en su nombre. Si existe una política de escalado con el mismo nombre, la nueva política la sobrescribirá.

```
aws autoscaling put-scaling-policy --auto-scaling-group-name my-asg \
  --policy-name alb1000-target-tracking-scaling-policy \
  --policy-type TargetTrackingScaling \
  --target-tracking-configuration file://config.json
```

Contenido de `config.json`:

```
{
     "TargetValue": 1000.0,
     "PredefinedMetricSpecification": {
          "PredefinedMetricType": "ALBRequestCountPerTarget",
          "ResourceLabel": "app/my-alb/778d41231b141a0f/targetgroup/my-alb-target-
group/943f017f100becff"
     }
}
```

Salida:

```
{
```

```
    "PolicyARN": "arn:aws:autoscaling:region:account-id:scalingPolicy:228f02c2-
c665-4bfd-aaac-8b04080bea3c:autoScalingGroupName/my-asg:policyName/alb1000-target-
tracking-scaling-policy",
    "Alarms": [
        {
            "AlarmARN": "arn:aws:cloudwatch:region:account-id:alarm:TargetTracking-
my-asg-AlarmHigh-fc0e4183-23ac-497e-9992-691c9980c38e",
            "AlarmName": "TargetTracking-my-asg-AlarmHigh-
fc0e4183-23ac-497e-9992-691c9980c38e"
        },
        {
            "AlarmARN": "arn:aws:cloudwatch:region:account-id:alarm:TargetTracking-
my-asg-AlarmLow-61a39305-ed0c-47af-bd9e-471a352ee1a2",
            "AlarmName": "TargetTracking-my-asg-AlarmLow-61a39305-ed0c-47af-
bd9e-471a352ee1a2"
        }
    ]
}
```

Para ver más ejemplos, consulte Example scaling policies for the AWS Command Line Interface (AWS CLI) en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte PutScalingPolicy en la Referencia de comandos de la AWS CLI.

`put-scheduled-update-group-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-scheduled-update-group-action`.

AWS CLI

Ejemplo 1: añadir una acción programada a un grupo de escalado automático

En este ejemplo, se añade la acción programada especificada al grupo de escalado automático especificado.

```
aws autoscaling put-scheduled-update-group-action \
    --auto-scaling-group-name my-asg \
    --scheduled-action-name my-scheduled-action \
    --start-time "2023-05-12T08:00:00Z" \
    --min-size 2 \
```

```
    --max-size 6 \
    --desired-capacity 4
```

Este comando no genera ninguna salida. Si existe una acción programada con el mismo nombre, la nueva acción programada la sobrescribirá.

Para ver más ejemplos, consulte Escalado programado en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 2: especificar una programación recurrente

En este ejemplo, se crea una acción programada para escalar un programa recurrente cuya ejecución está prevista para las 00:30 h del primero de enero, junio y diciembre de cada año.

```
aws autoscaling put-scheduled-update-group-action \
    --auto-scaling-group-name my-asg \
    --scheduled-action-name my-recurring-action \
    --recurrence "30 0 1 1,6,12 *" \
    --min-size 2 \
    --max-size 6 \
    --desired-capacity 4
```

Este comando no genera ninguna salida. Si existe una acción programada con el mismo nombre, la nueva acción programada la sobrescribirá.

Para obtener más información, consulte Escalado programado en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte PutScheduledUpdateGroupAction en la Referencia de comandos de la AWS CLI.

`put-warm-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-warm-pool`.

AWS CLI

Creación de un grupo de calentamiento

En el ejemplo siguiente, se crea un grupo de calentamiento para el grupo de escalado automático especificado.

```
aws autoscaling put-warm-pool \
    --auto-scaling-group-name my-asg \
    --min-size 2
```

Este comando no genera ninguna salida. Si ya existe un grupo de calentamiento, se actualizará.

Para obtener más información, consulte Grupos de calentamiento para Amazon EC2 Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener más información sobre la API, consulte PutWarmPool en la Referencia de comandos de la AWS CLI.

`record-lifecycle-action-heartbeat`

En el siguiente ejemplo de código, se muestra cómo utilizar `record-lifecycle-action-heartbeat`.

AWS CLI

Registro del latido de una acción del ciclo de vida

En este ejemplo, se registra el latido de una acción del ciclo de vida para mantener la instancia en estado pendiente.

```
aws autoscaling record-lifecycle-action-heartbeat \
    --lifecycle-hook-name my-launch-hook \
    --auto-scaling-group-name my-asg \
    --lifecycle-action-token bcd2f1b8-9a78-44d3-8a7a-4dd07d7cf635
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Enlaces de ciclo de vida de Amazon EC2 Auto Scaling en la guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte RecordLifecycleActionHeartbeat en la Referencia de comandos de la AWS CLI.

`resume-processes`

En el siguiente ejemplo de código, se muestra cómo utilizar `resume-processes`.

AWS CLI

Reanudación de un proceso suspendido

En este ejemplo, se reanuda el proceso de escalado suspendido especificado para el grupo de escalado automático especificado.

```
aws autoscaling resume-processes \
    --auto-scaling-group-name my-asg \
    --scaling-processes AlarmNotification
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Suspending and resuming scaling processes en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte ResumeProcesses en la Referencia de comandos de la AWS CLI.

`rollback-instance-refresh`

En el siguiente ejemplo de código, se muestra cómo utilizar `rollback-instance-refresh`.

AWS CLI

Reversión de la actualización de una instancia

En el siguiente ejemplo de `rollback-instance-refresh`, se revierte la actualización de instancia en curso del grupo de escalado automático especificado.

```
aws autoscaling rollback-instance-refresh \
    --auto-scaling-group-name my-asg
```

Salida:

```
{
    "InstanceRefreshId": "08b91cf7-8fa6-48af-b6a6-d227f40f1b9b"
}
```

Para obtener más información, consulte Inversión de cambios con una reversión en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte RollbackInstanceRefresh en la Referencia de comandos de la AWS CLI.

`set-desired-capacity`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-desired-capacity`.

AWS CLI

Fijación de la capacidad deseada inicial para el grupo de escalado automático

En este ejemplo, se establece la capacidad deseada para el grupo de escalado automático especificado.

```
aws autoscaling set-desired-capacity \
    --auto-scaling-group-name my-asg \
    --desired-capacity 2 \
    --honor-cooldown
```

Este comando vuelve a la petición si se ejecuta correctamente.

- Para obtener información sobre la API, consulte SetDesiredCapacity en la Referencia de comandos de la AWS CLI.

`set-instance-health`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-instance-health`.

AWS CLI

Comprobación del estado de una instancia

En este ejemplo se establece el estado de la instancia especificada en `Unhealthy`.

```
aws autoscaling set-instance-health \
    --instance-id i-061c63c5eb45f0416 \
    --health-status Unhealthy
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte SetInstanceHealth en la Referencia de comandos de la AWS CLI.

`set-instance-protection`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-instance-protection`.

AWS CLI

Ejemplo 1: habilitar la configuración de protección de instancias para una instancia

En este ejemplo, se habilita la protección de instancias para la instancia especificada.

```
aws autoscaling set-instance-protection \
    --instance-ids i-061c63c5eb45f0416 \
    --auto-scaling-group-name my-asg --protected-from-scale-in
```

Este comando no genera ninguna salida.

Ejemplo 2: deshabilitar la configuración de protección de instancias para una instancia

En este ejemplo, se deshabilita la protección de instancias para la instancia especificada.

```
aws autoscaling set-instance-protection \
    --instance-ids i-061c63c5eb45f0416 \
    --auto-scaling-group-name my-asg \
    --no-protected-from-scale-in
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte SetInstanceProtection en la Referencia de comandos de la AWS CLI.

`start-instance-refresh`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-instance-refresh`.

AWS CLI

Ejemplo 1: cómo iniciar una actualización de instancias mediante parámetros de línea de comandos

En el siguiente ejemplo de `start-instance-refresh`, se inicia una actualización de instancias mediante argumentos de línea de comandos. El parámetro `preferences` opcional especifica un `InstanceWarmup` de `60` segundos y un `MinHealthyPercentage` de `50` %.

```
aws autoscaling start-instance-refresh \
    --auto-scaling-group-name my-asg \
    --preferences '{"InstanceWarmup": 60, "MinHealthyPercentage": 50}'
```

Salida:

```
{
    "InstanceRefreshId": "08b91cf7-8fa6-48af-b6a6-d227f40f1b9b"
}
```

Para obtener más información, consulte Start an instance refresh en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 2: cómo iniciar la actualización de una instancia mediante un archivo JSON

En el siguiente ejemplo de `start-instance-refresh`, se inicia una actualización de una instancia mediante un archivo JSON. Puede especificar el grupo de escalado automático y definir la configuración y las preferencias que desee en un archivo JSON, como se muestra en el siguiente ejemplo.

```
aws autoscaling start-instance-refresh \
    --cli-input-json file://config.json
```

Contenido de `config.json`:

```
{
    "AutoScalingGroupName": "my-asg",
    "DesiredConfiguration": {
        "LaunchTemplate": {
            "LaunchTemplateId": "lt-068f72b729example",
            "Version": "$Default"
        }
    },
    "Preferences": {
        "InstanceWarmup": 60,
        "MinHealthyPercentage": 50,
        "AutoRollback": true,
        "ScaleInProtectedInstances": Ignore,
        "StandbyInstances": Terminate
    }
```

```
}
```

Salida:

```
{
    "InstanceRefreshId": "08b91cf7-8fa6-48af-b6a6-d227f40f1b9b"
}
```

Para obtener más información, consulte Start an instance refresh en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener detalles sobre la API, consulte StartInstanceRefresh en la Referencia de comandos de la AWS CLI.

`suspend-processes`

En el siguiente ejemplo de código, se muestra cómo utilizar `suspend-processes`.

AWS CLI

Suspensión de los procesos de escalado automático

En este ejemplo, se suspende el proceso de escalado especificado para el grupo de escalado automático especificado.

```
aws autoscaling suspend-processes \
    --auto-scaling-group-name my-asg \
    --scaling-processes AlarmNotification
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Suspending and resuming scaling processes en la Guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte SuspendProcesses en la Referencia de comandos de la AWS CLI.

`terminate-instance-in-auto-scaling-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `terminate-instance-in-auto-scaling-group`.

AWS CLI

Finalización de una instancia en su grupo de escalado automático

En este ejemplo, se termina la instancia especificada del grupo de escalado automático especificado sin actualizar el tamaño del grupo. Amazon EC2 Auto Scaling lanza una instancia de remplazo una vez que finalice la instancia especificada.

```
aws autoscaling terminate-instance-in-auto-scaling-group \
    --instance-id i-061c63c5eb45f0416 \
    --no-should-decrement-desired-capacity
```

Salida:

```
{
    "Activities": [
        {
            "ActivityId": "8c35d601-793c-400c-fcd0-f64a27530df7",
            "AutoScalingGroupName": "my-asg",
            "Description": "Terminating EC2 instance: i-061c63c5eb45f0416",
            "Cause": "",
            "StartTime": "2020-10-31T20:34:25.680Z",
            "StatusCode": "InProgress",
            "Progress": 0,
            "Details": "{\"Subnet ID\":\"subnet-6194ea3b\",\"Availability Zone\":
\"us-west-2c\"}"
        }
    ]
}
```

- Para obtener información sobre la API, consulte TerminateInstanceInAutoScalingGroup en la Referencia de comandos de la AWS CLI.

`update-auto-scaling-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-auto-scaling-group`.

AWS CLI

Ejemplo 1: Actualización de los límites de tamaño de un grupo de escalado automático

En este ejemplo, se actualiza el grupo de escalado automático especificado con un tamaño mínimo de 2 y un tamaño máximo de 10.

```
aws autoscaling update-auto-scaling-group \
    --auto-scaling-group-name my-asg \
    --min-size 2 \
    --max-size 10
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Establecer límites de capacidad para su grupo de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 2: Adición de comprobaciones de estado de Elastic Load Balancing y especificar qué zonas de disponibilidad y subredes se deben utilizar

En este ejemplo, se actualiza el grupo de escalado automático especificado para añadir comprobaciones de estado de Elastic Load Balancing. Este comando también actualiza el valor de `--vpc-zone-identifier` con una lista de ID de subred en varias zonas de disponibilidad.

```
aws autoscaling update-auto-scaling-group \
    --auto-scaling-group-name my-asg \
    --health-check-type ELB \
    --health-check-grace-period 600 \
    --vpc-zone-identifier "subnet-5ea0c127,subnet-6194ea3b,subnet-c934b782"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Elastic Load Balancing y Amazon EC2 Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 3: actualización del grupo con ubicación y la política de terminación

En este ejemplo, se actualizan el grupo con ubicación y la política de terminación que se van a utilizar.

```
aws autoscaling update-auto-scaling-group \
    --auto-scaling-group-name my-asg \
    --placement-group my-placement-group \
    --termination-policies "OldestInstance"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Grupos de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 4: uso de la versión más reciente de la plantilla de lanzamiento

En este ejemplo, se actualiza el grupo de escalado automático para utilizar la versión más reciente de la plantilla de lanzamiento.

```
aws autoscaling update-auto-scaling-group \
    --auto-scaling-group-name my-asg \
    --launch-template LaunchTemplateId=lt-1234567890abcde12,Version='$Latest'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Plantillas de lanzamiento en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 5: uso de una versión específica de la plantilla de lanzamiento

En este ejemplo, se actualiza el grupo de escalado automático especificado para utilizar una versión específica de una plantilla de lanzamiento en lugar de la versión más reciente o predeterminada.

```
aws autoscaling update-auto-scaling-group \
    --auto-scaling-group-name my-asg \
    --launch-template LaunchTemplateName=my-template-for-auto-scaling,Version='2'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Plantillas de lanzamiento en la Guía del usuario de Amazon EC2 Auto Scaling.

Ejemplo 6: definición de una política de instancias mixtas y habilitar el reequilibrio de la capacidad

En este ejemplo, se actualiza el grupo de escalado automático especificado para que utilice una política de instancias mixtas y se habilita el reequilibrio de la capacidad. Esta estructura le permite especificar grupos con capacidades bajo demanda y de spot y utilizar distintas plantillas de lanzamiento para diferentes arquitecturas.

```
aws autoscaling update-auto-scaling-group \
    --cli-input-json file://~/config.json
```

Contenido de `config.json`:

```
{
    "AutoScalingGroupName": "my-asg",
    "CapacityRebalance": true,
    "MixedInstancesPolicy": {
        "LaunchTemplate": {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template-for-x86",
                "Version": "$Latest"
            },
            "Overrides": [
                {
                    "InstanceType": "c6g.large",
                    "LaunchTemplateSpecification": {
                        "LaunchTemplateName": "my-launch-template-for-arm",
                        "Version": "$Latest"
                    }
                },
                {
                    "InstanceType": "c5.large"
                },
                {
                    "InstanceType": "c5a.large"
                }
            ]
        },
        "InstancesDistribution": {
            "OnDemandPercentageAboveBaseCapacity": 50,
            "SpotAllocationStrategy": "capacity-optimized"
        }
    }
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte la sección sobre Grupos de escalado automático con varios tipos de instancia y opciones de compra en la guía del usuario de Amazon EC2 Auto Scaling.

- Para obtener información sobre la API, consulte UpdateAutoScalingGroup en la Referencia de comandos de la AWS CLI.

Ejemplos de Auto Scaling Plans que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar situaciones comunes usando AWS Command Line Interface con planes de escalado automático.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-scaling-plan`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-scaling-plan`.

AWS CLI

Creación de un plan de escalado

En el siguiente ejemplo de `create-scaling-plan`, se crea un plan de escalado denominado `my-scaling-plan` mediante un archivo JSON ya creado (denominado config.json). La estructura del plan de escalado incluye una instrucción de escalado para un grupo de escalado automático denominado `my-asg`. Especifica la propiedad `TagFilters` como el origen de la aplicación y permite el escalado predictivo y el escalado dinámico.

```
aws autoscaling-plans create-scaling-plan \
    --scaling-plan-name my-scaling-plan \
    --cli-input-json file://~/config.json
```

Contenido del archivo `config.json`:

```
{
    "ApplicationSource": {
        "TagFilters": [
            {
                "Key": "purpose",
                "Values": [
                    "my-application"
                ]
            }
        ]
    },
    "ScalingInstructions": [
        {
            "ServiceNamespace": "autoscaling",
            "ResourceId": "autoScalingGroup/my-asg",
            "ScalableDimension": "autoscaling:autoScalingGroup:DesiredCapacity",
            "ScheduledActionBufferTime": 300,
            "PredictiveScalingMaxCapacityBehavior":
 "SetForecastCapacityToMaxCapacity",
            "PredictiveScalingMode": "ForecastAndScale",
            "PredefinedLoadMetricSpecification": {
                "PredefinedLoadMetricType": "ASGTotalCPUUtilization"
            },
            "ScalingPolicyUpdateBehavior": "ReplaceExternalPolicies",
            "MinCapacity": 1,
            "MaxCapacity": 4,
            "TargetTrackingConfigurations": [
                {
                    "PredefinedScalingMetricSpecification": {
                        "PredefinedScalingMetricType": "ASGAverageCPUUtilization"
                    },
                    "TargetValue": 50
                }
            ]
        }
    ]
}
```

Salida:

```
{
"ScalingPlanVersion": 1
```

```
}
```

Para obtener más información, consulte la Guía del usuario de AWS Auto Scaling de aplicaciones.

- Para obtener información sobre la API, consulte CreateScalingPlan en la Referencia de comandos de la AWS CLI.

`delete-scaling-plan`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-scaling-plan`.

AWS CLI

Eliminación de un plan de escalado

En el siguiente ejemplo de `delete-scaling-plan`, se elimina el plan de escalado especificado.

```
aws autoscaling-plans delete-scaling-plan \
    --scaling-plan-name my-scaling-plan \
    --scaling-plan-version 1
```

Este comando no genera ninguna salida.

Para obtener más información, consulte la Guía del usuario de AWS Auto Scaling de aplicaciones.

- Para obtener información sobre la API, consulte DeleteScalingPlan en la Referencia de comandos de la AWS CLI.

`describe-scaling-plan-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-scaling-plan-resources`.

AWS CLI

Descripción de los recursos escalables de un plan de escalado

En el siguiente de `describe-scaling-plan-resources`, se muestran detalles sobre el único recurso escalable (un grupo de escalado automático) que está asociado al plan de escalado especificado.

```
aws autoscaling-plans describe-scaling-plan-resources \
    --scaling-plan-name my-scaling-plan \
    --scaling-plan-version 1
```

Salida:

```
{
    "ScalingPlanResources": [
        {
            "ScalableDimension": "autoscaling:autoScalingGroup:DesiredCapacity",
            "ScalingPlanVersion": 1,
            "ResourceId": "autoScalingGroup/my-asg",
            "ScalingStatusCode": "Active",
            "ScalingStatusMessage": "Target tracking scaling policies have been
 applied to the resource.",
            "ScalingPolicies": [
                {
                    "PolicyName": "AutoScaling-my-asg-b1ab65ae-4be3-4634-bd64-
c7471662b251",
                    "PolicyType": "TargetTrackingScaling",
                    "TargetTrackingConfiguration": {
                        "PredefinedScalingMetricSpecification": {
                            "PredefinedScalingMetricType":
 "ALBRequestCountPerTarget",
                            "ResourceLabel": "app/my-alb/f37c06a68c1748aa/
targetgroup/my-target-group/6d4ea56ca2d6a18d"
                        },
                        "TargetValue": 40.0
                    }
                }
            ],
            "ServiceNamespace": "autoscaling",
            "ScalingPlanName": "my-scaling-plan"
        }
    ]
}
```

Para obtener más información, consulte What Is AWS Auto Scaling? en la Guía del usuario de AWS Auto Scaling de aplicaciones.

- Para obtener información sobre la API, consulte DescribeScalingPlanResources en la Referencia de comandos de la AWS CLI.

`describe-scaling-plans`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-scaling-plans`.

AWS CLI

Descripción de un plan de escalado

En el siguiente ejemplo de `describe-scaling-plans`, se muestran los detalles del plan de escalado especificado.

```
aws autoscaling-plans describe-scaling-plans \
    --scaling-plan-names scaling-plan-with-asg-and-ddb
```

Salida:

```
{
    "ScalingPlans": [
        {
            "LastMutatingRequestTime": 1565388443.963,
            "ScalingPlanVersion": 1,
            "CreationTime": 1565388443.963,
            "ScalingInstructions": [
                {
                    "ScalingPolicyUpdateBehavior": "ReplaceExternalPolicies",
                    "ScalableDimension":
 "autoscaling:autoScalingGroup:DesiredCapacity",
                    "TargetTrackingConfigurations": [
                        {
                            "PredefinedScalingMetricSpecification": {
                                "PredefinedScalingMetricType":
 "ASGAverageCPUUtilization"
                            },
                            "TargetValue": 50.0,
                            "EstimatedInstanceWarmup": 300,
                            "DisableScaleIn": false
                        }
                    ],
                    "ResourceId": "autoScalingGroup/my-asg",
                    "DisableDynamicScaling": false,
                    "MinCapacity": 1,
                    "ServiceNamespace": "autoscaling",
                    "MaxCapacity": 10
```

```
                },
                {
                    "ScalingPolicyUpdateBehavior": "ReplaceExternalPolicies",
                    "ScalableDimension": "dynamodb:table:ReadCapacityUnits",
                    "TargetTrackingConfigurations": [
                        {
                            "PredefinedScalingMetricSpecification": {
                                "PredefinedScalingMetricType":
"DynamoDBReadCapacityUtilization"
                            },
                            "TargetValue": 50.0,
                            "ScaleInCooldown": 60,
                            "DisableScaleIn": false,
                            "ScaleOutCooldown": 60
                        }
                    ],
                    "ResourceId": "table/my-table",
                    "DisableDynamicScaling": false,
                    "MinCapacity": 5,
                    "ServiceNamespace": "dynamodb",
                    "MaxCapacity": 10000
                },
                {
                    "ScalingPolicyUpdateBehavior": "ReplaceExternalPolicies",
                    "ScalableDimension": "dynamodb:table:WriteCapacityUnits",
                    "TargetTrackingConfigurations": [
                        {
                            "PredefinedScalingMetricSpecification": {
                                "PredefinedScalingMetricType":
"DynamoDBWriteCapacityUtilization"
                            },
                            "TargetValue": 50.0,
                            "ScaleInCooldown": 60,
                            "DisableScaleIn": false,
                            "ScaleOutCooldown": 60
                        }
                    ],
                    "ResourceId": "table/my-table",
                    "DisableDynamicScaling": false,
                    "MinCapacity": 5,
                    "ServiceNamespace": "dynamodb",
                    "MaxCapacity": 10000
                }
            ],
```

```
            "ApplicationSource": {
                "TagFilters": [
                    {
                        "Values": [
                            "my-application-id"
                        ],
                        "Key": "application"
                    }
                ]
            },
            "StatusStartTime": 1565388455.836,
            "ScalingPlanName": "scaling-plan-with-asg-and-ddb",
            "StatusMessage": "Scaling plan has been created and applied to all
 resources.",
            "StatusCode": "Active"
        }
    ]
}
```

Para obtener más información, consulte What Is AWS Auto Scaling? en la Guía del usuario de AWS Auto Scaling de aplicaciones.

- Para obtener información sobre la API, consulte DescribeScalingPlans en la Referencia de comandos de la AWS CLI.

`get-scaling-plan-resource-forecast-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-scaling-plan-resource-forecast-data`.

AWS CLI

Recuperación de los datos de previsión de carga

En este ejemplo, se recuperan los datos de previsión de carga de un recurso escalable (un grupo de escalado automático) que está asociado al plan de escalado especificado.

```
aws autoscaling-plans get-scaling-plan-resource-forecast-data \
    --scaling-plan-name my-scaling-plan \
    --scaling-plan-version 1 \
    --service-namespace "autoscaling" \
    --resource-id autoScalingGroup/my-asg \
    --scalable-dimension "autoscaling:autoScalingGroup:DesiredCapacity" \
```

```
    --forecast-data-type "LoadForecast" \
    --start-time "2019-08-30T00:00:00Z" \
    --end-time "2019-09-06T00:00:00Z"
```

Salida:

```
{
    "Datapoints": [...]
}
```

Para obtener más información, consulte What Is AWS Auto Scaling? en la Guía del usuario de AWS Auto Scaling de aplicaciones.

- Para obtener información sobre la API, consulte GetScalingPlanResourceForecastData en la Referencia de comandos de la AWS CLI.

`update-scaling-plan`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-scaling-plan`.

AWS CLI

Actualización de un plan de escalado

En el siguiente ejemplo de `update-scaling-plan`, se modifica la métrica de escalado de un grupo de escalado automático en el plan de escalado especificado.

```
aws autoscaling-plans update-scaling-plan \
    --scaling-plan-name my-scaling-plan \
    --scaling-plan-version 1 \
    --scaling-instructions
 '{"ScalableDimension":"autoscaling:autoScalingGroup:DesiredCapacity","ResourceId":"autoScal
my-asg","ServiceNamespace":"autoscaling","TargetTrackingConfigurations":
[{"PredefinedScalingMetricSpecification":
 {"PredefinedScalingMetricType":"ALBRequestCountPerTarget","ResourceLabel":"app/my-
alb/f37c06a68c1748aa/targetgroup/my-target-
group/6d4ea56ca2d6a18d"},"TargetValue":40.0}],"MinCapacity": 1,"MaxCapacity": 10}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte What Is AWS Auto Scaling? en la Guía del usuario de AWS Auto Scaling de aplicaciones.

- Para obtener información sobre la API, consulte UpdateScalingPlan en la Referencia de comandos de la AWS CLI.

AWS Backup Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS Backup.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-backup-plan`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-backup-plan`.

AWS CLI

Cómo crear un plan de copias de seguridad

En el siguiente ejemplo de `create-backup-plan`, se crea el plan de copias de seguridad especificado con un período de retención de 35 días.

```
aws backup create-backup-plan \
--backup-plan "{\"BackupPlanName\":\"Example-Backup-Plan\",\"Rules\":[{\"RuleName\":
\"DailyBackups\",\"ScheduleExpression\":\"cron(0 5 ? * * *)\",\"StartWindowMinutes
\":480,\"TargetBackupVaultName\":\"Default\",\"Lifecycle\":{\"DeleteAfterDays
\":35}}]}"
```

Salida:

```
{
```

```
    "BackupPlanId": "1fa3895c-a7f5-484a-a371-2dd6a1a9f729",
    "BackupPlanArn": "arn:aws:backup:us-west-2:123456789012:backup-plan:1fa3895c-
a7f5-484a-a371-2dd6a1a9f729",
    "CreationDate": 1568928754.747,
    "VersionId": "ZjQ2ZTI5YWQtZDg5Yi00MzYzLWJmZTAtMDI1MzhlMDhjYjEz"
}
```

Para obtener más información, consulte Creating a Backup Plan en la Guía para desarrolladores de AWS Backup.

- Para obtener información sobre la API, consulte CreateBackupPlan en la Referencia de comandos de la AWS CLI.

`create-backup-vault`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-backup-vault`.

AWS CLI

Cómo crear un almacén de copias de seguridad

En el siguiente ejemplo de `create-backup-vault`, se crea un almacén de copia de seguridad con el nombre especificado.

```
aws backup create-backup-vault
    --backup-vault-name sample-vault
```

Este comando no genera ninguna salida. Salida:

```
{
    "BackupVaultName": "sample-vault",
    "BackupVaultArn": "arn:aws:backup:us-west-2:123456789012:backup-vault:sample-
vault",
    "CreationDate": 1568928338.385
}
```

Para obtener más información, consulte Creating a Backup Vault en la Guía para desarrolladores AWS Backup.

- Para obtener información sobre la API, consulte CreateBackupVault en la Referencia de comandos de la AWS CLI.

`get-backup-plan-from-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-backup-plan-from-template`.

AWS CLI

Para obtener un plan de copias de seguridad existente a partir de una plantilla

En el siguiente ejemplo de `get-backup-plan-from-template`, se obtiene un plan de copias de seguridad existente a partir de una plantilla que especifica una copia de seguridad diaria con un período de retención de 35 días.

```
aws backup get-backup-plan-from-template \
    --backup-plan-template-id "87c0c1ef-254d-4180-8fef-2e76a2c38aaa"
```

Salida:

```
{
    "BackupPlanDocument": {
        "Rules": [
            {
                "RuleName": "DailyBackups",
                "ScheduleExpression": "cron(0 5 ? * * *)",
                "StartWindowMinutes": 480,
                "Lifecycle": {
                    "DeleteAfterDays": 35
                }
            }
        ]
    }
}
```

Para obtener más información, consulte Creating a Backup Plan en la Guía para desarrolladores de AWS Backup.

- Para obtener información sobre la API, consulte GetBackupPlanFromTemplate en la Referencia de comandos de la AWS CLI.

`get-backup-plan`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-backup-plan`.

AWS CLI

Para obtener los detalles de un plan de copias de seguridad

En el siguiente ejemplo de `get-backup-plan`, se muestran los detalles del plan de copias de seguridad especificado.

```
aws backup get-backup-plan \
    --backup-plan-id "fcbf5d8f-bd77-4f3a-9c97-f24fb3d373a5"
```

Salida:

```
{
    "BackupPlan": {
        "BackupPlanName": "Example-Backup-Plan",
        "Rules": [
            {
                "RuleName": "DailyBackups",
                "TargetBackupVaultName": "Default",
                "ScheduleExpression": "cron(0 5 ? * * *)",
                "StartWindowMinutes": 480,
                "CompletionWindowMinutes": 10080,
                "Lifecycle": {
                    "DeleteAfterDays": 35
                },
                "RuleId": "70e0ccdc-e9df-4e83-82ad-c1e5a9471cc3"
            }
        ]
    },
    "BackupPlanId": "fcbf5d8f-bd77-4f3a-9c97-f24fb3d373a5",
    "BackupPlanArn": "arn:aws:backup:us-west-2:123456789012:backup-plan:fcbf5d8f-
bd77-4f3a-9c97-f24fb3d373a5",
    "VersionId": "NjQ2ZTZkODktMGVhNy00MmQ0LWE4YjktZTkwNTQ3OTkyYTcw",
    "CreationDate": 1568926091.57
}
```

Para obtener más información, consulte Creating a Backup Plan en la Guía para desarrolladores de AWS Backup.

- Para obtener información sobre la API, consulte GetBackupPlan en la Referencia de comandos de la AWS CLI.

`list-backup-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-backup-jobs`.

AWS CLI

Ejemplo 1: cómo obtener una lista de todos los trabajos de copia de seguridad

En el siguiente de `list-backup-jobs`, se muestran los metadatos sobre los trabajos de copia de seguridad de la cuenta de AWS.

```
aws backup list-backup-jobs
```

Salida:

```
{
    "BackupJobs": [
        {
            "BackupJobId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "BackupVaultName": "Default",
            "BackupVaultArn": "arn:aws:backup:us-west-2:123456789012:backup-
vault:Default",
            "ResourceArn": "arn:aws:ec2:us-west-2:123456789012:instance/
i-12345678901234567",
            "CreationDate": 1600721892.929,
            "State": "CREATED",
            "PercentDone": "0.0",
            "IamRoleArn": "arn:aws:iam::123456789012:role/service-role/
AWSBackupDefaultServiceRole",
            "StartBy": 1600725492.929,
            "ResourceType": "EC2"
        },
        {
            "BackupJobId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "BackupVaultName": "Default",
            "BackupVaultArn": "arn:aws:backup:us-west-2:123456789012:backup-
vault:Default",
            "RecoveryPointArn": "arn:aws:backup:us-west-2:123456789012:recovery-
point:a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "ResourceArn": "arn:aws:elasticfilesystem:us-west-2:123456789012:file-
system/fs-12345678",
            "CreationDate": 1600721724.77,
            "CompletionDate": 1600721744.488,
```

```
            "State": "COMPLETED",
            "PercentDone": "100.0",
            "BackupSizeInBytes": 71,
            "IamRoleArn": "arn:aws:iam::123456789012:role/service-role/
AWSBackupDefaultServiceRole",
            "StartBy": 1600725324.77,
            "ResourceType": "EFS"
        }
    ]
}
```

Para obtener más información, consulte Creating a Backup en la Guía para desarrolladores de AWS Backup.

Ejemplo 2: cómo obtener una lista de los trabajos de copia de seguridad completados

En el siguiente de `list-backup-jobs`, se muestran los metadatos sobre los trabajos de copia de seguridad completados de la cuenta de AWS.

```
aws backup list-backup-jobs \
    --by-state COMPLETED
```

Salida:

```
{
    "BackupJobs": [
        {
            "BackupJobId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "BackupVaultName": "Default",
            "BackupVaultArn": "arn:aws:backup:us-west-2:123456789012:backup-
vault:Default",
            "RecoveryPointArn": "arn:aws:backup:us-west-2:123456789012:recovery-
point:a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "ResourceArn": "arn:aws:elasticfilesystem:us-west-2:123456789012:file-
system/fs-12345678",
            "CreationDate": 1600721724.77,
            "CompletionDate": 1600721744.488,
            "State": "COMPLETED",
            "PercentDone": "100.0",
            "BackupSizeInBytes": 71,
            "IamRoleArn": "arn:aws:iam::123456789012:role/service-role/
AWSBackupDefaultServiceRole",
```

```
            "StartBy": 1600725324.77,
            "ResourceType": "EFS"
        }
    ]
}
```

Para obtener más información, consulte Creating a Backup en la Guía para desarrolladores de AWS Backup.

- Para obtener información sobre la API, consulte ListBackupJobs en la Referencia de comandos de la AWS CLI.

AWS Batch Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS Batch.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`cancel-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-job`.

AWS CLI

Para cancelar un trabajo

En este ejemplo, se cancela un trabajo con el ID de trabajo especificado.

Comando:

```
aws batch cancel-job --job-id bcf0b186-a532-4122-842e-2ccab8d54efb --
reason "Cancelling job."
```

- Para obtener más información sobre la API, consulte CancelJob en la Referencia de comandos de la AWS CLI.

`create-compute-environment`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-compute-environment`.

AWS CLI

Cómo crear un entorno informático administrado con instancias bajo demanda

En este ejemplo, se crea un entorno informático administrado con tipos de instancias C4 específicos que se lanzan bajo demanda. El entorno informático se denomina C4OnDemand.

Comando:

```
aws batch create-compute-environment --cli-input-json file://<path_to_json_file>/
C4OnDemand.json
```

Formato de archivo JSON:

```
{
  "computeEnvironmentName": "C4OnDemand",
  "type": "MANAGED",
  "state": "ENABLED",
  "computeResources": {
    "type": "EC2",
    "minvCpus": 0,
    "maxvCpus": 128,
    "desiredvCpus": 48,
    "instanceTypes": [
      "c4.large",
      "c4.xlarge",
      "c4.2xlarge",
      "c4.4xlarge",
      "c4.8xlarge"
    ],
```

```
    "subnets": [
      "subnet-220c0e0a",
      "subnet-1a95556d",
      "subnet-978f6dce"
    ],
    "securityGroupIds": [
      "sg-cf5093b2"
    ],
    "ec2KeyPair": "id_rsa",
    "instanceRole": "ecsInstanceRole",
    "tags": {
      "Name": "Batch Instance - C4OnDemand"
    }
  },
  "serviceRole": "arn:aws:iam::012345678910:role/AWSBatchServiceRole"
}
```

Salida:

```
{
    "computeEnvironmentName": "C4OnDemand",
    "computeEnvironmentArn": "arn:aws:batch:us-east-1:012345678910:compute-
environment/C4OnDemand"
}
```

Creación de un entorno informático administrado con instancias de spot

En este ejemplo, se crea un entorno informático administrado con el tipo de instancia M4 que se lanza cuando el precio de puja de spot es igual o inferior al 20 % del precio bajo demanda del tipo de instancia. El entorno informático se denomina M4Spot.

Comando:

```
aws batch create-compute-environment --cli-input-json file://<path_to_json_file>/
M4Spot.json
```

Formato de archivo JSON:

```
{
  "computeEnvironmentName": "M4Spot",
  "type": "MANAGED",
```

```
  "state": "ENABLED",
  "computeResources": {
    "type": "SPOT",
    "spotIamFleetRole": "arn:aws:iam::012345678910:role/aws-ec2-spot-fleet-role",
    "minvCpus": 0,
    "maxvCpus": 128,
    "desiredvCpus": 4,
    "instanceTypes": [
      "m4"
    ],
    "bidPercentage": 20,
    "subnets": [
      "subnet-220c0e0a",
      "subnet-1a95556d",
      "subnet-978f6dce"
    ],
    "securityGroupIds": [
      "sg-cf5093b2"
    ],
    "ec2KeyPair": "id_rsa",
    "instanceRole": "ecsInstanceRole",
    "tags": {
      "Name": "Batch Instance - M4Spot"
    }
  },
  "serviceRole": "arn:aws:iam::012345678910:role/AWSBatchServiceRole"
}
```

Salida:

```
{
    "computeEnvironmentName": "M4Spot",
    "computeEnvironmentArn": "arn:aws:batch:us-east-1:012345678910:compute-
environment/M4Spot"
}
```

- Para obtener información sobre la API, consulte CreateComputeEnvironment en la Referencia de comandos de la AWS CLI.

`create-job-queue`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-job-queue`.

AWS CLI

Creación de una cola de trabajos de baja prioridad con un único entorno informático

En este ejemplo, se crea una cola de trabajos llamada LowPriority que utiliza el entorno informático M4Spot.

Comando:

```
aws batch create-job-queue --cli-input-json file://<path_to_json_file>/
LowPriority.json
```

Formato de archivo JSON:

```
{
  "jobQueueName": "LowPriority",
  "state": "ENABLED",
  "priority": 10,
  "computeEnvironmentOrder": [
    {
      "order": 1,
      "computeEnvironment": "M4Spot"
    }
  ]
}
```

Salida:

```
{
    "jobQueueArn": "arn:aws:batch:us-east-1:012345678910:job-queue/LowPriority",
    "jobQueueName": "LowPriority"
}
```

Creación de una cola de trabajos de alta prioridad con dos entornos informáticos

En este ejemplo, se crea una cola de trabajos denominada HighPriority que utiliza el entorno informático C4OnDemand con un orden de 1 y el entorno informático M4Spot con un orden de 2. El programador intentará colocar primero los trabajos del entorno informático C4OnDemand.

Comando:

```
aws batch create-job-queue --cli-input-json file://<path_to_json_file>/
HighPriority.json
```

Formato de archivo JSON:

```
{
  "jobQueueName": "HighPriority",
  "state": "ENABLED",
  "priority": 1,
  "computeEnvironmentOrder": [
    {
      "order": 1,
      "computeEnvironment": "C4OnDemand"
    },
    {
      "order": 2,
      "computeEnvironment": "M4Spot"
    }
  ]
}
```

Salida:

```
{
    "jobQueueArn": "arn:aws:batch:us-east-1:012345678910:job-queue/HighPriority",
    "jobQueueName": "HighPriority"
}
```

- Para obtener información sobre la API, consulte CreateJobQueue en la Referencia de comandos de la AWS CLI.

`delete-compute-environment`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-compute-environment`.

AWS CLI

Eliminación de entornos informáticos

En este ejemplo, se elimina el entorno informático P2OnDemand.

Comando:

```
aws batch delete-compute-environment --compute-environment P2OnDemand
```

- Para obtener detalles sobre la API, consulte DeleteComputeEnvironment en la Referencia de comandos de la AWS CLI.

`delete-job-queue`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-job-queue`.

AWS CLI

Eliminación de una cola de trabajos

En este ejemplo, se elimina la cola de trabajos GPGPU.

Comando:

```
aws batch delete-job-queue --job-queue GPGPU
```

- Para obtener información sobre la API, consulte DeleteJobQueue en la Referencia de comandos de la AWS CLI.

`deregister-job-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-job-definition`.

AWS CLI

Anulación del registro de una definición de trabajo

En este ejemplo se anula el registro de una definición de trabajo llamada sleep10.

Comando:

```
aws batch deregister-job-definition --job-definition sleep10
```

- Para obtener información sobre la API, consulte DeregisterJobDefinition en la Referencia de comandos de la AWS CLI.

`describe-compute-environments`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-compute-environments`.

AWS CLI

Descripción de entornos informáticos

En este ejemplo, se describe el entorno informático de P2onDemand.

Comando:

```
aws batch describe-compute-environments --compute-environments P2OnDemand
```

Salida:

```
{
    "computeEnvironments": [
        {
            "status": "VALID",
            "serviceRole": "arn:aws:iam::012345678910:role/AWSBatchServiceRole",
            "computeEnvironmentArn": "arn:aws:batch:us-east-1:012345678910:compute-
environment/P2OnDemand",
            "computeResources": {
                "subnets": [
                    "subnet-220c0e0a",
                    "subnet-1a95556d",
                    "subnet-978f6dce"
                ],
                "tags": {
                    "Name": "Batch Instance - P2OnDemand"
                },
                "desiredvCpus": 48,
                "minvCpus": 0,
                "instanceTypes": [
                    "p2"
                ],
                "securityGroupIds": [
                    "sg-cf5093b2"
                ],
                "instanceRole": "ecsInstanceRole",
                "maxvCpus": 128,
                "type": "EC2",
```

```
                "ec2KeyPair": "id_rsa"
            },
            "statusReason": "ComputeEnvironment Healthy",
            "ecsClusterArn": "arn:aws:ecs:us-east-1:012345678910:cluster/
P2OnDemand_Batch_2c06f29d-d1fe-3a49-879d-42394c86effc",
            "state": "ENABLED",
            "computeEnvironmentName": "P2OnDemand",
            "type": "MANAGED"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeComputeEnvironments en la Referencia de comandos de la AWS CLI.

`describe-job-definitions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-job-definitions`.

AWS CLI

Descripción de las definiciones de trabajos activas

En este ejemplo, se describen todas las definiciones de trabajos activas.

Comando:

```
aws batch describe-job-definitions --status ACTIVE
```

Salida:

```
{
    "jobDefinitions": [
        {
            "status": "ACTIVE",
            "jobDefinitionArn": "arn:aws:batch:us-east-1:012345678910:job-
definition/sleep60:1",
            "containerProperties": {
                "mountPoints": [],
                "parameters": {},
                "image": "busybox",
                "environment": {},
```

```
                "vcpus": 1,
                "command": [
                    "sleep",
                    "60"
                ],
                "volumes": [],
                "memory": 128,
                "ulimits": []
            },
            "type": "container",
            "jobDefinitionName": "sleep60",
            "revision": 1
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeJobDefinitions en la Referencia de comandos de la AWS CLI.

`describe-job-queues`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-job-queues`.

AWS CLI

Descripción de una cola de trabajos

En este ejemplo, se describe la cola de trabajos HighPriority.

Comando:

```
aws batch describe-job-queues --job-queues HighPriority
```

Salida:

```
{
    "jobQueues": [
        {
            "status": "VALID",
            "jobQueueArn": "arn:aws:batch:us-east-1:012345678910:job-queue/
HighPriority",
            "computeEnvironmentOrder": [
```

```
                {
                    "computeEnvironment": "arn:aws:batch:us-
east-1:012345678910:compute-environment/C4OnDemand",
                    "order": 1
                }
            ],
            "statusReason": "JobQueue Healthy",
            "priority": 1,
            "state": "ENABLED",
            "jobQueueName": "HighPriority"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeJobQueues en la Referencia de comandos de la AWS CLI.

`describe-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-jobs`.

AWS CLI

Descripción de un trabajo

En el siguiente ejemplo de `describe-jobs`, se describe el trabajo con el ID de trabajo especificado.

```
aws batch describe-jobs \
    --jobs bcf0b186-a532-4122-842e-2ccab8d54efb
```

Salida:

```
{
    "jobs": [
        {
            "status": "SUBMITTED",
            "container": {
                "mountPoints": [],
                "image": "busybox",
                "environment": [],
                "vcpus": 1,
```

```
                "command": [
                    "sleep",
                    "60"
                ],
                "volumes": [],
                "memory": 128,
                "ulimits": []
            },
            "parameters": {},
            "jobDefinition": "arn:aws:batch:us-east-1:012345678910:job-definition/
sleep60:1",
            "jobQueue": "arn:aws:batch:us-east-1:012345678910:job-queue/
HighPriority",
            "jobId": "bcf0b186-a532-4122-842e-2ccab8d54efb",
            "dependsOn": [],
            "jobName": "example",
            "createdAt": 1480483387803
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeJobs en la Referencia de comandos de la AWS CLI.

`list-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-jobs`.

AWS CLI

Generación de una lista de los trabajos en ejecución

En este ejemplo, se genera una lista de los trabajos en ejecución de la cola de trabajos HighPriority.

Comando:

```
aws batch list-jobs --job-queue HighPriority
```

Salida:

```
{
```

```
    "jobSummaryList": [
        {
            "jobName": "example",
            "jobId": "e66ff5fd-a1ff-4640-b1a2-0b0a142f49bb"
        }
    ]
}
```

Generación de una lista de trabajos enviados

En este ejemplo, se genera una lista de los trabajos de la cola de trabajos HighPriority que tienen el estado de trabajo SUBMITED.

Comando:

```
aws batch list-jobs --job-queue HighPriority --job-status SUBMITTED
```

Salida:

```
{
    "jobSummaryList": [
        {
            "jobName": "example",
            "jobId": "68f0c163-fbd4-44e6-9fd1-25b14a434786"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListJobs en la Referencia de comandos de la AWS CLI.

`register-job-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-job-definition`.

AWS CLI

Registro de una definición de trabajo

En este ejemplo, se registra una definición de trabajo de un trabajo de contenedor sencillo.

Comando:

```
aws batch register-job-definition --job-definition-name sleep30 --type container --
container-properties '{ "image": "busybox", "vcpus": 1, "memory": 128, "command":
 [ "sleep", "30"]}'
```

Salida:

```
{
    "jobDefinitionArn": "arn:aws:batch:us-east-1:012345678910:job-definition/
sleep30:1",
    "jobDefinitionName": "sleep30",
    "revision": 1
}
```

- Para obtener más información sobre la API, consulte RegisterJobDefinition en Referencia de comandos de la AWS CLI.

`submit-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `submit-job`.

AWS CLI

Envío de un trabajo

En este ejemplo, se envía un trabajo de contenedor sencillo denominado example a la cola de trabajos HighPriority.

Comando:

```
aws batch submit-job --job-name example --job-queue HighPriority  --job-
definition sleep60
```

Salida:

```
{
    "jobName": "example",
    "jobId": "876da822-4198-45f2-a252-6cea32512ea8"
}
```

- Para obtener más información sobre la API, consulte SubmitJob en Referencia de comandos de la AWS CLI.

`terminate-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `terminate-job`.

AWS CLI

Terminación de un trabajo

En este ejemplo, se termina el trabajo con el ID de trabajo especificado.

Comando:

```
aws batch terminate-job --job-id 61e743ed-35e4-48da-b2de-5c8333821c84 --
reason "Terminating job."
```

- Para obtener información sobre la API, consulte TerminateJob en la Referencia de comandos de la AWS CLI.

`update-compute-environment`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-compute-environment`.

AWS CLI

Actualización de un entorno informático

En este ejemplo, se deshabilita el entorno informático P2OnDemand para que se pueda eliminar.

Comando:

```
aws batch update-compute-environment --compute-environment P2OnDemand --
state DISABLED
```

Salida:

```
{
    "computeEnvironmentName": "P2OnDemand",
    "computeEnvironmentArn": "arn:aws:batch:us-east-1:012345678910:compute-
environment/P2OnDemand"
}
```

- Para obtener información sobre la API, consulte UpdateComputeEnvironment en la Referencia de comandos de la AWS CLI.

`update-job-queue`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-job-queue`.

AWS CLI

Actualización de una cola de trabajos

En este ejemplo, se deshabilita una cola de trabajos para que se pueda eliminar.

Comando:

```
aws batch update-job-queue --job-queue GPGPU --state DISABLED
```

Salida:

```
{
    "jobQueueArn": "arn:aws:batch:us-east-1:012345678910:job-queue/GPGPU",
    "jobQueueName": "GPGPU"
}
```

- Para obtener información sobre la API, consulte UpdateJobQueue en la Referencia de comandos de la AWS CLI.

AWS Budgets Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS Budgets.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-budget`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-budget`.

AWS CLI

Creación de un presupuesto de costos y uso

En el siguiente comando de `create-budget`, se crea un presupuesto de costos y uso.

```
aws budgets create-budget \
    --account-id 111122223333 \
    --budget file://budget.json \
    --notifications-with-subscribers file://notifications-with-subscribers.json
```

Contenido de `budget.json`:

```
{
    "BudgetLimit": {
        "Amount": "100",
        "Unit": "USD"
    },
    "BudgetName": "Example Tag Budget",
    "BudgetType": "COST",
    "CostFilters": {
        "TagKeyValue": [
            "user:Key$value1",
            "user:Key$value2"
        ]
    },
    "CostTypes": {
        "IncludeCredit": true,
        "IncludeDiscount": true,
        "IncludeOtherSubscription": true,
        "IncludeRecurring": true,
        "IncludeRefund": true,
        "IncludeSubscription": true,
        "IncludeSupport": true,
        "IncludeTax": true,
```

```
        "IncludeUpfront": true,
        "UseBlended": false
    },
    "TimePeriod": {
        "Start": 1477958399,
        "End": 3706473600
    },
    "TimeUnit": "MONTHLY"
}
```

Contenido de `notifications-with-subscribers.json`:

```
[
    {
        "Notification": {
            "ComparisonOperator": "GREATER_THAN",
            "NotificationType": "ACTUAL",
            "Threshold": 80,
            "ThresholdType": "PERCENTAGE"
        },
        "Subscribers": [
            {
                "Address": "example@example.com",
                "SubscriptionType": "EMAIL"
            }
        ]
    }
]
```

- Para obtener información sobre la API, consulte CreateBudget en la Referencia de comandos de la AWS CLI.

`create-notification`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-notification`.

AWS CLI

Creación de una notificación para el presupuesto de costos y uso especificado

En este ejemplo, se crea una notificación para el presupuesto de costos y uso especificado.

Comando:

```
aws budgets create-notification --account-id 111122223333 --budget-name "Example
 Budget" --
notification NotificationType=ACTUAL,ComparisonOperator=GREATER_THAN,Threshold=80,ThresholdT
 --subscriber SubscriptionType=EMAIL,Address=example@example.com
```

- Para obtener información sobre la API, consulte CreateNotification en la Referencia de comandos de la AWS CLI.

`create-subscriber`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-subscriber`.

AWS CLI

Creación de un suscriptor para una notificación asociada a un presupuesto de costos y uso

En este ejemplo, se crea un suscriptor para la notificación especificada.

Comando:

```
aws budgets create-subscriber --account-id 111122223333 --budget-name "Example
 Budget" --
notification NotificationType=ACTUAL,ComparisonOperator=GREATER_THAN,Threshold=80,ThresholdT
 --subscriber SubscriptionType=EMAIL,Address=example@example.com
```

- Para obtener información sobre la API, consulte CreateSubscriber en la Referencia de comandos de la AWS CLI.

`delete-budget`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-budget`.

AWS CLI

Eliminación de un presupuesto de costos y uso

En este ejemplo, se elimina el presupuesto de costos y uso especificado.

Comando:

```
aws budgets delete-budget --account-id 111122223333 --budget-name "Example Budget"
```

- Para obtener información sobre la API, consulte DeleteBudget en la Referencia de comandos de la AWS CLI.

`delete-notification`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-notification`.

AWS CLI

Eliminación de una notificación de un presupuesto

En este ejemplo, se elimina la notificación especificada del presupuesto especificado.

Comando:

```
aws budgets delete-notification --account-id 111122223333 --budget-name "Example
 Budget" --
notification NotificationType=ACTUAL,ComparisonOperator=GREATER_THAN,Threshold=80,ThresholdT
```

- Para obtener información sobre la API, consulte DeleteNotification en la Referencia de comandos de la AWS CLI.

`delete-subscriber`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-subscriber`.

AWS CLI

Eliminación de un suscriptor de una notificación

En este ejemplo, se elimina el suscriptor especificado de la notificación especificada.

Comando:

```
aws budgets delete-subscriber --account-id 111122223333 --budget-name "Example
 Budget" --
notification NotificationType=ACTUAL,ComparisonOperator=GREATER_THAN,Threshold=80,ThresholdT
 --subscriber SubscriptionType=EMAIL,Address=example@example.com
```

- Para obtener información sobre la API, consulte DeleteSubscriber en la Referencia de comandos de la AWS CLI.

describe-budget

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-budget`.

AWS CLI

Recuperación de un presupuesto asociado a una cuenta

En este ejemplo, se recupera el presupuesto de costos y uso especificado.

Comando:

```
aws budgets describe-budget --account-id 111122223333 --budget-name "Example Budget"
```

Salida:

```
{
   "Budget": {
       "CalculatedSpend": {
           "ForecastedSpend": {
               "Amount": "2641.548000000000229192664846777915954589843 75",
               "Unit": "USD"
           },
           "ActualSpend": {
               "Amount": "604.456000000000017280399333685636520385742 1875",
               "Unit": "USD"
           }
       },
       "BudgetType": "COST",
       "BudgetLimit": {
           "Amount": "100",
           "Unit": "USD"
       },
       "BudgetName": "Example Budget",
       "CostTypes": {
           "IncludeOtherSubscription": true,
           "IncludeUpfront": true,
           "IncludeRefund": true,
           "UseBlended": false,
           "IncludeDiscount": true,
           "UseAmortized": false,
           "IncludeTax": true,
           "IncludeCredit": true,
```

```
            "IncludeSupport": true,
            "IncludeRecurring": true,
            "IncludeSubscription": true
        },
        "TimeUnit": "MONTHLY",
        "TimePeriod": {
            "Start": 1477958399.0,
            "End": 3706473600.0
        },
        "CostFilters": {
            "AZ": [
                "us-east-1"
            ]
        }
    }
}
```

- Para obtener información sobre la API, consulte DescribeBudget en la Referencia de comandos de la AWS CLI.

`describe-budgets`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-budgets`.

AWS CLI

Recuperación de los presupuestos asociados a una cuenta

En este ejemplo, se recuperan los presupuestos de costos y uso de una cuenta.

Comando:

```
aws budgets describe-budgets --account-id 111122223333 --max-results 20
```

Salida:

```
{
    "Budgets": [
        {
            "CalculatedSpend": {
                "ForecastedSpend": {
```

```
                "Amount": "2641.548000000000229192664846777915954589843 75",
                "Unit": "USD"
            },
            "ActualSpend": {
                "Amount": "604.456000000000017280399333685636520385742 1875",
                "Unit": "USD"
            }
        },
        "BudgetType": "COST",
        "BudgetLimit": {
            "Amount": "100",
            "Unit": "USD"
        },
        "BudgetName": "Example Budget",
        "CostTypes": {
            "IncludeOtherSubscription": true,
            "IncludeUpfront": true,
            "IncludeRefund": true,
            "UseBlended": false,
            "IncludeDiscount": true,
            "UseAmortized": false,
            "IncludeTax": true,
            "IncludeCredit": true,
            "IncludeSupport": true,
            "IncludeRecurring": true,
            "IncludeSubscription": true
        },
        "TimeUnit": "MONTHLY",
        "TimePeriod": {
            "Start": 1477958399.0,
            "End": 3706473600.0
        },
        "CostFilters": {
            "AZ": [
                "us-east-1"
            ]
        }
    }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeBudgets en la Referencia de comandos de la AWS CLI.

describe-notifications-for-budget

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-notifications-for-budget`.

AWS CLI

Recuperación de las notificaciones de un presupuesto

En este ejemplo, se recuperan las notificaciones de un presupuesto de costos y uso.

Comando:

```
aws budgets describe-notifications-for-budget --account-id 111122223333 --budget-name "Example Budget" --max-results 5
```

Salida:

```
{
   "Notifications": [
       {
           "Threshold": 80.0,
           "ComparisonOperator": "GREATER_THAN",
           "NotificationType": "ACTUAL"
       }
   ]
}
```

- Para obtener información sobre la API, consulte DescribeNotificationsForBudget en la Referencia de comandos de la AWS CLI.

describe-subscribers-for-notification

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-subscribers-for-notification`.

AWS CLI

Recuperación de los suscriptores de una notificación de presupuesto

En este ejemplo, se recuperan los suscriptores de una notificación de presupuesto de costos y uso.

Comando:

```
aws budgets describe-subscribers-for-notification --
account-id 111122223333 --budget-name "Example Budget" --
notification NotificationType=ACTUAL,ComparisonOperator=GREATER_THAN,Threshold=80,ThresholdT
 --max-results 5
```

Salida:

```
{
   "Subscribers": [
       {
           "SubscriptionType": "EMAIL",
           "Address": "example2@example.com"
       },
       {
           "SubscriptionType": "EMAIL",
           "Address": "example@example.com"
       }
   ]
}
```

- Para obtener información sobre la API, consulte DescribeSubscribersForNotification en la Referencia de comandos de la AWS CLI.

`update-budget`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-budget`.

AWS CLI

Sustitución de un presupuesto por un presupuesto de costos y uso

En este ejemplo, se sustituye un presupuesto de costos y uso por otro nuevo.

Comando:

```
aws budgets update-budget --account-id 111122223333 --new-budget file://new-
budget.json
```

new-budget.json:

```
{
    "BudgetLimit": {
       "Amount": "100",
       "Unit": "USD"
    },
    "BudgetName": "Example Budget",
    "BudgetType": "COST",
    "CostFilters": {
       "AZ" : [ "us-east-1" ]
    },
    "CostTypes": {
       "IncludeCredit": false,
       "IncludeDiscount": true,
       "IncludeOtherSubscription": true,
       "IncludeRecurring": true,
       "IncludeRefund": true,
       "IncludeSubscription": true,
       "IncludeSupport": true,
       "IncludeTax": true,
       "IncludeUpfront": true,
       "UseBlended": false,
       "UseAmortized": true
    },
    "TimePeriod": {
       "Start": 1477958399,
       "End": 3706473600
    },
    "TimeUnit": "MONTHLY"
}
```

- Para obtener información sobre la API, consulte UpdateBudget en la Referencia de comandos de la AWS CLI.

`update-notification`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-notification`.

AWS CLI

Creación de una notificación para un presupuesto de costos y uso

En este ejemplo, se sustituye una notificación del 80 % de un presupuesto de costos y uso por una notificación del 90 %.

Comando:

```
aws budgets update-notification --account-id 111122223333 --budget-name "Example
 Budget" --old-notification
  NotificationType=ACTUAL,ComparisonOperator=GREATER_THAN,Threshold=80,ThresholdType=PERCENT
 --new-notification
  NotificationType=ACTUAL,ComparisonOperator=GREATER_THAN,Threshold=90,ThresholdType=PERCENT
```

- Para obtener información acerca de la API, consulte UpdateNotification en la Referencia de comandos de la AWS CLI.

`update-subscriber`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-subscriber`.

AWS CLI

Sustitución de un suscriptor de un presupuesto de costos y uso

En este ejemplo, se sustituye un suscriptor de un presupuesto de costos y uso.

Comando:

```
aws budgets update-subscriber --account-id 111122223333 --budget-name "Example
 Budget" --
notification NotificationType=ACTUAL,ComparisonOperator=GREATER_THAN,Threshold=80,ThresholdT
 --old-subscriber SubscriptionType=EMAIL,Address=example@example.com --new-
subscriber SubscriptionType=EMAIL,Address=example2@example.com
```

- Para obtener información sobre la API, consulte UpdateSubscriber en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon Chime que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar situaciones comunes usando la AWS Command Line Interface con Amazon Chime.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-phone-number-with-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-phone-number-with-user`.

AWS CLI

Asociación de un número de teléfono a un usuario

En el siguiente ejemplo de `associate-phone-number-with-user`, se asocia el número de teléfono especificado a un usuario.

```
aws chime associate-phone-number-with-user \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --user-id 1ab2345c-67de-8901-f23g-45h678901j2k \
    --e164-phone-number "+12065550100"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing User Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte AssociatePhoneNumberWithUser en la Referencia de comandos de la AWS CLI.

`associate-signin-delegate-groups-with-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-signin-delegate-groups-with-account`.

AWS CLI

Para asociar grupos de delegados que inicien sesión

En el siguiente ejemplo de `associate-signin-delegate-groups-with-account`, se asocia el grupo de delegados de inicio de sesión especificado a la cuenta de Amazon Chime especificada.

```
aws chime associate-signin-delegate-groups-with-account \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --signin-delegate-groups GroupName=my_users
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing User Access and Permissions en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte AssociateSigninDelegateGroupsWithAccount en la Referencia de comandos de la AWS CLI.

`batch-create-room-membership`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-create-room-membership`.

AWS CLI

Creación de suscripciones a varias salas

En el siguiente ejemplo de `batch-create-room-membership`, se agregan varios usuarios a una sala de chat como miembros de dicha sala de chat. También se asignan roles de administrador y miembro a los usuarios.

```
aws chime batch-create-room-membership \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --room-id abcd1e2d-3e45-6789-01f2-3g45h67i890j \
    --membership-item-list "MemberId=1ab2345c-67de-8901-
f23g-45h678901j2k,Role=Administrator" "MemberId=2ab2345c-67de-8901-
f23g-45h678901j2k,Role=Member"
```

Salida:

```
{
    "ResponseMetadata": {
        "RequestId": "169ba401-d886-475f-8b3f-e01eac6fadfb",
        "HTTPStatusCode": 201,
        "HTTPHeaders": {
            "x-amzn-requestid": "169ba401-d886-475f-8b3f-e01eac6fadfb",
            "content-type": "application/json",
            "content-length": "13",
            "date": "Mon, 02 Dec 2019 22:46:58 GMT",
            "connection": "keep-alive"
        },
        "RetryAttempts": 0
    },
    "Errors": []
}
```

Para obtener más información, consulte Creating a Chat Room en la Guía del usuario de Amazon Chime.

- Para obtener información sobre la API, consulte BatchCreateRoomMembership en la Referencia de comandos de la AWS CLI.

`batch-delete-phone-number`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-delete-phone-number`.

AWS CLI

Eliminación de varios números de teléfono

En el siguiente ejemplo de `batch-delete-phone-number`, se eliminan todos los números de teléfono especificados.

```
aws chime batch-delete-phone-number \
    --phone-number-ids "%2B12065550100" "%2B12065550101"
```

Este comando no genera ninguna salida. Salida:

```
{
    "PhoneNumberErrors": []
}
```

Para obtener más información, consulte Working with Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener más información sobre la API, consulte BatchDeletePhoneNumber en la Referencia de comandos de la AWS CLI.

`batch-suspend-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-suspend-user`.

AWS CLI

Suspensión de varios usuarios

En el siguiente ejemplo de `batch-suspend-user`, se suspende a los usuarios indicados de la cuenta de Amazon Chime especificada.

```
aws chime batch-suspend-user \
    --account-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --user-id-list "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE" "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE" "a1b2c3d4-5678-90ab-cdef-44444EXAMPLE"
```

Salida:

```
{
    "UserErrors": []
}
```

- Para obtener información sobre de la API, consulte BatchSuspendUser en la Referencia de comandos de la AWS CLI

`batch-unsuspend-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-unsuspend-user`.

AWS CLI

Anulación de la suspensión de varios usuarios

En el siguiente ejemplo de `batch-unsuspend-user`, se anula la suspensión anterior de los usuarios indicados en la cuenta de Amazon Chime especificada.

```
aws chime batch-unsuspend-user \
    --account-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --user-id-list "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE" "a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE" "a1b2c3d4-5678-90ab-cdef-44444EXAMPLE"
```

Salida:

```
{
    "UserErrors": []
}
```

- Para obtener información sobre la API, consulte BatchUnsuspendUser en la Referencia de comandos de la AWS CLI.

`batch-update-phone-number`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-update-phone-number`.

AWS CLI

Actualización de varios tipos de productos de números de teléfono al mismo tiempo

En el siguiente ejemplo de `batch-update-phone-number`, se actualizan los tipos de producto de todos los números de teléfono especificados.

```
aws chime batch-update-phone-number \
    --update-phone-number-request-items PhoneNumberId=
%2B12065550100,ProductType=BusinessCalling PhoneNumberId=
%2B12065550101,ProductType=BusinessCalling
```

Salida:

```
{
    "PhoneNumberErrors": []
}
```

Actualización de varios nombres de llamadas de números de teléfono al mismo tiempo

En el siguiente ejemplo de `batch-update-phone-number`, se actualizan los nombres de llamadas de todos los números de teléfono especificados.

```
aws chime batch-update-phone-number \
    --update-phone-number-request-items PhoneNumberId=
%2B14013143874,CallingName=phonenumber1 PhoneNumberId=
%2B14013144061,CallingName=phonenumber2
```

Salida:

```
{
    "PhoneNumberErrors": []
}
```

Para obtener más información, consulte Working with Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte BatchUpdatePhoneNumber en la Referencia de comandos de la AWS CLI.

`batch-update-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-update-user`.

AWS CLI

Actualización de varios usuarios con un solo comando

En el siguiente ejemplo de `batch-update-user`, se actualiza el `LicenseType` de cada uno de los usuarios indicados en la cuenta de Amazon Chime especificada.

```
aws chime batch-update-user \
    --account-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE
    --update-user-request-items "UserId=a1b2c3d4-5678-90ab-
cdef-22222EXAMPLE,LicenseType=Basic" "UserId=a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE,LicenseType=Basic"
```

Salida:

```
{
    "UserErrors": []
}
```

- Para obtener detalles sobre la API, consulte BatchUpdateUser en la Referencia de comandos de la AWS CLI.

`create-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-account`.

AWS CLI

Creación de una cuenta

En el siguiente ejemplo de `create-account`, se crea una cuenta de Amazon Chime en la cuenta de AWS del administrador.

```
aws chime create-account \
    --name MyChimeAccount
```

Salida:

```
{
    "Account": {
        "AwsAccountId": "111122223333",
        "AccountId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
        "Name": "MyChimeAccount",
        "AccountType": "Team",
        "CreatedTimestamp": "2019-01-04T17:11:22.003Z",
        "DefaultLicense": "Pro",
        "SupportedLicenses": [
            "Basic",
            "Pro"
        ],
        "SigninDelegateGroups": [
            {
                "GroupName": "myGroup"
            },
        ]
    }
}
```

Para obtener más información, consulte Getting Started en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte CreateAccount en la Referencia de comandos de la AWS CLI.

`create-bot`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-bot`.

AWS CLI

Creación de un bot de Amazon Chime

En el siguiente ejemplo de `create-bot`, se crea un bot para la cuenta de Amazon Chime Enterprise especificada.

```
aws chime create-bot \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --display-name "myBot" \
    --domain "example.com"
```

Salida:

```
{
    "Bot": {
        "BotId": "123abcd4-5ef6-789g-0h12-34j56789012k",
        "UserId": "123abcd4-5ef6-789g-0h12-34j56789012k",
        "DisplayName": "myBot (Bot)",
        "BotType": "ChatBot",
        "Disabled": false,
        "CreatedTimestamp": "2019-09-09T18:05:56.749Z",
        "UpdatedTimestamp": "2019-09-09T18:05:56.749Z",
        "BotEmail": "myBot-chimebot@example.com",
        "SecurityToken": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
    }
}
```

Para obtener más información, consulte Integrate a Chat Bot with Amazon Chime en la Guía para desarrolladores de Amazon Chime.

- Para obtener información sobre la API, consulte CreateBot en la Referencia de comandos de la AWS CLI.

`create-phone-number-order`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-phone-number-order`.

AWS CLI

Creación de un pedido de números de teléfono

En el siguiente ejemplo de `create-phone-number-order`, se crea un pedido de números de teléfono para los números de teléfono especificados.

```
aws chime create-phone-number-order \
    --product-type VoiceConnector \
    --e164-phone-numbers "+12065550100" "+12065550101" "+12065550102"
```

Salida:

```
{
    "PhoneNumberOrder": {
        "PhoneNumberOrderId": "abc12345-de67-89f0-123g-h45i678j9012",
        "ProductType": "VoiceConnector",
        "Status": "Processing",
        "OrderedPhoneNumbers": [
            {
                "E164PhoneNumber": "+12065550100",
                "Status": "Processing"
            },
            {
               "E164PhoneNumber": "+12065550101",
               "Status": "Processing"
            },
            {
              "E164PhoneNumber": "+12065550102",
              "Status": "Processing"
            }
        ],
        "CreatedTimestamp": "2019-08-09T21:35:21.427Z",
        "UpdatedTimestamp": "2019-08-09T21:35:22.408Z"
    }
}
```

Para obtener más información, consulte Working with Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte CreatePhoneNumberOrder en la Referencia de comandos de la AWS CLI.

`create-room-membership`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-room-membership`.

AWS CLI

Creación de una suscripción de sala

El siguiente ejemplo de `create-room-membership`, se agrega el usuario especificado a la sala de chat como miembro de dicha sala de chat.

```
aws chime create-room-membership \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --room-id abcd1e2d-3e45-6789-01f2-3g45h67i890j \
    --member-id 1ab2345c-67de-8901-f23g-45h678901j2k
```

Salida:

```
{
    "RoomMembership": {
        "RoomId": "abcd1e2d-3e45-6789-01f2-3g45h67i890j",
        "Member": {
            "MemberId": "1ab2345c-67de-8901-f23g-45h678901j2k",
            "MemberType": "User",
            "Email": "janed@example.com",
            "FullName": "Jane Doe",
            "AccountId": "12a3456b-7c89-012d-3456-78901e23fg45"
        },
        "Role": "Member",
        "InvitedBy": "arn:aws:iam::111122223333:user/alejandro",
        "UpdatedTimestamp": "2019-12-02T22:36:41.969Z"
    }
}
```

Para obtener más información, consulte Creating a Chat Room en la Guía del usuario de Amazon Chime.

- Para obtener información sobre la API, consulte CreateRoomMembership en la Referencia de comandos de la AWS CLI.

`create-room`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-room`.

AWS CLI

Creación de una sala de chat

En el siguiente ejemplo de `create-room`, se crea una sala de chat para la cuenta de Amazon Chime especificada.

```
aws chime create-room \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --name chatRoom
```

Salida:

```
{
    "Room": {
        "RoomId": "abcd1e2d-3e45-6789-01f2-3g45h67i890j",
        "Name": "chatRoom",
        "AccountId": "12a3456b-7c89-012d-3456-78901e23fg45",
        "CreatedBy": "arn:aws:iam::111122223333:user/alejandro",
        "CreatedTimestamp": "2019-12-02T22:29:31.549Z",
        "UpdatedTimestamp": "2019-12-02T22:29:31.549Z"
    }
}
```

Para obtener más información, consulte Creating a Chat Room en la Guía del usuario de Amazon Chime.

- Para obtener información sobre la API, consulte CreateRoom en la Referencia de comandos de la AWS CLI.

`create-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-user`.

AWS CLI

Para crear un perfil de usuario para un dispositivo compartido

En el siguiente ejemplo de `create-user`, se crea un perfil de dispositivo compartido para la dirección de correo electrónico especificada.

```
aws chime create-user \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --email roomdevice@example.com \
    --user-type SharedDevice
```

Salida:

```
{
    "User": {
        "UserId": "1ab2345c-67de-8901-f23g-45h678901j2k",
        "AccountId": "12a3456b-7c89-012d-3456-78901e23fg45",
        "PrimaryEmail": "roomdevice@example.com",
        "DisplayName": "Room Device",
        "LicenseType": "Pro",
        "UserType": "SharedDevice",
        "UserRegistrationStatus": "Registered",
        "RegisteredOn": "2020-01-15T22:38:09.806Z",
        "AlexaForBusinessMetadata": {
            "IsAlexaForBusinessEnabled": false
        }
    }
}
```

Para obtener más información, consulte Preparing for Setup en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte CreateUser en la Referencia de comandos de la AWS CLI.

`delete-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-account`.

AWS CLI

Eliminación de una cuenta

En el siguiente ejemplo de `delete-account`, se elimina la cuenta especificada.

```
aws chime delete-account --account-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting Your Account en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte DeleteAccount en la Referencia de comandos de AWS CLI.

`delete-phone-number`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-phone-number`.

AWS CLI

Eliminación de un número de teléfono

En el siguiente ejemplo de `delete-phone-number`, se pasa el número de teléfono especificado a la cola de eliminación.

```
aws chime delete-phone-number \
    --phone-number-id "+12065550100"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte DeletePhoneNumber en la Referencia de comandos de la AWS CLI.

`delete-room-membership`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-room-membership`.

AWS CLI

Eliminación de la suscripción de un usuario a una sala de chat

En el siguiente ejemplo de `delete-room-membership`, se elimina al miembro especificado de la sala de chat indicada.

```
aws chime delete-room-membership \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --room-id abcd1e2d-3e45-6789-01f2-3g45h67i890j \
    --member-id 1ab2345c-67de-8901-f23g-45h678901j2k
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creating a Chat Room en la Guía del usuario de Amazon Chime.

- Para obtener información sobre la API, consulte DeleteRoomMembership en la Referencia de comandos de la AWS CLI.

`delete-room`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-room`.

AWS CLI

Eliminación de una sala de chat

En el siguiente ejemplo de `delete-room`, se borra la sala de chat especificada y se eliminan las suscripciones a dicha sala de chat.

```
aws chime delete-room \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --room-id abcd1e2d-3e45-6789-01f2-3g45h67i890j
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creating a Chat Room en la Guía del usuario de Amazon Chime.

- Para obtener información sobre la API, consulte DeleteRoom en la Referencia de comandos de la AWS CLI.

`disassociate-phone-number-from-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-phone-number-from-user`.

AWS CLI

Desasociación de un número de teléfono de un usuario

En el siguiente ejemplo de `disassociate-phone-number-from-user`, se desasocia un número de teléfono del usuario especificado.

```
aws chime disassociate-phone-number-from-user \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --user-id 1ab2345c-67de-8901-f23g-45h678901j2k
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing User Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte DisassociatePhoneNumberFromUser en la Referencia de comandos de la AWS CLI.

`disassociate-signin-delegate-groups-from-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-signin-delegate-groups-from-account`.

AWS CLI

Desasociación de grupos de delegados de inicio de sesión

En el siguiente ejemplo de `disassociate-signin-delegate-groups-from-account`, se desasocia el grupo de delegados de inicio de sesión especificado de la cuenta de Amazon Chime especificada.

```
aws chime disassociate-signin-delegate-groups-from-account \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --group-names "my_users"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing User Access and Permissions en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte DisassociateSigninDelegateGroupsFromAccount en la Referencia de comandos de la AWS CLI.

`get-account-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-account-settings`.

AWS CLI

Para obtener la configuración de una cuenta

En el siguiente ejemplo de `get-account-settings`, se obtiene la configuración de la cuenta especificada.

```
aws chime get-account-settings --account-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE
```

Salida:

```
{
    "AccountSettings": {
        "DisableRemoteControl": false,
        "EnableDialOut": false
    }
}
```

Para obtener más información, consulte Managing Your Amazon Chime Accounts en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte GetAccountSettings en la Referencia de comandos de la AWS CLI.

`get-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-account`.

AWS CLI

Para obtener los detalles de una cuenta

En siguiente ejemplo de `get-account`, se obtienen los detalles de la cuenta de Amazon Chime especificada.

```
aws chime get-account \
    --account-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE
```

Salida:

```
{
    "Account": {
        "AwsAccountId": "111122223333",
        "AccountId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
        "Name": "EnterpriseDirectory",
        "AccountType": "EnterpriseDirectory",
        "CreatedTimestamp": "2018-12-20T18:38:02.181Z",
        "DefaultLicense": "Pro",
        "SupportedLicenses": [
            "Basic",
            "Pro"
        ],
        "SigninDelegateGroups": [
            {
                "GroupName": "myGroup"
            },
        ]
    }
}
```

Para obtener más información, consulte Managing Your Amazon Chime Accounts en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte GetAccount en la Referencia de comandos de la AWS CLI.

`get-bot`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bot`.

AWS CLI

Para obtener los detalles de un bot

En el siguiente ejemplo de `get-bot`, se muestran los detalles del bot especificado.

```
aws chime get-bot \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --bot-id 123abcd4-5ef6-789g-0h12-34j56789012k
```

Salida:

```
{
    "Bot": {
        "BotId": "123abcd4-5ef6-789g-0h12-34j56789012k",
        "UserId": "123abcd4-5ef6-789g-0h12-34j56789012k",
        "DisplayName": "myBot (Bot)",
        "BotType": "ChatBot",
        "Disabled": false,
        "CreatedTimestamp": "2019-09-09T18:05:56.749Z",
        "UpdatedTimestamp": "2019-09-09T18:05:56.749Z",
        "BotEmail": "myBot-chimebot@example.com",
        "SecurityToken": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
    }
}
```

Para obtener más información, consulte Update Chat Bots en la Guía para desarrolladores de Amazon Chime.

- Para obtener información sobre la API, consulte GetBot en la Referencia de comandos de la AWS CLI.

`get-global-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-global-settings`.

AWS CLI

Para obtener la configuración global

En el siguiente ejemplo de `get-global-settings`, se obtienen los nombres de los buckets de S3 que se utilizan para almacenar los registros de detalles de llamadas de los Amazon Chime Business Calling y Amazon Chime Voice Connector asociados a la cuenta de AWS del administrador.

```
aws chime get-global-settings
```

Salida:

```
{
    "BusinessCalling": {
        "CdrBucket": "s3bucket"
    },
    "VoiceConnector": {
        "CdrBucket": "s3bucket"
    }
}
```

Para obtener más información, consulte Managing Global Settings en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte GetGlobalSettings en la Referencia de comandos de la AWS CLI.

`get-phone-number-order`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-phone-number-order`.

AWS CLI

Para obtener los detalles de un pedido de números de teléfono

En el siguiente ejemplo de `get-phone-number-order`, se muestran los detalles del pedido de números de teléfono especificado.

```
aws chime get-phone-number-order \
    --phone-number-order-id abc12345-de67-89f0-123g-h45i678j9012
```

Salida:

```
{
    "PhoneNumberOrder": {
        "PhoneNumberOrderId": "abc12345-de67-89f0-123g-h45i678j9012",
        "ProductType": "VoiceConnector",
        "Status": "Partial",
        "OrderedPhoneNumbers": [
```

```
            {
              "E164PhoneNumber": "+12065550100",
              "Status": "Acquired"
            },
            {
                "E164PhoneNumber": "+12065550101",
                "Status": "Acquired"
            },
            {
                "E164PhoneNumber": "+12065550102",
                "Status": "Failed"
            }
        ],
        "CreatedTimestamp": "2019-08-09T21:35:21.427Z",
        "UpdatedTimestamp": "2019-08-09T21:35:31.926Z"
    }
}
```

Para obtener más información, consulte Working with Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte GetPhoneNumberOrder en la Referencia de comandos de la AWS CLI.

`get-phone-number-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-phone-number-settings`.

AWS CLI

Para obtener el nombre de una llamada saliente

En el siguiente ejemplo de `get-phone-number-settings`, se obtiene el nombre de llamada saliente predeterminada de la cuenta de AWS del usuario iniciador.

```
aws chime get-phone-number-settings
```

Este comando no genera ninguna salida. Salida:

```
{
    "CallingName": "myName",
    "CallingNameUpdatedTimestamp": "2019-10-28T18:56:42.911Z"
```

```
}
```

Para obtener más información, consulte Working with Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte GetPhoneNumberSettings en la Referencia de comandos de la AWS CLI.

`get-phone-number`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-phone-number`.

AWS CLI

Para obtener detalles del número de teléfono

En el siguiente ejemplo de `get-phone-number`, se muestran los detalles del número de teléfono especificado.

```
aws chime get-phone-number \
    --phone-number-id +12065550100
```

Salida:

```
{
    "PhoneNumber": {
        "PhoneNumberId": "%2B12065550100",
        "E164PhoneNumber": "+12065550100",
        "Type": "Local",
        "ProductType": "VoiceConnector",
        "Status": "Unassigned",
        "Capabilities": {
            "InboundCall": true,
            "OutboundCall": true,
            "InboundSMS": true,
            "OutboundSMS": true,
            "InboundMMS": true,
            "OutboundMMS": true
        },
       "Associations": [
            {
                "Value": "abcdef1ghij2klmno3pqr4",
```

```
                "Name": "VoiceConnectorId",
                "AssociatedTimestamp": "2019-10-28T18:40:37.453Z"
            }
        ],
        "CallingNameStatus": "UpdateInProgress",
        "CreatedTimestamp": "2019-08-09T21:35:21.445Z",
        "UpdatedTimestamp": "2019-08-09T21:35:31.745Z"
    }
}
```

Para obtener más información, consulte Working with Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte GetPhoneNumber en la Referencia de comandos de la AWS CLI.

`get-room`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-room`.

AWS CLI

Para obtener los detalles sobre una sala de chat

En el siguiente ejemplo de `get-room`, se muestran los detalles de la sala de chat especificada.

```
aws chime get-room \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --room-id abcd1e2d-3e45-6789-01f2-3g45h67i890j
```

Salida:

```
{
    "Room": {
        "RoomId": "abcd1e2d-3e45-6789-01f2-3g45h67i890j",
        "Name": "chatRoom",
        "AccountId": "12a3456b-7c89-012d-3456-78901e23fg45",
        "CreatedBy": "arn:aws:iam::111122223333:user/alejandro",
        "CreatedTimestamp": "2019-12-02T22:29:31.549Z",
        "UpdatedTimestamp": "2019-12-02T22:29:31.549Z"
    }
}
```

Para obtener más información, consulte Creating a Chat Room en la Guía del usuario de Amazon Chime.

- Para obtener información sobre la API, consulte GetRoom en la Referencia de comandos de la AWS CLI.

`get-user-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-user-settings`.

AWS CLI

Para obtener la configuración del usuario

En el siguiente ejemplo de `get-user-settings`, se muestra la configuración de usuario especificada.

```
aws chime get-user-settings \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --user-id 1ab2345c-67de-8901-f23g-45h678901j2k
```

Salida:

```
{
    "UserSettings": {
        "Telephony": {
            "InboundCalling": true,
            "OutboundCalling": true,
            "SMS": true
        }
    }
}
```

Para obtener más información, consulte Managing User Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte GetUserSettings en la Referencia de comandos de la AWS CLI.

`get-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-user`.

AWS CLI

Para obtener los detalles de un usuario

En el siguiente ejemplo de `get-user`, se obtienen los detalles del usuario especificado.

```
aws chime get-user \
    --account-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --user-id a1b2c3d4-5678-90ab-cdef-22222EXAMPLE
```

Salida:

```
{
    "User": {
        "UserId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
        "AccountId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
        "PrimaryEmail": "marthar@example.com",
        "DisplayName": "Martha Rivera",
        "LicenseType": "Pro",
        "UserRegistrationStatus": "Registered",
        "RegisteredOn": "2018-12-20T18:45:25.231Z",
        "InvitedOn": "2018-12-20T18:45:25.231Z",
        "AlexaForBusinessMetadata": {
            "IsAlexaForBusinessEnabled": False,
            "AlexaForBusinessRoomArn": "null"
        },
        "PersonalPIN": "XXXXXXXXXX"
    }
}
```

Para obtener más información, consulte Managing Users en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte GetUser en la Referencia de comandos de la AWS CLI.

`invite-users`

En el siguiente ejemplo de código, se muestra cómo utilizar `invite-users`.

AWS CLI

Invitación a los usuarios a unirse a Amazon Chime

En el siguiente ejemplo de `invite-users`, se envía un correo electrónico para invitar a un usuario a la cuenta de Amazon Chime especificada.

```
aws chime invite-users \
    --account-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --user-email-list "alejandror@example.com" "janed@example.com"
```

Salida:

```
{
    "Invites": [
        {
            "InviteId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
            "Status": "Pending",
            "EmailAddress": "alejandror@example.com",
            "EmailStatus": "Sent"
        }
        {
            "InviteId": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
            "Status": "Pending",
            "EmailAddress": "janed@example.com",
            "EmailStatus": "Sent"
        }
    ]
}
```

Para obtener más información, consulte Inviting and Suspending Users en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte InviteUsers en la Referencia de comandos de la AWS CLI.

`list-accounts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-accounts`.

AWS CLI

Generación de una lista de cuentas

En el siguiente ejemplo de `list-accounts`, se genera una lista de las cuentas de Amazon Chime en la cuenta de AWS del administrador.

```
aws chime list-accounts
```

Salida:

```
{
    "Accounts": [
        {
            "AwsAccountId": "111122223333",
            "AccountId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "Name": "First Chime Account",
            "AccountType": "EnterpriseDirectory",
            "CreatedTimestamp": "2018-12-20T18:38:02.181Z",
            "DefaultLicense": "Pro",
            "SupportedLicenses": [
                "Basic",
                "Pro"
            ],
            "SigninDelegateGroups": [
                {
                    "GroupName": "myGroup"
                },
            ]
        },
        {
            "AwsAccountId": "111122223333",
            "AccountId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
            "Name": "Second Chime Account",
            "AccountType": "Team",
            "CreatedTimestamp": "2018-09-04T21:44:22.292Z",
            "DefaultLicense": "Pro",
            "SupportedLicenses": [
                "Basic",
                "Pro"
            ],
            "SigninDelegateGroups": [
                {
                    "GroupName": "myGroup"
                },
            ]
        }
    ]
}
```

Para obtener más información, consulte Managing Your Amazon Chime Accounts en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte ListAccounts en la Referencia de comandos de la AWS CLI.

`list-bots`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-bots`.

AWS CLI

Para obtener una lista de bots

En el siguiente ejemplo de `list-bots`, se obtiene una lista de bots asociada a la cuenta de Amazon Chime Enterprise especificada.

```
aws chime list-bots \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45
```

Salida:

```
{
    "Bot": {
        "BotId": "123abcd4-5ef6-789g-0h12-34j56789012k",
        "UserId": "123abcd4-5ef6-789g-0h12-34j56789012k",
        "DisplayName": "myBot (Bot)",
        "BotType": "ChatBot",
        "Disabled": false,
        "CreatedTimestamp": "2019-09-09T18:05:56.749Z",
        "UpdatedTimestamp": "2019-09-09T18:05:56.749Z",
        "BotEmail": "myBot-chimebot@example.com",
        "SecurityToken": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
    }
}
```

Para obtener más información, consulte Use Chat Bots with Amazon Chime en la Guía para desarrolladores de Amazon Chime.

- Para obtener información sobre la API, consulte ListBots en la Referencia de comandos de la AWS CLI.

`list-phone-number-orders`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-phone-number-orders`.

AWS CLI

Generación de una lista de pedidos de números de teléfono

En el siguiente ejemplo de `list-phone-number-orders`, se genera una lista de los pedidos de números de teléfono asociados a la cuenta de Amazon Chime del administrador.

```
aws chime list-phone-number-orders
```

Salida:

```
{
    "PhoneNumberOrders": [
        {
            "PhoneNumberOrderId": "abc12345-de67-89f0-123g-h45i678j9012",
            "ProductType": "VoiceConnector",
            "Status": "Partial",
            "OrderedPhoneNumbers": [
                {
                    "E164PhoneNumber": "+12065550100",
                    "Status": "Acquired"
                },
                {
                    "E164PhoneNumber": "+12065550101",
                    "Status": "Acquired"
                },
                {
                    "E164PhoneNumber": "+12065550102",
                    "Status": "Failed"
                }
            ],
            "CreatedTimestamp": "2019-08-09T21:35:21.427Z",
            "UpdatedTimestamp": "2019-08-09T21:35:31.926Z"
        }
        {
            "PhoneNumberOrderId": "cba54321-ed76-09f5-321g-h54i876j2109",
            "ProductType": "BusinessCalling",
            "Status": "Partial",
            "OrderedPhoneNumbers": [
```

```
                {
                    "E164PhoneNumber": "+12065550103",
                    "Status": "Acquired"
                },
                {
                    "E164PhoneNumber": "+12065550104",
                    "Status": "Acquired"
                },
                {
                    "E164PhoneNumber": "+12065550105",
                    "Status": "Failed"
                }
            ],
            "CreatedTimestamp": "2019-08-09T21:35:21.427Z",
            "UpdatedTimestamp": "2019-08-09T21:35:31.926Z"
        }
    ]
}
```

Para obtener más información, consulte Working with Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte ListPhoneNumberOrders en la Referencia de comandos de la AWS CLI.

`list-phone-numbers`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-phone-numbers`.

AWS CLI

Generación de una lista de números de teléfono de una cuenta de Amazon Chime

En el siguiente ejemplo de `list-phone-numbers`, se genera una lista de los números de teléfono asociados a la cuenta de Amazon Chime del administrador.

```
aws chime list-phone-numbers
```

Este comando no genera ninguna salida. Salida:

```
{
    "PhoneNumbers": [
        {
```

```
            "PhoneNumberId": "%2B12065550100",
            "E164PhoneNumber": "+12065550100",
            "Type": "Local",
            "ProductType": "VoiceConnector",
            "Status": "Assigned",
            "Capabilities": {
                "InboundCall": true,
                "OutboundCall": true,
                "InboundSMS": true,
                "OutboundSMS": true,
                "InboundMMS": true,
                "OutboundMMS": true
            },
            "Associations": [
                {
                    "Value": "abcdef1ghij2klmno3pqr4",
                    "Name": "VoiceConnectorId",
                    "AssociatedTimestamp": "2019-10-28T18:40:37.453Z"
                }
            ],
            "CallingNameStatus": "UpdateInProgress",
            "CreatedTimestamp": "2019-08-12T22:10:20.521Z",
            "UpdatedTimestamp": "2019-10-28T18:42:07.964Z"
        },
        {
            "PhoneNumberId": "%2B12065550101",
            "E164PhoneNumber": "+12065550101",
            "Type": "Local",
            "ProductType": "VoiceConnector",
            "Status": "Assigned",
            "Capabilities": {
                "InboundCall": true,
                "OutboundCall": true,
                "InboundSMS": true,
                "OutboundSMS": true,
                "InboundMMS": true,
                "OutboundMMS": true
            },
            "Associations": [
                {
                    "Value": "abcdef1ghij2klmno3pqr4",
                    "Name": "VoiceConnectorId",
                    "AssociatedTimestamp": "2019-10-28T18:40:37.511Z"
                }
```

```
            ],
            "CallingNameStatus": "UpdateInProgress",
            "CreatedTimestamp": "2019-08-12T22:10:20.521Z",
            "UpdatedTimestamp": "2019-10-28T18:42:07.960Z"
        }
    ]
}
```

Para obtener más información, consulte Working with Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte ListPhoneNumbers en la Referencia de comandos de la AWS CLI.

`list-room-memberships`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-room-memberships`.

AWS CLI

Generación de una lista de suscripciones a la sala

En el siguiente ejemplo de `list-room-memberships`, se muestra una lista de los detalles de suscripción de la sala de chat especificada.

```
aws chime list-room-memberships \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --room-id abcd1e2d-3e45-6789-01f2-3g45h67i890j
```

Salida:

```
{
    "RoomMemberships": [
        {
            "RoomId": "abcd1e2d-3e45-6789-01f2-3g45h67i890j",
            "Member": {
                "MemberId": "2ab2345c-67de-8901-f23g-45h678901j2k",
                "MemberType": "User",
                "Email": "zhangw@example.com",
                "FullName": "Zhang Wei",
                "AccountId": "12a3456b-7c89-012d-3456-78901e23fg45"
            },
            "Role": "Member",
```

```
            "InvitedBy": "arn:aws:iam::111122223333:user/alejandro",
            "UpdatedTimestamp": "2019-12-02T22:46:58.532Z"
        },
        {
            "RoomId": "abcd1e2d-3e45-6789-01f2-3g45h67i890j",
            "Member": {
                "MemberId": "1ab2345c-67de-8901-f23g-45h678901j2k",
                "MemberType": "User",
                "Email": "janed@example.com",
                "FullName": "Jane Doe",
                "AccountId": "12a3456b-7c89-012d-3456-78901e23fg45"
            },
            "Role": "Administrator",
            "InvitedBy": "arn:aws:iam::111122223333:user/alejandro",
            "UpdatedTimestamp": "2019-12-02T22:46:58.532Z"
        }
    ]
}
```

Para obtener más información, consulte Creating a Chat Room en la Guía del usuario de Amazon Chime.

- Para obtener información sobre la API, consulte ListRoomMemberships en la Referencia de comandos de la AWS CLI.

`list-rooms`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-rooms`.

AWS CLI

Generación de una lista de salas de chat

En el siguiente ejemplo de `list-rooms`, se muestra una lista de salas de chat en la cuenta especificada. La lista se filtra para incluir solo las salas de chat a las que pertenece el miembro especificado.

```
aws chime list-rooms \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --member-id 1ab2345c-67de-8901-f23g-45h678901j2k
```

Salida:

```
{
    "Room": {
        "RoomId": "abcd1e2d-3e45-6789-01f2-3g45h67i890j",
        "Name": "teamRoom",
        "AccountId": "12a3456b-7c89-012d-3456-78901e23fg45",
        "CreatedBy": "arn:aws:iam::111122223333:user/alejandro",
        "CreatedTimestamp": "2019-12-02T22:29:31.549Z",
        "UpdatedTimestamp": "2019-12-02T22:33:19.310Z"
    }
}
```

Para obtener más información, consulte Creating a Chat Room en la Guía del usuario de Amazon Chime.

- Para obtener información sobre la API, consulte ListRooms en la Referencia de comandos de la AWS CLI.

`list-users`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-users`.

AWS CLI

Generación de una lista de los usuarios de una cuenta

En el siguiente ejemplo de `list-users`, se genera una lista de los usuarios de la cuenta de Amazon Chime especificada.

```
aws chime list-users --account-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE
```

Salida:

```
{
    "Users": [
        {
            "UserId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
            "AccountId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "PrimaryEmail": "mariag@example.com",
            "DisplayName": "Maria Garcia",
            "LicenseType": "Pro",
            "UserType": "PrivateUser",
            "UserRegistrationStatus": "Registered",
```

```
            "RegisteredOn": "2018-12-20T18:45:25.231Z"
            "AlexaForBusinessMetadata": {
                "IsAlexaForBusinessEnabled": false
            }
        },
        {
            "UserId": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
            "AccountId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "PrimaryEmail": "richardr@example.com",
            "DisplayName": "Richard Roe",
            "LicenseType": "Pro",
            "UserType": "PrivateUser",
            "UserRegistrationStatus": "Registered",
            "RegisteredOn": "2018-12-20T18:45:45.415Z"
            "AlexaForBusinessMetadata": {
                "IsAlexaForBusinessEnabled": false
            }
        },
        {
            "UserId": "a1b2c3d4-5678-90ab-cdef-44444EXAMPLE",
            "AccountId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "PrimaryEmail": "saanvis@example.com",
            "DisplayName": "Saanvi Sarkar",
            "LicenseType": "Basic",
            "UserType": "PrivateUser",
            "UserRegistrationStatus": "Registered",
            "RegisteredOn": "2018-12-20T18:46:57.747Z"
            "AlexaForBusinessMetadata": {
                "IsAlexaForBusinessEnabled": false
            }
        },
        {
            "UserId": "a1b2c3d4-5678-90ab-cdef-55555EXAMPLE",
            "AccountId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "PrimaryEmail": "wxiulan@example.com",
            "DisplayName": "Wang Xiulan",
            "LicenseType": "Basic",
            "UserType": "PrivateUser",
            "UserRegistrationStatus": "Registered",
            "RegisteredOn": "2018-12-20T18:47:15.390Z"
            "AlexaForBusinessMetadata": {
                "IsAlexaForBusinessEnabled": false
            }
        }
```

```
    ]
}
```

Para obtener más información, consulte Managing Users en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte ListUsers en la Referencia de comandos de la AWS CLI.

`logout-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `logout-user`.

AWS CLI

Cierre de sesión de un usuario

En el siguiente ejemplo de `logout-user`, se cierra la sesión del usuario especificado.

```
aws chime logout-user \
    --account-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --user-id a1b2c3d4-5678-90ab-cdef-22222EXAMPLE
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte LogoutUser en la Referencia de comandos de la AWS CLI.

`regenerate-security-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `regenerate-security-token`.

AWS CLI

Regeneración de un token de seguridad

En el siguiente ejemplo de `regenerate-security-token`, se regenera el token de seguridad del bot especificado.

```
aws chime regenerate-security-token \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
```

```
    --bot-id 123abcd4-5ef6-789g-0h12-34j56789012k
```

Salida:

```
{
    "Bot": {
        "BotId": "123abcd4-5ef6-789g-0h12-34j56789012k",
        "UserId": "123abcd4-5ef6-789g-0h12-34j56789012k",
        "DisplayName": "myBot (Bot)",
        "BotType": "ChatBot",
        "Disabled": false,
        "CreatedTimestamp": "2019-09-09T18:05:56.749Z",
        "UpdatedTimestamp": "2019-09-09T18:05:56.749Z",
        "BotEmail": "myBot-chimebot@example.com",
        "SecurityToken": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
    }
}
```

Para obtener más información, consulte Authenticate Chat Bot Requests en la Guía para desarrolladores de Amazon Chime.

- Para obtener información sobre la API, consulte RegenerateSecurityToken en la Referencia de comandos de la AWS CLI.

`reset-personal-pin`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-personal-pin`.

AWS CLI

Restablecimiento del PIN personal para reuniones de un usuario

En el siguiente ejemplo de `reset-personal-pin`, se restablece el PIN personal para reuniones de un usuario especificado.

```
aws chime reset-personal-pin \
    --account-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE
    --user-id a1b2c3d4-5678-90ab-cdef-22222EXAMPLE
```

Salida:

```
{
```

```
    "User": {
        "UserId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
        "AccountId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
        "PrimaryEmail": "mateo@example.com",
        "DisplayName": "Mateo Jackson",
        "LicenseType": "Pro",
        "UserType": "PrivateUser",
        "UserRegistrationStatus": "Registered",
        "RegisteredOn": "2018-12-20T18:45:25.231Z",
        "AlexaForBusinessMetadata": {
            "IsAlexaForBusinessEnabled": False,
            "AlexaForBusinessRoomArn": "null"
        },
        "PersonalPIN": "XXXXXXXXXX"
    }
}
```

Para obtener más información, consulte Changing Personal Meeting PINs en la Guía para desarrolladores de Amazon Chime.

- Para obtener información sobre la API, consulte ResetPersonalPin en la Referencia de comandos de la AWS CLI.

`restore-phone-number`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-phone-number`.

AWS CLI

Restauración de un número de teléfono

En el siguiente ejemplo de `restore-phone-number`, se restaura el número de teléfono especificado desde la cola de eliminación.

```
aws chime restore-phone-number \
    --phone-number-id "+12065550100"
```

Salida:

```
{
    "PhoneNumber": {
        "PhoneNumberId": "%2B12065550100",
```

```
        "E164PhoneNumber": "+12065550100",
        "Type": "Local",
        "ProductType": "BusinessCalling",
        "Status": "Unassigned",
        "Capabilities": {
            "InboundCall": true,
            "OutboundCall": true,
            "InboundSMS": true,
            "OutboundSMS": true,
            "InboundMMS": true,
            "OutboundMMS": true
        },
        "Associations": [],
        "CreatedTimestamp": "2019-08-09T21:35:21.445Z",
        "UpdatedTimestamp": "2019-08-12T22:06:36.355Z"
    }
}
```

Para obtener más información, consulte Working with Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte RestorePhoneNumber en la Referencia de comandos de la AWS CLI.

`search-available-phone-numbers`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-available-phone-numbers`.

AWS CLI

Búsqueda de números de teléfono disponibles

En el siguiente ejemplo de `search-available-phone-numbers`, se buscan los números de teléfono disponibles por código de área.

```
aws chime search-available-phone-numbers \
    --area-code "206"
```

Salida:

```
{
    "E164PhoneNumbers": [
```

```
        "+12065550100",
        "+12065550101",
        "+12065550102",
        "+12065550103",
        "+12065550104",
        "+12065550105",
        "+12065550106",
        "+12065550107",
        "+12065550108",
        "+12065550109",
    ]
}
```

Para obtener más información, consulte Working with Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte SearchAvailablePhoneNumbers en la Referencia de comandos de la AWS CLI.

`update-account-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-account-settings`.

AWS CLI

Actualización de la configuración de la cuenta

En el siguiente ejemplo de `update-account-settings`, se desactiva el control remoto de las pantallas compartidas en la cuenta de Amazon Chime especificada.

```
aws chime update-account-settings \
    --account-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --account-settings DisableRemoteControl=true
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte UpdateAccountSettings en la Referencia de comandos de la AWS CLI.

`update-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-account`.

AWS CLI

Actualización de una cuenta

En el siguiente ejemplo de `update-account`, se actualiza el nombre de la cuenta especificada.

```
aws chime update-account \
    --account-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --name MyAccountName
```

Salida:

```
{
    "Account": {
        "AwsAccountId": "111122223333",
        "AccountId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
        "Name": "MyAccountName",
        "AccountType": "Team",
        "CreatedTimestamp": "2018-09-04T21:44:22.292Z",
        "DefaultLicense": "Pro",
        "SupportedLicenses": [
            "Basic",
            "Pro"
        ],
        "SigninDelegateGroups": [
            {
                "GroupName": "myGroup"
            },
        ]
    }
}
```

Para obtener más información, consulte Renaming Your Account en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte UpdateAccount en la Referencia de comandos de la AWS CLI.

`update-bot`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-bot`.

AWS CLI

Actualización de un bot

En el siguiente ejemplo de `update-bot`, se actualiza el estado del bot especificado para detener su ejecución.

```
aws chime update-bot \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --bot-id 123abcd4-5ef6-789g-0h12-34j56789012k \
    --disabled
```

Salida:

```
{
    "Bot": {
        "BotId": "123abcd4-5ef6-789g-0h12-34j56789012k",
        "UserId": "123abcd4-5ef6-789g-0h12-34j56789012k",
        "DisplayName": "myBot (Bot)",
        "BotType": "ChatBot",
        "Disabled": true,
        "CreatedTimestamp": "2019-09-09T18:05:56.749Z",
        "UpdatedTimestamp": "2019-09-09T18:05:56.749Z",
        "BotEmail": "myBot-chimebot@example.com",
        "SecurityToken": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
    }
}
```

Para obtener más información, consulte Update Chat Bots en la Guía para desarrolladores de Amazon Chime.

- Para obtener información sobre la API, consulte UpdateBot en la Referencia de comandos de la AWS CLI.

`update-global-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-global-settings`.

AWS CLI

Actualización de la configuración global

En el siguiente ejemplo de `update-global-settings`, se actualizan los buckets de S3 que se utilizan para almacenar los registros de detalles de llamadas de los Amazon Chime Business Calling y Amazon Chime Voice Connector asociados a la cuenta de AWS del administrador.

```
aws chime update-global-settings \
    --business-calling CdrBucket="s3bucket" \
    --voice-connector CdrBucket="s3bucket"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing Global Settings en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte UpdateGlobalSettings en la Referencia de comandos de la AWS CLI.

`update-phone-number-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-phone-number-settings`.

AWS CLI

Actualización del nombre de llamada saliente

En el siguiente ejemplo de `update-phone-number-settings`, se actualiza el nombre de llamada saliente predeterminado de la cuenta de AWS del administrador.

```
aws chime update-phone-number-settings \
    --calling-name "myName"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte UpdatePhoneNumberSettings en la Referencia de comandos de la AWS CLI.

`update-phone-number`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-phone-number`.

AWS CLI

Ejemplo 1: actualizar el tipo de producto de un número de teléfono

En el siguiente ejemplo de `update-phone-number`, se actualiza el tipo de producto del número de teléfono especificado.

```
aws chime update-phone-number \
    --phone-number-id "+12065550100" \
    --product-type "BusinessCalling"
```

Salida:

```
{
    "PhoneNumber": {
        "PhoneNumberId": "%2B12065550100",
        "E164PhoneNumber": "+12065550100",
        "Type": "Local",
        "ProductType": "BusinessCalling",
        "Status": "Unassigned",
        "Capabilities": {
            "InboundCall": true,
            "OutboundCall": true,
            "InboundSMS": true,
            "OutboundSMS": true,
            "InboundMMS": true,
            "OutboundMMS": true
        },
        "Associations": [],
        "CallingName": "phonenumber1",
        "CreatedTimestamp": "2019-08-09T21:35:21.445Z",
        "UpdatedTimestamp": "2019-08-12T21:44:07.591Z"
    }
}
```

Ejemplo 2: cómo actualizar el nombre de la llamada saliente de un número de teléfono

En el siguiente ejemplo de `update-phone-number`, se actualiza el nombre de la llamada saliente del número de teléfono especificado.

aws chime update-phone-number --phone-number-id "+12065550100" --calling-name "phonenumber2"

Salida:

```
{
    "PhoneNumber": {
        "PhoneNumberId": "%2B12065550100",
        "E164PhoneNumber": "+12065550100",
        "Type": "Local",
        "ProductType": "BusinessCalling",
        "Status": "Unassigned",
        "Capabilities": {
            "InboundCall": true,
            "OutboundCall": true,
            "InboundSMS": true,
            "OutboundSMS": true,
            "InboundMMS": true,
            "OutboundMMS": true
        },
        "Associations": [],
        "CallingName": "phonenumber2",
        "CreatedTimestamp": "2019-08-09T21:35:21.445Z",
        "UpdatedTimestamp": "2019-08-12T21:44:07.591Z"
    }
}
```

Para obtener más información, consulte Working with Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información sobre la API, consulte UpdatePhoneNumber en la Referencia de comandos de la AWS CLI.

`update-room-membership`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-room-membership`.

AWS CLI

Creación de una suscripción de sala

En el siguiente ejemplo de `update-room-membership`, se cambia el rol del miembro de la sala de chat especificado a `Administrator`.

```
aws chime update-room-membership \
```

```
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --room-id abcd1e2d-3e45-6789-01f2-3g45h67i890j \
    --member-id 1ab2345c-67de-8901-f23g-45h678901j2k \
    --role Administrator
```

Salida:

```
{
    "RoomMembership": {
        "RoomId": "abcd1e2d-3e45-6789-01f2-3g45h67i890j",
        "Member": {
            "MemberId": "1ab2345c-67de-8901-f23g-45h678901j2k",
            "MemberType": "User",
            "Email": "sofiamartinez@example.com",
            "FullName": "Sofia Martinez",
            "AccountId": "12a3456b-7c89-012d-3456-78901e23fg45"
        },
        "Role": "Administrator",
        "InvitedBy": "arn:aws:iam::111122223333:user/admin",
        "UpdatedTimestamp": "2019-12-02T22:40:22.931Z"
    }
}
```

Para obtener más información, consulte Creating a Chat Room en la Guía del usuario de Amazon Chime.

- Para obtener información sobre la API, consulte UpdateRoomMembership en la Referencia de comandos de la AWS CLI.

`update-room`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-room`.

AWS CLI

Actualización de una sala de chat

En el siguiente ejemplo de `update-room`, se cambia el nombre de la sala de chat especificada.

```
aws chime update-room \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --room-id abcd1e2d-3e45-6789-01f2-3g45h67i890j \
```

```
    --name teamRoom
```

Salida:

```
{
    "Room": {
        "RoomId": "abcd1e2d-3e45-6789-01f2-3g45h67i890j",
        "Name": "teamRoom",
        "AccountId": "12a3456b-7c89-012d-3456-78901e23fg45",
        "CreatedBy": "arn:aws:iam::111122223333:user/alejandro",
        "CreatedTimestamp": "2019-12-02T22:29:31.549Z",
        "UpdatedTimestamp": "2019-12-02T22:33:19.310Z"
    }
}
```

Para obtener más información, consulte Creating a Chat Room en la Guía del usuario de Amazon Chime.

- Para obtener información sobre la API, consulte UpdateRoom en la Referencia de comandos de la AWS CLI.

`update-user-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-user-settings`.

AWS CLI

Actualización de la configuración del usuario

En el siguiente ejemplo de `update-user-settings`, se permite al usuario especificado realizar llamadas entrantes y salientes, así como enviar y recibir mensajes SMS.

```
aws chime update-user-settings \
    --account-id 12a3456b-7c89-012d-3456-78901e23fg45 \
    --user-id 1ab2345c-67de-8901-f23g-45h678901j2k \
    --user-settings "Telephony={InboundCalling=true,OutboundCalling=true,SMS=true}"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing User Phone Numbers en la Guía de administración de Amazon Chime.

- Para obtener información acerca de la API, consulte UpdateUserSettings en la Referencia de comandos de la AWS CLI.

`update-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-user`.

AWS CLI

Actualización de detalles del usuario

En este ejemplo se actualizan los detalles especificados del usuario especificado.

Comando:

```
aws chime update-user \
    --account-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --user-id a1b2c3d4-5678-90ab-cdef-22222EXAMPLE \
    --license-type "Basic"
```

Salida:

```
{
    "User": {
        "UserId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE"
    }
}
```

- Para obtener información sobre la API, consulte UpdateUser en la Referencia de comandos de la AWS CLI.

Ejemplos de API de control en la nube que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar situaciones comunes usando la AWS Command Line Interface con API de control en la nube.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-resource`.

AWS CLI

Creación de un recurso

En el siguiente ejemplo de `create-resource`, se crea un recurso AWS::Kinesis::Stream, denominado ResourceExample, con un período de retención de 168 horas y un recuento de tres particiones.

```
aws cloudcontrol create-resource \
    --type-name AWS::Kinesis::Stream \
    --desired-state "{\"Name\": \"ResourceExample\",\"RetentionPeriodHours\":168,
 \"ShardCount\":3}"
```

Salida:

```
{
    "ProgressEvent": {
        "EventTime": 1632506656.706,
        "TypeName": "AWS::Kinesis::Stream",
        "OperationStatus": "IN_PROGRESS",
        "Operation": "CREATE",
        "Identifier": "ResourceExample",
        "RequestToken": "20999d87-e304-4725-ad84-832dcbfd7fc5"
    }
}
```

Para obtener más información, consulte Creating a resource en la Guía del usuario de API de control en la nube.

- Para obtener información sobre la API, consulte CreateResource en la Referencia de comandos de la AWS CLI.

`delete-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-resource`.

AWS CLI

Para eliminar un recurso

En el siguiente ejemplo de `delete-resource`, se elimina un recurso AWS::Kinesis::Stream con el identificador ResourceExample de la cuenta de AWS.

```
aws cloudcontrol delete-resource \
    --type-name AWS::Kinesis::Stream \
    --identifier ResourceExample
```

Salida:

```
{
    "ProgressEvent": {
        "TypeName": "AWS::Kinesis::Stream",
        "Identifier": "ResourceExample",
        "RequestToken": "e48f26ff-d0f9-4ab8-a878-120db1edf111",
        "Operation": "DELETE",
        "OperationStatus": "IN_PROGRESS",
        "EventTime": 1632950300.14
    }
}
```

Para obtener más información, consulte Deleting a resource en la Guía del usuario de API de control en la nube.

- Para obtener información sobre la API, consulte DeleteResource en la Referencia de comandos de la AWS CLI.

`get-resource-request-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource-request-status`.

AWS CLI

Obtención de la información de estado de una solicitud de recursos

En el siguiente ejemplo de `get-resource-request-status`, se ofrece información sobre la solicitud de recurso especificada.

```
aws cloudcontrol get-resource-request-status \
    --request-token "e1a6b86e-46bd-41ac-bfba-001234567890"
```

Salida:

```
{
    "ProgressEvent": {
        "TypeName": "AWS::Kinesis::Stream",
        "Identifier": "Demo",
        "RequestToken": "e1a6b86e-46bd-41ac-bfba-001234567890",
        "Operation": "CREATE",
        "OperationStatus": "FAILED",
        "EventTime": 1632950268.481,
        "StatusMessage": "Resource of type 'AWS::Kinesis::Stream' with identifier
 'Demo' already exists.",
        "ErrorCode": "AlreadyExists"
    }
}
```

Para obtener más información, consulte Managing resource operation requests en la Guía del usuario de API de control en la nube.

- Para obtener información sobre la API, consulte GetResourceRequestStatus en la Referencia de comandos de la AWS CLI.

`get-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource`.

AWS CLI

Obtención del estado actual de un recurso

En el siguiente ejemplo de `get-resource`, se indica el estado actual del recurso AWS::Kinesis::Stream denominado ResourceExample.

```
aws cloudcontrol get-resource \
    --type-name AWS::Kinesis::Stream \
    --identifier ResourceExample
```

Salida:

```
{
    "TypeName": "AWS::Kinesis::Stream",
    "ResourceDescription": {
        "Identifier": "ResourceExample",
        "Properties": "{\"Arn\":\"arn:aws:kinesis:us-west-2:099908667365:stream/
ResourceExample\",\"RetentionPeriodHours\":168,\"Name\":\"ResourceExample\",
\"ShardCount\":3}"
    }
}
```

Para obtener más información, consulte Reading a resource's current state en la Guía del usuario de API de control en la nube.

- Para obtener detalles sobre la API, consulte GetResource en la Referencia de comandos de la AWS CLI.

`list-resource-requests`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-requests`.

AWS CLI

Generación de una lista de las solicitudes de operaciones de recursos activas

En el siguiente ejemplo de `list-resource-requests`, se genera una lista de las solicitudes de recursos para las operaciones CREATE y UPDATE que han fallado en la cuenta de AWS.

```
aws cloudcontrol list-resource-requests \
    --resource-request-status-filter Operations=CREATE,OperationStatuses=FAILED
```

Salida:

```
{
    "ResourceRequestStatusSummaries": [
        {
```

```
            "TypeName": "AWS::Kinesis::Stream",
            "Identifier": "Demo",
            "RequestToken": "e1a6b86e-46bd-41ac-bfba-633abcdfdbd7",
            "Operation": "CREATE",
            "OperationStatus": "FAILED",
            "EventTime": 1632950268.481,
            "StatusMessage": "Resource of type 'AWS::Kinesis::Stream' with
 identifier 'Demo' already exists.",
            "ErrorCode": "AlreadyExists"
        }
    ]
}
```

Para obtener más información, consulte Managing resource operation requests en la Guía del usuario de API de control en la nube.

- Para obtener información sobre la API, consulte ListResourceRequests en la Referencia de comandos de la AWS CLI.

`list-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resources`.

AWS CLI

Generación de una lista de los recursos de un tipo determinado

En el siguiente ejemplo de `list-resources`, se genera una lista de los recursos AWS::Kinesis::Stream aprovisionados en la cuenta de AWS.

```
aws cloudcontrol list-resources \
    --type-name AWS::Kinesis::Stream
```

Salida:

```
{
    "TypeName": "AWS::Kinesis::Stream",
    "ResourceDescriptions": [
        {
            "Identifier": "MyKinesisStream",
            "Properties": "{\"Name\":\"MyKinesisStream\"}"
        },
```

```
        {
            "Identifier": "AnotherStream",
            "Properties": "{\"Name\":\"AnotherStream\"}"
        }
    ]
}
```

Para obtener más información, consulte Discovering resources en la Guía del usuario de API de control en la nube.

- Para obtener más información sobre la API, consulte ListResources en la Referencia de comandos de la AWS CLI.

`update-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-resource`.

AWS CLI

Actualización de las propiedades de un recurso existente

En el siguiente ejemplo de `update-resource`, se actualiza la política de retención de un recurso AWS::Logs::LogGroup denominado ExampleLogGroup a 90 días.

```
aws cloudcontrol update-resource \
    --type-name AWS::Logs::LogGroup \
    --identifier ExampleLogGroup \
    --patch-document "[{\"op\":\"replace\",\"path\":\"/RetentionInDays\",\"value
\":90}]"
```

Salida:

```
{
    "ProgressEvent": {
        "EventTime": "2021-08-09T18:17:15.219Z",
        "TypeName": "AWS::Logs::LogGroup",
        "OperationStatus": "IN_PROGRESS",
        "Operation": "UPDATE",
        "Identifier": "ExampleLogGroup",
        "RequestToken": "5f40c577-3534-4b20-9599-0b0123456789"
    }
}
```

Para obtener más información, consulte Updating a resource en la Guía del usuario de API de control en la nube.

- Para obtener información sobre la API, consulte UpdateResource en la Referencia de comandos de la AWS CLI.

AWS Cloud Map Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS Cloud Map.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-http-namespace`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-http-namespace`.

AWS CLI

Creación de un espacio de nombres de HTTP

En el siguiente ejemplo de `create-http-namespace` se crea el espacio de nombres de HTTP `example.com`.

```
aws servicediscovery create-http-namespace \
    --name example.com \
    --creator-request-id example-request-id
```

Salida:

```
{
    "OperationId": "gv4g5meo7ndmeh4fqskygvk23d2fijwa-k9302yzd"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar `get-operation`. Para obtener más información, consulte get-operation.

Para obtener más información sobre la creación de un espacio de nombres, consulte Creación de un espacio de nombres de AWS Cloud Map para agrupar servicios de aplicación en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener detalles de la API, consulte CreateHttpNamespace en Referencia de comandos de la AWS CLI.

`create-private-dns-namespace`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-private-dns-namespace`.

AWS CLI

Para crear un espacio de nombres de DNS privado

En el siguiente ejemplo de `create-private-dns-namespace`, se crea un espacio de nombres de DNS privado.

```
aws servicediscovery create-private-dns-namespace \
    --name example.com \
    --vpc vpc-1c56417b
```

Salida:

```
{
    "OperationId": "gv4g5meo7ndmeh4fqskygvk23d2fijwa-k9302yzd"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar `get-operation`. Para obtener más información, consulte get-operation.

Para obtener más información, consulte Creating namespaces en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener detalles sobre la API, consulte CreatePrivateDnsNamespace en la Referencia de comandos de la AWS CLI.

`create-public-dns-namespace`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-public-dns-namespace`.

AWS CLI

Creación de un espacio de nombres DNS público

En el siguiente ejemplo de `create-public-dns-namespace` se crea el espacio de nombres de DNS público `example.com`.

```
aws servicediscovery create-public-dns-namespace \
    --name example-public-dns.com \
    --creator-request-id example-public-request-id \
    --properties DnsProperties={SOA={TTL=60}}
```

Salida:

```
{
    "OperationId": "gv4g5meo7ndmeh4fqskygvk23d2fijwa-k9302yzd"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar `get-operation`.

Para obtener más información sobre la creación de un espacio de nombres, consulte Creación de un espacio de nombres de AWS Cloud Map para agrupar servicios de aplicación en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener detalles de la API, consulte CreatePublicDnsNamespace en Referencia de comandos de la AWS CLI.

`create-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-service`.

AWS CLI

Ejemplo 1: Creación de un servicio con un ID de espacio de nombres

En el siguiente ejemplo de `create-service`, se crea un servicio.

```
aws servicediscovery create-service \
    --name myservice \
    --namespace-id  ns-ylexjili4cdxy3xm \
    --dns-config "RoutingPolicy=MULTIVALUE,DnsRecords=[{Type=A,TTL=60}]"
```

Salida:

```
{
    "Service": {
        "Id": "srv-abcd1234xmpl5678",
        "Arn": "arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
abcd1234xmpl5678",
        "ResourceOwner": "123456789012",
        "Name": "myservice",
        "NamespaceId": "ns-abcd1234xmpl5678",
        "DnsConfig": {
            "NamespaceId": "ns-abcd1234xmpl5678",
            "RoutingPolicy": "MULTIVALUE",
            "DnsRecords": [
                {
                    "Type": "A",
                    "TTL": 60
                }
            ]
        },
        "Type": "DNS_HTTP",
        "CreateDate": "2025-08-18T13:45:31.023000-05:00",
        "CreatorRequestId": "abcd1234-5678-90ab-cdef-xmpl12345678",
        "CreatedByAccount": "123456789012"
    }
}
```

Para obtener más información, consulte Creación de un servicio de AWS Cloud Map para un componente de aplicación en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Creación de un servicio con un ARN de espacio de nombres

En el ejemplo de `create-service` siguiente, se crea un servicio con un ARN de espacio de nombres en lugar de un ID de espacio de nombres. Es necesario especificar un ARN de espacio de nombres al crear un servicio en un espacio de nombres compartido.

```
aws servicediscovery create-service \
    --name myservice-arn \
    --namespace-id arn:aws:servicediscovery:us-west-2:123456789012:namespace/ns-abcd1234xmpl5678 \
    --dns-config "RoutingPolicy=MULTIVALUE,DnsRecords=[{Type=A,TTL=60}]"
```

Salida:

```
{
    "Service": {
        "Id": "srv-abcd1234xmpl5678",
        "Arn": "arn:aws:servicediscovery:us-west-2:123456789012:service/srv-abcd1234xmpl5678",
        "ResourceOwner": "123456789012",
        "Name": "myservice-arn",
        "NamespaceId": "ns-abcd1234xmpl5678",
        "DnsConfig": {
            "NamespaceId": "ns-abcd1234xmpl5678",
            "RoutingPolicy": "MULTIVALUE",
            "DnsRecords": [
                {
                    "Type": "A",
                    "TTL": 60
                }
            ]
        },
        "Type": "DNS_HTTP",
        "CreateDate": "2025-08-18T13:45:31.023000-05:00",
        "CreatorRequestId": "abcd1234-5678-90ab-cdef-xmpl12345678",
        "CreatedByAccount": "123456789012"
    }
}
```

Para obtener más información, consulte Espacios de nombres de AWS Cloud Map compartidos en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener información sobre la API, consulte CreateService en la Referencia de comandos de la AWS CLI.

`delete-namespace`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-namespace`.

AWS CLI

Ejemplo 1: Eliminación de un espacio de nombres

En el siguiente ejemplo de `delete-namespace`, se elimina un espacio de nombres.

```
aws servicediscovery delete-namespace \
    --id ns-abcd1234xmpl5678
```

Salida:

```
{
    "OperationId": "abcd1234-5678-90ab-cdef-xmpl12345678"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar `get-operation`. Para obtener más información, consulte get-operation.

Para obtener más información, consulte Eliminación de un espacio de nombres de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Eliminación de un espacio de nombres mediante el ARN del espacio de nombres

En el ejemplo de `delete-namespace` siguiente, se elimina un espacio de nombres mediante su ARN.

```
aws servicediscovery delete-namespace \
    --id arn:aws:servicediscovery:us-west-2:123456789012:namespace/ns-
abcd1234xmpl5678
```

Salida:

```
{
    "OperationId": "abcd1234-5678-90ab-cdef-xmpl12345678"
}
```

Para obtener más información, consulte Eliminación de un espacio de nombres de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener información sobre la API, consulte DeleteNamespace en la Referencia de comandos de la AWS CLI.

`delete-service-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-service-attributes`.

AWS CLI

Ejemplo 1: Eliminación de un atributo de servicio

En el siguiente ejemplo de `delete-service-attributes`, se elimina un atributo de servicio con la clave `Port` asociada al servicio especificado.

```
aws servicediscovery delete-service-attributes \
    --service-id srv-abcd1234xmpl5678 \
    --attributes Port
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Servicios de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Eliminación de un atributo de servicio con ARN

En el ejemplo de `delete-service-attributes` siguiente, se elimina un atributo de servicio mediante el ARN del servicio. Es necesario especificar el ARN para eliminar los atributos asociados a los servicios creados en los espacios de nombres compartidos con la cuenta.

```
aws servicediscovery delete-service-attributes \
    --service-id arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
abcd1234xmpl5678 \
    --attributes Port
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Servicios de AWS Cloud Map y Espacios de nombres de AWS Cloud Map compartidos en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener detalles sobre la API, consulte DeleteServiceAttributes en la Referencia de comandos de la AWS CLI.

`delete-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-service`.

AWS CLI

Ejemplo 1: Eliminación de un servicio

En el siguiente ejemplo de `delete-service`, se elimina un servicio.

```
aws servicediscovery delete-service \
    --id srv-abcd1234xmpl5678
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de un servicio de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Eliminación de un servicio con ARN

En el ejemplo de `delete-service` siguiente, se elimina un servicio con su ARN.

```
aws servicediscovery delete-service \
    --id arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
abcd1234xmpl5678
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de un servicio de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener información sobre la API, consulte DeleteService en la Referencia de comandos de la AWS CLI.

`deregister-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-instance`.

AWS CLI

Ejemplo 1: Anulación del registro de una instancia de servicio

En el siguiente ejemplo de `deregister-instance`, se anula el registro de una instancia de servicio.

```
aws servicediscovery deregister-instance \
    --service-id srv-p5zdwlg5uvvzjita \
    --instance-id myservice-53
```

Salida:

```
{
    "OperationId": "4yejorelbukcjzpnr6tlmrghsjwpngf4-k98rnaiq"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar `get-operation`. Para obtener más información, consulte get-operation.

Para obtener más información, consulte Deregistering service instances en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Anulación del registro de una instancia de servicio mediante el ARN de servicio para espacios de nombres compartidos

En el ejemplo de `deregister-instance` siguiente, se anula el registro de una instancia de servicio mediante un ARN de servicio en lugar de un ID de servicio. Es necesario especificar un ARN al anular el registro de instancias de los servicios creados en los espacios de nombres que se comparten con la cuenta.

```
aws servicediscovery deregister-instance \
    --service-id arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
p5zdwlg5uvvzjita \
    --instance-id web-server-01
```

Salida:

```
{
    "OperationId": "gv4g5meo7ndmkqjrhpn39wk42xmpl"
}
```

Para obtener más información, consulte Espacios de nombres de AWS Cloud Map compartidos y Anulación del registro de una instancia de servicio de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener información acerca de la API, consulte DeregisterInstance en la Referencia de comandos de la AWS CLI.

`discover-instances-revision`

En el siguiente ejemplo de código, se muestra cómo utilizar `discover-instances-revision`.

AWS CLI

Ejemplo 1: Detección de la revisión de una instancia

En el siguiente ejemplo de `discover-instances-revision`, se descubre la revisión creciente de una instancia.

```
aws servicediscovery discover-instances-revision \
    --namespace-name example.com \
    --service-name myservice
```

Salida:

```
{
    "InstancesRevision": 123456
}
```

Para obtener más información, consulte Instancias de servicio de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Detección de la revisión de instancias de una cuenta de propietario específica

En el ejemplo de `discover-instances-revision` siguiente, se detecta la revisión de instancias de una cuenta de propietario específica. El parámetro owner-account es necesario para las instancias de los espacios de nombres que se comparten con la cuenta.

```
aws servicediscovery discover-instances-revision \
    --namespace-name shared-namespace \
    --service-name shared-service \
    --owner-account 123456789111
```

Salida:

```
{
```

```
    "InstancesRevision": 1234567890
}
```

Para obtener más información, consulte Espacios de nombre de AWS Cloud Map compartidos e Instancias de servicio de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener detalles de la API, consulte DiscoverInstancesRevision en Referencia de comandos de la AWS CLI.

`discover-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `discover-instances`.

AWS CLI

Ejemplo 1: Detección de instancias registradas

En el siguiente ejemplo de `discover-instances`, se descubren instancias registradas.

```
aws servicediscovery discover-instances \
    --namespace-name example.com \
    --service-name myservice \
    --max-results 10 \
    --health-status ALL
```

Salida:

```
{
    "Instances": [
        {
            "InstanceId": "myservice-53",
            "NamespaceName": "example.com",
            "ServiceName": "myservice",
            "HealthStatus": "UNKNOWN",
            "Attributes": {
                "AWS_INSTANCE_IPV4": "172.2.1.3",
                "AWS_INSTANCE_PORT": "808"
            }
        }
    ],
    "InstancesRevision": 85648075627387284
}
```

Para obtener más información, consulte Instancias de servicio de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Detección de instancias de una cuenta de propietario específica

En el ejemplo de `discover-instances` siguiente, se detectan instancias registradas de una cuenta de propietario específica. Este parámetro es necesario para detectar instancias en espacios de nombres que se comparten con la cuenta.

```
aws servicediscovery discover-instances \
    --namespace-name shared-namespace \
    --service-name shared-service \
    --owner-account 123456789111
```

Salida:

```
{
    "Instances": [
        {
            "InstanceId": "shared-instance-1234",
            "NamespaceName": "shared-namespace",
            "ServiceName": "shared-service",
            "HealthStatus": "HEALTHY",
            "Attributes": {
                "AWS_INSTANCE_IPV4": "203.0.113.75",
                "AWS_INSTANCE_PORT": "80"
            }
        }
    ],
    "InstancesRevision": 1234567890
}
```

Para obtener más información, consulte Espacios de nombre de AWS Cloud Map compartidos e Instancias de servicio de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener más detalles sobre la API, consulte DiscoverInstances en la Referencia de comandos de la AWS CLI.

`get-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-instance`.

AWS CLI

Ejemplo 1: Obtención de los detalles de una instancia

En el siguiente ejemplo de `get-instance`, se obtienen los atributos de un servicio.

```
aws servicediscovery get-instance \
    --service-id srv-e4anhexample0004
    --instance-id i-abcd1234
```

Salida:

```
{
    "ResourceOwner": "123456789012",
    "Instance": {
        "Id": "arn:aws:servicediscovery:us-west-2:111122223333;:service/srv-
e4anhexample0004",
        "Attributes": {
            "AWS_INSTANCE_IPV4": "192.0.2.44",
            "AWS_INSTANCE_PORT": "80",
            "color": "green",
            "region": "us-west-2",
            "stage": "beta"
        },
        "CreatedByAccount": "123456789012"
    }
}
```

Para obtener más información, consulte Instancias de servicio de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Obtención de los detalles de una instancia mediante el ARN de servicio para espacios de nombres compartidos

En el ejemplo de `get-instance` siguiente, se obtienen los atributos de una instancia mediante un ARN de servicio en lugar de un ID de servicio. Es necesario especificar un ARN para obtener detalles de las instancias asociadas a los espacios de nombres que se comparten con la cuenta. La instancia devuelta en este ejemplo se registró por cuenta `123456789111` en un espacio de nombres propiedad de la cuenta `123456789012`.

```
aws servicediscovery get-instance \
```

```
    --service-id arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
p5zdwlg5uvvzjita \
    --instance-id web-server-01
```

Salida:

```
{
    "ResourceOwner": "123456789012",
    "Instance": {
        "Id": "web-server-01",
        "Attributes": {
            "AWS_INSTANCE_IPV4": "203.0.113.15",
            "AWS_INSTANCE_PORT": "80"
        },
        "CreatedByAccount": "123456789111"
    }
}
```

Para obtener más información sobre los espacios de nombres entre cuentas compartidos, consulte Espacios de nombres de AWS Cloud Map compartidos en la Guía para desarrolladores de AWS.

- Para obtener información sobre la API, consulte GetInstance en la Referencia de comandos de la AWS CLI.

`get-instances-health-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-instances-health-status`.

AWS CLI

Ejemplo 1: Obtención del estado de las instancias asociadas a un servicio

En el siguiente ejemplo de `get-instances-health-status`, se obtiene el estado de las instancias asociadas al servicio especificado.

```
aws servicediscovery get-instances-health-status \
    --service-id srv-e4anhexample0004
```

Salida:

```
{
```

```
    "Status": {
        "i-abcd1234": "HEALTHY",
        "i-abcd1235": "UNHEALTHY"
    }
}
```

Para obtener más información, consulte Instancias de servicio de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Obtención de los detalles de las instancias mediante el ARN de servicio para espacios de nombres compartidos

En el ejemplo de `get-instances-health-status` siguiente, se obtiene el estado de las instancias mediante un ARN de servicio en lugar de un ID de servicio. Es necesario especificar un ARN para obtener el estado de las instancias asociadas a los espacios de nombres que se comparten con la cuenta del solicitante.

```
aws servicediscovery get-instances-health-status \
    --service-id arn:aws:servicediscovery:us-west-2:123456789012:service/srv-p5zdwlg5uvvzjita
```

Salida:

```
{
    "Status": {
        "web-server-01": "HEALTHY",
        "web-server-02": "UNHEALTHY"
    }
}
```

Para obtener más información, consulte Instancias de servicios de AWS Cloud Map y Espacios de nombres de AWS Cloud Map compartidos en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener información sobre la API, consulte GetInstancesHealthStatus en la Referencia de comandos de la AWS CLI.

`get-namespace`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-namespace`.

AWS CLI

Ejemplo 1: Obtención de los detalles de un espacio de nombres

En el siguiente ejemplo de `get-namespace`, se recupera información sobre el espacio de nombres especificado.

```
aws servicediscovery get-namespace \
    --id ns-abcd1234xmpl5678
```

Salida:

```
{
    "Namespace": {
        "Id": "ns-abcd1234xmpl5678",
        "Arn": "arn:aws:servicediscovery:us-west-2:123456789012:namespace/ns-
abcd1234xmpl5678",
        "ResourceOwner": "123456789012",
        "Name": "example-http.com",
        "Type": "HTTP",
        "Description": "Example.com AWS Cloud Map HTTP Namespace",
        "Properties": {
            "DnsProperties": {},
            "HttpProperties": {
                "HttpName": "example-http.com"
            }
        },
        "CreateDate": "2024-02-23T13:35:21.874000-06:00",
        "CreatorRequestId": "abcd1234-5678-90ab-cdef-xmpl12345678"
    }
}
```

Para obtener más información, consulte Espacios de nombres de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Obtención de los detalles de un espacio de nombres mediante el ARN

En el siguiente ejemplo de `get-namespace`, se recupera información sobre el espacio de nombres especificado mediante su ARN. Es necesario especificar el ARN para recuperar los detalles de un espacio de nombres compartido con la cuenta.

```
aws servicediscovery get-namespace \
```

```
    --id arn:aws:servicediscovery:us-west-2:123456789012:namespace/ns-
abcd1234xmpl5678
```

Salida:

```
{
    "Namespace": {
        "Id": "ns-abcd1234xmpl5678",
        "Arn": "arn:aws:servicediscovery:us-west-2:123456789012:namespace/ns-
abcd1234xmpl5678",
        "ResourceOwner": "123456789012",
        "Name": "example-http.com",
        "Type": "HTTP",
        "Description": "Example.com AWS Cloud Map HTTP Namespace",
        "Properties": {
            "DnsProperties": {},
            "HttpProperties": {
                "HttpName": "example-http.com"
            }
        },
        "CreateDate": "2024-02-23T13:35:21.874000-06:00",
        "CreatorRequestId": "abcd1234-5678-90ab-cdef-xmpl12345678"
    }
}
```

Para obtener más información, consulte Espacios de nombres de AWS Cloud Map compartidos en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener detalles de la API, consulte GetNamespace en Referencia de comandos de AWS CLI.

`get-operation`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-operation`.

AWS CLI

Ejemplo 1: Obtención del resultado de una operación

En el siguiente ejemplo de `get-operation`, se obtiene el resultado de una operación de creación de espacio de nombres.

```
aws servicediscovery get-operation \
```

```
    --operation-id abcd1234xmpl5678abcd1234xmpl5678-abcd1234
```

Salida:

```
{
    "Operation": {
        "Id": "abcd1234xmpl5678abcd1234xmpl5678-abcd1234",
        "Type": "CREATE_NAMESPACE",
        "Status": "SUCCESS",
        "CreateDate": "2025-01-13T13:35:21.874000-06:00",
        "UpdateDate": "2025-01-13T13:36:02.469000-06:00",
        "Targets": {
            "NAMESPACE": "ns-abcd1234xmpl5678"
        }
    }
}
```

Para obtener más información, consulte Creación de un espacio de nombres de AWS Cloud Map para agrupar servicios de aplicación en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Obtención de una operación de una cuenta de propietario específica

En el ejemplo de `get-operation` siguiente, se obtiene el resultado de una operación asociada a una cuenta de propietario de espacio de nombres específica. Este parámetro es necesario para obtener el resultado de las operaciones asociadas a los espacios de nombres compartidos con la cuenta.

```
aws servicediscovery get-operation \
    --operation-id abcd1234xmpl5678abcd1234xmpl5678-abcd1234 \
    --owner-account 123456789111
```

Salida:

```
{
    "Operation": {
        "Id": "abcd1234xmpl5678abcd1234xmpl5678-abcd1234",
        "OwnerAccount": "123456789111",
        "Type": "CREATE_NAMESPACE",
        "Status": "SUCCESS",
        "CreateDate": "2025-01-13T13:35:21.874000-06:00",
        "UpdateDate": "2025-01-13T13:36:02.469000-06:00",
```

```
        "Targets": {
            "NAMESPACE": "ns-abcd1234xmpl5678"
        }
    }
}
```

Para obtener más información, consulte Espacios de nombres de AWS Cloud Map compartidos en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener información sobre la API, consulte GetOperation en la Referencia de comandos de la AWS CLI.

`get-service-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-attributes`.

AWS CLI

Ejemplo 1: Obtención de los atributos de un servicio

En el siguiente ejemplo de `get-service-attributes`, se obtienen los atributos de un servicio.

```
aws servicediscovery get-service-attributes \
    --service-id srv-abcd1234xmpl5678
```

Salida:

```
{
    "ServiceAttributes": {
        "ServiceArn": "arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
abcd1234xmpl5678",
        "ResourceOwner": "123456789012",
        "Attributes": {
            "Port": "80"
        }
    }
}
```

Para obtener más información, consulte Servicios de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Obtención de los atributos de un servicio mediante el ARN

En el ejemplo de `get-service-attributes` siguiente, se obtienen los atributos de un servicio mediante su ARN. Es necesario especificar un ARN para obtener los atributos de un servicio creado en un espacio de nombres compartido con la cuenta.

```
aws servicediscovery get-service-attributes \
    --service-id arn:aws:servicediscovery:us-west-2:123456789012:service/srv-abcd1234xmpl5678
```

Salida:

```
{
    "ServiceAttributes": {
        "ServiceArn": "arn:aws:servicediscovery:us-west-2:123456789012:service/srv-abcd1234xmpl5678",
        "ResourceOwner": "123456789012",
        "Attributes": {
            "Port": "80"
        }
    }
}
```

Para obtener más información, consulte Servicios de AWS Cloud Map y Espacios de nombres de AWS Cloud Map compartidos en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener información sobre la API, consulte GetServiceAttributes en la Referencia de comandos de la AWS CLI.

`get-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service`.

AWS CLI

Ejemplo 1: Obtención de la configuración de un servicio

En el siguiente ejemplo de `get-service`, se obtiene la configuración de un servicio especificado.

```
aws servicediscovery get-service \
    --id srv-abcd1234xmpl5678
```

Salida:

```
{
    "Service": {
        "Id": "srv-abcd1234xmpl5678",
        "Arn": "arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
abcd1234xmpl5678",
        "ResourceOwner": "123456789012",
        "Name": "test-service",
        "NamespaceId": "ns-abcd1234xmpl5678",
        "DnsConfig": {},
        "Type": "HTTP",
        "CreateDate": "2025-08-18T13:53:02.775000-05:00",
        "CreatorRequestId": "abcd1234-5678-90ab-cdef-xmpl12345678",
        "CreatedByAccount": "123456789012"
    }
}
```

Para obtener más información, consulte Servicios de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Obtención de la configuración de un servicio mediante el ARN

En el ejemplo de `get-service` siguiente, se obtiene la configuración de un servicio especificado mediante su ARN. Es necesario especificar el ARN para recuperar información sobre un servicio creado en un espacio de nombres que se comparte con la cuenta. La cuenta `123456789111` de la persona que llama creó el servicio en un espacio de nombres compartido por la cuenta `123456789012`.

```
aws servicediscovery get-service \
    --id arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
abcd1234xmpl5678
```

Salida:

```
{
    "Service": {
        "Id": "srv-abcd1234xmpl5678",
        "Arn": "arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
abcd1234xmpl5678",
        "ResourceOwner": "123456789012",
```

```
        "Name": "test-service",
        "NamespaceId": "ns-abcd1234xmpl5678",
        "DnsConfig": {},
        "Type": "HTTP",
        "CreateDate": "2025-08-18T13:53:02.775000-05:00",
        "CreatorRequestId": "abcd1234-5678-90ab-cdef-xmpl12345678",
        "CreatedByAccount": "123456789111"
    }
}
```

Para obtener más información, consulte Creación de un servicio de AWS Cloud Map para un componente de aplicación en los Espacios de nombres de AWS Cloud Map compartidos en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener información sobre la API, consulte GetService en la Referencia de comandos de la AWS CLI.

`list-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-instances`.

AWS CLI

Ejemplo 1: Muestra de las instancias de servicio

En el siguiente ejemplo de `list-instances`, se enumeran las instancias del servicio.

```
aws servicediscovery list-instances \
    --service-id srv-qzpwvt2tfqcegapy
```

Salida:

```
{
    "Instances": [
        {
            "Id": "i-06bdabbae60f65a4e",
            "Attributes": {
                "AWS_INSTANCE_IPV4": "172.2.1.3",
                "AWS_INSTANCE_PORT": "808"
            },
            "CreatedByAccount": "123456789012"
```

```
        }
    ],
    "ResourceOwner": "123456789012"
}
```

Para obtener más información, consulte Muestra de las instancias de servicio de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Muestra de las instancias de servicio mediante el ARN del servicio

En el ejemplo de `list-instances` siguiente, se muestran las instancias de servicio mediante un ARN de servicio en lugar de un ID de servicio. Es necesario especificar un ARN al mostrar las instancias asociadas a los espacios de nombres que se comparten con la cuenta.

```
aws servicediscovery list-instances \
    --service-id arn:aws:servicediscovery:us-west-2:123456789012:service/srv-p5zdwlg5uvvzjita
```

Salida:

```
{
    "ResourceOwner": "123456789012",
    "Instances": [
        {
            "Id": "web-server-01",
            "Attributes": {
                "AWS_INSTANCE_IPV4": "203.0.113.15",
                "AWS_INSTANCE_PORT": "80"
            },
            "CreatedByAccount": "123456789012"
        },
        {
            "Id": "web-server-02",
            "Attributes": {
                "AWS_INSTANCE_IPV4": "203.0.113.16",
                "AWS_INSTANCE_PORT": "80"
            },
            "CreatedByAccount": "123456789012"
        }
    ]
}
```

Para obtener más información sobre los espacios de nombres entre cuentas compartidos, consulte Espacios de nombres de AWS Cloud Map compartidos y Muestra de instancias de servicios de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener información sobre la API, consulte ListInstances en la Referencia de comandos de la AWS CLI.

`list-namespaces`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-namespaces`.

AWS CLI

Ejemplo 1: Muestra de los espacios de nombres

En el siguiente ejemplo de `list-namespaces`, se enumeran los espacios de nombres.

```
aws servicediscovery list-namespaces
```

Salida:

```
{
    "Namespaces": [
        {
            "Id": "ns-abcd1234xmpl5678",
            "Arn": "arn:aws:servicediscovery:us-west-2:123456789012:namespace/ns-
abcd1234xmpl5678",
            "ResourceOwner": "123456789012",
            "Name": "local",
            "Type": "DNS_PRIVATE",
            "Properties": {
                "DnsProperties": {
                    "HostedZoneId": "Z06752353VBUDTC32S84S",
                    "SOA": {}
                },
                "HttpProperties": {
                    "HttpName": "local"
                 }
            },
            "CreateDate": "2023-07-17T13:37:27.872000-05:00"
        },
        {
```

```
            "Id": "ns-abcd1234xmpl9012",
            "Arn": "arn:aws:servicediscovery:us-west-2:123456789012:namespace/ns-
abcd1234xmpl9012",
            "ResourceOwner": "123456789012",
            "Name": "My-second-namespace",
            "Type": "HTTP",
            "Description": "My second namespace",
            "Properties": {
                "DnsProperties": {
                    "SOA": {}
                },
                "HttpProperties": {
                    "HttpName": "My-second-namespace"
                }
            },
            "CreateDate": "2023-11-14T10:35:47.840000-06:00"
        }
    ]
}
```

Para obtener más información, consulte Muestra de espacios de nombres de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Muestra de los espacios de nombres compartidos por otras cuentas

En el ejemplo de `list-namespaces` siguiente, se muestran los espacios de nombres que otras cuentas de AWS que utilizan el filtro `RESOURCE_OWNER` comparten con la cuenta de la persona que llama.

```
aws servicediscovery list-namespaces \
    --filters Name=RESOURCE_OWNER,Values=OTHER_ACCOUNTS,Condition=EQ
```

Salida:

```
{
    "Namespaces": [
        {
            "Id": "ns-abcd1234xmpl5678",
            "Arn": "arn:aws:servicediscovery:us-west-2:123456789111:namespace/ns-
abcd1234xmpl5678",
            "ResourceOwner": "123456789111",
            "Name": "shared-namespace",
```

```
            "Type": "HTTP",
            "Description": "Namespace shared from another account",
            "Properties": {
                "DnsProperties": {
                    "SOA": {}
                },
                "HttpProperties": {
                    "HttpName": "shared-namespace"
                }
            },
            "CreateDate": "2025-01-13T13:35:21.874000-06:00"
        }
    ]
}
```

Para obtener más información, consulte Espacios de nombres de AWS Cloud Map compartidos en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener detalles de la API, consulte ListNamespaces en la Referencia de comandos de la AWS CLI.

`list-operations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-operations`.

AWS CLI

Enumeración de las operaciones que cumplen los criterios especificados

En el siguiente ejemplo de `list-operations`, se enumeran las operaciones que tienen un estado de `PENDING` o `SUCCESS`.

```
aws servicediscovery list-operations \
    --service-id srv-e4anhexample0004 \
    --filters Name=STATUS,Condition=IN,Values=PENDING,SUCCESS
```

Salida:

```
{
    "Operations": [
        {
            "Id": "76yy8ovhpdz0plmjzbsnqgnrqvpv2qdt-kexample",
```

```
            "Status": "SUCCESS"
        },
        {
            "Id": "prysnyzpji3u2ciy45nke83x2zanl7yk-dexample",
            "Status": "SUCCESS"
        },
        {
            "Id": "ko4ekftir7kzlbechsh7xvcdgcpk66gh-7example",
            "Status": "PENDING"
        }
    ]
}
```

Para obtener más información, consulte ¿Qué es AWS Cloud Map? en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener información sobre la API, consulte ListOperations en la Referencia de comandos de la AWS CLI.

`list-services`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-services`.

AWS CLI

Ejemplo 1: Muestra de los servicios

En el siguiente ejemplo de `list-services`, se enumeran los servicios.

```
aws servicediscovery list-services
```

Salida:

```
{
    "Services": [
        {
            "Id": "srv-p5zdwlg5uvvzjita",
            "Arn": "arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
p5zdwlg5uvvzjita",
            "Name": "myservice",
            "DnsConfig": {
                "RoutingPolicy": "MULTIVALUE",
```

```
                "DnsRecords": [
                    {
                        "Type": "A",
                        "TTL": 60
                    }
                ]
            },
            "CreateDate": 1587081768.334
        }
    ]
}
```

Para obtener más información, consulte Muestra de los servicios de AWS Cloud Map en un espacio de nombres en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Muestra de los servicios creados en espacios de nombres compartidos

En el ejemplo de `list-services` siguiente, se muestran los servicios que se crean en espacios de nombres compartidos con la cuenta de la persona que llama `123456789012` de otras cuentas de AWS que utilizan el filtro `RESOURCE_OWNER`.

```
aws servicediscovery list-services \
    --filters Name=RESOURCE_OWNER,Values=OTHER_ACCOUNTS,Condition=EQ
```

Salida:

```
{
    "Services": [
        {
            "Id": "srv-abcd1234xmpl5678",
            "Arn": "arn:aws:servicediscovery:us-west-2:123456789111:service/srv-
abcd1234xmpl5678",
            "ResourceOwner": "123456789111",
            "Name": "shared-service",
            "NamespaceId": "ns-abcd1234xmpl5678",
            "Type": "HTTP",
            "Description": "Service in shared namespace",
            "DnsConfig": {},
            "CreateDate": "2025-01-13T13:35:21.874000-06:00",
            "CreatorRequestId": "abcd1234-5678-90ab-cdef-xmpl12345678",
            "CreatedByAccount": "123456789012"
        }
```

```
    ]
}
```

Para obtener más información, consulte Espacios de nombres de AWS Cloud Map compartidos y Muestra de servicios de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener información sobre la API, consulte ListServices en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Enumeración de las etiquetas asociadas al recurso especificado

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran las etiquetas para el recurso especificado.

```
aws servicediscovery list-tags-for-resource \
    --resource-arn arn:aws:servicediscovery:us-west-2:123456789012:namespace/ns-e4anhexample0004
```

Salida:

```
{
    "Tags": [
        {
            "Key": "Project",
            "Value": "Zeta"
        },
        {
            "Key": "Department",
            "Value": "Engineering"
        }
    ]
}
```

Para obtener más información, consulte Etiquetado de los recursos de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`register-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-instance`.

AWS CLI

Ejemplo 1: Registro de una instancia de servicio mediante el ID de servicio

En el siguiente ejemplo de `register-instance`, se registra una instancia de servicio.

```
aws servicediscovery register-instance \
    --service-id srv-p5zdwlg5uvvzjita \
    --instance-id myservice-53 \
    --attributes=AWS_INSTANCE_IPV4=172.2.1.3,AWS_INSTANCE_PORT=808
```

Salida:

```
{
    "OperationId": "4yejorelbukcjzpnr6tlmrghsjwpngf4-k95yg2u7"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar `get-operation`. Para obtener más información, consulte get-operation.

Para obtener más información sobre cómo registrar una instancia, consulte Registro de un recurso como una instancia del servicio de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Registro de una instancia de servicio mediante el ARN de servicio

En el ejemplo de `register-instance` siguiente, se registra una instancia de servicio mediante un ARN de servicio. Es necesario especificar el ARN al registrar instancias de los servicios que se comparten con la cuenta.

```
aws servicediscovery register-instance \
    --service-id arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
p5zdwlg5uvvzjita \
    --instance-id web-server-01 \
```

```
    --attributes=AWS_INSTANCE_IPV4=203.0.113.15,AWS_INSTANCE_PORT=80
```

Salida:

```
{
    "OperationId": "gv4g5meo7ndmkqjrhpn39wk42xmpl"
}
```

Para obtener más información sobre los espacios de nombres entre cuentas compartidos, consulte Espacios de nombres de AWS Cloud Map compartidos en la Guía para desarrolladores de AWS.

- Para obtener información sobre la API, consulte RegisterInstance en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Asociación de las etiquetas al recurso especificado

En el siguiente ejemplo de `tag-resource` se asocia una etiqueta `Department` al valor `Engineering` con el espacio de nombres especificado.

```
aws servicediscovery tag-resource \
    --resource-arn arn:aws:servicediscovery:us-west-2:123456789012:namespace/ns-e4anhexample0004 \
    --tags Key=Department, Value=Engineering
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de los recursos de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de etiquetas del recurso especificado

En el siguiente ejemplo de `untag-resource`, se elimina una etiqueta `Department` de un espacio de nombres especificado.

```
aws servicediscovery untag-resource \
    --resource-arn arn:aws:servicediscovery:us-west-2:123456789012:namespace/ns-e4anhexample0004 \
    --tags Key=Department, Value=Engineering
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de los recursos de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-http-namespace`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-http-namespace`.

AWS CLI

Ejemplo 1: Actualización de un espacio de nombres de HTTP

En el siguiente ejemplo de `update-http-namespace`, se actualiza la descripción del espacio de nombres de HTTP especificado.

```
aws servicediscovery update-http-namespace \
    --id ns-abcd1234xmpl5678 \
    --updater-request-id abcd1234-5678-90ab-cdef-xmpl12345678 \
    --namespace Description="The updated namespace description."
```

Salida:

```
{
    "OperationId": "abcd1234-5678-90ab-cdef-xmpl12345678"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar `get-operation`. Para obtener más información, consulte get-operation.

Para obtener más información, consulte Espacios de nombres de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Actualización de un espacio de nombres de HTTP mediante el ARN

En el ejemplo de `update-http-namespace` siguiente, se actualiza el espacio de nombres de HTTP especificado mediante su ARN.

```
aws servicediscovery update-http-namespace \
    --id arn:aws:servicediscovery:us-west-2:123456789012:namespace/ns-abcd1234xmpl5678 \
    --updater-request-id abcd1234-5678-90ab-cdef-xmpl12345678 \
    --namespace Description="The updated namespace description."
```

Salida:

```
{
    "OperationId": "abcd1234-5678-90ab-cdef-xmpl12345678"
}
```

Para obtener más información, consulte Espacios de nombres de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener detalles de la API, consulte UpdateHttpNamespace en Referencia de comandos de la AWS CLI.

`update-instance-custom-health-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-instance-custom-health-status`.

AWS CLI

Ejemplo 1: Actualización de una comprobación de estado personalizada

En el siguiente ejemplo de `update-instance-custom-health-status` se actualiza el estado de la comprobación de estado personalizada para el servicio especificado y la instancia de servicio de ejemplo a `HEALTHY`.

```
aws servicediscovery update-instance-custom-health-status \
    --service-id srv-e4anhexample0004 \
    --instance-id example \
    --status HEALTHY
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de la comprobación de estado de los servicios de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Actualización de una comprobación de estado personalizada mediante el ARN de servicio

En el ejemplo de `update-instance-custom-health-status` siguiente, se actualiza el estado de la comprobación de estado personalizada mediante un ARN de servicio. Es necesario el ARN al actualizar el estado para instancias asociadas a los espacios de nombres que se comparten con la cuenta.

```
aws servicediscovery update-instance-custom-health-status \
    --service-id arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
p5zdwlg5uvvzjita \
    --instance-id web-server-01 \
    --status HEALTHY
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de comprobación de estado de servicio de AWS Cloud Map y Uso compartido del espacio de nombres de AWS Cloud Map entre cuentas en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener detalles de la API, consulte UpdateInstanceCustomHealthStatus en Referencia de comandos de la AWS CLI.

`update-private-dns-namespace`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-private-dns-namespace`.

AWS CLI

Ejemplo 1: Actualización de un espacio de nombres de DNS privado mediante un ID

En el ejemplo de `update-private-dns-namespace` siguiente, se actualiza la descripción de un espacio de nombres de DNS privado mediante el ID de un espacio de nombres.

```
aws servicediscovery update-private-dns-namespace \
    --id ns-abcd1234xmpl5678 \
    --updater-request-id abcd1234-5678-90ab-cdef-xmpl12345678 \
    --namespace Description="The updated namespace description."
```

Salida:

```
{
    "OperationId": "abcd1234-5678-90ab-cdef-xmpl12345678"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar `get-operation`.

Para obtener más información, consulte Espacios de nombres de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Actualización de un espacio de nombres de DNS privado mediante un ARN

En el ejemplo de `update-private-dns-namespace` siguiente, se actualiza un espacio de nombres de DNS privado mediante su ARN.

```
aws servicediscovery update-private-dns-namespace \
    --id arn:aws:servicediscovery:us-west-2:123456789012:namespace/ns-
abcd1234xmpl5678 \
    --updater-request-id abcd1234-5678-90ab-cdef-xmpl12345678 \
    --namespace Description="The updated namespace description."
```

Salida:

```
{
    "OperationId": "abcd1234-5678-90ab-cdef-xmpl12345678"
}
```

Para obtener más información, consulte Espacios de nombres de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener detalles de la API, consulte UpdatePrivateDnsNamespace en Referencia de comandos de la AWS CLI.

update-public-dns-namespace

En el siguiente ejemplo de código, se muestra cómo utilizar `update-public-dns-namespace`.

AWS CLI

Ejemplo 1: Actualización de un espacio de nombres de DNS público mediante un ID

En el ejemplo de `update-public-dns-namespace` siguiente, se actualiza la descripción de un espacio de nombres de DNS público mediante su ID.

```
aws servicediscovery update-public-dns-namespace \
    --id ns-abcd1234xmpl5678 \
    --updater-request-id abcd1234-5678-90ab-cdef-xmpl12345678 \
    --namespace Description="The updated namespace description."
```

Salida:

```
{
    "OperationId": "abcd1234-5678-90ab-cdef-xmpl12345678"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar `get-operation`.

Para obtener más información, consulte Espacios de nombres de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Actualización de un espacio de nombres de DNS público mediante el ARN

En el ejemplo de `update-public-dns-namespace` siguiente, se actualiza un espacio de nombres de DNS público mediante su ARN.

```
aws servicediscovery update-public-dns-namespace \
    --id arn:aws:servicediscovery:us-west-2:123456789012:namespace/ns-
abcd1234xmpl5678 \
    --updater-request-id abcd1234-5678-90ab-cdef-xmpl12345678 \
    --namespace Description="The updated namespace description."
```

Salida:

```
{
```

```
    "OperationId": "abcd1234-5678-90ab-cdef-xmpl12345678"
}
```

Para obtener más información, consulte Espacios de nombres de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener detalles de la API, consulte UpdatePublicDnsNamespace en la Referencia de comandos de la AWS CLI.

`update-service-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-service-attributes`.

AWS CLI

Ejemplo 1: Actualización de un servicio para agregar un atributo

En el siguiente ejemplo de `update-service-attributes`, se actualiza el servicio especificado para agregar un atributo de servicio con una clave `Port` y un valor `80`.

```
aws servicediscovery update-service-attributes \
    --service-id srv-abcd1234xmpl5678 \
    --attributes Port=80
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Servicios de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Actualización de atributos de servicio con ARN

En el ejemplo de `update-service-attributes` siguiente, se actualiza un servicio mediante su ARN para agregar un atributo de servicio. Es necesario especificar el ARN para agregar atributos a servicios creados en los espacios de nombres compartidos con la cuenta.

```
aws servicediscovery update-service-attributes \
    --service-id arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
abcd1234xmpl5678 \
    --attributes Port=80
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Servicios de AWS Cloud Map y Espacios de nombres de AWS Cloud Map compartidos en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener detalles de la API, consulte UpdateServiceAttributes en Referencia de comandos de AWS CLI.

`update-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-service`.

AWS CLI

Ejemplo 1: Actualización de un servicio

En el siguiente ejemplo de `update-service`, se actualiza un servicio para actualizar las opciones de configuración `DnsConfig` y `HealthCheckConfig`.

```
aws servicediscovery update-service \
    --id srv-abcd1234xmpl5678 \
    --
service "DnsConfig={DnsRecords=[{Type=A,TTL=60}]},HealthCheckConfig={Type=HTTP,ResourcePath=
```

Salida:

```
{
    "OperationId": "abcd1234-5678-90ab-cdef-xmpl12345678"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar `get-operation`.

Para obtener más información sobre la actualización de un servicio, consulte Actualización de un servicio de AWS Cloud Map en la Guía para desarrolladores de AWS Cloud Map.

Ejemplo 2: Actualización de un servicio mediante el ARN

En el ejemplo de `update-service` siguiente, se actualiza un servicio mediante su ARN. Es necesario especificar el ARN para servicios creados en los espacios de nombres compartidos con la cuenta.

```
aws servicediscovery update-service \
```

```
    --id arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
abcd1234xmpl5678 \
    --
service "DnsConfig={DnsRecords=[{Type=A,TTL=60}]},HealthCheckConfig={Type=HTTP,ResourcePath=
```

Salida:

```
{
    "OperationId": "abcd1234-5678-90ab-cdef-xmpl12345678"
}
```

Para obtener más información sobre la actualización de un servicio, consulte Actualización de un servicio de AWS Cloud Map y Espacios de nombres de AWS Cloud Map compartidos en la Guía para desarrolladores de AWS Cloud Map.

- Para obtener información sobre la API, consulte UpdateService en la Referencia de comandos de la AWS CLI.

AWS Cloud9 Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS Cloud9.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-environment-ec2`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-environment-ec2`.

AWS CLI

Creación de un entorno de desarrollo de AWS Cloud9 EC2

En el siguiente ejemplo de `create-environment-ec2`, se crea un entorno de desarrollo de AWS Cloud9 con la configuración especificada, se lanza una instancia de Amazon Elastic Compute Cloud (Amazon EC2) y, después, se realiza la conexión al entorno desde la instancia.

```
aws cloud9 create-environment-ec2 \
    --name my-demo-env \
    --description "My demonstration development environment." \
    --instance-type t2.micro --image-id amazonlinux-2023-x86_64 \
    --subnet-id subnet-1fab8aEX \
    --automatic-stop-time-minutes 60 \
    --owner-arn arn:aws:iam::123456789012:user/MyDemoUser
```

Salida:

```
{
    "environmentId": "8a34f51ce1e04a08882f1e811bd706EX"
}
```

Para obtener más información, consulte Creating an EC2 Environment en la Guía del usuario de AWS Cloud9.

- Para obtener información sobre la API, consulte CreateEnvironmentEc2 en la Referencia de comandos de la AWS CLI.

`create-environment-membership`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-environment-membership`.

AWS CLI

Adición de un miembro del entorno a un entorno de desarrollo de AWS Cloud9

En este ejemplo, se agrega el miembro de entorno especificado al entorno de desarrollo de AWS Cloud9 especificado.

Comando:

```
aws cloud9 create-environment-membership --environment-
id 8a34f51ce1e04a08882f1e811bd706EX --user-arn arn:aws:iam::123456789012:user/
AnotherDemoUser --permissions read-write
```

Salida:

```
{
  "membership": {
    "environmentId": "8a34f51ce1e04a08882f1e811bd706EX",
    "userId": "AIDAJ3LOROMOUXTBSU6EX",
    "userArn": "arn:aws:iam::123456789012:user/AnotherDemoUser",
    "permissions": "read-write"
  }
}
```

- Para obtener información sobre la API, consulte CreateEnvironmentMembership en la Referencia de comandos de la AWS CLI.

`delete-environment-membership`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-environment-membership`.

AWS CLI

Eliminación de un miembro de entorno de un entorno de desarrollo de AWS Cloud9

En este ejemplo, se elimina el miembro de entorno especificado del entorno de desarrollo de AWS Cloud9 especificado.

Comando:

```
aws cloud9 delete-environment-membership --environment-
id 8a34f51ce1e04a08882f1e811bd706EX --user-arn arn:aws:iam::123456789012:user/
AnotherDemoUser
```

Salida:

```
None.
```

- Para obtener información sobre la API, consulte DeleteEnvironmentMembership en la Referencia de comandos de la AWS CLI.

`delete-environment`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-environment`.

AWS CLI

Eliminación de un entorno de desarrollo de AWS Cloud9

En este ejemplo, se elimina el entorno de desarrollo de AWS Cloud9 especificado. Si hay una instancia de Amazon EC2 conectada al entorno, se termina también la instancia.

Comando:

```
aws cloud9 delete-environment --environment-id 8a34f51ce1e04a08882f1e811bd706EX
```

Salida:

```
None.
```

- Para obtener información sobre la API, consulte DeleteEnvironment en la Referencia de comandos de la AWS CLI.

`describe-environment-memberships`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-environment-memberships`.

AWS CLI

Para obtener información sobre los miembros de entorno de un entorno de desarrollo de AWS Cloud9

En este ejemplo, se obtiene información sobre los miembros de entorno de un entorno de desarrollo de AWS Cloud9 especificado.

Comando:

```
aws cloud9 describe-environment-memberships --environment-
id 8a34f51ce1e04a08882f1e811bd706EX
```

Salida:

```
{
  "memberships": [
    {
      "environmentId": "8a34f51ce1e04a08882f1e811bd706EX",
      "userId": "AIDAJ3LOROMOUXTBSU6EX",
      "userArn": "arn:aws:iam::123456789012:user/AnotherDemoUser",
      "permissions": "read-write"
    },
    {
      "environmentId": "8a34f51ce1e04a08882f1e811bd706EX",
      "userId": "AIDAJNUEDQAQWFELJDLEX",
      "userArn": "arn:aws:iam::123456789012:user/MyDemoUser",
      "permissions": "owner"
    }
  ]
}
```

Para obtener información sobre el propietario de un entorno de desarrollo de AWS Cloud9

En este ejemplo, se obtiene información sobre el propietario del entorno de desarrollo de AWS Cloud9 especificado.

Comando:

```
aws cloud9 describe-environment-memberships --environment-
id 8a34f51ce1e04a08882f1e811bd706EX --permissions owner
```

Salida:

```
{
  "memberships": [
    {
      "environmentId": "8a34f51ce1e04a08882f1e811bd706EX",
      "userId": "AIDAJNUEDQAQWFELJDLEX",
      "userArn": "arn:aws:iam::123456789012:user/MyDemoUser",
      "permissions": "owner"
    }
  ]
}
```

Para obtener información sobre un miembro de entorno de varios entornos de desarrollo de AWS Cloud9

En este ejemplo, se obtiene información sobre el miembro de entorno especificado de varios entornos de desarrollo de AWS Cloud9.

Comando:

```
aws cloud9 describe-environment-memberships --user-
arn arn:aws:iam::123456789012:user/MyDemoUser
```

Salida:

```
{
  "memberships": [
    {
      "environmentId": "10a75714bd494714929e7f5ec4125aEX",
      "lastAccess": 1516213427.0,
      "userId": "AIDAJNUEDQAQWFELJDLEX",
      "userArn": "arn:aws:iam::123456789012:user/MyDemoUser",
      "permissions": "owner"
    },
    {
      "environmentId": "1980b80e5f584920801c09086667f0EX",
      "lastAccess": 1516144884.0,
      "userId": "AIDAJNUEDQAQWFELJDLEX",
      "userArn": "arn:aws:iam::123456789012:user/MyDemoUser",
      "permissions": "owner"
    }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeEnvironmentMemberships en la Referencia de comandos de la AWS CLI.

`describe-environment-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-environment-status`.

AWS CLI

Para obtener información de estado de un entorno de desarrollo de AWS Cloud9

En este ejemplo, se obtiene información sobre el entorno de desarrollo de AWS Cloud9 especificado.

Comando:

```
aws cloud9 describe-environment-status --environment-
id 685f892f431b45c2b28cb69eadcdb0EX
```

Salida:

```
{
  "status": "ready",
  "message": "Environment is ready to use"
}
```

- Para obtener información sobre la API, consulte DescribeEnvironmentStatus en la Referencia de comandos de la AWS CLI.

`describe-environments`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-environments`.

AWS CLI

Para obtener información sobre los entornos de desarrollo de AWS Cloud9

En este ejemplo, se obtiene información sobre los entornos de desarrollo de AWS Cloud9 especificados.

Comando:

```
aws cloud9 describe-environments --environment-
ids 685f892f431b45c2b28cb69eadcdb0EX 349c86d4579e4e7298d500ff57a6b2EX
```

Salida:

```
{
  "environments": [
    {
      "id": "685f892f431b45c2b28cb69eadcdb0EX",
```

```
      "name": "my-demo-ec2-env",
      "description": "Created from CodeStar.",
      "type": "ec2",
      "arn": "arn:aws:cloud9:us-
east-1:123456789012:environment:685f892f431b45c2b28cb69eadcdb0EX",
      "ownerArn": "arn:aws:iam::123456789012:user/MyDemoUser",
      "lifecycle": {
        "status": "CREATED"
      }
    },
    {
      "id": "349c86d4579e4e7298d500ff57a6b2EX",
      "name": my-demo-ssh-env",
      "description": "",
      "type": "ssh",
      "arn": "arn:aws:cloud9:us-
east-1:123456789012:environment:349c86d4579e4e7298d500ff57a6b2EX",
      "ownerArn": "arn:aws:iam::123456789012:user/MyDemoUser",
      "lifecycle": {
        "status": "CREATED"
      }
    }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeEnvironments en la Referencia de comandos de la AWS CLI.

`list-environments`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-environments`.

AWS CLI

Para obtener una lista de los identificadores de entorno de desarrollo de AWS Cloud9 disponibles

En este ejemplo, se obtiene una lista de los identificadores de entorno de desarrollo de AWS Cloud9 disponibles.

Comando:

```
aws cloud9 list-environments
```

Salida:

```
{
  "environmentIds": [
    "685f892f431b45c2b28cb69eadcdb0EX",
    "1980b80e5f584920801c09086667f0EX"
  ]
}
```

- Para obtener información sobre la API, consulte ListEnvironments en la Referencia de comandos de la AWS CLI.

update-environment-membership

En el siguiente ejemplo de código, se muestra cómo utilizar `update-environment-membership`.

AWS CLI

Cambio de la configuración de un miembro de entorno existente de un entorno de desarrollo de AWS Cloud9

En este ejemplo, se cambia la configuración del miembro de entorno existente especificado del entorno de desarrollo de AWS Cloud9 especificado.

Comando:

```
aws cloud9 update-environment-membership --environment-
id 8a34f51ce1e04a08882f1e811bd706EX --user-arn arn:aws:iam::123456789012:user/
AnotherDemoUser --permissions read-only
```

Salida:

```
{
  "membership": {
    "environmentId": "8a34f51ce1e04a08882f1e811bd706EX",
    "userId": "AIDAJ3LOROMOUXTBSU6EX",
    "userArn": "arn:aws:iam::123456789012:user/AnotherDemoUser",
    "permissions": "read-only"
  }
}
```

- Para obtener información sobre la API, consulte UpdateEnvironmentMembership en la Referencia de comandos de la AWS CLI.

`update-environment`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-environment`.

AWS CLI

Cambio de la configuración de un entorno de desarrollo de AWS Cloud9 existente

En este ejemplo, se cambia la configuración especificada del entorno de desarrollo de AWS Cloud9 existente especificado.

Comando:

```
aws cloud9 update-environment --environment-id 8a34f51ce1e04a08882f1e811bd706EX
 --name my-changed-demo-env --description "My changed demonstration development
 environment."
```

Salida:

```
None.
```

- Para obtener información sobre la API, consulte UpdateEnvironment en la Referencia de comandos de la AWS CLI.

CloudFormation Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con CloudFormation.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`activate-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `activate-type`.

AWS CLI

Activación de un tipo

En el siguiente ejemplo de `activate-type`, se activa una extensión pública de terceros y la pone a disposición para su uso en plantillas de pila.

```
aws cloudformation activate-type \
    --region us-west-2 \
    --type RESOURCE \
    --type-name Example::Test::1234567890abcdef0 \
    --type-name-alias Example::Test::Alias
```

Salida:

```
{
    "Arn": "arn:aws:cloudformation:us-west-2:123456789012:type/resource/Example-
Test-Alias"
}
```

Para obtener más información, consulte Uso del registro de AWS CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte ActivateType en la Referencia de comandos de la AWS CLI.

`batch-describe-type-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-describe-type-configurations`.

AWS CLI

Descripción por lotes de una configuración de tipo

En el siguiente ejemplo de `batch-describe-type-configurations`, se configuran los datos del tipo.

```
aws cloudformation batch-describe-type-configurations \
    --region us-west-2 \
    --type-configuration-identifiers TypeArn="arn:aws:cloudformation:us-
west-2:123456789012:type/resource/Example-Test-
Type,TypeConfigurationAlias=MyConfiguration"
```

Salida:

```
{
    "Errors": [],
    "UnprocessedTypeConfigurations": [],
    "TypeConfigurations": [
        {
            "Arn": "arn:aws:cloudformation:us-west-2:123456789012:type/resource/
Example-Test-Type",
            "Alias": "MyConfiguration",
            "Configuration": "{\n        \"Example\": {\n            \"ApiKey\":
 \"examplekey\",\n            \"ApplicationKey\": \"examplekey1\",\n
 \"ApiURL\": \"exampleurl\"\n            }\n}",
            "LastUpdated": "2021-10-01T15:25:46.210000+00:00",
            "TypeArn": "arn:aws:cloudformation:us-east-1:123456789012:type/resource/
Example-Test-Type"
        }
    ]
}
```

Para obtener más información, consulte Uso del registro de AWS CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte BatchDescribeTypeConfigurations en la Referencia de comandos de la AWS CLI.

`cancel-update-stack`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-update-stack`.

AWS CLI

Cancelación de una actualización de pila en progreso

El comando `cancel-update-stack` a continuación cancela una actualización de pila en la pila `myteststack`:

```
aws cloudformation cancel-update-stack --stack-name myteststack
```

- Para ver detalles de la API, consulte CancelUpdateStack en la Referencia de comandos de la AWS CLI.

`continue-update-rollback`

En el siguiente ejemplo de código, se muestra cómo utilizar `continue-update-rollback`.

AWS CLI

Nuevo intento de reversión de actualizaciones

El ejemplo de `continue-update-rollback` a continuación reanuda una operación de reversión a partir de un intento fallido previo de una actualización de pila.

```
aws cloudformation continue-update-rollback \
    --stack-name my-stack
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte ContinueUpdateRollback en la Referencia de comandos de la AWS CLI.

`create-change-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-change-set`.

AWS CLI

Creación de un conjunto de cambios

En el siguiente ejemplo de `create-change-set`, se crea un conjunto de cambios con la capacidad `CAPABILITY_IAM`. El archivo `template.yaml` es una plantilla de AWS CloudFormation en la carpeta actual que define una pila con recursos de IAM.

```
aws cloudformation create-change-set \
```

```
    --stack-name my-application \
    --change-set-name my-change-set \
    --template-body file://template.yaml \
    --capabilities CAPABILITY_IAM
```

Salida:

```
{
    "Id": "arn:aws:cloudformation:us-west-2:123456789012:changeSet/my-change-set/
bc9555ba-a949-xmpl-bfb8-f41d04ec5784",
    "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-application/
d0a825a0-e4cd-xmpl-b9fb-061c69e99204"
}
```

- Para obtener información sobre la API, consulte CreateChangeSet en la Referencia de comandos de la AWS CLI.

`create-generated-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-generated-template`.

AWS CLI

Creación de una plantilla generada a partir de recursos analizados

En el ejemplo de `create-generated-template` siguiente, se crea una plantilla generada denominada `MyTemplate` a partir de los recursos analizados.

```
aws cloudformation create-generated-template \
    --generated-template-name MyTemplate \
    --resources file://resources.json
```

Contenido de `resources.json`:

```
[
    {
        "ResourceType": "AWS::EKS::Cluster",
        "LogicalResourceId":"MyCluster",
        "ResourceIdentifier": {
            "ClusterName": "MyAppClusterName"
        }
```

```
    },
    {
        "ResourceType": "AWS::AutoScaling::AutoScalingGroup",
        "LogicalResourceId":"MyASG",
        "ResourceIdentifier": {
            "AutoScalingGroupName": "MyAppASGName"
        }
    },
    {
        "ResourceType": "AWS::EKS::Nodegroup",
        "LogicalResourceId":"MyNodegroup",
        "ResourceIdentifier": {
            "NodegroupName": "MyAppNodegroupName"
        }
    },
    {
        "ResourceType": "AWS::IAM::Role",
        "LogicalResourceId":"MyRole",
        "ResourceIdentifier": {
            "RoleId": "arn:aws::iam::123456789012:role/MyAppIAMRole"
        }
    }
]
```

Salida:

```
{
  "Arn":
    "arn:aws:cloudformation:us-east-1:123456789012:generatedtemplate/7fc8512c-
d8cb-4e02-b266-d39c48344e48",
  "Name": "MyTemplate"
}
```

Para obtener más información, consulte Crear una plantilla de CloudFormation a partir de recursos analizados con el generador de IaC en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte CreateGeneratedTemplate en la Referencia de comandos de la AWS CLI.

`create-stack-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-stack-instances`.

AWS CLI

Creación de instancias de pila

En el siguiente ejemplo de `create-stack-instances`, se crean instancias de un conjunto de pilas en dos cuentas y en cuatro regiones. La configuración de tolerancia a errores garantiza que se intente la actualización en todas las cuentas y regiones, incluso si no se pueden crear algunas pilas.

```
aws cloudformation create-stack-instances \
    --stack-set-name my-stack-set \
    --accounts 123456789012 223456789012 \
    --regions us-east-1 us-east-2 us-west-1 us-west-2 \
    --operation-preferences FailureToleranceCount=7
```

Salida:

```
{
    "OperationId": "d7995c31-83c2-xmpl-a3d4-e9ca2811563f"
}
```

Para crear un conjunto de pilas, utilice el comando `create-stack-set`.

- Para obtener información sobre la API, consulte CreateStackInstances en la Referencia de comandos de la AWS CLI.

`create-stack-refactor`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-stack-refactor`.

AWS CLI

Creación de la definición de pila para una operación de refactorización de pila

En el ejemplo de `create-stack-refactor` siguiente, se crea la definición de pila para la refactorización de la pila.

```
aws cloudformation create-stack-refactor \
    --stack-definitions \
      StackName=Stack1,TemplateBody@=file://template1-updated.yaml \
```

```
    StackName=Stack2,TemplateBody@=file://template2-updated.yaml
```

Salida:

```
{
    "StackRefactorId": "9c384f70-4e07-4ed7-a65d-fee5eb430841"
}
```

Para obtener más información, consulte Refactorización de pilas en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte CreateStackRefactor en la Referencia de comandos de la AWS CLI.

`create-stack-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-stack-set`.

AWS CLI

Creación de un conjunto de pilas

En el siguiente ejemplo de `create-stack-set`, se crea un conjunto de pilas con la plantilla de archivo YAML especificada. `template.yaml` es una plantilla de AWS CloudFormation en la carpeta actual que define una pila.

```
aws cloudformation create-stack-set \
    --stack-set-name my-stack-set \
    --template-body file://template.yaml \
    --description "SNS topic"
```

Salida:

```
{
    "StackSetId": "my-stack-set:8d0f160b-d157-xmpl-a8e6-c0ce8e5d8cc1"
}
```

Para añadir instancias de pila al conjunto de pilas, utilice el comando `create-stack-instances`.

- Para obtener información sobre la API, consulte CreateStackSet en la Referencia de comandos de la AWS CLI.

`create-stack`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-stack`.

AWS CLI

Creación de una pila de AWS CloudFormation

En el siguiente ejemplo de `create-stacks`, se crea una pila con el nombre `myteststack` mediante la plantilla `sampletemplate.json`:

```
aws cloudformation create-stack --stack-name myteststack --template-body file://
sampletemplate.json --parameters ParameterKey=KeyPairName,ParameterValue=TestKey
 ParameterKey=SubnetIDs,ParameterValue=SubnetID1\\,SubnetID2
```

Salida:

```
{
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896"
}
```

Para obtener más información, consulte Pilas en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte CreateStack en la Referencia de comandos de la AWS CLI.

`deactivate-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `deactivate-type`.

AWS CLI

Desactivación de un tipo

En el siguiente ejemplo de `deactivate-type`, se desactiva una extensión pública previamente activada en dicha cuenta y región.

```
aws cloudformation deactivate-type \
    --region us-west-2 \
    --type MODULE \
    --type-name Example::Test::Type::MODULE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso del registro de AWS CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte DeactivateType en la Referencia de comandos de la AWS CLI.

`delete-change-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-change-set`.

AWS CLI

Eliminación de un conjunto de cambios

En el siguiente ejemplo de `delete-change-set`, se elimina un conjunto de cambios especificando el nombre del conjunto de cambios y el nombre de la pila.

```
aws cloudformation delete-change-set \
    --stack-name my-stack \
    --change-set-name my-change-set
```

Este comando no genera ninguna salida.

En el siguiente ejemplo de `delete-change-set`, se elimina un conjunto de cambios especificando el ARN completo del conjunto de cambios.

```
aws cloudformation delete-change-set \
    --change-set-name arn:aws:cloudformation:us-east-2:123456789012:changeSet/my-change-set/4eca1a01-e285-xmpl-8026-9a1967bfb4b0
```

Este comando no genera ninguna salida.

- Para obtener más información sobre la API, consulte DeleteChangeSet en la Referencia de comandos de la AWS CLI.

`delete-generated-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-generated-template`.

AWS CLI

Eliminación de una plantilla generada

En el ejemplo de `delete-generated-template` siguiente, se elimina la plantilla especificada.

```
aws cloudformation delete-generated-template \
    --generated-template-name MyTemplate
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Generación de plantillas a partir de los recursos existentes en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte DeleteGeneratedTemplate en la Referencia de comandos de la AWS CLI.

`delete-stack-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-stack-instances`.

AWS CLI

Eliminación de instancias de pila

En el siguiente ejemplo de `delete-stack-instances`, se eliminan instancias de un conjunto de pilas en dos cuentas y en dos regiones, y se terminan las pilas.

```
aws cloudformation delete-stack-instances \
    --stack-set-name my-stack-set \
    --accounts 123456789012 567890123456 \
    --regions us-east-1 us-west-1 \
    --no-retain-stacks
```

Salida:

```
{
```

```
    "OperationId": "ad49f10c-fd1d-413f-a20a-8de6e2fa8f27"
}
```

Para eliminar un conjunto de pilas vacío, utilice el comando `delete-stack-set`.

- Para obtener información sobre la API, consulte DeleteStackInstances en la Referencia de comandos de la AWS CLI.

`delete-stack-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-stack-set`.

AWS CLI

Eliminación de un conjunto de pilas

Con el siguiente comando se elimina el conjunto de pilas vacío especificado. El conjunto de pilas debe estar vacío.

```
aws cloudformation delete-stack-set \
    --stack-set-name my-stack-set
```

Este comando no genera ninguna salida.

Para eliminar instancias del conjunto de pilas, utilice el comando `delete-stack-instances`.

- Para obtener información sobre la API, consulte DeleteStackSet en la Referencia de comandos de la AWS CLI.

`delete-stack`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-stack`.

AWS CLI

Eliminación de una pila

En el siguiente ejemplo de `delete-stack`, se elimina la pila especificada.

```
aws cloudformation delete-stack \
```

```
    --stack-name my-stack
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteStack en la Referencia de comandos de la AWS CLI.

deploy

En el siguiente ejemplo de código, se muestra cómo utilizar `deploy`.

AWS CLI

Con el siguiente comando, se despliega la plantilla denominada `template.json` en una pila llamada `my-new-stack`:

```
aws cloudformation deploy --template-file /path_to_template/template.json
 --stack-name my-new-stack --parameter-overrides Key1=Value1 Key2=Value2 --
tags Key1=Value1 Key2=Value2
```

- Para obtener información sobre la API, consulte Deploy en la Referencia de comandos de la AWS CLI.

deregister-type

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-type`.

AWS CLI

Anulación del registro de una versión de tipo

En el siguiente ejemplo de `deregister-type`, se elimina la versión de tipo especificada del uso activo en el registro de CloudFormation, de manera que ya no se pueda utilizar en las operaciones de CloudFormation.

```
aws cloudformation deregister-type \
    --type RESOURCE \
    --type-name My::Logs::LogGroup \
    --version-id 00000002
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso del registro de CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte DeregisterType en la Referencia de comandos de la AWS CLI.

`describe-account-limits`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-account-limits`.

AWS CLI

Obtención de información sobre los límites de la cuenta

Con el siguiente comando, se genera una lista de los límites regionales de la cuenta actual.

```
aws cloudformation describe-account-limits
```

Salida:

```
{
    "AccountLimits": [
        {
            "Name": "StackLimit",
            "Value": 200
        },
        {
            "Name": "StackOutputsLimit",
            "Value": 60
        },
        {
            "Name": "ConcurrentResourcesLimit",
            "Value": 2500
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeAccountLimits en la Referencia de comandos de la AWS CLI.

describe-change-set

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-change-set`.

AWS CLI

Obtención de información sobre un conjunto de cambios

En el siguiente ejemplo de `describe-change-set`, se muestran los detalles del conjunto de cambios especificado por el nombre del conjunto de cambios y el nombre de la pila.

```
aws cloudformation describe-change-set \
    --change-set-name my-change-set \
    --stack-name my-stack
```

En el siguiente ejemplo de `describe-change-set`, se muestran los detalles del conjunto de cambios especificando por el ARN completo del conjunto de cambios:

```
aws cloudformation describe-change-set \
    --change-set-name arn:aws:cloudformation:us-west-2:123456789012:changeSet/my-change-set/bc9555ba-a949-xmpl-bfb8-f41d04ec5784
```

Salida:

```
{
    "Changes": [
        {
            "Type": "Resource",
            "ResourceChange": {
                "Action": "Modify",
                "LogicalResourceId": "function",
                "PhysicalResourceId": "my-function-SEZV4XMPL4S5",
                "ResourceType": "AWS::Lambda::Function",
                "Replacement": "False",
                "Scope": [
                    "Properties"
                ],
                "Details": [
                    {
                        "Target": {
                            "Attribute": "Properties",
```

```
                            "Name": "Timeout",
                            "RequiresRecreation": "Never"
                        },
                        "Evaluation": "Static",
                        "ChangeSource": "DirectModification"
                    }
                ]
            }
        }
    ],
    "ChangeSetName": "my-change-set",
    "ChangeSetId": "arn:aws:cloudformation:us-west-2:123456789012:changeSet/my-
change-set/4eca1a01-e285-xmpl-8026-9a1967bfb4b0",
    "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-stack/
d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
    "StackName": "my-stack",
    "Description": null,
    "Parameters": null,
    "CreationTime": "2019-10-02T05:20:56.651Z",
    "ExecutionStatus": "AVAILABLE",
    "Status": "CREATE_COMPLETE",
    "StatusReason": null,
    "NotificationARNs": [],
    "RollbackConfiguration": {},
    "Capabilities": [
        "CAPABILITY_IAM"
    ],
    "Tags": null
}
```

- Para obtener información sobre la API, consulte DescribeChangeSet en la Referencia de comandos de la AWS CLI.

`describe-generated-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-generated-template`.

AWS CLI

Descripción de una plantilla generada

En el ejemplo de `describe-generated-template` siguiente, se describe la plantilla especificada.

```
aws cloudformation describe-generated-template \
    --generated-template-name MyTemplate
```

Salida:

```
{
    "GeneratedTemplateId": "arn:aws:cloudformation:us-
east-1:123456789012:generatedTemplate/7d881acf-f307-4ded-910e-f8fb49b96894",
    "GeneratedTemplateName": "MyTemplate",
    "Resources": [
        {
            "ResourceType": "AWS::EC2::SecurityGroup",
            "LogicalResourceId": "EC2SecurityGroup",
            "ResourceIdentifier": {
                "Id": "sg-1234567890abcdef0"
            },
            "ResourceStatus": "COMPLETE",
            "ResourceStatusReason": "Resource Template complete",
            "Warnings": []
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "LogicalResourceId": "EC2Instance",
            "ResourceIdentifier": {
                "InstanceId": "i-1234567890abcdef0"
            },
            "ResourceStatus": "COMPLETE",
            "ResourceStatusReason": "Resource Template complete",
            "Warnings": []
        },
        {
            "ResourceType": "AWS::EC2::KeyPair",
            "LogicalResourceId": "EC2KeyPairSshkeypair",
            "ResourceIdentifier": {
                "KeyName": "sshkeypair"
            },
            "ResourceStatus": "COMPLETE",
            "ResourceStatusReason": "Resource Template complete",
            "Warnings": []
        }
    ],
    "Status": "COMPLETE",
    "StatusReason": "All resources complete",
```

```
    "CreationTime": "2025-09-23T19:38:06.435000+00:00",
    "LastUpdatedTime": "2025-09-23T19:38:10.798000+00:00",
    "Progress": {
        "ResourcesSucceeded": 3,
        "ResourcesFailed": 0,
        "ResourcesProcessing": 0,
        "ResourcesPending": 0
    },
    "TemplateConfiguration": {
        "DeletionPolicy": "RETAIN",
        "UpdateReplacePolicy": "RETAIN"
    },
    "TotalWarnings": 0
}
```

Para obtener más información, consulte Generación de plantillas a partir de los recursos existentes en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte DescribeGeneratedTemplate en la Referencia de comandos de la AWS CLI.

`describe-publisher`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-publisher`.

AWS CLI

Descripción de un publicador

En el siguiente ejemplo de `describe-publisher`, se configura la información de un publicador.

```
aws cloudformation describe-publisher \
    --region us-west-2 \
    --publisher-id 000q6TfUovXsEMmgKowxDZLlwqr2QUsh
```

Salida:

```
{
    "PublisherId": "000q6TfUovXsEMmgKowxDZLlwqr2QUshd2e75c8c",
    "PublisherStatus": "VERIFIED",
    "IdentityProvider": "AWS_Marketplace",
    "PublisherProfile": "https://aws.amazon.com/marketplace/seller-profile?
id=2c5dc1f0-17cd-4259-8e46-822a83gdtegd"
```

```
}
```

Para obtener más información, consulte Uso del registro de AWS CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte DescribePublisher en la Referencia de comandos de la AWS CLI.

`describe-resource-scan`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-resource-scan`.

AWS CLI

Cómo describir un escaneo de recursos

En el ejemplo de `describe-resource-scan` siguiente, se describe el análisis de recursos con el ID de análisis especificado.

```
aws cloudformation describe-resource-scan --region \
    --resource-scan-id arn:aws:cloudformation:us-
east-1:123456789012:resourceScan/0a699f15-489c-43ca-a3ef-3e6ecfa5da60
```

Salida:

```
{
    "ResourceScanId": "arn:aws:cloudformation:us-
east-1:123456789012:resourceScan/0a699f15-489c-43ca-a3ef-3e6ecfa5da60",
    "Status": "COMPLETE",
    "StartTime": "2025-08-21T03:10:38.485000+00:00",
    "EndTime": "2025-08-21T03:20:28.485000+00:00",
    "PercentageCompleted": 100.0,
    "ResourceTypes": [
        "AWS::CloudFront::CachePolicy",
        "AWS::CloudFront::OriginRequestPolicy",
        "AWS::EC2::DHCPOptions",
        "AWS::EC2::InternetGateway",
        "AWS::EC2::KeyPair",
        "AWS::EC2::NetworkAcl",
        "AWS::EC2::NetworkInsightsPath",
        "AWS::EC2::NetworkInterface",
        "AWS::EC2::PlacementGroup",
```

```
        "AWS::EC2::Route",
        "AWS::EC2::RouteTable",
        "AWS::EC2::SecurityGroup",
        "AWS::EC2::Subnet",
        "AWS::EC2::SubnetCidrBlock",
        "AWS::EC2::SubnetNetworkAclAssociation",
        "AWS::EC2::SubnetRouteTableAssociation",
        ...
    ],
    "ResourcesRead": 676
}
```

Para obtener más información, consulte Generación de plantillas a partir de los recursos existentes en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte DescribeResourceScan en la Referencia de comandos de la AWS CLI.

`describe-stack-drift-detection-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stack-drift-detection-status`.

AWS CLI

Comprobación del estado de una operación de detección de desviaciones

En el siguiente ejemplo de `describe-stack-drift-detection-status`, se muestra el estado de una operación de detección de desviaciones. Se puede obtener el ID ejecutando el comando `detect-stack-drift`.

```
aws cloudformation describe-stack-drift-detection-status \
    --stack-drift-detection-id 1a229160-e4d9-xmpl-ab67-0a4f93df83d4
```

Salida:

```
{
    "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-stack/
d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
    "StackDriftDetectionId": "1a229160-e4d9-xmpl-ab67-0a4f93df83d4",
    "StackDriftStatus": "DRIFTED",
    "DetectionStatus": "DETECTION_COMPLETE",
```

```
    "DriftedStackResourceCount": 1,
    "Timestamp": "2019-10-02T05:54:30.902Z"
}
```

- Para obtener información sobre la API, consulte DescribeStackDriftDetectionStatus en la Referencia de comandos de la AWS CLI.

`describe-stack-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stack-events`.

AWS CLI

Descripción de los eventos de la pila

En el siguiente ejemplo de `describe-stack-events`, se muestran los dos eventos más recientes de la pila especificada.

```
aws cloudformation describe-stack-events \
    --stack-name my-stack \
    --max-items 2

{
    "StackEvents": [
        {
            "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-
stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
            "EventId": "4e1516d0-e4d6-xmpl-b94f-0a51958a168c",
            "StackName": "my-stack",
            "LogicalResourceId": "my-stack",
            "PhysicalResourceId": "arn:aws:cloudformation:us-
west-2:123456789012:stack/my-stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
            "ResourceType": "AWS::CloudFormation::Stack",
            "Timestamp": "2019-10-02T05:34:29.556Z",
            "ResourceStatus": "UPDATE_COMPLETE"
        },
        {
            "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-
stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
            "EventId": "4dd3c810-e4d6-xmpl-bade-0aaf8b31ab7a",
            "StackName": "my-stack",
            "LogicalResourceId": "my-stack",
```

```
            "PhysicalResourceId": "arn:aws:cloudformation:us-
west-2:123456789012:stack/my-stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
            "ResourceType": "AWS::CloudFormation::Stack",
            "Timestamp": "2019-10-02T05:34:29.127Z",
            "ResourceStatus": "UPDATE_COMPLETE_CLEANUP_IN_PROGRESS"
        }
    ],

 "NextToken": "eyJOZXh0VG9XMPLiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAyfQ=="
}
```

- Para obtener información sobre la API, consulte DescribeStackEvents en la Referencia de comandos de la AWS CLI.

`describe-stack-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stack-instance`.

AWS CLI

Descripción de una instancia de pila

Con el siguiente comando se describe una instancia del conjunto de pilas especificado en la cuenta y la región especificadas. El conjunto de pilas se encuentra en la región y la cuenta actuales, y la instancia se encuentra en la región `us-west-2` de la cuenta `123456789012`.

```
aws cloudformation describe-stack-instance \
    --stack-set-name my-stack-set \
    --stack-instance-account 123456789012 \
    --stack-instance-region us-west-2
```

Salida:

```
{
    "StackInstance": {
        "StackSetId": "enable-config:296a3360-xmpl-40af-be78-9341e95bf743",
        "Region": "us-west-2",
        "Account": "123456789012",
        "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/
StackSet-enable-config-e6cac20f-xmpl-46e9-8314-53e0d4591532/4287f9a0-e615-
xmpl-894a-12b31d3117be",
        "ParameterOverrides": [],
```

```
        "Status": "OUTDATED",
        "StatusReason": "ResourceLogicalId:ConfigBucket,
 ResourceType:AWS::S3::Bucket, ResourceStatusReason:You have attempted to create
 more buckets than allowed (Service: Amazon S3; Status Code: 400; Error Code:
 TooManyBuckets; Request ID: F7F21CXMPL580224; S3 Extended Request ID: egd/
Fdt89BXMPLyiqbMNljVk55Yqqvi3NYW2nKLUVWhUGEhNfCmZdyj967lhriaG/dWMobSO40o=)."
    }
}
```

- Para obtener información sobre la API, consulte DescribeStackInstance en la Referencia de comandos de la AWS CLI.

`describe-stack-refactor`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stack-refactor`.

AWS CLI

Descripción de una operación de refactorización de pilas

En el ejemplo de `describe-stack-refactor` siguiente, se describe la operación de refactorización de pilas con el ID de refactorización de pila especificado.

```
aws cloudformation describe-stack-refactor \
    --stack-refactor-id 9c384f70-4e07-4ed7-a65d-fee5eb430841
```

Salida:

```
{
    "StackRefactorId": "9c384f70-4e07-4ed7-a65d-fee5eb430841",
    "StackIds": [
        "arn:aws:cloudformation:us-east-1:123456789012:stack/
Stack1/3e6a1ff0-94b1-11f0-aa6f-0a88d2e03acf",
        "arn:aws:cloudformation:us-east-1:123456789012:stack/
Stack2/5da91650-94b1-11f0-81cf-0a23500e151b"
    ],
    "ExecutionStatus": "AVAILABLE",
    "Status": "CREATE_COMPLETE"
}
```

Para obtener más información, consulte Refactorización de pilas en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte DescribeStackRefactor en la Referencia de comandos de la AWS CLI.

`describe-stack-resource-drifts`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stack-resource-drifts`.

AWS CLI

Obtención de información sobre los recursos desviados de la definición de pila

En el siguiente comando, se muestra información acerca de los recursos desviados de la pila especificada. Para iniciar la detección de desviaciones, utilice el comando `detect-stack-drift`:

```
aws cloudformation describe-stack-resource-drifts \
    --stack-name my-stack
```

El resultado muestra una función de AWS Lambda que se ha modificado fuera de banda:

```
{
    "StackResourceDrifts": [
        {
            "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-
stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
            "LogicalResourceId": "function",
            "PhysicalResourceId": "my-function-SEZV4XMPL4S5",
            "ResourceType": "AWS::Lambda::Function",
            "ExpectedProperties": "{\"Description\":\"Write a file to S3.\",
\"Environment\":{\"Variables\":{\"bucket\":\"my-stack-bucket-1vc62xmplgguf
\"}},\"Handler\":\"index.handler\",\"MemorySize\":128,\"Role\":
\"arn:aws:iam::123456789012:role/my-functionRole-HIZXMPLEOM9E\",\"Runtime\":
\"nodejs10.x\",\"Tags\":[{\"Key\":\"lambda:createdBy\",\"Value\":\"SAM\"}],\"Timeout
\":900,\"TracingConfig\":{\"Mode\":\"Active\"}}",
            "ActualProperties": "{\"Description\":\"Write a file to S3.\",
\"Environment\":{\"Variables\":{\"bucket\":\"my-stack-bucket-1vc62xmplgguf
\"}},\"Handler\":\"index.handler\",\"MemorySize\":256,\"Role\":
\"arn:aws:iam::123456789012:role/my-functionRole-HIZXMPLEOM9E\",\"Runtime\":
\"nodejs10.x\",\"Tags\":[{\"Key\":\"lambda:createdBy\",\"Value\":\"SAM\"}],\"Timeout
\":22,\"TracingConfig\":{\"Mode\":\"Active\"}}",
            "PropertyDifferences": [
                {
```

```
                    "PropertyPath": "/MemorySize",
                    "ExpectedValue": "128",
                    "ActualValue": "256",
                    "DifferenceType": "NOT_EQUAL"
                },
                {
                    "PropertyPath": "/Timeout",
                    "ExpectedValue": "900",
                    "ActualValue": "22",
                    "DifferenceType": "NOT_EQUAL"
                }
            ],
            "StackResourceDriftStatus": "MODIFIED",
            "Timestamp": "2019-10-02T05:54:44.064Z"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeStackResourceDrifts en la Referencia de comandos de la AWS CLI.

`describe-stack-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stack-resource`.

AWS CLI

Obtención de información sobre un recurso de pila

En el siguiente ejemplo de `describe-stack-resource`, se muestran los detalles del recurso con el nombre `MyFunction` en la pila especificada.

```
aws cloudformation describe-stack-resource \
    --stack-name MyStack \
    --logical-resource-id MyFunction
```

Salida:

```
{
    "StackResourceDetail": {
        "StackName": "MyStack",
```

```
        "StackId": "arn:aws:cloudformation:us-east-2:123456789012:stack/MyStack/
d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
        "LogicalResourceId": "MyFunction",
        "PhysicalResourceId": "my-function-SEZV4XMPL4S5",
        "ResourceType": "AWS::Lambda::Function",
        "LastUpdatedTimestamp": "2019-10-02T05:34:27.989Z",
        "ResourceStatus": "UPDATE_COMPLETE",
        "Metadata": "{}",
        "DriftInformation": {
            "StackResourceDriftStatus": "IN_SYNC"
        }
    }
}
```

- Para obtener información sobre la API, consulte DescribeStackResource en la Referencia de comandos de la AWS CLI.

`describe-stack-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stack-resources`.

AWS CLI

Obtención de información sobre un recurso de pila

En el siguiente ejemplo de `describe-stack-resources`, se muestran los detalles de los recursos en la pila especificada.

```
aws cloudformation describe-stack-resources \
    --stack-name my-stack
```

Salida:

```
{
    "StackResources": [
        {
            "StackName": "my-stack",
            "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-
stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
            "LogicalResourceId": "bucket",
            "PhysicalResourceId": "my-stack-bucket-1vc62xmplgguf",
```

```
            "ResourceType": "AWS::S3::Bucket",
            "Timestamp": "2019-10-02T04:34:11.345Z",
            "ResourceStatus": "CREATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "IN_SYNC"
            }
        },
        {
            "StackName": "my-stack",
            "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-
stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
            "LogicalResourceId": "function",
            "PhysicalResourceId": "my-function-SEZV4XMPL4S5",
            "ResourceType": "AWS::Lambda::Function",
            "Timestamp": "2019-10-02T05:34:27.989Z",
            "ResourceStatus": "UPDATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "IN_SYNC"
            }
        },
        {
            "StackName": "my-stack",
            "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-
stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
            "LogicalResourceId": "functionRole",
            "PhysicalResourceId": "my-functionRole-HIZXMPLEOM9E",
            "ResourceType": "AWS::IAM::Role",
            "Timestamp": "2019-10-02T04:34:06.350Z",
            "ResourceStatus": "CREATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "IN_SYNC"
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeStackResources en la Referencia de comandos de la AWS CLI.

`describe-stack-set-operation`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stack-set-operation`.

AWS CLI

Obtención de información sobre una operación de conjunto de pilas

En el siguiente ejemplo de describe-stack-set-operation, se muestran los detalles de una operación de actualización en el conjunto de pilas especificado.

```
aws cloudformation describe-stack-set-operation \
    --stack-set-name enable-config \
    --operation-id 35d45ebc-ed88-xmpl-ab59-0197a1fc83a0
```

Salida:

```
{
    "StackSetOperation": {
        "OperationId": "35d45ebc-ed88-xmpl-ab59-0197a1fc83a0",
        "StackSetId": "enable-config:296a3360-xmpl-40af-be78-9341e95bf743",
        "Action": "UPDATE",
        "Status": "SUCCEEDED",
        "OperationPreferences": {
            "RegionOrder": [
                "us-east-1",
                "us-west-2",
                "eu-west-1",
                "us-west-1"
            ],
            "FailureToleranceCount": 7,
            "MaxConcurrentCount": 2
        },
        "AdministrationRoleARN": "arn:aws:iam::123456789012:role/
AWSCloudFormationStackSetAdministrationRole",
        "ExecutionRoleName": "AWSCloudFormationStackSetExecutionRole",
        "CreationTimestamp": "2019-10-03T16:28:44.377Z",
        "EndTimestamp": "2019-10-03T16:42:08.607Z"
    }
}
```

- Para obtener información sobre la API, consulte DescribeStackSetOperation en la Referencia de comandos de la AWS CLI.

`describe-stack-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stack-set`.

AWS CLI

Obtención de información sobre un conjunto de pilas

En el siguiente ejemplo de describe-stack-set, se muestran los detalles del conjunto de pilas especificado.

```
aws cloudformation describe-stack-set \
    --stack-set-name my-stack-set
```

Salida:

```
{
    "StackSet": {
        "StackSetName": "my-stack-set",
        "StackSetId": "my-stack-set:296a3360-xmpl-40af-be78-9341e95bf743",
        "Description": "Create an Amazon SNS topic",
        "Status": "ACTIVE",
        "TemplateBody": "AWSTemplateFormatVersion: '2010-09-09'\nDescription: An AWS
 SNS topic\nResources:\n  topic:\n    Type: AWS::SNS::Topic",
        "Parameters": [],
        "Capabilities": [],
        "Tags": [],
        "StackSetARN": "arn:aws:cloudformation:us-west-2:123456789012:stackset/
enable-config:296a3360-xmpl-40af-be78-9341e95bf743",
        "AdministrationRoleARN": "arn:aws:iam::123456789012:role/
AWSCloudFormationStackSetAdministrationRole",
        "ExecutionRoleName": "AWSCloudFormationStackSetExecutionRole"
    }
}
```

- Para obtener información sobre la API, consulte DescribeStackSet en la Referencia de comandos de la AWS CLI.

`describe-stacks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stacks`.

AWS CLI

Descripción de las pilas de AWS CloudFormation

En el siguiente ejemplo de `describe-stacks`, se muestra la información del resumen para la pila `myteststack`:

```
aws cloudformation describe-stacks --stack-name myteststack
```

Salida:

```
{
    "Stacks":  [
        {
            "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896",
            "Description": "AWS CloudFormation Sample Template S3_Bucket: Sample
 template showing how to create a publicly accessible S3 bucket. **WARNING** This
 template creates an S3 bucket. You will be billed for the AWS resources used if you
 create a stack from this template.",
            "Tags": [],
            "Outputs": [
                {
                    "Description": "Name of S3 bucket to hold website content",
                    "OutputKey": "BucketName",
                    "OutputValue": "myteststack-s3bucket-jssofi1zie2w"
                }
            ],
            "StackStatusReason": null,
            "CreationTime": "2013-08-23T01:02:15.422Z",
            "Capabilities": [],
            "StackName": "myteststack",
            "StackStatus": "CREATE_COMPLETE",
            "DisableRollback": false
        }
    ]
}
```

Para obtener más información, consulte Pilas en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte DescribeStacks en la Referencia de comandos de la AWS CLI.

`describe-type-registration`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-type-registration`.

AWS CLI

Obtención de información del registro de tipo

En el siguiente ejemplo de `describe-type-registration`, se muestra información sobre el registro del tipo especificado, incluidos el estado, el tipo y la versión actuales de dicho tipo.

```
aws cloudformation describe-type-registration \
    --registration-token a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "ProgressStatus": "COMPLETE",
    "TypeArn": "arn:aws:cloudformation:us-west-2:123456789012:type/resource/My-Logs-
LogGroup",
    "Description": "Deployment is currently in DEPLOY_STAGE of status COMPLETED; ",
    "TypeVersionArn": "arn:aws:cloudformation:us-west-2:123456789012:type/resource/
My-Logs-LogGroup/00000001"
}
```

Para obtener más información, consulte Uso del registro de CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte DescribeTypeRegistration en la Referencia de comandos de la AWS CLI.

`describe-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-type`.

AWS CLI

Obtención de información de tipo

En el siguiente ejemplo de `describe-type`, se muestra información del tipo especificado.

```
aws cloudformation describe-type \
```

```
    --type-name My::Logs::LogGroup \
    --type RESOURCE
```

Salida:

```
{
    "SourceUrl": "https://github.com/aws-cloudformation/aws-cloudformation-resource-
providers-logs.git",
    "Description": "Customized resource derived from AWS::Logs::LogGroup",
    "TimeCreated": "2019-12-03T23:29:33.321Z",
    "Visibility": "PRIVATE",
    "TypeName": "My::Logs::LogGroup",
    "LastUpdated": "2019-12-03T23:29:33.321Z",
    "DeprecatedStatus": "LIVE",
    "ProvisioningType": "FULLY_MUTABLE",
    "Type": "RESOURCE",
    "Arn": "arn:aws:cloudformation:us-west-2:123456789012:type/resource/My-Logs-
LogGroup/00000001",
    "Schema": "[details omitted]"
}
```

Para obtener más información, consulte Uso del registro de CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte DescribeType en la Referencia de comandos de la AWS CLI.

`detect-stack-drift`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-stack-drift`.

AWS CLI

Detección de recursos desviados

En el siguiente ejemplo de `detect-stack-drift`, se inicia la detección de desviación en la pila especificada.

```
aws cloudformation detect-stack-drift \
    --stack-name my-stack
```

Salida:

```
{
    "StackDriftDetectionId": "1a229160-e4d9-xmpl-ab67-0a4f93df83d4"
}
```

A continuación, puede utilizar este ID con el comando `describe-stack-resource-drifts` para describir los recursos desviados.

- Para obtener información sobre la API, consulte DetectStackDrift en la Referencia de comandos de la AWS CLI.

`detect-stack-resource-drift`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-stack-resource-drift`.

AWS CLI

Detección de la desviación de un recurso

En el siguiente ejemplo de `detect-stack-resource-drift`, se comprueba la desviación un recurso denominado `MyFunction` en una pila llamada `MyStack`:

```
aws cloudformation detect-stack-resource-drift \
   --stack-name MyStack \
   --logical-resource-id MyFunction
```

El resultado muestra una función de AWS Lambda que se ha modificado fuera de banda:

```
{
    "StackResourceDrift": {
        "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/MyStack/
d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
        "LogicalResourceId": "MyFunction",
        "PhysicalResourceId": "my-function-SEZV4XMPL4S5",
        "ResourceType": "AWS::Lambda::Function",
        "ExpectedProperties": "{\"Description\":\"Write a file to S3.\",
\"Environment\":{\"Variables\":{\"bucket\":\"my-stack-bucket-1vc62xmplgguf
\"}},\"Handler\":\"index.handler\",\"MemorySize\":128,\"Role\":
\"arn:aws:iam::123456789012:role/my-functionRole-HIZXMPLEOM9E\",\"Runtime\":
\"nodejs10.x\",\"Tags\":[{\"Key\":\"lambda:createdBy\",\"Value\":\"SAM\"}],\"Timeout
\":900,\"TracingConfig\":{\"Mode\":\"Active\"}}",
        "ActualProperties": "{\"Description\":\"Write a file to S3.\",\"Environment
\":{\"Variables\":{\"bucket\":\"my-stack-bucket-1vc62xmplgguf\"}},\"Handler\":
```

```
\"index.handler\",\"MemorySize\":256,\"Role\":\"arn:aws:iam::123456789012:role/
my-functionRole-HIZXMPLEOM9E\",\"Runtime\":\"nodejs10.x\",\"Tags\":[{\"Key\":
\"lambda:createdBy\",\"Value\":\"SAM\"}],\"Timeout\":22,\"TracingConfig\":{\"Mode\":
\"Active\"}}",
        "PropertyDifferences": [
            {
                "PropertyPath": "/MemorySize",
                "ExpectedValue": "128",
                "ActualValue": "256",
                "DifferenceType": "NOT_EQUAL"
            },
            {
                "PropertyPath": "/Timeout",
                "ExpectedValue": "900",
                "ActualValue": "22",
                "DifferenceType": "NOT_EQUAL"
            }
        ],
        "StackResourceDriftStatus": "MODIFIED",
        "Timestamp": "2019-10-02T05:58:47.433Z"
    }
}
```

- Para obtener información sobre la API, consulte DetectStackResourceDrift en la Referencia de comandos de la AWS CLI.

`detect-stack-set-drift`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-stack-set-drift`.

AWS CLI

Detección de la desviación en un conjunto de pilas y en todas las instancias de pila asociadas

En el siguiente ejemplo de `detect-stack-set-drift`, se inician las operaciones de detección de desviaciones en el conjunto de pilas especificado, incluidas todas las instancias de pila asociadas a dicho conjunto de pilas, y se indica un ID de operación que se puede utilizar para realizar un seguimiento del estado de la operación de desviación.

```
aws cloudformation detect-stack-set-drift \
    --stack-set-name stack-set-drift-example
```

Salida:

```
{
    "OperationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Para obtener más información, consulte Detección de cambios de configuración no administrados en conjuntos de pilas en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte DetectStackSetDrift en la Referencia de comandos de la AWS CLI.

`estimate-template-cost`

En el siguiente ejemplo de código, se muestra cómo utilizar `estimate-template-cost`.

AWS CLI

Cálculo del costo de una plantilla

En el siguiente ejemplo de `estimate-template-cost`, se genera un cálculo del costo para una plantilla con el nombre `template.yaml` en la carpeta actual.

```
aws cloudformation estimate-template-cost \
    --template-body file://template.yaml
```

Salida:

```
{
    "Url": "http://calculator.s3.amazonaws.com/calc5.html?
key=cloudformation/7870825a-xmpl-4def-92e7-c4f8dd360cca"
}
```

- Para obtener información sobre la API, consulte EstimateTemplateCost en la Referencia de comandos de la AWS CLI.

`execute-change-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `execute-change-set`.

AWS CLI

Ejecución de un conjunto de cambios

En el siguiente ejemplo de `execute-change-set`, se ejecuta un conjunto de cambios especificado por el nombre del conjunto de cambios y el nombre de la pila.

```
aws cloudformation execute-change-set \
    --change-set-name my-change-set \
    --stack-name my-stack
```

En el siguiente ejemplo de `execute-change-set`, se ejecuta un conjunto de cambios especificado por el ARN completo del conjunto de cambios.

```
aws cloudformation execute-change-set \
    --change-set-name arn:aws:cloudformation:us-west-2:123456789012:changeSet/my-change-set/bc9555ba-a949-xmpl-bfb8-f41d04ec5784
```

- Para obtener información sobre la API, consulte ExecuteChangeSet en la Referencia de comandos de la AWS CLI.

`execute-stack-refactor`

En el siguiente ejemplo de código, se muestra cómo utilizar `execute-stack-refactor`.

AWS CLI

Finalización de una operación de refactorización de pilas

En el ejemplo de `execute-stack-refactor` siguiente, se completa la operación de refactorización de pilas con el ID de refactorización de pila especificado.

```
aws cloudformation execute-stack-refactor \
    --stack-refactor-id 9c384f70-4e07-4ed7-a65d-fee5eb430841
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Refactorización de pilas en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte ExecuteStackRefactor en la Referencia de comandos de la AWS CLI.

`get-stack-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-stack-policy`.

AWS CLI

Visualización de una política de pilas

En el siguiente ejemplo de `get-stack-policy`, se muestra la política de pilas de la pila especificada. Para adjuntar una política a una pila, utilice el comando `set-stack-policy`.

```
aws cloudformation get-stack-policy \
    --stack-name my-stack
```

Salida:

```
{
    "StackPolicyBody": "{\n  \"Statement\" : [\n    {\n      \"Effect\" :
 \"Allow\",\n      \"Action\" : \"Update:*\",\n      \"Principal\": \"*\",\n
     \"Resource\" : \"*\"\n    },\n    {\n      \"Effect\" : \"Deny\",\n
 \"Action\" : \"Update:*\",\n      \"Principal\": \"*\",\n      \"Resource\" :
 \"LogicalResourceId/bucket\"\n    }\n  ]\n}\n"
}
```

- Para obtener información sobre la API, consulte GetStackPolicy en la Referencia de comandos de la AWS CLI.

`get-template-summary`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-template-summary`.

AWS CLI

Visualización de un resumen de plantilla

Con el siguiente comando, se muestra información resumida sobre los recursos y los metadatos del archivo de plantilla especificado.

```
aws cloudformation get-template-summary \
   --template-body file://template.yaml
```

Salida:

```
{
    "Parameters": [],
    "Description": "A VPC and subnets.",
    "ResourceTypes": [
        "AWS::EC2::VPC",
        "AWS::EC2::Subnet",
        "AWS::EC2::Subnet",
        "AWS::EC2::RouteTable",
        "AWS::EC2::VPCEndpoint",
        "AWS::EC2::SubnetRouteTableAssociation",
        "AWS::EC2::SubnetRouteTableAssociation",
        "AWS::EC2::VPCEndpoint"
    ],
    "Version": "2010-09-09"
}
```

- Para obtener información sobre la API, consulte GetTemplateSummary en la Referencia de comandos de la AWS CLI.

`get-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-template`.

AWS CLI

Visualización del cuerpo de la plantilla de una pila de AWS CloudFormation

En el siguiente ejemplo de `get-template`, se muestra la plantilla para la pila `myteststack`:

```
aws cloudformation get-template --stack-name myteststack
```

Salida:

```
{
    "TemplateBody": {
        "AWSTemplateFormatVersion": "2010-09-09",
        "Outputs": {
            "BucketName": {
                "Description": "Name of S3 bucket to hold website content",
                "Value": {
                    "Ref": "S3Bucket"
                }
```

```
            }
        },
        "Description": "AWS CloudFormation Sample Template S3_Bucket: Sample
 template showing how to create a publicly accessible S3 bucket. **WARNING** This
 template creates an S3 bucket. You will be billed for the AWS resources used if you
 create a stack from this template.",
        "Resources": {
            "S3Bucket": {
                "Type": "AWS::S3::Bucket",
                "Properties": {
                    "AccessControl": "PublicRead"
                }
            }
        }
    }
}
```

- Para obtener información sobre la API, consulte GetTemplate en la Referencia de comandos de la AWS CLI.

`list-change-sets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-change-sets`.

AWS CLI

Generación de una lista de conjuntos de cambios

En el siguiente ejemplo de `list-change-sets`, se genera una lista de los conjuntos de cambios pendientes de la pila especificada.

```
aws cloudformation list-change-sets \
   --stack-name my-stack
```

Salida:

```
{
    "Summaries": [
        {
            "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-
stack/d0a825a0-e4cd-xmpl-b9fb-061c69e99204",
            "StackName": "my-stack",
```

```
            "ChangeSetId": "arn:aws:cloudformation:us-west-2:123456789012:changeSet/
my-change-set/70160340-7914-xmpl-bcbf-128a1fa78b5d",
            "ChangeSetName": "my-change-set",
            "ExecutionStatus": "AVAILABLE",
            "Status": "CREATE_COMPLETE",
            "CreationTime": "2019-10-02T05:38:54.297Z"
        }
    ]
}
```

- Para obtener detalles de la API, consulte ListChangeSets en la Referencia de comandos de la AWS CLI.

`list-exports`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-exports`.

AWS CLI

Generación de una lista de exportaciones

En el siguiente ejemplo de `list-exports`, se muestra una lista de las exportaciones de las pilas de la región actual.

```
aws cloudformation list-exports
```

Salida:

```
{
    "Exports": [
        {
            "ExportingStackId": "arn:aws:cloudformation:us-
west-2:123456789012:stack/private-vpc/99764070-b56c-xmpl-bee8-062a88d1d800",
            "Name": "private-vpc-subnet-a",
            "Value": "subnet-07b410xmplddcfa03"
        },
        {
            "ExportingStackId": "arn:aws:cloudformation:us-
west-2:123456789012:stack/private-vpc/99764070-b56c-xmpl-bee8-062a88d1d800",
            "Name": "private-vpc-subnet-b",
            "Value": "subnet-075ed3xmplebd2fb1"
        },
```

```
        {
            "ExportingStackId": "arn:aws:cloudformation:us-
west-2:123456789012:stack/private-vpc/99764070-b56c-xmpl-bee8-062a88d1d800",
            "Name": "private-vpc-vpcid",
            "Value": "vpc-011d7xmpl100e9841"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListExports en la Referencia de comandos de la AWS CLI.

`list-generated-templates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-generated-templates`.

AWS CLI

Muestra de las plantillas generadas

En el ejemplo de `list-generated-templates` siguiente, se muestran todas las plantillas generadas.

```
aws cloudformation list-generated-templates
```

Salida:

```
{
    "Summaries": [
        {
            "GeneratedTemplateId": "arn:aws:cloudformation:us-
east-1:123456789012:generatedtemplate/7fc8512c-d8cb-4e02-b266-d39c48344e48",
            "GeneratedTemplateName": "MyTemplate",
            "Status": "COMPLETE",
            "StatusReason": "All resources complete",
            "CreationTime": "2025-09-23T20:13:24.283000+00:00",
            "LastUpdatedTime": "2025-09-23T20:13:28.610000+00:00",
            "NumberOfResources": 4
        },
        {
            "GeneratedTemplateId": "arn:aws:cloudformation:us-
east-1:123456789012:generatedTemplate/f10dd1c4-edc6-4823-8153-ab6112b8d051",
```

```
            "GeneratedTemplateName": "MyEC2InstanceTemplate",
            "Status": "COMPLETE",
            "StatusReason": "All resources complete",
            "CreationTime": "2024-08-08T19:35:49.790000+00:00",
            "LastUpdatedTime": "2024-08-08T19:35:52.207000+00:00",
            "NumberOfResources": 3
        },
        {
            "GeneratedTemplateId": "arn:aws:cloudformation:us-
east-1:123456789012:generatedTemplate/e5a1c89f-7ce2-41bd-9bdf-75b7c852e3ca",
            "GeneratedTemplateName": "MyEKSNodeGroupTemplate",
            "Status": "COMPLETE",
            "StatusReason": "All resources complete",
            "CreationTime": "2024-07-16T20:39:27.883000+00:00",
            "LastUpdatedTime": "2024-07-16T20:39:35.766000+00:00",
            "NumberOfResources": 4
        }
    ]
}
```

Para obtener más información, consulte Generación de plantillas a partir de los recursos existentes en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte ListGeneratedTemplates en la Referencia de comandos de la AWS CLI.

`list-imports`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-imports`.

AWS CLI

Generación de una lista de importaciones

En el siguiente `list-imports` ejemplo, se genera una lista de las pilas que importan la exportación especificada. Para obtener la lista de las exportaciones disponibles, utilice el comando `list-exports`.

```
aws cloudformation list-imports \
    --export-name private-vpc-vpcid
```

Salida:

```
{
    "Imports": [
        "my-database-stack"
    ]
}
```

- Para obtener información sobre la API, consulte ListImports en la Referencia de comandos de la AWS CLI.

`list-resource-scan-related-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-scan-related-resources`.

AWS CLI

Muestra de los recursos relacionados de un análisis de recursos

En el ejemplo de `list-resource-scan-related-resources` siguiente, se muestran los recursos del análisis de recursos especificado que están relacionados con los recursos en `resources.json`.

```
aws cloudformation list-resource-scan-related-resources \
    --resource-scan-id arn:aws:cloudformation:us-
east-1:123456789012:resourceScan/0a699f15-489c-43ca-a3ef-3e6ecfa5da60 \
    --resources file://resources.json
```

Contenido de `resources.json`:

```
[
    {
        "ResourceType": "AWS::EKS::Cluster",
        "ResourceIdentifier": {
            "ClusterName": "MyAppClusterName"
        }
    },
    {
        "ResourceType": "AWS::AutoScaling::AutoScalingGroup",
        "ResourceIdentifier": {
            "AutoScalingGroupName": "MyAppASGName"
        }
```

```
    }
]
```

Salida:

```
{
    "RelatedResources": [
        {
            "ResourceType": "AWS::EKS::Nodegroup",
            "ResourceIdentifier": {
                "NodegroupName": "MyAppNodegroupName"
            },
            "ManagedByStack": false
        },
        {
            "ResourceType": "AWS::IAM::Role",
            "ResourceIdentifier": {
                "RoleId": "arn:aws::iam::123456789012:role/MyAppIAMRole"
            },
            "ManagedByStack": false
        }
    ]
}
```

Para obtener más información, consulte Crear una plantilla de CloudFormation a partir de recursos analizados con el generador de IaC en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte ListResourceScanRelatedResources en la Referencia de comandos de la AWS CLI.

`list-resource-scan-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-scan-resources`.

AWS CLI

Muestra de los recursos de un análisis de recursos

En el ejemplo de `list-resource-scan-resources` siguiente, se muestran los recursos del análisis de recursos especificado, filtrado por identificador de recursos.

```
aws cloudformation list-resource-scan-resources \
```

```
    --resource-scan-id arn:aws:cloudformation:us-
east-1:123456789012:resourceScan/0a699f15-489c-43ca-a3ef-3e6ecfa5da60 \
    --resource-identifier MyApp
```

Salida:

```
{
    "Resources": [
        {
            "ResourceType": "AWS::EKS::Cluster",
            "ResourceIdentifier": {
                "ClusterName": "MyAppClusterName"
            },
            "ManagedByStack": false
        },
        {
            "ResourceType": "AWS::AutoScaling::AutoScalingGroup",
            "ResourceIdentifier": {
                "AutoScalingGroupName": "MyAppASGName"
            },
            "ManagedByStack": false
        }
    ]
}
```

Para obtener más información, consulte Crear una plantilla de CloudFormation a partir de recursos analizados con el generador de IaC en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte ListResourceScanResources en la Referencia de comandos de la AWS CLI.

`list-stack-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-stack-instances`.

AWS CLI

Generación de una lista de las instancias de una pila

En el siguiente ejemplo de `list-stack-instances`, se genera una lista de las instancias creadas a partir del conjunto de pilas especificado.

```
aws cloudformation list-stack-instances \
```

```
    --stack-set-name enable-config
```

La salida del ejemplo incluye detalles sobre una pila que no se ha podido actualizar debido a un error:

```
{
    "Summaries": [
        {
            "StackSetId": "enable-config:296a3360-xmpl-40af-be78-9341e95bf743",
            "Region": "us-west-2",
            "Account": "123456789012",
            "StackId": "arn:aws:cloudformation:ap-northeast-1:123456789012:stack/
StackSet-enable-config-35a6ac50-d9f8-4084-86e4-7da34d5de4c4/a1631cd0-e5fb-xmpl-
b474-0aa20f14f06e",
            "Status": "CURRENT"
        },
        {
            "StackSetId": "enable-config:296a3360-xmpl-40af-be78-9341e95bf743",
            "Region": "us-west-2",
            "Account": "123456789012",
            "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/
StackSet-enable-config-e6cac20f-xmpl-46e9-8314-53e0d4591532/eab53680-e5fa-xmpl-
ba14-0a522351f81e",
            "Status": "OUTDATED",
            "StatusReason": "ResourceLogicalId:ConfigDeliveryChannel,
 ResourceType:AWS::Config::DeliveryChannel, ResourceStatusReason:Failed to put
 delivery channel 'StackSet-enable-config-e6cac20f-xmpl-46e9-8314-53e0d4591532-
ConfigDeliveryChannel-1OJWJ7XD59WR0' because the maximum number of delivery
 channels: 1 is reached. (Service: AmazonConfig; Status Code: 400; Error Code:
 MaxNumberOfDeliveryChannelsExceededException; Request ID: d14b34a0-ef7c-xmpl-
acf8-8a864370ae56)."
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListStackInstances en la Referencia de comandos de la AWS CLI.

`list-stack-refactor-actions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-stack-refactor-actions`.

AWS CLI

Muestra de las acciones de una operación de refactorización de pila

En el ejemplo de `list-stack-refactor-actions` siguiente, se muestran las acciones para la operación de refactorización de pilas con el ID de refactorización de pila especificado.

```
aws cloudformation list-stack-refactor-actions \
    --stack-refactor-id 9c384f70-4e07-4ed7-a65d-fee5eb430841
```

Salida:

```
{
    "StackRefactorActions": [
        {
            "Action": "MOVE",
            "Entity": "RESOURCE",
            "PhysicalResourceId": "MyTestLambdaRole",
            "Description": "No configuration changes detected.",
            "Detection": "AUTO",
            "TagResources": [],
            "UntagResources": [],
            "ResourceMapping": {
                "Source": {
                    "StackName": "arn:aws:cloudformation:us-
east-1:123456789012:stack/Stack1/3e6a1ff0-94b1-11f0-aa6f-0a88d2e03acf",
                    "LogicalResourceId": "MyLambdaRole"
                },
                "Destination": {
                    "StackName": "arn:aws:cloudformation:us-
east-1:123456789012:stack/Stack2/5da91650-94b1-11f0-81cf-0a23500e151b",
                    "LogicalResourceId": "MyLambdaRole"
                }
            }
        },
        {
            "Action": "MOVE",
            "Entity": "RESOURCE",
            "PhysicalResourceId": "MyTestFunction",
            "Description": "Resource configuration changes will be validated during
 refactor execution.",
            "Detection": "AUTO",
            "TagResources": [
```

```
                {
                    "Key": "aws:cloudformation:stack-name",
                    "Value": "Stack2"
                },
                {
                    "Key": "aws:cloudformation:logical-id",
                    "Value": "MyFunction"
                },
                {
                    "Key": "aws:cloudformation:stack-id",
                    "Value": "arn:aws:cloudformation:us-east-1:123456789012:stack/
Stack2/5da91650-94b1-11f0-81cf-0a23500e151b"
                }
            ],
            "UntagResources": [
                "aws:cloudformation:stack-name",
                "aws:cloudformation:logical-id",
                "aws:cloudformation:stack-id"
            ],
            "ResourceMapping": {
                "Source": {
                    "StackName": "arn:aws:cloudformation:us-
east-1:123456789012:stack/Stack1/3e6a1ff0-94b1-11f0-aa6f-0a88d2e03acf",
                    "LogicalResourceId": "MyFunction"
                },
                "Destination": {
                    "StackName": "arn:aws:cloudformation:us-
east-1:123456789012:stack/Stack2/5da91650-94b1-11f0-81cf-0a23500e151b",
                    "LogicalResourceId": "MyFunction"
                }
            }
        }
    ]
}
```

Para obtener más información, consulte Refactorización de pilas en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte ListStackRefactorActions en la Referencia de comandos de la AWS CLI.

`list-stack-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-stack-resources`.

AWS CLI

Enumeración de los recursos de una pila

En el siguiente comando, se muestra la lista de los recursos en la pila especificada.

```
aws cloudformation list-stack-resources \
    --stack-name my-stack
```

Salida:

```
{
    "StackResourceSummaries": [
        {
            "LogicalResourceId": "bucket",
            "PhysicalResourceId": "my-stack-bucket-1vc62xmplgguf",
            "ResourceType": "AWS::S3::Bucket",
            "LastUpdatedTimestamp": "2019-10-02T04:34:11.345Z",
            "ResourceStatus": "CREATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "IN_SYNC"
            }
        },
        {
            "LogicalResourceId": "function",
            "PhysicalResourceId": "my-function-SEZV4XMPL4S5",
            "ResourceType": "AWS::Lambda::Function",
            "LastUpdatedTimestamp": "2019-10-02T05:34:27.989Z",
            "ResourceStatus": "UPDATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "IN_SYNC"
            }
        },
        {
            "LogicalResourceId": "functionRole",
            "PhysicalResourceId": "my-functionRole-HIZXMPLEOM9E",
            "ResourceType": "AWS::IAM::Role",
            "LastUpdatedTimestamp": "2019-10-02T04:34:06.350Z",
            "ResourceStatus": "CREATE_COMPLETE",
```

```
            "DriftInformation": {
                "StackResourceDriftStatus": "IN_SYNC"
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListStackResources en la Referencia de comandos de la AWS CLI.

`list-stack-set-operation-results`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-stack-set-operation-results`.

AWS CLI

Generación de una lista de los resultados de la operación del conjunto de pilas

Con el siguiente comando, se muestran los resultados de una operación de actualización en las instancias del conjunto de pilas especificado.

```
aws cloudformation list-stack-set-operation-results \
    --stack-set-name enable-config \
    --operation-id 35d45ebc-ed88-xmpl-ab59-0197a1fc83a0
```

Salida:

```
{
    "Summaries": [
        {
            "Account": "223456789012",
            "Region": "us-west-2",
            "Status": "SUCCEEDED",
            "AccountGateResult": {
                "Status": "SKIPPED",
                "StatusReason": "Function not found: arn:aws:lambda:eu-
west-1:223456789012:function:AWSCloudFormationStackSetAccountGate"
            }
        },
        {
            "Account": "223456789012",
```

```
            "Region": "ap-south-1",
            "Status": "CANCELLED",
            "StatusReason": "Cancelled since failure tolerance has exceeded"
        }
    ]
}
```

Nota: El estado `SKIPPED` de `AccountGateResult` es el esperado para las operaciones que se realizan correctamente, a menos que se cree una función de puerta de cuenta.

- Para obtener información sobre la API, consulte ListStackSetOperationResults en la Referencia de comandos de la AWS CLI.

`list-stack-set-operations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-stack-set-operations`.

AWS CLI

Generación de una lista de las operaciones de conjuntos de pilas

En el siguiente ejemplo de `list-stack-set-operations`, se muestra la lista de las operaciones más recientes del conjunto de pilas especificado.

```
aws cloudformation list-stack-set-operations \
    --stack-set-name my-stack-set
```

Salida:

```
{
    "Summaries": [
        {
            "OperationId": "35d45ebc-ed88-xmpl-ab59-0197a1fc83a0",
            "Action": "UPDATE",
            "Status": "SUCCEEDED",
            "CreationTimestamp": "2019-10-03T16:28:44.377Z",
            "EndTimestamp": "2019-10-03T16:42:08.607Z"
        },
        {
            "OperationId": "891aa98f-7118-xmpl-00b2-00954d1dd0d6",
            "Action": "UPDATE",
            "Status": "FAILED",
```

```
            "CreationTimestamp": "2019-10-03T15:43:53.916Z",
            "EndTimestamp": "2019-10-03T15:45:58.925Z"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListStackSetOperations en la Referencia de comandos de la AWS CLI.

`list-stack-sets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-stack-sets`.

AWS CLI

Generación de una lista de conjuntos de pilas

En el siguiente ejemplo de `list-stack-sets`, se muestra la lista de los conjuntos de pilas en la región y la cuenta actuales.

```
aws cloudformation list-stack-sets
```

Salida:

```
{
    "Summaries": [
        {
            "StackSetName": "enable-config",
            "StackSetId": "enable-config:296a3360-xmpl-40af-be78-9341e95bf743",
            "Description": "Enable AWS Config",
            "Status": "ACTIVE"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListStackSets en la Referencia de comandos de la AWS CLI.

`list-stacks`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-stacks`.

AWS CLI

Enumeración de las pilas de AWS CloudFormation

En el siguiente ejemplo de `list-stacks`, se muestra un resumen de todas las pilas que tienen el estado `CREATE_COMPLETE`:

```
aws cloudformation list-stacks --stack-status-filter CREATE_COMPLETE
```

Salida:

```
[
    {
        "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
myteststack/466df9e0-0dff-08e3-8e2f-5088487c4896",
        "TemplateDescription": "AWS CloudFormation Sample Template S3_Bucket: Sample
 template showing how to create a publicly accessible S3 bucket. **WARNING** This
 template creates an S3 bucket. You will be billed for the AWS resources used if you
 create a stack from this template.",
        "StackStatusReason": null,
        "CreationTime": "2013-08-26T03:27:10.190Z",
        "StackName": "myteststack",
        "StackStatus": "CREATE_COMPLETE"
    }
]
```

- Para obtener información sobre la API, consulte ListStacks en la Referencia de comandos de la AWS CLI.

`list-type-registrations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-type-registrations`.

AWS CLI

Generación de una lista de los registros completados de un tipo

En el siguiente ejemplo de `list-type-registrations`, se muestra una lista de los registros de tipo completados para el tipo especificado.

```
aws cloudformation list-type-registrations \
```

```
    --type RESOURCE \
    --type-name My::Logs::LogGroup \
    --registration-status-filter COMPLETE
```

Salida:

```
{
    "RegistrationTokenList": [
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333"
    ]
}
```

Para obtener más información, consulte Uso del registro de CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte ListTypeRegistrations en la Referencia de comandos de la AWS CLI.

`list-type-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-type-versions`.

AWS CLI

Generación de una lista de versiones de una extensión

En el siguiente ejemplo de `list-type-versions`, se muestra información resumida sobre las versiones de una extensión.

```
aws cloudformation list-type-versions \
  --endpoint https://example.com \
  --region us-west-2 \
  --type RESOURCE \
  --type-name My::Resource::Example \
  --publisher-id 123456789012
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso del registro de AWS CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte ListTypeVersions en la Referencia de comandos de la AWS CLI.

`list-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-types`.

AWS CLI

Generación de una lista de los tipos de recursos privados de una cuenta

En el siguiente ejemplo de `list-types`, se muestra una lista de los tipos de recursos privados registrados en ese momento en la cuenta de AWS actual.

```
aws cloudformation list-types
```

Salida:

```
{
    "TypeSummaries": [
        {
            "Description": "WordPress blog resource for internal use",
            "LastUpdated": "2019-12-04T18:28:15.059Z",
            "TypeName": "My::WordPress::BlogExample",
            "TypeArn": "arn:aws:cloudformation:us-west-2:123456789012:type/resource/
My-WordPress-BlogExample",
            "DefaultVersionId": "00000005",
            "Type": "RESOURCE"
        },
        {
            "Description": "Customized resource derived from AWS::Logs::LogGroup",
            "LastUpdated": "2019-12-04T18:28:15.059Z",
            "TypeName": "My::Logs::LogGroup",
            "TypeArn": "arn:aws:cloudformation:us-west-2:123456789012:type/resource/
My-Logs-LogGroup",
            "DefaultVersionId": "00000003",
            "Type": "RESOURCE"
        }
    ]
}
```

Para obtener más información, consulte Uso del registro de CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener más información sobre la API, consulte ListTypes en Referencia de comandos de la AWS CLI.

`package`

En el siguiente ejemplo de código, se muestra cómo utilizar `package`.

AWS CLI

Con el siguiente comando, se exporta una plantilla denominada `template.json` cargando los artefactos locales en el bucket de S3 `bucket-name`, y se escribe la plantilla exportada en `packaged-template.json`:

```
aws cloudformation package --template-file /path_to_template/template.json --s3-
bucket bucket-name --output-template-file packaged-template.json --use-json
```

- Para obtener información sobre la API, consulte Package en la Referencia de comandos de la AWS CLI.

`publish-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `publish-type`.

AWS CLI

Publicación de una extensión

En el siguiente ejemplo de `publish-type`, se publica la extensión especificada en el registro de CloudFormation como extensión pública de esta región.

```
aws cloudformation publish-type \
  --region us-west-2 \
  --type RESOURCE \
  --type-name Example::Test::1234567890abcdef0
```

Salida:

```
{
```

```
    "PublicTypeArn":"arn:aws:cloudformation:us-west-2::type/
resource/000q6TfUovXsEMmgKowxDZLlwqr2QUshd2e75c8c/Example-
Test-1234567890abcdef0/1.0.0"
}
```

Para obtener más información, consulte Uso del registro de AWS CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte PublishType en la Referencia de comandos de la AWS CLI.

`register-publisher`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-publisher`.

AWS CLI

Registro de un publicador

En el siguiente ejemplo de `register-publisher`, se registra un publicador y se acepta el parámetro de términos y condiciones.

```
aws cloudformation register-publisher \
  --region us-west-2 \
  --accept-terms-and-conditions
```

Salida:

```
{
    "PublisherId": "000q6TfUovXsEMmgKowxDZLlwqr2QUshd2e75c8c"
}
```

Para obtener más información, consulte Uso del registro de AWS CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte RegisterPublisher en la Referencia de comandos de la AWS CLI.

`register-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-type`.

AWS CLI

Registro un tipo de recurso

En el siguiente ejemplo de `register-type`, se registra el tipo de recurso especificado como un tipo de recurso privado en la cuenta del usuario.

```
aws cloudformation register-type \
    --type-name My::Organization::ResourceName \
    --schema-handler-package s3://bucket_name/my-organization-resource_name.zip \
    --type RESOURCE
```

Salida:

```
{
    "RegistrationToken": "f5525280-104e-4d35-bef5-8f1f1example"
}
```

Para obtener más información, consulte Registering Resource Providers en la Guía del usuario de CloudFormation Command Line Interface para desarrollo de tipos.

- Para obtener información sobre la API, consulte RegisterType en la Referencia de comandos de la AWS CLI.

`set-stack-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-stack-policy`.

AWS CLI

Aplicación de una política de pila

En el siguiente ejemplo de `set-stack-policy`, se deshabilitan las actualizaciones del recurso especificado en la pila especificada. `stack-policy.json` es un documento de JSON que describe las operaciones permitidas en los recursos de la pila.

```
aws cloudformation set-stack-policy \
    --stack-name my-stack \
    --stack-policy-body file://stack-policy.json
```

Salida:

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "Update:*",
      "Principal": "*",
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : "Update:*",
      "Principal": "*",
      "Resource" : "LogicalResourceId/bucket"
    }
  ]
}
```

- Para obtener información sobre la API, consulte SetStackPolicy en la Referencia de comandos de la AWS CLI.

`set-type-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-type-configuration`.

AWS CLI

Configuración de datos

En el siguiente ejemplo de `set-type-configuration`, se especifican los datos de configuración de una extensión de CloudFormation registrada en la cuenta y región especificadas.

```
aws cloudformation set-type-configuration \
    --region us-west-2 \
    --type RESOURCE \
    --type-name Example::Test::Type \
    --configuration-alias default \
    --configuration "{\"CredentialKey\": \"testUserCredential\"}"
```

Salida:

```
{
```

```
    "ConfigurationArn": "arn:aws:cloudformation:us-west-2:123456789012:type-
configuration/resource/Example-Test-Type/default"
}
```

Para obtener más información, consulte Uso del registro de AWS CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte SetTypeConfiguration en la Referencia de comandos de la AWS CLI.

`set-type-default-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-type-default-version`.

AWS CLI

Definición de la versión predeterminada del tipo

En el siguiente ejemplo de `set-type-default-version`, se establece que la versión de tipo especificada se utilice como predeterminada para dicho tipo.

```
aws cloudformation set-type-default-version \
    --type RESOURCE \
    --type-name My::Logs::LogGroup \
    --version-id 00000003
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso del registro de CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte SetTypeDefaultVersion en la Referencia de comandos de la AWS CLI.

`signal-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `signal-resource`.

AWS CLI

Indicación de un recurso

En el siguiente ejemplo de `signal-resource`, se indica `success` para cumplir la condición de espera denominada `MyWaitCondition` en la pila llamada `my-stack`.

```
aws cloudformation signal-resource \
    --stack-name my-stack \
    --logical-resource-id MyWaitCondition \
    --unique-id 1234 \
    --status SUCCESS
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte SignalResource en la Referencia de comandos de la AWS CLI.

`start-resource-scan`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-resource-scan`.

AWS CLI

Inicio de un escaneo de recursos

En el ejemplo de `start-resource-scan` siguiente, se inicia un análisis de recursos que analiza todos los recursos existentes en la cuenta y región actuales.

```
aws cloudformation start-resource-scan
```

Salida:

```
{
    "ResourceScanId":
      "arn:aws:cloudformation:us-
east-1:123456789012:resourceScan/0a699f15-489c-43ca-a3ef-3e6ecfa5da60"
}
```

Para obtener más información, consulte Inicio de un análisis de recursos con el generador de IaC de CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para ver detalles de la API, consulte StartResourceScan en la Referencia de comandos de la AWS CLI.

`stop-stack-set-operation`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-stack-set-operation`.

AWS CLI

Detención de una operación de conjunto de pilas

En el siguiente ejemplo de `stop-stack-set-operation`, se detiene una operación de actualización en curso en el conjunto de pilas especificado.

```
aws cloudformation stop-stack-set-operation \
    --stack-set-name my-stack-set \
    --operation-id 1261cd27-490b-xmpl-ab42-793a896c69e6
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte StopStackSetOperation en la Referencia de comandos de la AWS CLI.

`test-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `test-type`.

AWS CLI

Prueba de una extensión

En el siguiente ejemplo de `test-type`, se prueba una extensión registrada a fin de asegurarse de que cumple con todos los requisitos necesarios para publicarse en el registro de CloudFormation.

```
aws cloudformation test-type \
    --arn arn:aws:cloudformation:us-west-2:123456789012:type/resource/Sample-Test-Resource123/00000001
```

Salida:

```
{
    "TypeVersionArn": "arn:aws:cloudformation:us-west-2:123456789012:type/resource/Sample-Test-Resource123/00000001"
```

```
}
```

Para obtener más información, consulte Uso del registro de AWS CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte TestType en la Referencia de comandos de la AWS CLI.

`update-stack-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-stack-instances`.

AWS CLI

Actualización de instancias de pila

En el siguiente ejemplo de `update-stack-instances`, se vuelve a intentar actualizar las instancias de pila de dos cuentas en dos regiones con la configuración más reciente. La configuración de tolerancia a errores especificada garantiza que se intente la actualización en todas las cuentas y regiones, incluso si no se pueden actualizar algunas pilas.

```
aws cloudformation update-stack-instances \
    --stack-set-name my-stack-set \
    --accounts 123456789012 567890123456 \
    --regions us-east-1 us-west-2 \
    --operation-preferences FailureToleranceCount=3
```

Salida:

```
{
    "OperationId": "103ebdf2-21ea-xmpl-8892-de5e30733132"
}
```

- Para obtener información sobre la API, consulte UpdateStackInstances en la Referencia de comandos de la AWS CLI.

`update-stack-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-stack-set`.

AWS CLI

Actualización de un conjunto de pilas

En el siguiente ejemplo de `update-stack-set`, se añade una etiqueta con el nombre de clave `Owner` y un valor de `IT` a las instancias de pila en el conjunto de pilas especificado.

```
aws cloudformation update-stack-set \
    --stack-set-name my-stack-set \
    --use-previous-template \
    --tags Key=Owner,Value=IT
```

Salida:

```
{
    "OperationId": "e2b60321-6cab-xmpl-bde7-530c6f47950e"
}
```

- Para obtener información sobre la API, consulte UpdateStackSet en la Referencia de la API de la AWS CLI.

`update-stack`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-stack`.

AWS CLI

Actualización de las pilas de AWS CloudFormation

En el siguiente ejemplo de `update-stack`, se actualiza la plantilla y los parámetros de entrada de la pila `mystack`:

```
aws cloudformation update-stack --stack-name mystack --
template-url https://s3.amazonaws.com/sample/updated.template --
parameters ParameterKey=KeyPairName,ParameterValue=SampleKeyPair
 ParameterKey=SubnetIDs,ParameterValue=SampleSubnetID1\\,SampleSubnetID2
```

En el siguiente ejemplo de `update-stack`, se actualiza únicamente el valor de parámetro `SubnetIDs` para la pila `mystack`. Si no se especifica un valor de parámetro, se utilizará el valor predeterminado que esté especificado en la plantilla:

```
aws cloudformation update-stack --stack-name mystack --
template-url https://s3.amazonaws.com/sample/updated.template
 --parameters ParameterKey=KeyPairName,UsePreviousValue=true
 ParameterKey=SubnetIDs,ParameterValue=SampleSubnetID1\\,UpdatedSampleSubnetID2
```

En el siguiente ejemplo de `update-stack`, se agregan dos temas de notificaciones de pila en la pila `mystack`:

```
aws cloudformation update-stack --stack-name mystack --use-previous-template --
notification-arns "arn:aws:sns:use-east-1:123456789012:mytopic1" "arn:aws:sns:us-
east-1:123456789012:mytopic2"
```

Para obtener más información, consulte Actualizaciones de pila de AWS CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte UpdateStack en la Referencia de comandos de la AWS CLI.

update-termination-protection

En el siguiente ejemplo de código, se muestra cómo utilizar `update-termination-protection`.

AWS CLI

Activación de la protección contra terminación

En el siguiente ejemplo de `update-termination-protection`, se habilita la protección contra terminación en la pila especificada.

```
aws cloudformation update-termination-protection \
    --stack-name my-stack \
    --enable-termination-protection
```

Salida:

```
{
    "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-stack/
d0a825a0-e4cd-xmpl-b9fb-061c69e99204"
}
```

- Para obtener información sobre la API, consulte UpdateTerminationProtection en la Referencia de comandos de la AWS CLI.

`validate-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `validate-template`.

AWS CLI

Validación de una plantilla de AWS CloudFormation

En el siguiente ejemplo de `validate-template`, se valida la plantilla `sampletemplate.json`:

```
aws cloudformation validate-template --template-body file://sampletemplate.json
```

Salida:

```
{
    "Description": "AWS CloudFormation Sample Template S3_Bucket: Sample template
 showing how to create a publicly accessible S3 bucket. **WARNING** This template
 creates an S3 bucket. You will be billed for the AWS resources used if you create a
 stack from this template.",
    "Parameters": [],
    "Capabilities": []
}
```

Para obtener más información, consulte Trabajo con plantillas de AWS CloudFormation en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte ValidateTemplate en la Referencia de comandos de la AWS CLI.

Ejemplos de CloudFront que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con CloudFront.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-distribution-tenant-web-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-distribution-tenant-web-acl`.

AWS CLI

Asociación de una ACL web con un inquilino de distribución de CloudFront

En el siguiente ejemplo de `associate-distribution-tenant-web-acl`, se asocia una ACL web con una distribución de CloudFront con ETag `E13V1IB3VIYABC`.

```
aws cloudfront associate-distribution-tenant-web-acl \
    --id dt_2wjDZi3hD1ivOXf6rpZJO1AB \
    --if-match E13V1IB3VIYABC \
    --web-acl-arn arn:aws:wafv2:us-east-1:123456789012:global/webacl/web-global-example/626900da-5f64-418b-ba9b-743f37123ABC
```

Salida:

```
{
    "ETag": "E1VC38T7YXBABC",
    "Id": "dt_2wjDZi3hD1ivOXf6rpZJO1AB",
    "WebACLArn": "arn:aws:wafv2:us-east-1:123456789012:global/webacl/web-global-example/626900da-5f64-418b-ba9b-743f37123ABC"
}
```

Para obtener más información, consulte Uso de protecciones de AWS WAF en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte AssociateDistributionTenantWebAcl en la Referencia de comandos de la AWS CLI.

`associate-distribution-web-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-distribution-web-acl`.

AWS CLI

Asociación de una ACL web con una distribución de CloudFront

En el siguiente ejemplo de `associate-distribution-web-acl`, se asocia una ACL web con una distribución de CloudFront.

```
aws cloudfront associate-distribution-web-acl \
    --id E1XNX8R2GOAABC \
    --if-match E2YWS1C2J3OABC \
    --web-acl-arn arn:aws:wafv2:us-east-1:123456789012:global/webacl/web-global-example/626900da-5f64-418b-ba9b-743f3746cABC
```

Salida:

```
{
    "ETag": "E3QE7ED60U0ABC",
    "Id": "E1XNX8R2GOAABC",
    "WebACLArn": "arn:aws:wafv2:us-east-1:123456789012:global/webacl/web-global-example/626900da-5f64-418b-ba9b-743f3746cABC"
}
```

Para obtener más información, consulte Uso de protecciones de AWS WAF en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte AssociateDistributionWebAcl en la Referencia de comandos de la AWS CLI.

`create-cloud-front-origin-access-identity`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-cloud-front-origin-access-identity`.

AWS CLI

Creación de una identidad de acceso de origen de CloudFront

En el siguiente ejemplo, se crea una identidad de acceso de origen (OAI) de CloudFront facilitando la configuración de la OAI como argumento de línea de comandos:

```
aws cloudfront create-cloud-front-origin-access-identity \
    --cloud-front-origin-access-identity-config \
        CallerReference="cli-example",Comment="Example OAI"
```

Puede lograr lo mismo facilitando la configuración de la OAI en un archivo JSON, como se muestra en el siguiente ejemplo:

```
aws cloudfront create-cloud-front-origin-access-identity \
    --cloud-front-origin-access-identity-config file://OAI-config.json
```

El archivo `OAI-config.json` es un documento JSON en el directorio actual que contiene lo siguiente:

```
{
    "CallerReference": "cli-example",
    "Comment": "Example OAI"
}
```

Tanto si facilita la configuración de la OAI con un argumento de línea de comandos o con un archivo JSON, el resultado será el mismo:

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/origin-access-identity/
cloudfront/E74FTE3AEXAMPLE",
    "ETag": "E2QWRUHEXAMPLE",
    "CloudFrontOriginAccessIdentity": {
        "Id": "E74FTE3AEXAMPLE",
        "S3CanonicalUserId":
 "cd13868f797c227fbea2830611a26fe0a21ba1b826ab4bed9b7771c9aEXAMPLE",
        "CloudFrontOriginAccessIdentityConfig": {
            "CallerReference": "cli-example",
            "Comment": "Example OAI"
        }
    }
}
```

- Para obtener información sobre la API, consulte CreateCloudFrontOriginAccessIdentity en la Referencia de comandos de la AWS CLI.

`create-connection-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-connection-group`.

AWS CLI

Creación de un grupo de conexiones en CloudFront

En el siguiente ejemplo de `create-connection-group`, se crea un grupo de conexiones habilitado, especifica una lista de IP estáticas de Anycast y desactiva IPv6.

```
aws cloudfront create-connection-group \
    --name cg-with-anycast-ip-list \
    --no-ipv6-enabled \
    --enabled \
    --anycast-ip-list-id aip_CCkW6gKrDiBD4n78123ABC \
    --tags "Items=[{Key=abc,Value=123}]"
```

Salida:

```
{
    "ETag": "E23ZP02F085ABC",
    "ConnectionGroup": {
        "Id": "cg_2yb6uj74B4PCbfhT31WFdiSABC",
        "Name": "cg-with-anycast-ip-list",
        "Arn": "arn:aws:cloudfront::123456789012:connection-group/
cg_2yb6uj74B4PCbfhT31WFdiSABC",
        "CreatedTime": "2025-06-16T16:25:50.061000+00:00",
        "LastModifiedTime": "2025-06-16T16:25:50.061000+00:00",
        "Tags": {
            "Items": [
                {
                    "Key": "abc",
                    "Value": "123"
                }
            ]
        },
        "Ipv6Enabled": false,
        "RoutingEndpoint": "dj6xusxq65abc.cloudfront.net",
        "AnycastIpListId": "aip_CCkW6gKrDiBD4n78123ABC",
        "Status": "InProgress",
        "Enabled": true,
        "IsDefault": false
```

```
    }
}
```

Para obtener más información, consulte Creación de un grupo de conexiones personalizado (opcional) en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte CreateConnectionGroup en la Referencia de comandos de la AWS CLI.

`create-distribution-tenant`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-distribution-tenant`.

AWS CLI

Ejemplo 1: creación de un inquilino de distribución de CloudFront que utiliza un certificado personalizado

En el siguiente ejemplo de `create-distribution-tenant` se crea un inquilino de distribución de CloudFront que especifica personalizaciones para desactivar WAF, agregar restricciones geográficas y usar otro certificado TLS.

```
aws cloudfront create-distribution-tenant \
    --cli-input-json file://tenant.json
```

Contenido de `tenant.json`:

```
{
    "DistributionId": "E1XNX8R2GOAABC",
    "Domains": [
        {
            "Domain": "example.com"
        }
    ],
    "Parameters": [
        {
            "Name": "testParam",
            "Value": "defaultValue"
        }
    ],
    "ConnectionGroupId": "cg_2whCJoXMYCjHcxaLGrkllvyABC",
    "Enabled": false,
```

```
    "Tags": {
        "Items": [
            {
                "Key": "tag",
                "Value": "tagValue"
            }
        ]
    },
    "Name": "new-tenant-customizations",
    "Customizations": {
        "GeoRestrictions": {
            "Locations": ["DE"],
            "RestrictionType": "whitelist"
        },
        "WebAcl": {
            "Action": "disable"
        },
        "Certificate": {
            "Arn": "arn:aws:acm:us-east-1:123456789012:certificate/ec53f564-
ea5a-4e4a-a0a2-e3c989449abc"
        }
    }
}
```

Salida:

```
{
    "ETag": "E23ZP02F085ABC",
    "DistributionTenant": {
        "Id": "dt_2yN5tYwVbPKr7m2IB69M1yp1AB",
        "DistributionId": "E1XNX8R2GOAABC",
        "Name": "new-tenant-customizations",
        "Arn": "arn:aws:cloudfront::123456789012:distribution-tenant/
dt_2yN5tYwVbPKr7m2IB69M1yp1AB",
        "Domains": [
            {
                "Domain": "example.com",
                "Status": "active"
            }
        ],
        "Tags": {
            "Items": [
                {
```

```
                    "Key": "tag",
                    "Value": "tagValue"
                }
            ]
        },
        "Customizations": {
            "WebAcl": {
                "Action": "disable"
            },
            "Certificate": {
                "Arn": "arn:aws:acm:us-east-1:123456789012:certificate/ec53f564-
ea5a-4e4a-a0a2-e3c989449abc"
            },
            "GeoRestrictions": {
                "RestrictionType": "whitelist",
                "Locations": [
                    "DE"
                ]
            }
        },
        "Parameters": [
            {
                "Name": "testParam",
                "Value": "defaultValue"
            }
        ],
        "ConnectionGroupId": "cg_2whCJoXMYCjHcxaLGrkllvyABC",
        "CreatedTime": "2025-06-11T17:20:06.432000+00:00",
        "LastModifiedTime": "2025-06-11T17:20:06.432000+00:00",
        "Enabled": false,
        "Status": "InProgress"
    }
}
```

Ejemplo 2: creación de un inquilino de distribución con un certificado heredado

En el siguiente ejemplo de `create-distribution-tenant` se crea un inquilino de distribución y se especifica un certificado TLS heredado de la distribución de varios inquilinos.

```
aws cloudfront create-distribution-tenant \
    --cli-input-json file://tenant.json
```

Contenido de `tenant.json`:

```
{
    "DistributionId": "E1HVIAU7U12ABC",
    "Domains": [
        {
            "Domain": "example.com"
        }
    ],
    "Parameters": [
        {
            "Name": "tenantName",
            "Value": "first-tenant"
        }
    ],
    "Enabled": true,
    "Name": "new-tenant-no-cert"
}
```

Salida:

```
{
    "ETag": "E23ZP02F0ABC",
    "DistributionTenant": {
        "Id": "dt_2zhRB0vBe0B72LZCVy1mgzI1AB",
        "DistributionId": "E1HVIAU7U12ABC",
        "Name": "new-tenant-no-cert",
        "Arn": "arn:aws:cloudfront::123456789012:distribution-tenant/
dt_2zhRB0vBe0B72LZCVy1mgzI1AB",
        "Domains": [
            {
                "Domain": "example.com",
                "Status": "active"
            }
        ],
        "Parameters": [
            {
                "Name": "tenantName",
                "Value": "first-tenant"
            }
        ],
        "ConnectionGroupId": "cg_2yQEwpipGFN0hhA0ZemPabOABC",
        "CreatedTime": "2025-07-10T20:59:38.414000+00:00",
        "LastModifiedTime": "2025-07-10T20:59:38.414000+00:00",
        "Enabled": true,
```

```
        "Status": "InProgress"
    }
}
```

Ejemplo 3: creación de un inquilino de distribución de CloudFront mediante un token de validación alojado en CloudFront

En el siguiente ejemplo de `create-distribution-tenant` se crea un inquilino de distribución y se utiliza un token de validación alojado en CloudFront para el nombre de dominio.

```
aws cloudfront create-distribution-tenant \
    --cli-input-json file://tenant.json
```

Contenido de `tenant.json`:

```
{
    "DistributionId": "E2GJ5J9QN12ABC",
    "Domains": [
        {
            "Domain": "example.com"
        }
    ],
    "Parameters": [
        {
            "Name": "tenantName",
            "Value": "first-tenant"
        }
    ],
    "ConnectionGroupId": "cg_2yQEwpipGFN0hhA0ZemPabOABC",
    "Enabled": true,
    "Name": "new-tenant-cf-hosted",
    "ManagedCertificateRequest": {
        "ValidationTokenHost": "cloudfront"
    }
}
```

Importante: Para ejecutar correctamente este comando, debe configurar un registro de DNS CNAME que apunte el nuevo dominio (example.com) al punto de conexión de enrutamiento del grupo de conexión asociado con el inquilino de distribución. Este registro CNAME también debe propagarse antes de que CloudFront pueda completar correctamente esta solicitud.

Salida:

```
{
    "ETag": "E23ZP02F0ABC",
    "DistributionTenant": {
        "Id": "dt_2zhStKrA524GvvTWJX92Ozl1AB",
        "DistributionId": "E2GJ5J9QN12ABC",
        "Name": "new-tenant-cf-hosted",
        "Arn": "arn:aws:cloudfront::123456789012:distribution-tenant/
dt_2zhStKrA524GvvTWJX92Ozl1AB",
        "Domains": [
            {
                "Domain": "example.com",
                "Status": "inactive"
            }
        ],
        "Parameters": [
            {
                "Name": "tenantName",
                "Value": "first-tenant"
            }
        ],
        "ConnectionGroupId": "cg_2zhSaGatwwXjTjE42nneZzqABC",
        "CreatedTime": "2025-07-10T21:13:46.416000+00:00",
        "LastModifiedTime": "2025-07-10T21:13:46.416000+00:00",
        "Enabled": true,
        "Status": "InProgress"
    }
}
```

Ejemplo 4: creación de un inquilino de distribución de CloudFront mediante un token de validación autoalojado

En el siguiente ejemplo de `create-distribution-tenant` se crea un inquilino de distribución de CloudFront y utiliza un token de validación autoalojado.

```
aws cloudfront create-distribution-tenant \
    --cli-input-json file://tenant.json
```

Contenido de `tenant.json`:

```
{
    "DistributionId": "E2GJ5J9QN12ABC",
    "Domains": [
```

```
        {
            "Domain": "example.com"
        }
    ],
    "Parameters": [
        {
            "Name": "tenantName",
            "Value": "first-tenant"
        }
    ],
    "Enabled": true,
    "Name": "new-tenant-self-hosted",
    "ManagedCertificateRequest": {
        "ValidationTokenHost": "self-hosted"
    }
}
```

Salida:

```
{
    "ETag": "E23ZP02F0ABC",
    "DistributionTenant": {
        "Id": "dt_2zhTFBV93OfFJJ3YMdNM5BC1AB",
        "DistributionId": "E2GJ5J9QN12ABC",
        "Name": "new-tenant-self-hosted",
        "Arn": "arn:aws:cloudfront::123456789012:distribution-tenant/
dt_2zhTFBV93OfFJJ3YMdNM5BC1AB",
        "Domains": [
            {
                "Domain": "example.com",
                "Status": "inactive"
            }
        ],
        "Parameters": [
            {
                "Name": "tenantName",
                "Value": "first-tenant"
            }
        ],
        "ConnectionGroupId": "cg_2yQEwpipGFN0hhA0ZemPabOABC",
        "CreatedTime": "2025-07-10T21:16:39.828000+00:00",
        "LastModifiedTime": "2025-07-10T21:16:39.828000+00:00",
        "Enabled": true,
```

```
        "Status": "InProgress"
    }
}
```

Importante: Después de ejecutar este comando, el inquilino de distribución se creará sin validación. Para validar la solicitud de certificado administrado y configurar el DNS cuando esté listo para empezar a recibir tráfico, consulte Finalización de la configuración del dominio en la Guía para desarrolladores de Amazon CloudFront.

Para obtener más información sobre la creación de inquilinos de distribución, consulte Creación de una distribución en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte CreateDistributionTenant en la Referencia de comandos de la AWS CLI.

`create-distribution-with-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-distribution-with-tags`.

AWS CLI

Creación de una distribución de CloudFront con etiquetas

En el siguiente ejemplo de `create-distribution-with-tags`, se crea una distribución con dos etiquetas que proporcionan la configuración de la distribución y las etiquetas en un archivo JSON denominado `dist-config-with-tags.json`.

```
aws cloudfront create-distribution-with-tags \
    --distribution-config-with-tags file://dist-config-with-tags.json
```

El archivo `dist-config-with-tags.json` es un documento JSON en la carpeta actual. Observe el objeto `Tags` situado en la parte superior del archivo, que contiene dos etiquetas:

`Name = ExampleDistributionProject = ExampleProject`

Contenido de `dist-config-with-tags.json`:

```
{
    "Tags": {
        "Items": [
            {
                "Key": "Name",
```

```
                "Value": "ExampleDistribution"
            },
            {
                "Key": "Project",
                "Value": "ExampleProject"
            }
        ]
    },
    "DistributionConfig": {
        "CallerReference": "cli-example",
        "Aliases": {
            "Quantity": 0
        },
        "DefaultRootObject": "index.html",
        "Origins": {
            "Quantity": 1,
            "Items": [
                {
                    "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                    "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                    "OriginPath": "",
                    "CustomHeaders": {
                        "Quantity": 0
                    },
                    "S3OriginConfig": {
                        "OriginAccessIdentity": ""
                    }
                }
            ]
        },
        "OriginGroups": {
            "Quantity": 0
        },
        "DefaultCacheBehavior": {
            "TargetOriginId": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
            "ForwardedValues": {
                "QueryString": false,
                "Cookies": {
                    "Forward": "none"
                },
                "Headers": {
                    "Quantity": 0
                },
                "QueryStringCacheKeys": {
```

```
                "Quantity": 0
            }
        },
        "TrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ViewerProtocolPolicy": "allow-all",
        "MinTTL": 0,
        "AllowedMethods": {
            "Quantity": 2,
            "Items": [
                "HEAD",
                "GET"
            ],
            "CachedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ]
            }
        },
        "SmoothStreaming": false,
        "DefaultTTL": 86400,
        "MaxTTL": 31536000,
        "Compress": false,
        "LambdaFunctionAssociations": {
            "Quantity": 0
        },
        "FieldLevelEncryptionId": ""
    },
    "CacheBehaviors": {
        "Quantity": 0
    },
    "CustomErrorResponses": {
        "Quantity": 0
    },
    "Comment": "",
    "Logging": {
        "Enabled": false,
        "IncludeCookies": false,
        "Bucket": "",
        "Prefix": ""
```

```
        },
        "PriceClass": "PriceClass_All",
        "Enabled": true,
        "ViewerCertificate": {
            "CloudFrontDefaultCertificate": true,
            "MinimumProtocolVersion": "TLSv1",
            "CertificateSource": "cloudfront"
        },
        "Restrictions": {
            "GeoRestriction": {
                "RestrictionType": "none",
                "Quantity": 0
            }
        },
        "WebACLId": "",
        "HttpVersion": "http2",
        "IsIPV6Enabled": true
    }
}
```

Salida:

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/distribution/
EDFDVBD6EXAMPLE",
    "ETag": "E2QWRUHEXAMPLE",
    "Distribution": {
        "Id": "EDFDVBD6EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EDFDVBD6EXAMPLE",
        "Status": "InProgress",
        "LastModifiedTime": "2019-12-04T23:35:41.433Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
```

```
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                        "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-
example",
                "ForwardedValues": {
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
                    "Headers": {
                        "Quantity": 0
                    },
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
                },
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
```

```
                    "GET"
                ],
                "CachedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ]
                }
            },
            "SmoothStreaming": false,
            "DefaultTTL": 86400,
            "MaxTTL": 31536000,
            "Compress": false,
            "LambdaFunctionAssociations": {
                "Quantity": 0
            },
            "FieldLevelEncryptionId": ""
        },
        "CacheBehaviors": {
            "Quantity": 0
        },
        "CustomErrorResponses": {
            "Quantity": 0
        },
        "Comment": "",
        "Logging": {
            "Enabled": false,
            "IncludeCookies": false,
            "Bucket": "",
            "Prefix": ""
        },
        "PriceClass": "PriceClass_All",
        "Enabled": true,
        "ViewerCertificate": {
            "CloudFrontDefaultCertificate": true,
            "MinimumProtocolVersion": "TLSv1",
            "CertificateSource": "cloudfront"
        },
        "Restrictions": {
            "GeoRestriction": {
                "RestrictionType": "none",
                "Quantity": 0
            }
```

```
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

- Para obtener información sobre la API, consulte CreateDistributionWithTags en la Referencia de comandos de la AWS CLI.

`create-distribution`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-distribution`.

AWS CLI

Ejemplo 1: creación de una distribución de CloudFront

En el siguiente ejemplo de `create-distribution` se crea una distribución para un bucket de S3 denominado `amzn-s3-demo-bucket` y también se especifica `index.html` como el objeto raíz predeterminado mediante argumentos de línea de comandos.

```
aws cloudfront create-distribution \
    --origin-domain-name amzn-s3-demo-bucket.s3.amazonaws.com \
    --default-root-object index.html
```

Salida:

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/distribution/
EMLARXS9EXAMPLE",
    "ETag": "E9LHASXEXAMPLE",
    "Distribution": {
        "Id": "EMLARXS9EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EMLARXS9EXAMPLE",
        "Status": "InProgress",
        "LastModifiedTime": "2019-11-22T00:55:15.705Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
```

```
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                        "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-
example",
                "ForwardedValues": {
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
                    "Headers": {
                        "Quantity": 0
                    },
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
                },
                "TrustedSigners": {
                    "Enabled": false,
```

```
                "Quantity": 0
            },
            "ViewerProtocolPolicy": "allow-all",
            "MinTTL": 0,
            "AllowedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ],
                "CachedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ]
                }
            },
            "SmoothStreaming": false,
            "DefaultTTL": 86400,
            "MaxTTL": 31536000,
            "Compress": false,
            "LambdaFunctionAssociations": {
                "Quantity": 0
            },
            "FieldLevelEncryptionId": ""
        },
        "CacheBehaviors": {
            "Quantity": 0
        },
        "CustomErrorResponses": {
            "Quantity": 0
        },
        "Comment": "",
        "Logging": {
            "Enabled": false,
            "IncludeCookies": false,
            "Bucket": "",
            "Prefix": ""
        },
        "PriceClass": "PriceClass_All",
        "Enabled": true,
        "ViewerCertificate": {
            "CloudFrontDefaultCertificate": true,
```

```
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

Ejemplo 2: creación de una distribución de CloudFront mediante un archivo JSON

En el siguiente ejemplo de `create-distribution` se crea una distribución para un bucket de S3 denominado `amzn-s3-demo-bucket` y también se especifica `index.html` como objeto raíz predeterminado mediante un archivo JSON.

```
aws cloudfront create-distribution \
    --distribution-config file://dist-config.json
```

Contenido de `dist-config.json`:

```
{
    "CallerReference": "cli-example",
    "Aliases": {
        "Quantity": 0
    },
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                "OriginPath": "",
                "CustomHeaders": {
                    "Quantity": 0
                },
```

```
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "OriginGroups": {
        "Quantity": 0
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            },
            "Headers": {
                "Quantity": 0
            },
            "QueryStringCacheKeys": {
                "Quantity": 0
            }
        },
        "TrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ViewerProtocolPolicy": "allow-all",
        "MinTTL": 0,
        "AllowedMethods": {
            "Quantity": 2,
            "Items": [
                "HEAD",
                "GET"
            ],
            "CachedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ]
            }
        },
        "SmoothStreaming": false,
```

```
        "DefaultTTL": 86400,
        "MaxTTL": 31536000,
        "Compress": false,
        "LambdaFunctionAssociations": {
            "Quantity": 0
        },
        "FieldLevelEncryptionId": ""
    },
    "CacheBehaviors": {
        "Quantity": 0
    },
    "CustomErrorResponses": {
        "Quantity": 0
    },
    "Comment": "",
    "Logging": {
        "Enabled": false,
        "IncludeCookies": false,
        "Bucket": "",
        "Prefix": ""
    },
    "PriceClass": "PriceClass_All",
    "Enabled": true,
    "ViewerCertificate": {
        "CloudFrontDefaultCertificate": true,
        "MinimumProtocolVersion": "TLSv1",
        "CertificateSource": "cloudfront"
    },
    "Restrictions": {
        "GeoRestriction": {
            "RestrictionType": "none",
            "Quantity": 0
        }
    },
    "WebACLId": "",
    "HttpVersion": "http2",
    "IsIPV6Enabled": true
}
```

Consulte el ejemplo 1 para ver una salida de muestra.

Ejemplo 3: creación de una distribución de varios inquilinos de CloudFront con un certificado

En el siguiente ejemplo de `create-distribution` se crea una distribución de CloudFront con compatibilidad para varios inquilinos y se especifica un certificado TLS.

```
aws cloudfront create-distribution \
    --distribution-config file://dist-config.json
```

Contenido de `dist-config.json`:

```
{
    "CallerReference": "cli-example-with-cert",
    "Comment": "CLI example distribution",
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "DomainName": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "OriginPath": "/{{tenantName}}",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
        "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
        "ViewerProtocolPolicy": "allow-all",
        "AllowedMethods": {
            "Quantity": 2,
            "Items": ["HEAD", "GET"],
            "CachedMethods": {
                "Quantity": 2,
                "Items": ["HEAD", "GET"]
            }
        }
    },
    "Enabled": true,
    "ViewerCertificate": {
```

```
        "ACMCertificateArn": "arn:aws:acm:us-
east-1:123456789012:certificate/191306a1-db01-49ca-90ef-fc414ee5dabc",
        "SSLSupportMethod": "sni-only"
    },
    "HttpVersion": "http2",
    "ConnectionMode": "tenant-only",
    "TenantConfig": {
        "ParameterDefinitions": [
            {
                "Name": "tenantName",
                "Definition": {
                    "StringSchema": {
                        "Comment": "tenantName parameter",
                        "DefaultValue": "root",
                        "Required": false
                    }
                }
            }
        ]
    }
}
```

Salida:

```
{
    "Location": "https://cloudfront.amazonaws.com/2020-05-31/distribution/
E1HVIAU7UABC",
    "ETag": "E20LT7R1BABC",
    "Distribution": {
        "Id": "E1HVIAU7U12ABC",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/E1HVIAU7U12ABC",
        "Status": "InProgress",
        "LastModifiedTime": "2025-07-10T20:33:31.117000+00:00",
        "InProgressInvalidationBatches": 0,
        "DomainName": "example.com",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ActiveTrustedKeyGroups": {
            "Enabled": false,
            "Quantity": 0
        },
```

```
        "DistributionConfig": {
            "CallerReference": "cli-example-with-cert",
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                        "DomainName": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                        "OriginPath": "/{{tenantName}}",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        },
                        "ConnectionAttempts": 3,
                        "ConnectionTimeout": 10,
                        "OriginShield": {
                            "Enabled": false
                        },
                        "OriginAccessControlId": ""
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "TrustedKeyGroups": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": ["HEAD", "GET"],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": ["HEAD", "GET"]
                    }
                },
```

```
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": "",
                "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
                "GrpcConfig": {
                    "Enabled": false
                }
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "CLI example distribution",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": false,
                "ACMCertificateArn": "arn:aws:acm:us-
east-1:123456789012:certificate/1954f095-11b6-4daf-9952-0c308a00abc",
                "SSLSupportMethod": "sni-only",
                "MinimumProtocolVersion": "TLSv1.2_2021",
                "Certificate": "arn:aws:acm:us-
east-1:123456789012:certificate/1954f095-11b6-4daf-9952-0c308a00abc",
                "CertificateSource": "acm"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
```

```
            "HttpVersion": "http2",
            "TenantConfig": {
                "ParameterDefinitions": [
                    {
                        "Name": "tenantName",
                        "Definition": {
                            "StringSchema": {
                                "Comment": "tenantName parameter",
                                "DefaultValue": "root",
                                "Required": false
                            }
                        }
                    }
                ]
            },
            "ConnectionMode": "tenant-only"
        }
    }
}
```

Para obtener más información, consulte Trabajo con distribuciones en la Guía para desarrolladores de Amazon CloudFront.

Ejemplo 4: creación de una distribución de varios inquilinos de CloudFront sin un certificado

En el siguiente ejemplo de `create-distribution` se crea una distribución de CloudFront con compatibilidad para varios inquilinos, pero sin un certificado TLS.

```
aws cloudfront create-distribution \
    --distribution-config file://dist-config.json
```

Contenido de `dist-config.json`:

```
{
    "CallerReference": "cli-example",
    "Comment": "CLI example distribution",
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "DomainName": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
```

```
                "OriginPath": "/{{tenantName}}",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
        "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
        "ViewerProtocolPolicy": "allow-all",
        "AllowedMethods": {
            "Quantity": 2,
            "Items": [
                "HEAD",
                "GET"
            ],
            "CachedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ]
            }
        }
    },
    "Enabled": true,
    "HttpVersion": "http2",
    "ConnectionMode": "tenant-only",
    "TenantConfig": {
        "ParameterDefinitions": [
            {
                "Name": "tenantName",
                "Definition": {
                    "StringSchema": {
                        "Comment": "tenantName parameter",
                        "DefaultValue": "root",
                        "Required": false
                    }
                }
            }
```

```
        ]
    }
}
```

Salida:

```
{
    "Location": "https://cloudfront.amazonaws.com/2020-05-31/distribution/
E2GJ5J9QN12ABC",
    "ETag": "E37YLVVQIABC",
    "Distribution": {
        "Id": "E2GJ5J9QNABC",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/E2GJ5J9QN12ABC",
        "Status": "InProgress",
        "LastModifiedTime": "2025-07-10T20:35:20.565000+00:00",
        "InProgressInvalidationBatches": 0,
        "DomainName": "example.com",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ActiveTrustedKeyGroups": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example-no-cert",
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                        "DomainName": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                        "OriginPath": "/{{tenantName}}",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        },
                        "ConnectionAttempts": 3,
```

```
                    "ConnectionTimeout": 10,
                    "OriginShield": {
                        "Enabled": false
                    },
                    "OriginAccessControlId": ""
                }
            ]
        },
        "OriginGroups": {
            "Quantity": 0
        },
        "DefaultCacheBehavior": {
            "TargetOriginId": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
            "TrustedKeyGroups": {
                "Enabled": false,
                "Quantity": 0
            },
            "ViewerProtocolPolicy": "allow-all",
            "AllowedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ],
                "CachedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ]
                }
            },
            "Compress": false,
            "LambdaFunctionAssociations": {
                "Quantity": 0
            },
            "FunctionAssociations": {
                "Quantity": 0
            },
            "FieldLevelEncryptionId": "",
            "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
            "GrpcConfig": {
                "Enabled": false
            }
```

```
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "CLI example distribution",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "SSLSupportMethod": "sni-only",
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "TenantConfig": {
                "ParameterDefinitions": [
                    {
                        "Name": "tenantName",
                        "Definition": {
                            "StringSchema": {
                                "Comment": "tenantName parameter",
                                "DefaultValue": "root",
                                "Required": false
                            }
                        }
                    }
                ]
            },
            "ConnectionMode": "tenant-only"
```

```
        }
    }
}
```

Para obtener más información, consulte Configuración de distribuciones en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte CreateDistribution en la Referencia de comandos de la AWS CLI.

`create-field-level-encryption-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-field-level-encryption-config`.

AWS CLI

Creación de una configuración de cifrado en el nivel de campo de CloudFront

En el siguiente ejemplo se crea una configuración de cifrado en el nivel de campo facilitando los parámetros de configuración en un archivo JSON denominado `fle-config.json`. Para poder crear una configuración de cifrado en el nivel de campo, debe tener un perfil de cifrado en el nivel de campo. Para crear un perfil, consulte el comando create-field-level-encryption-profile.

Para obtener más información sobre el cifrado en el nivel de campo de CloudFront, consulte Uso del cifrado en el nivel de campo para ayudar a proteger la información confidencial en la Guía para desarrolladores de Amazon CloudFront.

```
aws cloudfront create-field-level-encryption-config \
    --field-level-encryption-config file://fle-config.json
```

El archivo `fle-config.json` es un documento JSON en la carpeta actual que contiene lo siguiente:

```
{
    "CallerReference": "cli-example",
    "Comment": "Example FLE configuration",
    "QueryArgProfileConfig": {
        "ForwardWhenQueryArgProfileIsUnknown": true,
        "QueryArgProfiles": {
            "Quantity": 0
```

```
        }
    },
    "ContentTypeProfileConfig": {
        "ForwardWhenContentTypeIsUnknown": true,
        "ContentTypeProfiles": {
            "Quantity": 1,
            "Items": [
                {
                    "Format": "URLEncoded",
                    "ProfileId": "P280MFCLSYOCVU",
                    "ContentType": "application/x-www-form-urlencoded"
                }
            ]
        }
    }
}
```

Salida:

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/field-level-encryption/
C3KM2WVD605UAY",
    "ETag": "E2P4Z4VU7TY5SG",
    "FieldLevelEncryption": {
        "Id": "C3KM2WVD605UAY",
        "LastModifiedTime": "2019-12-10T21:30:18.974Z",
        "FieldLevelEncryptionConfig": {
            "CallerReference": "cli-example",
            "Comment": "Example FLE configuration",
            "QueryArgProfileConfig": {
                "ForwardWhenQueryArgProfileIsUnknown": true,
                "QueryArgProfiles": {
                    "Quantity": 0,
                    "Items": []
                }
            },
            "ContentTypeProfileConfig": {
                "ForwardWhenContentTypeIsUnknown": true,
                "ContentTypeProfiles": {
                    "Quantity": 1,
                    "Items": [
                        {
                            "Format": "URLEncoded",
```

```
                            "ProfileId": "P280MFCLSYOCVU",
                            "ContentType": "application/x-www-form-urlencoded"
                        }
                    ]
                }
            }
        }
    }
}
```

- Para obtener información sobre la API, consulte CreateFieldLevelEncryptionConfig en la Referencia de comandos de la AWS CLI.

`create-field-level-encryption-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-field-level-encryption-profile`.

AWS CLI

Creación de un perfil de cifrado en el nivel de campo de CloudFront

En el siguiente ejemplo se crea un perfil de cifrado en el nivel de campo facilitando los parámetros en un archivo JSON denominado `fle-profile-config.json`. Para poder crear un perfil de cifrado en el nivel de campo, debe tener una clave pública de CloudFront. Para crear una clave pública de CloudFront, consulte el comando create-public-key.

Para obtener más información sobre el cifrado en el nivel de campo de CloudFront, consulte Uso del cifrado en el nivel de campo para ayudar a proteger la información confidencial en la Guía para desarrolladores de Amazon CloudFront.

```
aws cloudfront create-field-level-encryption-profile \
    --field-level-encryption-profile-config file://fle-profile-config.json
```

El archivo `fle-profile-config.json` es un documento JSON en la carpeta actual que contiene lo siguiente:

```
{
    "Name": "ExampleFLEProfile",
    "CallerReference": "cli-example",
    "Comment": "FLE profile for AWS CLI example",
```

```
    "EncryptionEntities": {
        "Quantity": 1,
        "Items": [
            {
                "PublicKeyId": "K2K8NC4HVFE3M0",
                "ProviderId": "ExampleFLEProvider",
                "FieldPatterns": {
                    "Quantity": 1,
                    "Items": [
                        "ExampleSensitiveField"
                    ]
                }
            }
        ]
    }
}
```

Salida:

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/field-level-encryption-
profile/PPK0UOSIF5WSV",
    "ETag": "E2QWRUHEXAMPLE",
    "FieldLevelEncryptionProfile": {
        "Id": "PPK0UOSIF5WSV",
        "LastModifiedTime": "2019-12-10T01:03:16.537Z",
        "FieldLevelEncryptionProfileConfig": {
            "Name": "ExampleFLEProfile",
            "CallerReference": "cli-example",
            "Comment": "FLE profile for AWS CLI example",
            "EncryptionEntities": {
                "Quantity": 1,
                "Items": [
                    {
                        "PublicKeyId": "K2K8NC4HVFE3M0",
                        "ProviderId": "ExampleFLEProvider",
                        "FieldPatterns": {
                            "Quantity": 1,
                            "Items": [
                                "ExampleSensitiveField"
                            ]
                        }
                    }
```

```
                ]
            }
        }
    }
}
```

- Para obtener información sobre la API, consulte CreateFieldLevelEncryptionProfile en la Referencia de comandos de la AWS CLI.

`create-invalidation-for-distribution-tenant`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-invalidation-for-distribution-tenant`.

AWS CLI

Creación de una invalidación de CloudFront para un inquilino de distribución

En el siguiente ejemplo de `create-invalidation-for-distribution-tenant`, se crea una invalidación para todos los archivos en un inquilino de distribución de CloudFront.

```
aws cloudfront create-invalidation-for-distribution-tenant \
    --id dt_2wjDZi3hD1ivOXf6rpZJO1AB \
    --invalidation-batch '{"Paths": {"Quantity": 1, "Items": ["/*"]},
 "CallerReference": "invalidation-$(date +%s)"}'
```

Salida:

```
{
    "Location": "https://cloudfront.amazonaws.com/2020-05-31/distribution-tenant/
dt_2wjDZi3hD1ivOXf6rpZJO1AB/invalidation/I2JGL2F1ZAA426PGG0YLLKABC",
    "Invalidation": {
        "Id": "I2JGL2F1ZAA426PGG0YLLKABC",
        "Status": "InProgress",
        "CreateTime": "2025-05-07T16:59:25.947000+00:00",
        "InvalidationBatch": {
            "Paths": {
                "Quantity": 1,
                "Items": [
                    "/*"
                ]
            },
```

```
            "CallerReference": "invalidation-$(date +%s)"
        }
    }
}
```

Para obtener más información, consulte Invalidación de archivos para eliminar contenido en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte CreateInvalidationForDistributionTenant en la Referencia de comandos de la AWS CLI.

`create-invalidation`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-invalidation`.

AWS CLI

Creación de una invalidación para una distribución de CloudFront

En el siguiente ejemplo de `create-invalidation` se crea una invalidación para los archivos indicados en la distribución de CloudFront especificada:

```
aws cloudfront create-invalidation \
    --distribution-id EDFDVBD6EXAMPLE \
    --paths "/example-path/example-file.jpg" "/example-path/example-file2.png"
```

Salida:

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/distribution/
EDFDVBD6EXAMPLE/invalidation/I1JLWSDAP8FU89",
    "Invalidation": {
        "Id": "I1JLWSDAP8FU89",
        "Status": "InProgress",
        "CreateTime": "2019-12-05T18:24:51.407Z",
        "InvalidationBatch": {
            "Paths": {
                "Quantity": 2,
                "Items": [
                    "/example-path/example-file2.png",
                    "/example-path/example-file.jpg"
                ]
            },
```

```
            "CallerReference": "cli-1575570291-670203"
        }
    }
}
```

En el ejemplo anterior, la CLI de AWS generó automáticamente un `CallerReference` aleatorio. Para especificar su propia `CallerReference` o para evitar pasar los parámetros de invalidación como argumentos de la línea de comandos, puede utilizar un archivo JSON. En el siguiente ejemplo se crea una invalidación para dos archivos y se proporcionan los parámetros de invalidación en un archivo JSON denominado `inv-batch.json`:

```
aws cloudfront create-invalidation \
    --distribution-id EDFDVBD6EXAMPLE \
    --invalidation-batch file://inv-batch.json
```

Contenido de `inv-batch.json`:

```
{
    "Paths": {
        "Quantity": 2,
        "Items": [
            "/example-path/example-file.jpg",
            "/example-path/example-file2.png"
        ]
    },
    "CallerReference": "cli-example"
}
```

Salida:

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/distribution/
EDFDVBD6EXAMPLE/invalidation/I2J0I21PCUYOIK",
    "Invalidation": {
        "Id": "I2J0I21PCUYOIK",
        "Status": "InProgress",
        "CreateTime": "2019-12-05T18:40:49.413Z",
        "InvalidationBatch": {
            "Paths": {
                "Quantity": 2,
                "Items": [
                    "/example-path/example-file.jpg",
```

```
                    "/example-path/example-file2.png"
                ]
            },
            "CallerReference": "cli-example"
        }
    }
}
```

- Para obtener información sobre la API, consulte CreateInvalidation en la Referencia de comandos de la AWS CLI.

`create-public-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-public-key`.

AWS CLI

Para crear una clave pública de CloudFront

En el siguiente ejemplo se crea una clave pública de CloudFront proporcionando los parámetros en un archivo JSON denominado `pub-key-config.json`. Para poder usar este comando, debe tener una clave pública codificada en PEM. Para obtener más información, consulte Crear un par de claves RSA en la Guía para desarrolladores de Amazon CloudFront.

```
aws cloudfront create-public-key \
    --public-key-config file://pub-key-config.json
```

El archivo `pub-key-config.json` es un documento JSON en la carpeta actual que contiene lo siguiente. Tenga en cuenta que la clave pública está codificada con el formato PEM.

```
{
    "CallerReference": "cli-example",
    "Name": "ExampleKey",
    "EncodedKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxPMbCA2Ks0lnd7IR+3pw
\nwd3H/7jPGwj8bLUmore7bX+oeGpZ6QmLAe/1UOWcmZX2u70dYcSIzB1ofZtcn4cJ
\nenHBAzO3ohBY/L1tQGJfS2A+omnN6H16VZE1JCK8XSJyfze7MDLcUyHZETdxuvRb
\nA9X343/vMAuQPnhinFJ8Wdy8YBXSPpy7r95ylUQd9LfYTBzVZYG2tSesplcOkjM3\n2Uu
+oMWxQAw1NINnSLPinMVsutJy6ZqlV3McWNWe4T+STGtWhrPNqJEn45sIcCx4\nq
+kGZ2NQ0FyIyT2eiLKOX5Rgb/a36E/aMk4VoDsaenBQgG7WLTnstb9sr7MIhS6A\nrwIDAQAB\n-----END
 PUBLIC KEY-----\n",
    "Comment": "example public key"
```

```
}
```

Salida:

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/public-key/
KDFB19YGCR002",
    "ETag": "E2QWRUHEXAMPLE",
    "PublicKey": {
        "Id": "KDFB19YGCR002",
        "CreatedTime": "2019-12-05T18:51:43.781Z",
        "PublicKeyConfig": {
            "CallerReference": "cli-example",
            "Name": "ExampleKey",
            "EncodedKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxPMbCA2Ks0lnd7IR+3pw
\nwd3H/7jPGwj8bLUmore7bX+oeGpZ6QmLAe/1UOWcmZX2u70dYcSIzB1ofZtcn4cJ
\nenHBAzO3ohBY/L1tQGJfS2A+omnN6H16VZE1JCK8XSJyfze7MDLcUyHZETdxuvRb
\nA9X343/vMAuQPnhinFJ8Wdy8YBXSPpy7r95ylUQd9LfYTBzVZYG2tSesplcOkjM3\n2Uu
+oMWxQAw1NINnSLPinMVsutJy6ZqlV3McWNWe4T+STGtWhrPNqJEn45sIcCx4\nq
+kGZ2NQ0FyIyT2eiLKOX5Rgb/a36E/aMk4VoDsaenBQgG7WLTnstb9sr7MIhS6A\nrwIDAQAB\n-----END
 PUBLIC KEY-----\n",
            "Comment": "example public key"
        }
    }
}
```

- Para obtener información sobre la API, consulte CreatePublicKey en la Referencia de comandos de la AWS CLI.

`delete-cloud-front-origin-access-identity`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-cloud-front-origin-access-identity`.

AWS CLI

Eliminación de la identidad de acceso de origen de CloudFront

En el siguiente ejemplo, se elimina la identidad de acceso de origen (OAI) con el ID `E74FTE3AEXAMPLE`. Para eliminar una OAI, debe tener el ID de la OAI y `ETag`. El ID de OAI se devuelve en la salida de los comandos create-cloud-front-origin-access-identity y list-cloud-

front-origin-access-identities. Para obtener la ETag, utilice el comando get-cloud-front-origin-access-identity o get-cloud-front-origin-access-identity-config. Use la opción --if-match para proporcionar la ETag de la OAI.

```
aws cloudfront delete-cloud-front-origin-access-identity \
    --id E74FTE3AEXAMPLE \
    --if-match E2QWRUHEXAMPLE
```

Si se ejecuta correctamente, este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteCloudFrontOriginAccessIdentity en la Referencia de comandos de la AWS CLI.

delete-connection-group

En el siguiente ejemplo de código, se muestra cómo utilizar delete-connection-group.

AWS CLI

Eliminación de un grupo de conexión

En el siguiente ejemplo de delete-connection-group, se elimina un grupo de conexiones. El grupo de conexiones debe estar desactivado y no se puede asociar con ningún recurso de CloudFront.

```
aws cloudfront delete-connection-group \
    --id cg_2wjLpjbHkLUdhWAjHllcOeABC \
    --if-match ETVPDKIKX0DABC
```

Si se ejecuta correctamente, este comando no genera ninguna salida.

Para obtener más información sobre la administración de grupos de conexiones, consulte Creación de un grupo de conexiones personalizado (opcional) en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte DeleteConnectionGroup en la Referencia de comandos de AWS CLI.

delete-distribution-tenant

En el siguiente ejemplo de código, se muestra cómo utilizar delete-distribution-tenant.

AWS CLI

Eliminación de un inquilino de distribución

En el siguiente ejemplo de `delete-distribution-tenant`, se elimina un inquilino de distribución con ETag `ETVPDKIKX0DABC`. El inquilino de distribución debe estar desactivado y no se puede asociar a ningún recurso de CloudFront.

```
aws cloudfront delete-distribution-tenant \
    --id dt_2wjMUbg3NHZEQ7OfoalP5zi1AB \
    --if-match ETVPDKIKX0DABC
```

Si se ejecuta correctamente, este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de una distribución en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte DeleteDistributionTenant en la Referencia de comandos de la AWS CLI.

`delete-distribution`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-distribution`.

AWS CLI

Eliminación de una distribución de CloudFront

En el siguiente ejemplo se elimina la distribución de CloudFront con el ID `EDFDVBD6EXAMPLE`. Antes de eliminar una distribución, debe deshabilitarla. Para deshabilitar una distribución, utilice el comando update-distribution. Para obtener más información, consulte los ejemplos de update-distribution.

Cuando una distribución está deshabilitada, puede eliminarla. Para eliminar una distribución, debe usar la opción `--if-match` para proporcionar la `ETag` de la distribución. Para obtener la `ETag`, utilice el comando get-distribution o get-distribution-config.

```
aws cloudfront delete-distribution \
    --id EDFDVBD6EXAMPLE \
    --if-match E2QWRUHEXAMPLE
```

Cuando tenga éxito, este comando no tiene salida.

- Para obtener información sobre la API, consulte DeleteDistribution en la Referencia de comandos de la AWS CLI.

`delete-field-level-encryption-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-field-level-encryption-config`.

AWS CLI

Eliminación de una configuración de cifrado en el nivel de campo de CloudFront

En el siguiente ejemplo se elimina la configuración de cifrado en el nivel de campo de CloudFront con el ID `C3KM2WVD605UAY`. Para eliminar una configuración de cifrado en el nivel de campo, debe tener el ID y la `ETag`. El ID se obtiene con la salida de los comandos create-field-level-encryption-config y list-field-level-encryption-configs. Para obtener la `ETag`, utilice el comando get-field-level-encryption o get-field-level-encryption-config. Utilice la opción `--if-match` para proporcionar la `ETag` de la configuración.

```
aws cloudfront delete-field-level-encryption-config \
    --id C3KM2WVD605UAY \
    --if-match E26M4BIAV81ZF6
```

Si se ejecuta correctamente, este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteFieldLevelEncryptionConfig en la Referencia de comandos de la AWS CLI.

`delete-field-level-encryption-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-field-level-encryption-profile`.

AWS CLI

Eliminación de un perfil de cifrado en el nivel de campo de CloudFront

En el siguiente ejemplo se elimina el perfil de cifrado en el nivel de campo de CloudFront con el ID `PPK0UOSIF5WSV`. Para eliminar un perfil de cifrado en el nivel de campo, debe tener el ID y

la ETag. El ID se obtiene con la salida de los comandos create-field-level-encryption-profile y list-field-level-encryption-profiles. Para obtener la ETag, utilice el comando get-field-level-encryption-profile o get-field-level-encryption-profile-config. Use la opción --if-match para proporcionar la ETag del perfil.

```
aws cloudfront delete-field-level-encryption-profile \
    --id PPK0UOSIF5WSV \
    --if-match EJETYFJ9CL66D
```

Si se ejecuta correctamente, este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteFieldLevelEncryptionProfile en la Referencia de comandos de la AWS CLI.

delete-public-key

En el siguiente ejemplo de código, se muestra cómo utilizar delete-public-key.

AWS CLI

Eliminación de una clave pública de CloudFront

En el siguiente ejemplo se elimina la clave pública de CloudFront con el ID KDFB19YGCR002. Para eliminar una clave pública, debe tener el ID y la ETag. El ID se obtiene con la salida de los comandos create-public-key y list-public-keys. Para obtener la ETag, utilice el comando get-public-key o get-public-key-config. Use la opción --if-match para proporcionar la ETag de la clave pública.

```
aws cloudfront delete-public-key \
    --id KDFB19YGCR002 \
    --if-match E2QWRUHEXAMPLE
```

Si se ejecuta correctamente, este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeletePublicKey en la Referencia de comandos de la AWS CLI.

disassociate-distribution-tenant-web-acl

En el siguiente ejemplo de código, se muestra cómo utilizar disassociate-distribution-tenant-web-acl.

AWS CLI

Desasociación de una ACL web de un inquilino de distribución

En el siguiente ejemplo de `disassociate-distribution-tenant-web-acl`, se desasocia una ACL web de un inquilino de distribución con ETag `E1PA6795UKMABC`.

```
aws cloudfront disassociate-distribution-tenant-web-acl \
    --id dt_2wjDZi3hD1ivOXf6rpZJOSNE1AB \
    --if-match E1PA6795UKMABC
```

Salida:

```
{
    "ETag": "E13V1IB3VIYABC",
    "Id": "dt_2wjDZi3hD1ivOXf6rpZJOSNE1AB"
}
```

Para obtener más información, consulte Desactivación de las protecciones de seguridad de AWS WAF en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte DisassociateDistributionTenantWebAcl en la Referencia de comandos de la AWS CLI.

`disassociate-distribution-web-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-distribution-web-acl`.

AWS CLI

Desasociación de una ACL web de una distribución de CloudFront

En el siguiente ejemplo de `disassociate-distribution-web-acl`, se elimina la asociación entre una ACL web y una distribución de CloudFront con ETag `E13V1IB3VIYABC`.

```
aws cloudfront disassociate-distribution-web-acl \
    --id E1XNX8R2GOAABC \
    --if-match EEZQ9Z24VM1ABC
```

Salida:

```
{
    "ETag": "E2YWS1C2J3OABC",
    "Id": "E1XNX8R2GOAABC"
}
```

Para obtener más información, consulte Desactivación de las protecciones de seguridad de AWS WAF en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte DisassociateDistributionWebAcl en la Referencia de comandos de la AWS CLI.

`get-cloud-front-origin-access-identity-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-cloud-front-origin-access-identity-config`.

AWS CLI

Obtención de una configuración de identidad de acceso de origen de CloudFront

En el siguiente ejemplo se obtienen metadatos sobre la identidad de acceso de origen (OAI) con el ID `E74FTE3AEXAMPLE`, incluida su `ETag`. El ID de OAI se devuelve en la salida de los comandos create-cloud-front-origin-access-identity y list-cloud-front-origin-access-identities.

```
aws cloudfront get-cloud-front-origin-access-identity-config --id E74FTE3AEXAMPLE
```

Salida:

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "CloudFrontOriginAccessIdentityConfig": {
        "CallerReference": "cli-example",
        "Comment": "Example OAI"
    }
}
```

- Para obtener información sobre la API, consulte GetCloudFrontOriginAccessIdentityConfig en la Referencia de comandos de la AWS CLI.

`get-cloud-front-origin-access-identity`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-cloud-front-origin-access-identity`.

AWS CLI

Obtención de la identidad de acceso de origen de CloudFront

En el siguiente ejemplo se obtiene la identidad de acceso de origen (OAI) de CloudFront con el ID `E74FTE3AEXAMPLE`, incluida su `ETag` y el ID canónico de S3 asociado. El ID de OAI se devuelve en la salida de los comandos create-cloud-front-origin-access-identity y list-cloud-front-origin-access-identities.

```
aws cloudfront get-cloud-front-origin-access-identity --id E74FTE3AEXAMPLE
```

Salida:

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "CloudFrontOriginAccessIdentity": {
        "Id": "E74FTE3AEXAMPLE",
        "S3CanonicalUserId":
 "cd13868f797c227fbea2830611a26fe0a21ba1b826ab4bed9b7771c9aEXAMPLE",
        "CloudFrontOriginAccessIdentityConfig": {
            "CallerReference": "cli-example",
            "Comment": "Example OAI"
        }
    }
}
```

- Para obtener información sobre la API, consulte GetCloudFrontOriginAccessIdentity en la Referencia de comandos de la AWS CLI.

`get-connection-group-by-routing-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-connection-group-by-routing-endpoint`.

AWS CLI

Obtención de un grupo de conexiones mediante el punto de conexión de enrutamiento

En el siguiente ejemplo de `get-connection-group-by-routing-endpoint`, se recupera información sobre un grupo de conexiones mediante su punto de conexión de enrutamiento.

```
aws cloudfront get-connection-group-by-routing-endpoint \
    --routing-endpoint dvdg9gprgabc.cloudfront.net
```

Salida:

```
{
    "ETag": "E23ZP02F085ABC",
    "ConnectionGroup": {
        "Id": "cg_2wjDWTBKTlRB87cAaUQFaakABC",
        "Name": "connection-group-2",
        "Arn": "arn:aws:cloudfront::123456789012:connection-group/
cg_2wjDWTBKTlRB87cAaUQFaakABC",
        "CreatedTime": "2025-05-06T15:42:00.790000+00:00",
        "LastModifiedTime": "2025-05-06T15:42:00.790000+00:00",
        "Ipv6Enabled": true,
        "RoutingEndpoint": "dvdg9gprgabc.cloudfront.net",
        "Status": "Deployed",
        "Enabled": true,
        "IsDefault": false
    }
}
```

Para obtener más información, consulte Creación de un grupo de conexiones personalizado (opcional) en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte GetConnectionGroupByRoutingEndpoint en la Referencia de comandos de la AWS CLI.

`get-connection-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-connection-group`.

AWS CLI

Obtención de un grupo de conexiones de CloudFront

En el siguiente ejemplo de `get-connection-group`, se recupera información sobre un grupo de conexiones de CloudFront.

```
aws cloudfront get-connection-group \
    --identifier cg_2wjDWTBKTlRB87cAaUQFaakABC
```

Salida:

```
{
    "ETag": "E23ZP02F085ABC",
    "ConnectionGroup": {
        "Id": "cg_2wjDWTBKTlRB87cAaUQFaakABC",
        "Name": "connection-group-2",
        "Arn": "arn:aws:cloudfront::123456789012:connection-group/
cg_2wjDWTBKTlRB87cAaUQFaakABC",
        "CreatedTime": "2025-05-06T15:42:00.790000+00:00",
        "LastModifiedTime": "2025-05-06T15:42:00.790000+00:00",
        "Ipv6Enabled": true,
        "RoutingEndpoint": "dvdg9gprgabc.cloudfront.net",
        "Status": "Deployed",
        "Enabled": true,
        "IsDefault": false
    }
}
```

Para obtener más información, consulte Creación de un grupo de conexiones personalizado (opcional) en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte GetConnectionGroup en la Referencia de comandos de la AWS CLI.

`get-distribution-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-distribution-config`.

AWS CLI

Obtención de la configuración de distribución de CloudFront

En el siguiente ejemplo se obtienen metadatos sobre la distribución de CloudFront con el ID `EDFDVBD6EXAMPLE`, incluida su `ETag`. El ID de distribución se devuelve en los comandos create-distribution y list-distributions.

```
aws cloudfront get-distribution-config \
```

```
    --id EDFDVBD6EXAMPLE
```

Salida:

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "DistributionConfig": {
        "CallerReference": "cli-example",
        "Aliases": {
            "Quantity": 0
        },
        "DefaultRootObject": "index.html",
        "Origins": {
            "Quantity": 1,
            "Items": [
                {
                    "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                    "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                    "OriginPath": "",
                    "CustomHeaders": {
                        "Quantity": 0
                    },
                    "S3OriginConfig": {
                        "OriginAccessIdentity": ""
                    }
                }
            ]
        },
        "OriginGroups": {
            "Quantity": 0
        },
        "DefaultCacheBehavior": {
            "TargetOriginId": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
            "ForwardedValues": {
                "QueryString": false,
                "Cookies": {
                    "Forward": "none"
                },
                "Headers": {
                    "Quantity": 0
                },
                "QueryStringCacheKeys": {
                    "Quantity": 0
```

```
                }
            },
            "TrustedSigners": {
                "Enabled": false,
                "Quantity": 0
            },
            "ViewerProtocolPolicy": "allow-all",
            "MinTTL": 0,
            "AllowedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ],
                "CachedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ]
                }
            },
            "SmoothStreaming": false,
            "DefaultTTL": 86400,
            "MaxTTL": 31536000,
            "Compress": false,
            "LambdaFunctionAssociations": {
                "Quantity": 0
            },
            "FieldLevelEncryptionId": ""
        },
        "CacheBehaviors": {
            "Quantity": 0
        },
        "CustomErrorResponses": {
            "Quantity": 0
        },
        "Comment": "",
        "Logging": {
            "Enabled": false,
            "IncludeCookies": false,
            "Bucket": "",
            "Prefix": ""
        },
```

```
        "PriceClass": "PriceClass_All",
        "Enabled": true,
        "ViewerCertificate": {
            "CloudFrontDefaultCertificate": true,
            "MinimumProtocolVersion": "TLSv1",
            "CertificateSource": "cloudfront"
        },
        "Restrictions": {
            "GeoRestriction": {
                "RestrictionType": "none",
                "Quantity": 0
            }
        },
        "WebACLId": "",
        "HttpVersion": "http2",
        "IsIPV6Enabled": true
    }
}
```

- Para obtener información sobre la API, consulte GetDistributionConfig en la Referencia de comandos de la AWS CLI.

`get-distribution-tenant-by-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-distribution-tenant-by-domain`.

AWS CLI

Obtención de información del inquilino de distribución según dominio

En el siguiente ejemplo de `get-distribution-tenant-by-domain`, se recupera información sobre un inquilino de distribución mediante el dominio especificado.

```
aws cloudfront get-distribution-tenant-by-domain \
    --domain example.com
```

Salida:

```
{
    "ETag": "E23ZP02F085ABC",
    "DistributionTenant": {
```

```
        "Id": "dt_2xVInRKCfUzQHgxosDs9hiLk1AB",
        "DistributionId": "E1XNX8R2GOAABC",
        "Name": "example-tenant-4",
        "Arn": "arn:aws:cloudfront::123456789012:distribution-tenant/
dt_2xVInRKCfUzQHgxosDs9hiLk1AB",
        "Domains": [
            {
                "Domain": "example.com",
                "Status": "active"
            }
        ],
        "Parameters": [
            {
                "Name": "testParam",
                "Value": "defaultValue"
            }
        ],
        "ConnectionGroupId": "cg_2whCJoXMYCjHcxaLGrkllvyABC",
        "CreatedTime": "2025-05-23T16:16:20.871000+00:00",
        "LastModifiedTime": "2025-05-23T16:16:20.871000+00:00",
        "Enabled": false,
        "Status": "Deployed"
    }
}
```

Para obtener más información, consulte Comprender cómo funcionan las distribuciones multiinquilinon en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte GetDistributionTenantByDomain en la Referencia de comandos de la AWS CLI.

`get-distribution-tenant`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-distribution-tenant`.

AWS CLI

Obtención de detalles sobre un inquilino de distribución de CloudFront

En el siguiente ejemplo de `get-distribution-tenant`, se recupera información sobre un inquilino de distribución de CloudFront.

```
aws cloudfront get-distribution-tenant \
```

```
    --id dt_2wjDZi3hD1ivOXf6rpZJOSNE1AB
```

Salida:

```
{
    "ETag": "E23ZP02F085ABC",
    "DistributionTenant": {
        "Id": "dt_2wjDZi3hD1ivOXf6rpZJOSNE1AB",
        "DistributionId": "E1XNX8R2GOAABC",
        "Name": "example-tenant-2",
        "Arn": "arn:aws:cloudfront::123456789012:distribution-tenant/
dt_2wjDZi3hD1ivOXf6rpZJOSNE1AB",
        "Domains": [
            {
                "Domain": "example.com",
                "Status": "inactive"
            }
        ],
        "ConnectionGroupId": "cg_2wjDWTBKTlRB87cAaUQFaakABC",
        "CreatedTime": "2025-05-06T15:42:28.542000+00:00",
        "LastModifiedTime": "2025-05-06T15:42:37.724000+00:00",
        "Enabled": true,
        "Status": "InProgress"
    }
}
```

Para obtener más información, consulte Comprender cómo funcionan las distribuciones multiinquilinon en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte GetDistributionTenant en la Referencia de comandos de la AWS CLI.

`get-distribution`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-distribution`.

AWS CLI

Obtención de una distribución de CloudFront

En el siguiente ejemplo de `get-distribution`, se obtiene la distribución de CloudFront con el ID `EDFDVBD6EXAMPLE`, incluida su `ETag`. El ID de distribución se devuelve en los comandos create-distribution y list-distributions.

```
aws cloudfront get-distribution \
    --id EDFDVBD6EXAMPLE
```

Salida:

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "Distribution": {
        "Id": "EDFDVBD6EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EDFDVBD6EXAMPLE",
        "Status": "Deployed",
        "LastModifiedTime": "2019-12-04T23:35:41.433Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                        "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
```

```
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-
example",
                "ForwardedValues": {
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
                    "Headers": {
                        "Quantity": 0
                    },
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
                },
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
```

```
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

- Para obtener información sobre la API, consulte GetDistribution en la Referencia de comandos de la AWS CLI.

`get-field-level-encryption-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-field-level-encryption-config`.

AWS CLI

Obtención de metadatos sobre una configuración de cifrado en el nivel de campo de CloudFront

En el siguiente ejemplo se obtienen metadatos sobre la configuración de cifrado en el nivel de campo de CloudFront con el ID `C3KM2WVD605UAY`, incluida la `ETag`:

```
aws cloudfront get-field-level-encryption-config --id C3KM2WVD605UAY
```

Salida:

```
{
    "ETag": "E2P4Z4VU7TY5SG",
    "FieldLevelEncryptionConfig": {
        "CallerReference": "cli-example",
        "Comment": "Example FLE configuration",
        "QueryArgProfileConfig": {
            "ForwardWhenQueryArgProfileIsUnknown": true,
            "QueryArgProfiles": {
                "Quantity": 0,
                "Items": []
            }
        },
        "ContentTypeProfileConfig": {
            "ForwardWhenContentTypeIsUnknown": true,
            "ContentTypeProfiles": {
                "Quantity": 1,
                "Items": [
                    {
                        "Format": "URLEncoded",
                        "ProfileId": "P280MFCLSYOCVU",
                        "ContentType": "application/x-www-form-urlencoded"
                    }
                ]
            }
        }
    }
}
```

- Para obtener información sobre la API, consulte GetFieldLevelEncryptionConfig en la Referencia de comandos de la AWS CLI.

`get-field-level-encryption-profile-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-field-level-encryption-profile-config`.

AWS CLI

Obtención de una configuración de perfil de cifrado en el nivel de campo de CloudFront

En el siguiente ejemplo se obtienen metadatos sobre el perfil de cifrado en el nivel de campo de CloudFront con el ID `PPK0UOSIF5WSV`, incluida la `ETag`:

```
aws cloudfront get-field-level-encryption-profile-config --id PPK0UOSIF5WSV
```

Salida:

```
{
    "ETag": "E1QQG65FS2L2GC",
    "FieldLevelEncryptionProfileConfig": {
        "Name": "ExampleFLEProfile",
        "CallerReference": "cli-example",
        "Comment": "FLE profile for AWS CLI example",
        "EncryptionEntities": {
            "Quantity": 1,
            "Items": [
                {
                    "PublicKeyId": "K2K8NC4HVFE3M0",
                    "ProviderId": "ExampleFLEProvider",
                    "FieldPatterns": {
                        "Quantity": 1,
                        "Items": [
                            "ExampleSensitiveField"
                        ]
                    }
                }
            ]
        }
    }
}
```

- Para obtener información sobre la API, consulte GetFieldLevelEncryptionProfileConfig en la Referencia de comandos de la AWS CLI.

`get-field-level-encryption-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-field-level-encryption-profile`.

AWS CLI

Obtención de un perfil de cifrado en el nivel de campo de CloudFront

En el siguiente ejemplo se obtiene el perfil de cifrado en el nivel de campo de CloudFront con el ID `PPK0UOSIF5WSV`, incluida la `ETag`:

```
aws cloudfront get-field-level-encryption-profile --id PPK0UOSIF5WSV
```

Salida:

```
{
    "ETag": "E1QQG65FS2L2GC",
    "FieldLevelEncryptionProfile": {
        "Id": "PPK0UOSIF5WSV",
        "LastModifiedTime": "2019-12-10T01:03:16.537Z",
        "FieldLevelEncryptionProfileConfig": {
            "Name": "ExampleFLEProfile",
            "CallerReference": "cli-example",
            "Comment": "FLE profile for AWS CLI example",
            "EncryptionEntities": {
                "Quantity": 1,
                "Items": [
                    {
                        "PublicKeyId": "K2K8NC4HVFE3M0",
                        "ProviderId": "ExampleFLEProvider",
                        "FieldPatterns": {
                            "Quantity": 1,
                            "Items": [
                                "ExampleSensitiveField"
                            ]
                        }
                    }
                ]
```

```
            }
        }
    }
}
```

- Para obtener información sobre la API, consulte GetFieldLevelEncryptionProfile en la Referencia de comandos de la AWS CLI.

`get-field-level-encryption`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-field-level-encryption`.

AWS CLI

Obtención de una configuración de cifrado en el nivel de campo de CloudFront

En el siguiente ejemplo se obtiene la configuración de cifrado en el nivel de campo de CloudFront con el ID `C3KM2WVD605UAY`, incluida la `ETag`:

```
aws cloudfront get-field-level-encryption --id C3KM2WVD605UAY
```

Salida:

```
{
    "ETag": "E2P4Z4VU7TY5SG",
    "FieldLevelEncryption": {
        "Id": "C3KM2WVD605UAY",
        "LastModifiedTime": "2019-12-10T21:30:18.974Z",
        "FieldLevelEncryptionConfig": {
            "CallerReference": "cli-example",
            "Comment": "Example FLE configuration",
            "QueryArgProfileConfig": {
                "ForwardWhenQueryArgProfileIsUnknown": true,
                "QueryArgProfiles": {
                    "Quantity": 0,
                    "Items": []
                }
            },
            "ContentTypeProfileConfig": {
                "ForwardWhenContentTypeIsUnknown": true,
                "ContentTypeProfiles": {
                    "Quantity": 1,
```

```
                    "Items": [
                        {
                            "Format": "URLEncoded",
                            "ProfileId": "P280MFCLSYOCVU",
                            "ContentType": "application/x-www-form-urlencoded"
                        }
                    ]
                }
            }
        }
    }
}
```

- Para obtener información sobre la API, consulte GetFieldLevelEncryption en la Referencia de comandos de la AWS CLI.

`get-invalidation-for-distribution-tenant`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-invalidation-for-distribution-tenant`.

AWS CLI

Obtención de una invalidación de un inquilino de distribución

En el siguiente ejemplo de `get-invalidation-for-distribution-tenant`, se obtiene información sobre una invalidación de un inquilino de distribución.

```
aws cloudfront get-invalidation-for-distribution-tenant \
    --distribution-tenant-id dt_2wjDZi3hD1ivOXf6rpZJOSNE1AB \
    --id I4CU23QAPKMUDUU06F9OFGFABC
```

Salida:

```
{
    "Invalidation": {
        "Id": "I4CU23QAPKMUDUU06F9OFGFABC",
        "Status": "Completed",
        "CreateTime": "2025-05-06T15:46:12.824000+00:00",
        "InvalidationBatch": {
            "Paths": {
                "Quantity": 2,
```

```
                "Items": [
                    "/example/invalidation",
                    "/more/invalidations"
                ]
            },
            "CallerReference": "007ee5a6-d0a0-42be-bb61-e7b915969b48"
        }
    }
}
```

Para obtener más información, consulte Invalidación de archivos para eliminar contenido en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte GetInvalidationForDistributionTenant en la Referencia de comandos de la AWS CLI.

`get-invalidation`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-invalidation`.

AWS CLI

Obtención de una invalidación de CloudFront

En el siguiente ejemplo se obtiene la invalidación con el ID `I2J0I21PCUYOIK` de la distribución de CloudFront con el ID `EDFDVBD6EXAMPLE`:

```
aws cloudfront get-invalidation --id I2J0I21PCUYOIK --distribution-
id EDFDVBD6EXAMPLE
```

Salida:

```
{
    "Invalidation": {
        "Status": "Completed",
        "InvalidationBatch": {
            "Paths": {
                "Items": [
                    "/example-path/example-file.jpg",
                    "/example-path/example-file-2.jpg"
                ],
                "Quantity": 2
            },
```

```
            "CallerReference": "cli-example"
        },
        "Id": "I2J0I21PCUYOIK",
        "CreateTime": "2019-12-05T18:40:49.413Z"
    }
}
```

- Para obtener información sobre la API, consulte GetInvalidation en la Referencia de comandos de la AWS CLI.

`get-managed-certificate-details`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-managed-certificate-details`.

AWS CLI

Obtención de los detalles del certificado administrado

En el siguiente ejemplo de `get-managed-certificate-details`, se recuperan los detalles de un certificado de ACM administrado por CloudFront.

```
aws cloudfront get-managed-certificate-details \
    --identifier dt_2wjDZi3hD1ivOXf6rpZJOSNE1AB
```

Salida:

```
{
    "ManagedCertificateDetails": {
        "CertificateArn": "arn:aws:acm:us-
east-1:123456789012:certificate/655dc1fe-6d37-451d-a013-c2db3a034abc",
        "CertificateStatus": "pending-validation",
        "ValidationTokenHost": "self-hosted",
        "ValidationTokenDetails": [
            {
                "Domain": "example.com",
                "RedirectTo": "validation.us-east-1.acm-
validations.aws/123456789012/.well-known/pki-validation/
b315c9ae21284e7918bb9f3f422ab1c7.txt",
                "RedirectFrom": "example.com/.well-known/pki-validation/
b315c9ae21284e7918bb9f3f422ac3c7.txt"
            }
```

```
        ]
    }
}
```

Para obtener más información, consulte Solicitud de certificados para el inquilino de distribución de CloudFront en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte GetManagedCertificateDetails en la Referencia de comandos de la AWS CLI.

`get-public-key-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-public-key-config`.

AWS CLI

Obtención de una configuración de clave pública de CloudFront

En el siguiente ejemplo se obtienen metadatos sobre la clave pública de CloudFront con el ID `KDFB19YGCR002`, incluida la `ETag`. El ID de clave pública se obtiene con los comandos create-public-key y list-public-keys.

```
aws cloudfront get-public-key-config --id KDFB19YGCR002
```

Salida:

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "PublicKeyConfig": {
        "CallerReference": "cli-example",
        "Name": "ExampleKey",
        "EncodedKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxPMbCA2Ks0lnd7IR+3pw
\nwd3H/7jPGwj8bLUmore7bX+oeGpZ6QmLAe/1UOWcmZX2u70dYcSIzB1ofZtcn4cJ
\nenHBAzO3ohBY/L1tQGJfS2A+omnN6H16VZE1JCK8XSJyfze7MDLcUyHZETdxuvRb
\nA9X343/vMAuQPnhinFJ8Wdy8YBXSPpy7r95ylUQd9LfYTBzVZYG2tSesplcOkjM3\n2Uu
+oMWxQAw1NINnSLPinMVsutJy6ZqlV3McWNWe4T+STGtWhrPNqJEn45sIcCx4\nq
+kGZ2NQ0FyIyT2eiLKOX5Rgb/a36E/aMk4VoDsaenBQgG7WLTnstb9sr7MIhS6A\nrwIDAQAB\n-----END
 PUBLIC KEY-----\n",
        "Comment": "example public key"
    }
}
```

- Para obtener información sobre la API, consulte GetPublicKeyConfig en la Referencia de comandos de la AWS CLI.

`get-public-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-public-key`.

AWS CLI

Creación de una clave pública de CloudFront

En el siguiente ejemplo se obtiene la clave pública de CloudFront con el ID `KDFB19YGCR002`, incluida la `ETag`. El ID de clave pública se obtiene con los comandos create-public-key y list-public-keys.

```
aws cloudfront get-public-key --id KDFB19YGCR002
```

Salida:

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "PublicKey": {
        "Id": "KDFB19YGCR002",
        "CreatedTime": "2019-12-05T18:51:43.781Z",
        "PublicKeyConfig": {
            "CallerReference": "cli-example",
            "Name": "ExampleKey",
            "EncodedKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxPMbCA2Ks0lnd7IR+3pw
\nwd3H/7jPGwj8bLUmore7bX+oeGpZ6QmLAe/1UOWcmZX2u70dYcSIzB1ofZtcn4cJ
\nenHBAzO3ohBY/L1tQGJfS2A+omnN6H16VZE1JCK8XSJyfze7MDLcUyHZETdxuvRb
\nA9X343/vMAuQPnhinFJ8Wdy8YBXSPpy7r95ylUQd9LfYTBzVZYG2tSesplcOkjM3\n2Uu
+oMWxQAw1NINnSLPinMVsutJy6ZqlV3McWNWe4T+STGtWhrPNqJEn45sIcCx4\nq
+kGZ2NQ0FyIyT2eiLKOX5Rgb/a36E/aMk4VoDsaenBQgG7WLTnstb9sr7MIhS6A\nrwIDAQAB\n-----END
 PUBLIC KEY-----\n",
            "Comment": "example public key"
        }
    }
}
```

- Para obtener información sobre la API, consulte GetPublicKey en la Referencia de comandos de la AWS CLI.

`list-cloud-front-origin-access-identities`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-cloud-front-origin-access-identities`.

AWS CLI

Enumeración de las identidades de acceso de origen de CloudFront

En el siguiente ejemplo se obtiene una lista de las identidades de acceso de origen (OAI) de CloudFront de la cuenta de AWS:

```
aws cloudfront list-cloud-front-origin-access-identities
```

Salida:

```
{
    "CloudFrontOriginAccessIdentityList": {
        "Items": [
            {
                "Id": "E74FTE3AEXAMPLE",
                "S3CanonicalUserId":
 "cd13868f797c227fbea2830611a26fe0a21ba1b826ab4bed9b7771c9aEXAMPLE",
                "Comment": "Example OAI"
            },
            {
                "Id": "EH1HDMBEXAMPLE",
                "S3CanonicalUserId":
 "1489f6f2e6faacaae7ff64c4c3e6956c24f78788abfc1718c3527c263bf7a17EXAMPLE",
                "Comment": "Test OAI"
            },
            {
                "Id": "E2X2C9TEXAMPLE",
                "S3CanonicalUserId":
 "cbfeebb915a64749f9be546a45b3fcfd3a31c779673c13c4dd460911ae402c2EXAMPLE",
                "Comment": "Example OAI #2"
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte ListCloudFrontOriginAccessIdentities en la Referencia de comandos de la AWS CLI.

`list-connection-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-connection-groups`.

AWS CLI

Muestra de los grupos de conexión

En el siguiente ejemplo de `list-connection-groups`, se muestran los grupos de conexión disponibles en la cuenta de AWS.

```
aws cloudfront list-connection-groups
```

Salida:

```
{
    "ConnectionGroups": [
        {
            "Id": "cg_2whCJoXMYCjHcxaLGrkllvyABC",
            "Name": "CreatedByCloudFront-cg_2whCJoXMYCjHcxaLGrkllvyABC",
            "Arn": "arn:aws:cloudfront::123456789012:connection-group/
cg_2whCJoXMYCjHcxaLGrkllvyABC",
            "RoutingEndpoint": "d3sx0pso7m5abc.cloudfront.net",
            "CreatedTime": "2025-05-05T22:32:29.630000+00:00",
            "LastModifiedTime": "2025-05-05T22:32:29.630000+00:00",
            "ETag": "E23ZP02F085ABC",
            "Enabled": true,
            "Status": "Deployed",
            "IsDefault": true
        },
        {
            "Id": "cg_2wjDWTBKTlRB87cAaUQFaakABC",
            "Name": "connection-group-2",
            "Arn": "arn:aws:cloudfront::123456789012:connection-group/
cg_2wjDWTBKTlRB87cAaUQFaakABC",
            "RoutingEndpoint": "dvdg9gprgabc.cloudfront.net",
            "CreatedTime": "2025-05-06T15:42:00.790000+00:00",
            "LastModifiedTime": "2025-05-06T15:42:00.790000+00:00",
            "ETag": "E23ZP02F085ABC",
            "Enabled": true,
            "Status": "Deployed",
            "IsDefault": false
        }
```

```
    ]
}
```

Para obtener más información, consulte Creación de un grupo de conexiones personalizado (opcional) en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte ListConnectionGroups en la Referencia de comandos de la AWS CLI.

`list-distribution-tenants-by-customization`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-distribution-tenants-by-customization`.

AWS CLI

Muestra de inquilinos de distribución según personalización

En el siguiente ejemplo de `list-distribution-tenants-by-customization`, se muestran los inquilinos de distribución que utilizan la ACL web especificada.

```
aws cloudfront list-distribution-tenants-by-customization \
    --web-acl-arn arn:aws:wafv2:us-east-1:123456789012:global/webacl/
CreatedByCloudFront-0273cd2f/a3c19bce-42b5-48a1-a8d4-b2bb2f28eabc
```

Salida:

```
{
    "DistributionTenantList": [
        {
            "Id": "dt_2wjDZi3hD1ivOXf6rpZJOSNE1AB",
            "DistributionId": "E1XNX8R2GOAABC",
            "Name": "example-tenant-2",
            "Arn": "arn:aws:cloudfront::123456789012:distribution-tenant/
dt_2wjDZi3hD1ivOXf6rpZJOSNE1AB",
            "Domains": [
                {
                    "Domain": "example.com",
                    "Status": "inactive"
                }
            ],
            "ConnectionGroupId": "cg_2wjDWTBKTlRB87cAaUQFaakABC",
```

```
            "Customizations": {
                "WebAcl": {
                    "Action": "override",
                    "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/webacl/
CreatedByCloudFront-0273cd2f/a3c19bce-42b5-48a1-a8d4-b2bb2f28eabc"
                },
                "GeoRestrictions": {
                    "RestrictionType": "whitelist",
                    "Locations": [
                        "AL"
                    ]
                }
            },
            "CreatedTime": "2025-05-06T15:42:28.542000+00:00",
            "LastModifiedTime": "2025-05-06T16:14:08.710000+00:00",
            "ETag": "E1F83G8C2ARABC",
            "Enabled": true,
            "Status": "Deployed"
        }
    ]
}
```

Para obtener más información, consulte Personalizaciones de inquilinos de distribución en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte ListDistributionTenantsByCustomization en la Referencia de comandos de la AWS CLI.

`list-distribution-tenants`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-distribution-tenants`.

AWS CLI

Muestra de los inquilinos de distribución de CloudFront

En el siguiente ejemplo de `list-distribution-tenants`, se muestran 3 inquilinos de distribución de CloudFront en la cuenta de AWS según el grupo de conexiones asociado.

```
aws cloudfront list-distribution-tenants \
    --association-filter ConnectionGroupId=cg_2whCJoXMYCjHcxaLGrkllvyABC \
    --max-items 3
```

Salida:


```
{
    "DistributionTenantList": [
        {
            "Id": "dt_2yMvQgam3QkJo2z54FDl91dk1AB",
            "DistributionId": "E1XNX8R2GOAABC",
            "Name": "new-tenant-customizations",
            "Arn": "arn:aws:cloudfront::123456789012:distribution-tenant/
dt_2yMvQgam3QkJo2z54FDl91dk1AB",
            "Domains": [
                {
                    "Domain": "example.com",
                    "Status": "active"
                }
            ],
            "ConnectionGroupId": "cg_2whCJoXMYCjHcxaLGrkllvyABC",
            "Customizations": {
                "WebAcl": {
                    "Action": "disable"
                },
                "GeoRestrictions": {
                    "RestrictionType": "whitelist",
                    "Locations": [
                        "DE"
                    ]
                }
            },
            "CreatedTime": "2025-06-11T15:54:02.142000+00:00",
            "LastModifiedTime": "2025-06-11T15:54:02.142000+00:00",
            "ETag": "E23ZP02F085ABC",
            "Enabled": false,
            "Status": "Deployed"
        },
        {
            "Id": "dt_2yMuV7NJuBcAB0cwwxMCBZQ1AB",
            "DistributionId": "E1XNX8R2GOAABC",
            "Name": "new-tenant",
            "Arn": "arn:aws:cloudfront::123456789012:distribution-tenant/
dt_2yMuV7NJuBcAB0cwwxMCBZQ1AB",
            "Domains": [
                {
                    "Domain": "1.example.com",
                    "Status": "active"
```

```
                }
            ],
            "ConnectionGroupId": "cg_2whCJoXMYCjHcxaLGrkllvyABC",
            "Customizations": {
                "GeoRestrictions": {
                    "RestrictionType": "whitelist",
                    "Locations": [
                        "DE"
                    ]
                }
            },
            "CreatedTime": "2025-06-11T15:46:23.466000+00:00",
            "LastModifiedTime": "2025-06-11T15:46:23.466000+00:00",
            "ETag": "E23ZP02F085ABC",
            "Enabled": false,
            "Status": "Deployed"
        },
        {
            "Id": "dt_2xVInRKCfUzQHgxosDs9hiLk1AB",
            "DistributionId": "E1XNX8R2GOAABC",
            "Name": "new-tenant-2",
            "Arn": "arn:aws:cloudfront::123456789012:distribution-tenant/
dt_2xVInRKCfUzQHgxosDs9hiLk1AB",
            "Domains": [
                {
                    "Domain": "2.example.com",
                    "Status": "active"
                }
            ],
            "ConnectionGroupId": "cg_2whCJoXMYCjHcxaLGrkllvyABC",
            "CreatedTime": "2025-05-23T16:16:20.871000+00:00",
            "LastModifiedTime": "2025-05-23T16:16:20.871000+00:00",
            "ETag": "E23ZP02F085ABC",
            "Enabled": false,
            "Status": "Deployed"
        }
    ],
    "NextToken": "eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAzfQ=="
}
```

Para obtener más información, consulte Comprender cómo funcionan las distribuciones multiinquilinon en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte ListDistributionTenants en la Referencia de comandos de la AWS CLI.

`list-distributions-by-connection-mode`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-distributions-by-connection-mode`.

AWS CLI

Muestra de las distribuciones de CloudFront según el modo de conexión

En el siguiente ejemplo de `list-distributions-by-connection-mode`, se muestran las distribuciones de CloudFront con el modo de conexión especificado.

```
aws cloudfront list-distributions-by-connection-mode \
    --connection-mode tenant-only
```

Salida:

```
{
    "DistributionList": {
        "Items": [
            {
                "Id": "E1XNX8R2GOAABC",
                "ARN": "arn:aws:cloudfront::123456789012:distribution/
E1XNX8R2GOAABC",
                "ETag": "EPT4JPJQDY1ABC",
                "Status": "Deployed",
                "LastModifiedTime": "2025-05-23T16:16:15.691000+00:00",
                "DomainName": "-",
                "Aliases": {
                    "Quantity": 0
                },
                "Origins": {
                    "Quantity": 1,
                    "Items": [
                        {
                            "Id": "example-cfn-simple-distribution123",
                            "DomainName": "example.com",
                            "OriginPath": "",
                            "CustomHeaders": {
```

```
                        "Quantity": 0
                    },
                    "S3OriginConfig": {
                        "OriginAccessIdentity": ""
                    },
                    "ConnectionAttempts": 3,
                    "ConnectionTimeout": 10,
                    "OriginShield": {
                        "Enabled": false
                    },
                    "OriginAccessControlId": "E2CJRMB5LKEABC"
                }
            ]
        },
        "OriginGroups": {
            "Quantity": 0
        },
        "DefaultCacheBehavior": {
            "TargetOriginId": "example-cfn-simple-distribution123",
            "TrustedKeyGroups": {
                "Enabled": false,
                "Quantity": 0
            },
            "ViewerProtocolPolicy": "allow-all",
            "AllowedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ],
                "CachedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ]
                }
            },
            "Compress": true,
            "LambdaFunctionAssociations": {
                "Quantity": 0
            },
            "FunctionAssociations": {
                "Quantity": 0
```

```
                    },
                    "FieldLevelEncryptionId": "",
                    "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5abc",
                    "GrpcConfig": {
                        "Enabled": false
                    }
                },
                "CacheBehaviors": {
                    "Quantity": 0
                },
                "CustomErrorResponses": {
                    "Quantity": 0
                },
                "Comment": "",
                "PriceClass": "PriceClass_All",
                "Enabled": true,
                "ViewerCertificate": {
                    "CloudFrontDefaultCertificate": false,
                    "ACMCertificateArn": "arn:aws:acm:us-
east-1:123456789012:certificate/ec53f564-ea5a-4e4a-a0a2-e3c989449abc",
                    "SSLSupportMethod": "sni-only",
                    "MinimumProtocolVersion": "TLSv1.2_2021",
                    "Certificate": "arn:aws:acm:us-east-1:123456789012:certificate/
ec53f564-ea5a-4e4a-a0a2-e3c989449abc",
                    "CertificateSource": "acm"
                },
                "Restrictions": {
                    "GeoRestriction": {
                        "RestrictionType": "none",
                        "Quantity": 0
                    }
                },
                "WebACLId": "arn:aws:wafv2:us-east-1:123456789012:global/webacl/web-
global-example/626900da-5f64-418b-ba9b-743f3746cabc",
                "HttpVersion": "http2",
                "IsIPV6Enabled": false,
                "Staging": false,
                "ConnectionMode": "tenant-only"
            }
        ]
    }
}
```

Para obtener más información, consulte Creación de un grupo de conexiones personalizado (opcional) en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte ListDistributionsByConnectionMode en la Referencia de comandos de la AWS CLI.

`list-distributions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-distributions`.

AWS CLI

Obtención de una lista de las distribuciones de CloudFront

En el siguiente ejemplo, se obtiene una lista de las distribuciones de CloudFront de la cuenta de AWS.

```
aws cloudfront list-distributions
```

Salida:

```
{
    "DistributionList": {
        "Items": [
            {
                "Id": "E23YS8OEXAMPLE",
                "ARN": "arn:aws:cloudfront::123456789012:distribution/
E23YS8OEXAMPLE",
                "Status": "Deployed",
                "LastModifiedTime": "2024-08-05T18:23:40.375000+00:00",
                "DomainName": "abcdefgh12ijk.cloudfront.net",
                "Aliases": {
                    "Quantity": 0
                },
                "Origins": {
                    "Quantity": 1,
                    "Items": [
                        {
                            "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                            "DomainName": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                            "OriginPath": "",
                            "CustomHeaders": {
```

```
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        },
                        "ConnectionAttempts": 3,
                        "ConnectionTimeout": 10,
                        "OriginShield": {
                            "Enabled": false
                        },
                        "OriginAccessControlId": "EIAP8PEXAMPLE"
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "TrustedKeyGroups": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
```

```
                    "Compress": true,
                    "LambdaFunctionAssociations": {
                        "Quantity": 0
                    },
                    "FunctionAssociations": {
                        "Quantity": 0
                    },
                    "FieldLevelEncryptionId": "",
                    "CachePolicyId": "658327ea-f89d-4fab-a63d-7e886EXAMPLE"
                },
                "CacheBehaviors": {
                    "Quantity": 0
                },
                "CustomErrorResponses": {
                    "Quantity": 0
                },
                "Comment": "",
                "PriceClass": "PriceClass_All",
                "Enabled": true,
                "ViewerCertificate": {
                    "CloudFrontDefaultCertificate": true,
                    "SSLSupportMethod": "vip",
                    "MinimumProtocolVersion": "TLSv1",
                    "CertificateSource": "cloudfront"
                },
                "Restrictions": {
                    "GeoRestriction": {
                        "RestrictionType": "none",
                        "Quantity": 0
                    }
                },
                "WebACLId": "",
                "HttpVersion": "HTTP2",
                "IsIPV6Enabled": true,
                "Staging": false
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte ListDistributions en la Referencia de comandos de la AWS CLI.

`list-domain-conflicts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-domain-conflicts`.

AWS CLI

Muestra de los conflictos de dominio de una distribución de CloudFront

En el siguiente ejemplo de `list-domain-conflicts`, se muestran los conflictos de dominio de una distribución de CloudFront.

```
aws cloudfront list-domain-conflicts \
    --domain example.com \
    --domain-control-validation-
resource "DistributionTenantId=dt_2x9GhoK0TZRsohWzv1b9It8J1AB"
```

Salida:

```
{
    "DomainConflicts": [
        {
            "Domain": "example.com",
            "ResourceType": "distribution-tenant",
            "ResourceId": "***************ohWzv1b9It8J1AB",
            "AccountId": "123456789012"
        }
    ]
}
```

Para obtener más información, consulte Mover un nombre de dominio alternativo a una distribución diferente en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte ListDomainConflicts en la Referencia de comandos de la AWS CLI.

`list-field-level-encryption-configs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-field-level-encryption-configs`.

AWS CLI

Generación de una lista de configuraciones de cifrado en el nivel de campo de CloudFront

En el siguiente ejemplo se obtiene una lista de las configuraciones de cifrado en el nivel de campo de CloudFront de la cuenta de AWS:

```
aws cloudfront list-field-level-encryption-configs
```

Salida:

```
{
    "FieldLevelEncryptionList": {
        "MaxItems": 100,
        "Quantity": 1,
        "Items": [
            {
                "Id": "C3KM2WVD605UAY",
                "LastModifiedTime": "2019-12-10T21:30:18.974Z",
                "Comment": "Example FLE configuration",
                "QueryArgProfileConfig": {
                    "ForwardWhenQueryArgProfileIsUnknown": true,
                    "QueryArgProfiles": {
                        "Quantity": 0,
                        "Items": []
                    }
                },
                "ContentTypeProfileConfig": {
                    "ForwardWhenContentTypeIsUnknown": true,
                    "ContentTypeProfiles": {
                        "Quantity": 1,
                        "Items": [
                            {
                                "Format": "URLEncoded",
                                "ProfileId": "P280MFCLSYOCVU",
                                "ContentType": "application/x-www-form-urlencoded"
                            }
                        ]
                    }
                }
            }
        ]
    }
```

```
}
```

- Para obtener información sobre la API, consulte ListFieldLevelEncryptionConfigs en la Referencia de comandos de la AWS CLI.

`list-field-level-encryption-profiles`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-field-level-encryption-profiles`.

AWS CLI

Generación de una lista de perfiles de cifrado en el nivel de campo de CloudFront

En el siguiente ejemplo se obtiene una lista de los perfiles de cifrado en el nivel de campo de CloudFront de la cuenta de AWS:

```
aws cloudfront list-field-level-encryption-profiles
```

Salida:

```
{
    "FieldLevelEncryptionProfileList": {
        "MaxItems": 100,
        "Quantity": 2,
        "Items": [
            {
                "Id": "P280MFCLSYOCVU",
                "LastModifiedTime": "2019-12-05T01:05:39.896Z",
                "Name": "ExampleFLEProfile",
                "EncryptionEntities": {
                    "Quantity": 1,
                    "Items": [
                        {
                            "PublicKeyId": "K2K8NC4HVFE3M0",
                            "ProviderId": "ExampleFLEProvider",
                            "FieldPatterns": {
                                "Quantity": 1,
                                "Items": [
                                    "ExampleSensitiveField"
                                ]
```

```
                            }
                        }
                    ]
                },
                "Comment": "FLE profile for AWS CLI example"
            },
            {
                "Id": "PPK0UOSIF5WSV",
                "LastModifiedTime": "2019-12-10T01:03:16.537Z",
                "Name": "ExampleFLEProfile2",
                "EncryptionEntities": {
                    "Quantity": 1,
                    "Items": [
                        {
                            "PublicKeyId": "K2ABC10EXAMPLE",
                            "ProviderId": "ExampleFLEProvider2",
                            "FieldPatterns": {
                                "Quantity": 1,
                                "Items": [
                                    "ExampleSensitiveField2"
                                ]
                            }
                        }
                    ]
                },
                "Comment": "FLE profile #2 for AWS CLI example"
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte ListFieldLevelEncryptionProfiles en la Referencia de comandos de la AWS CLI.

`list-invalidations-for-distribution-tenant`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-invalidations-for-distribution-tenant`.

AWS CLI

Muestra de invalidaciones para un inquilino de distribución de CloudFront

En el siguiente ejemplo de `list-invalidations-for-distribution-tenant`, se muestran las invalidaciones para un inquilino de distribución de CloudFront.

```
aws cloudfront list-invalidations-for-distribution-tenant \
    --id dt_2wjDZi3hD1ivOXf6rpZJOSNE1AB
```

Salida:

```
{
    "InvalidationList": {
        "Items": [
            {
                "Id": "I4CU23QAPKMUDUU06F9OFGFABC",
                "CreateTime": "2025-05-06T15:46:12.824000+00:00",
                "Status": "Completed"
            }
        ]
    }
}
```

Para obtener más información, consulte Invalidación de archivos para eliminar contenido en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte ListInvalidationsForDistributionTenant en la Referencia de comandos de la AWS CLI.

`list-invalidations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-invalidations`.

AWS CLI

Generación de una lista de invalidaciones de CloudFront

En el siguiente ejemplo se genera una lista de las invalidaciones de la distribución de CloudFront con el ID `EDFDVBD6EXAMPLE`:

```
aws cloudfront list-invalidations --distribution-id EDFDVBD6EXAMPLE
```

Salida:

```
{
    "InvalidationList": {
        "Marker": "",
        "Items": [
            {
                "Status": "Completed",
                "Id": "YNY2LI2BVJ4NJU",
                "CreateTime": "2019-08-31T21:15:52.042Z"
            }
        ],
        "IsTruncated": false,
        "MaxItems": 100,
        "Quantity": 1
    }
}
```

- Para obtener información sobre la API, consulte ListInvalidations en la Referencia de comandos de la AWS CLI.

`list-public-keys`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-public-keys`.

AWS CLI

Generación de una lista de claves públicas de CloudFront

En el siguiente ejemplo se genera una lista de las claves públicas de CloudFront de la cuenta de AWS:

```
aws cloudfront list-public-keys
```

Salida:

```
{
    "PublicKeyList": {
        "MaxItems": 100,
        "Quantity": 2,
        "Items": [
            {
                "Id": "K2K8NC4HVFE3M0",
                "Name": "ExampleKey",
```

```
                "CreatedTime": "2019-12-05T01:04:28.818Z",
                "EncodedKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxPMbCA2Ks0lnd7IR+3pw
\nwd3H/7jPGwj8bLUmore7bX+oeGpZ6QmLAe/1UOWcmZX2u70dYcSIzB1ofZtcn4cJ
\nenHBAzO3ohBY/L1tQGJfS2A+omnN6H16VZE1JCK8XSJyfze7MDLcUyHZETdxuvRb
\nA9X343/vMAuQPnhinFJ8Wdy8YBXSPpy7r95ylUQd9LfYTBzVZYG2tSesplcOkjM3\n2Uu
+oMWxQAw1NINnSLPinMVsutJy6ZqlV3McWNWe4T+STGtWhrPNqJEn45sIcCx4\nq
+kGZ2NQ0FyIyT2eiLKOX5Rgb/a36E/aMk4VoDsaenBQgG7WLTnstb9sr7MIhS6A\nrwIDAQAB\n-----END
 PUBLIC KEY-----\n",
                "Comment": "example public key"
            },
            {
                "Id": "K1S0LWQ2L5HTBU",
                "Name": "ExampleKey2",
                "CreatedTime": "2019-12-09T23:28:11.110Z",
                "EncodedKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApOCAg88A8+f4dujn9Izt
\n26LxtgAkn2opGgo/NKpMiaisyw5qlg3f1gol7FV6pYNl78iJg3EO8JBbwtlH
+cR9\nLGSf60NDeVhm76Oc39Np/vWgOdsGQcRbi9WmKZeSODqjQGzVZWqPmito3FzWVk6b
\nfVY5N36U/RdbVAJm95Km+qaMYlbIdF40t72bi3IkKYV5hlB2XoDjlQ9F6ajQKyTB
\nMHa3SN8q+3ZjQ4sJJ7D1V6r4wR8jDcFVD5NckWJmmgIVnkOQM37NYeoDnkaOuTpu\nha/
+3b8tOb2z3LBVHPkp85zJRAOXacSwf5rZtPYKBNFsixTa2n55k2r218mOkMC4\nUwIDAQAB\n-----END
 PUBLIC KEY-----",
                "Comment": "example public key #2"
            }
        ]
    }
}
```

- Para obtener detalles de la API, consulte ListPublicKeys en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Obtención de una lista de las etiquetas de una distribución de CloudFront

En el siguiente ejemplo se obtiene una lista de las etiquetas de una distribución de CloudFront:

```
aws cloudfront list-tags-for-resource \
```

```
    --resource arn:aws:cloudfront::123456789012:distribution/EDFDVBD6EXAMPLE
```

Salida:

```
{
    "Tags": {
        "Items": [
            {
                "Key": "DateCreated",
                "Value": "2019-12-04"
            },
            {
                "Key": "Name",
                "Value": "Example name"
            },
            {
                "Key": "Project",
                "Value": "Example project"
            }
        ]
    }
}
```

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`sign`

En el siguiente ejemplo de código, se muestra cómo utilizar `sign`.

AWS CLI

Firma de una URL de CloudFront

En el siguiente ejemplo, se firma una URL de CloudFront. Para firmar una URL, necesita el ID del par de claves (denominado ID de clave de acceso en la consola de administración de AWS) y la clave privada del par de claves de CloudFront del firmante de confianza. Para obtener más información sobre las URL firmadas, consulte Distribución de contenido privado con URL firmadas y cookies firmadas en la Guía para desarrolladores de Amazon CloudFront.

```
aws cloudfront sign \
```

```
    --url https://d111111abcdef8.cloudfront.net/private-content/private-file.html \
    --key-pair-id APKAEIBAERJR2EXAMPLE \
    --private-key file://cf-signer-priv-key.pem \
    --date-less-than 2020-01-01
```

Salida:

```
https://d111111abcdef8.cloudfront.net/private-content/private-
file.html?Expires=1577836800&Signature=nEXK7Kby47XKeZQKVc6pwkif6oZc-
JWSpDkH0UH7EBGGqvgurkecCbgL5VfUAXyLQuJxFwRQWscz-
owcq9KpmewCXrXQbPaJZNi9XSNwf4YKurPDQYaRQawKoeenH0GFteRf9ELK-
Bs3nljTLjtbgzIUt7QJNKXcWr8AuUYikzGdJ4-qzx6WnxXfH~fxg4-
GGl6l2kgCpXUB6Jx6K~Y3kpVOdzUPOIqFLHAnJojbhxqrVejomZZ2XrquDvNUCCIbePGnR3d24UPaLXG4FKOqNEaWDIB
GNvjRJxqWf93uMobeMOiVYahb-e0KItiQewGcm0eLZQ__&Key-Pair-Id=APKAEIBAERJR2EXAMPLE
```

- Para obtener información de la API, consulte Sign en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Etiquetado de una distribución de CloudFront

En el siguiente ejemplo de `tag-resource`, se agregan dos etiquetas a la distribución de CloudFront especificada.

```
aws cloudfront tag-resource \
    --resource arn:aws:cloudfront::123456789012:distribution/EDFDVBD6EXAMPLE \
    --tags 'Items=[{Key=Name,Value="Example name"},{Key=Project,Value="Example
 project"}]'
```

En lugar de usar argumentos de línea de comandos, puede proporcionar las etiquetas en un archivo JSON, como se muestra en el siguiente ejemplo:

```
aws cloudfront tag-resource \
    --resource arn:aws:cloudfront::123456789012:distribution/EDFDVBD6EXAMPLE \
    --tags file://tags.json
```

Contenido de `tags.json`:

```
{
    "Items": [
        {
            "Key": "Name",
            "Value": "Example name"
        },
        {
            "Key": "Project",
            "Value": "Example project"
        }
    ]
}
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de etiquetas de una distribución de CloudFront

En el siguiente ejemplo, se eliminan dos etiquetas de una distribución de CloudFront mediante argumentos de línea de comandos:

```
aws cloudfront untag-resource \
    --resource arn:aws:cloudfront::123456789012:distribution/EDFDVBD6EXAMPLE \
    --tag-keys Items=Name,Project
```

En lugar de usar argumentos de línea de comandos, puede proporcionar las claves de etiqueta en un archivo JSON, como se muestra en el siguiente ejemplo:

```
aws cloudfront untag-resource \
    --resource arn:aws:cloudfront::123456789012:distribution/EDFDVBD6EXAMPLE \
    --tag-keys file://tag-keys.json
```

El archivo `tag-keys.json` es un documento JSON en la carpeta actual que contiene lo siguiente:

```
{
    "Items": [
        "Name",
        "Project"
    ]
}
```

Si se ejecuta correctamente, este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-cloud-front-origin-access-identity

En el siguiente ejemplo de código, se muestra cómo utilizar `update-cloud-front-origin-access-identity`.

AWS CLI

Actualización de la identidad de acceso de origen de CloudFront

En el siguiente ejemplo, se actualiza la identidad de acceso de origen (OAI) con el ID `E74FTE3AEXAMPLE`. El único campo que puede actualizar es el de `Comment` de la OAI.

Para eliminar una OAI, debe tener el ID y la `ETag` de la OAI. El ID de OAI se devuelve en la salida de los comandos create-cloud-front-origin-access-identity y list-cloud-front-origin-access-identities. Para obtener la `ETag`, utilice el comando get-cloud-front-origin-access-identity o get-cloud-front-origin-access-identity-config. Use la opción `--if-match` para proporcionar la `ETag` de la OAI.

```
aws cloudfront update-cloud-front-origin-access-identity \
    --id E74FTE3AEXAMPLE \
    --if-match E2QWRUHEXAMPLE \
    --cloud-front-origin-access-identity-config \
        CallerReference=cli-example,Comment="Example OAI Updated"
```

Puede lograr lo mismo facilitando la configuración de la OAI en un archivo JSON, como se muestra en el siguiente ejemplo:

```
aws cloudfront update-cloud-front-origin-access-identity \
    --id E74FTE3AEXAMPLE \
    --if-match E2QWRUHEXAMPLE \
    --cloud-front-origin-access-identity-config file://OAI-config.json
```

El archivo `OAI-config.json` es un documento JSON en el directorio actual que contiene lo siguiente:

```
{
    "CallerReference": "cli-example",
    "Comment": "Example OAI Updated"
}
```

Tanto si facilita la configuración de la OAI con un argumento de línea de comandos o con un archivo JSON, el resultado será el mismo:

```
{
    "ETag": "E9LHASXEXAMPLE",
    "CloudFrontOriginAccessIdentity": {
        "Id": "E74FTE3AEXAMPLE",
        "S3CanonicalUserId":
 "cd13868f797c227fbea2830611a26fe0a21ba1b826ab4bed9b7771c9aEXAMPLE",
        "CloudFrontOriginAccessIdentityConfig": {
            "CallerReference": "cli-example",
            "Comment": "Example OAI Updated"
        }
    }
}
```

- Para obtener información acerca de la API, consulte UpdateCloudFrontOriginAccessIdentity en la Referencia de comandos de la AWS CLI.

`update-connection-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-connection-group`.

AWS CLI

Actualización de un grupo de conexiones de CloudFront

En el siguiente ejemplo de `update-connection-group`, se desactiva un grupo de conexiones de CloudFront y se desactiva IPv6.

```
aws cloudfront update-connection-group \
    --id cg_2yHsDkcPKeUlVkk3aEgLKcjABC \
    --no-ipv6-enabled \
    --no-enabled \
    --if-match E3UN6WX5RRO2ABC
```

Salida:

```
{
    "ETag": "E1F83G8C2ARABC",
    "ConnectionGroup": {
        "Id": "cg_2yHsDkcPKeUlVkk3aEgLKcjABC",
        "Name": "cg-example",
        "Arn": "arn:aws:cloudfront::123456789012:connection-group/
cg_2yHsDkcPKeUlVkk3aEgLKcjABC",
        "CreatedTime": "2025-06-09T20:58:35.481000+00:00",
        "LastModifiedTime": "2025-06-11T16:25:54.280000+00:00",
        "Ipv6Enabled": false,
        "RoutingEndpoint": "du9xp1elo1abc.cloudfront.net",
        "Status": "InProgress",
        "Enabled": false,
        "IsDefault": false
    }
}
```

Para obtener más información, consulte Creación de un grupo de conexiones personalizado (opcional) en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte UpdateConnectionGroup en la Referencia de comandos de la AWS CLI.

`update-distribution-tenant`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-distribution-tenant`.

AWS CLI

Actualización de un inquilino de distribución de CloudFront

En el siguiente ejemplo de `update-distribution-tenant`, se actualiza un inquilino de distribución de CloudFront con un nuevo valor de parámetro y se agrega un país a las restricciones geográficas.

```
aws cloudfront update-distribution-tenant \
    --cli-input-json file://update-tenant.json
```

Contenido de `update-tenant.json`:

```
{
    "Id": "dt_2yMvQgam3QkJo2z54FDl91dk1AB",
    "IfMatch": "E1F83G8C2ARABC",
    "Parameters": [
        {
            "Name": "testParam",
            "Value": "newParameterValue"
        }
    ],
    "Customizations": {
        "WebAcl": {
            "Action": "disable"
        },
        "GeoRestrictions": {
            "RestrictionType": "whitelist",
            "Locations": [
                "DE",
                "GB",
                "ES"
            ]
        }
    }
}
```

Salida:

```
{
    "ETag": "E1PA6795UKMABC",
    "DistributionTenant": {
        "Id": "dt_2yMvQgam3QkJo2z54FDl91dk1AB",
        "DistributionId": "E1XNX8R2GOAABC",
        "Name": "new-tenant-customizations",
```

```
        "Arn": "arn:aws:cloudfront::123456789012:distribution-tenant/
dt_2yMvQgam3QkJo2z54FDl91dk1AB",
        "Domains": [
            {
                "Domain": "example.com",
                "Status": "active"
            }
        ],
        "Customizations": {
            "WebAcl": {
                "Action": "disable"
            },
            "GeoRestrictions": {
                "RestrictionType": "whitelist",
                "Locations": [
                    "DE",
                    "ES",
                    "GB"
                ]
            }
        },
        "Parameters": [
            {
                "Name": "testParam",
                "Value": "newParameterValue"
            }
        ],
        "ConnectionGroupId": "cg_2whCJoXMYCjHcxaLGrkllvyABC",
        "CreatedTime": "2025-06-11T15:54:02.142000+00:00",
        "LastModifiedTime": "2025-06-11T16:42:45.531000+00:00",
        "Enabled": false,
        "Status": "InProgress"
    }
}
```

Para obtener más información, consulte Personalizaciones de inquilinos de distribución en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte UpdateDistributionTenant en la Referencia de comandos de la AWS CLI.

update-distribution

En el siguiente ejemplo de código, se muestra cómo utilizar update-distribution.

AWS CLI

Ejemplo 1: actualización de un objeto raíz predeterminado de una distribución de CloudFront

En el siguiente ejemplo, se actualiza el objeto raíz predeterminado a index.html para la distribución de CloudFront con el ID EDFDVBD6EXAMPLE.

```
aws cloudfront update-distribution \
    --id EDFDVBD6EXAMPLE \
    --default-root-object index.html
```

Salida:

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "Distribution": {
        "Id": "EDFDVBD6EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EDFDVBD6EXAMPLE",
        "Status": "InProgress",
        "LastModifiedTime": "2019-12-06T18:55:39.870Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "6b10378d-49be-4c4b-a642-419ccaf8f3b5",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "example-website",
                        "DomainName": "www.example.com",
                        "OriginPath": "",
```

```
                    "CustomHeaders": {
                        "Quantity": 0
                    },
                    "CustomOriginConfig": {
                        "HTTPPort": 80,
                        "HTTPSPort": 443,
                        "OriginProtocolPolicy": "match-viewer",
                        "OriginSslProtocols": {
                            "Quantity": 2,
                            "Items": [
                                "SSLv3",
                                "TLSv1"
                            ]
                        },
                        "OriginReadTimeout": 30,
                        "OriginKeepaliveTimeout": 5
                    }
                }
            ]
        },
        "OriginGroups": {
            "Quantity": 0
        },
        "DefaultCacheBehavior": {
            "TargetOriginId": "example-website",
            "ForwardedValues": {
                "QueryString": false,
                "Cookies": {
                    "Forward": "none"
                },
                "Headers": {
                    "Quantity": 1,
                    "Items": [
                        "*"
                    ]
                },
                "QueryStringCacheKeys": {
                    "Quantity": 0
                }
            },
            "TrustedSigners": {
                "Enabled": false,
                "Quantity": 0
            },
```

```
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
```

```
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http1.1",
            "IsIPV6Enabled": true
        }
    }
}
```

Ejemplo 2: actualización de una distribución de CloudFront

En el siguiente ejemplo se deshabilita la distribución de CloudFront con el ID de `EMLARXS9EXAMPLE` al proporcionar la configuración de distribución en un archivo JSON denominado `dist-config-disable.json`. Para actualizar una distribución, debe usar la opción `--if-match` para proporcionar la `ETag` de la distribución. Para obtener la `ETag`, utilice el comando get-distribution o get-distribution-config. Tenga en cuenta que el campo `Enabled` se ha establecido en `false` en el archivo JSON.

Una vez que utilice el siguiente ejemplo para deshabilitar una distribución, puede utilizar el comando delete-distribution para eliminarla.

```
aws cloudfront update-distribution \
    --id EMLARXS9EXAMPLE \
    --if-match E2QWRUHEXAMPLE \
    --distribution-config file://dist-config-disable.json
```

Contenido de `dist-config-disable.json`:

```
{
    "CallerReference": "cli-1574382155-496510",
    "Aliases": {
        "Quantity": 0
    },
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
```

```
            {
                "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-1574382155-273939",
                "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                "OriginPath": "",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "OriginGroups": {
        "Quantity": 0
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-bucket.s3.amazonaws.com-1574382155-273939",
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            },
            "Headers": {
                "Quantity": 0
            },
            "QueryStringCacheKeys": {
                "Quantity": 0
            }
        },
        "TrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ViewerProtocolPolicy": "allow-all",
        "MinTTL": 0,
        "AllowedMethods": {
            "Quantity": 2,
            "Items": [
                "HEAD",
                "GET"
            ],
            "CachedMethods": {
                "Quantity": 2,
```

```
                "Items": [
                    "HEAD",
                    "GET"
                ]
            }
        },
        "SmoothStreaming": false,
        "DefaultTTL": 86400,
        "MaxTTL": 31536000,
        "Compress": false,
        "LambdaFunctionAssociations": {
            "Quantity": 0
        },
        "FieldLevelEncryptionId": ""
    },
    "CacheBehaviors": {
        "Quantity": 0
    },
    "CustomErrorResponses": {
        "Quantity": 0
    },
    "Comment": "",
    "Logging": {
        "Enabled": false,
        "IncludeCookies": false,
        "Bucket": "",
        "Prefix": ""
    },
    "PriceClass": "PriceClass_All",
    "Enabled": false,
    "ViewerCertificate": {
        "CloudFrontDefaultCertificate": true,
        "MinimumProtocolVersion": "TLSv1",
        "CertificateSource": "cloudfront"
    },
    "Restrictions": {
        "GeoRestriction": {
            "RestrictionType": "none",
            "Quantity": 0
        }
    },
    "WebACLId": "",
    "HttpVersion": "http2",
    "IsIPV6Enabled": true
```

```
}
```

Salida:

```
{
    "ETag": "E9LHASXEXAMPLE",
    "Distribution": {
        "Id": "EMLARXS9EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EMLARXS9EXAMPLE",
        "Status": "InProgress",
        "LastModifiedTime": "2019-12-06T18:32:35.553Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-1574382155-496510",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-
bucket.s3.amazonaws.com-1574382155-273939",
                        "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
```

```
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-
bucket.s3.amazonaws.com-1574382155-273939",
                "ForwardedValues": {
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
                    "Headers": {
                        "Quantity": 0
                    },
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
                },
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
```

```
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": false,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

- Para obtener información acerca de la API, consulte UpdateDistribution en la Referencia de comandos de la AWS CLI.

`update-domain-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-domain-association`.

AWS CLI

Actualización de una asociación de dominio

En el siguiente ejemplo de `update-domain-association`, se actualiza una asociación de dominio para un inquilino de distribución con ETag `E23ZP02F085ABC`.

```
aws cloudfront update-domain-association \
    --domain example.com \
    --target-resource DistributionTenantId=dt_2x9GhoK0TZRsohWzv1b9It8J1AB \
    --if-match E23ZP02F085ABC
```

Salida:

```
{
    "ETag": "ETVPDKIKX0ABC",
    "Domain": "example.com",
    "ResourceId": "dt_2x9GhoK0TZRsohWzv1b9It8J1AB"
}
```

Para obtener más información, consulte Mover un nombre de dominio alternativo a una distribución diferente en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte UpdateDomainAssociation en la Referencia de comandos de la AWS CLI.

`update-field-level-encryption-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-field-level-encryption-config`.

AWS CLI

Actualización de una configuración de cifrado en el nivel de campo de CloudFront

En el siguiente ejemplo actualiza el campo `Comment` de la configuración de cifrado en el nivel de campo con el ID `C3KM2WVD605UAY` facilitando los parámetros en un archivo JSON.

Para actualizar una configuración de cifrado en el nivel de campo, debe tener el ID de la configuración y la `ETag`. El ID se obtiene con la salida de los comandos create-field-level-encryption-config y list-field-level-encryption-configs. Para obtener la `ETag`, utilice el comando get-field-level-encryption o get-field-level-encryption-config. Utilice la opción `--if-match` para proporcionar la `ETag` de la configuración.

```
aws cloudfront update-field-level-encryption-config \
```

```
    --id C3KM2WVD605UAY \
    --if-match E2P4Z4VU7TY5SG \
    --field-level-encryption-config file://fle-config.json
```

El archivo `fle-config.json` es un documento JSON en el directorio actual que contiene lo siguiente:

```
{
    "CallerReference": "cli-example",
    "Comment": "Updated example FLE configuration",
    "QueryArgProfileConfig": {
        "ForwardWhenQueryArgProfileIsUnknown": true,
        "QueryArgProfiles": {
            "Quantity": 0
        }
    },
    "ContentTypeProfileConfig": {
        "ForwardWhenContentTypeIsUnknown": true,
        "ContentTypeProfiles": {
            "Quantity": 1,
            "Items": [
                {
                    "Format": "URLEncoded",
                    "ProfileId": "P280MFCLSYOCVU",
                    "ContentType": "application/x-www-form-urlencoded"
                }
            ]
        }
    }
}
```

Salida:

```
{
    "ETag": "E26M4BIAV81ZF6",
    "FieldLevelEncryption": {
        "Id": "C3KM2WVD605UAY",
        "LastModifiedTime": "2019-12-10T22:26:26.170Z",
        "FieldLevelEncryptionConfig": {
            "CallerReference": "cli-example",
            "Comment": "Updated example FLE configuration",
            "QueryArgProfileConfig": {
                "ForwardWhenQueryArgProfileIsUnknown": true,
```

```
                "QueryArgProfiles": {
                    "Quantity": 0,
                    "Items": []
                }
            },
            "ContentTypeProfileConfig": {
                "ForwardWhenContentTypeIsUnknown": true,
                "ContentTypeProfiles": {
                    "Quantity": 1,
                    "Items": [
                        {
                            "Format": "URLEncoded",
                            "ProfileId": "P280MFCLSYOCVU",
                            "ContentType": "application/x-www-form-urlencoded"
                        }
                    ]
                }
            }
        }
    }
}
```

- Para obtener más información sobre la API, consulte UpdateFieldLevelEncryptionConfig en la Referencia de comandos de la AWS CLI.

`update-field-level-encryption-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-field-level-encryption-profile`.

AWS CLI

Actualización de un perfil de cifrado en el nivel de campo de CloudFront

En el siguiente ejemplo se actualiza el perfil de cifrado en el nivel de campo con el ID `PPK0UOSIF5WSV`. En este ejemplo, se actualiza el `Name` y el `Comment` del perfil y se agrega un segundo elemento `FieldPatterns` facilitando los parámetros en un archivo JSON.

Para actualizar un perfil de cifrado en el nivel de campo, debe tener el ID y la `ETag` del perfil. El ID se obtiene con la salida de los comandos create-field-level-encryption-profile y list-field-level-encryption-profiles. Para obtener la `ETag`, utilice el comando get-field-level-encryption-profile o

get-field-level-encryption-profile-config. Use la opción `--if-match` para proporcionar la `ETag` del perfil.

```
aws cloudfront update-field-level-encryption-profile \
    --id PPK0UOSIF5WSV \
    --if-match E1QQG65FS2L2GC \
    --field-level-encryption-profile-config file://fle-profile-config.json
```

El archivo `fle-profile-config.json` es un documento JSON en el directorio actual que contiene lo siguiente:

```
{
    "Name": "ExampleFLEProfileUpdated",
    "CallerReference": "cli-example",
    "Comment": "Updated FLE profile for AWS CLI example",
    "EncryptionEntities": {
        "Quantity": 1,
        "Items": [
            {
                "PublicKeyId": "K2K8NC4HVFE3M0",
                "ProviderId": "ExampleFLEProvider",
                "FieldPatterns": {
                    "Quantity": 2,
                    "Items": [
                        "ExampleSensitiveField",
                        "SecondExampleSensitiveField"
                    ]
                }
            }
        ]
    }
}
```

Salida:

```
{
    "ETag": "EJETYFJ9CL66D",
    "FieldLevelEncryptionProfile": {
        "Id": "PPK0UOSIF5WSV",
        "LastModifiedTime": "2019-12-10T19:05:58.296Z",
        "FieldLevelEncryptionProfileConfig": {
            "Name": "ExampleFLEProfileUpdated",
```

```
            "CallerReference": "cli-example",
            "Comment": "Updated FLE profile for AWS CLI example",
            "EncryptionEntities": {
                "Quantity": 1,
                "Items": [
                    {
                        "PublicKeyId": "K2K8NC4HVFE3M0",
                        "ProviderId": "ExampleFLEProvider",
                        "FieldPatterns": {
                            "Quantity": 2,
                            "Items": [
                                "ExampleSensitiveField",
                                "SecondExampleSensitiveField"
                            ]
                        }
                    }
                ]
            }
        }
    }
}
```

- Para obtener detalles sobre la API, consulte UpdateFieldLevelEncryptionProfile en la Referencia de comandos de la AWS CLI.

`verify-dns-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `verify-dns-configuration`.

AWS CLI

Verificación de la configuración de DNS de un dominio

En el siguiente ejemplo de `verify-dns-configuration`, se verifica la configuración de DNS de un dominio.

```
aws cloudfront verify-dns-configuration \
    --domain example.com \
    --identifier dt_2x9GhoK0TZRsohWzv1b9It8J1AB
```

Salida:

```
{
    "DnsConfigurationList": [
        {
            "Domain": "example.com",
            "Status": "valid-configuration"
        }
    ]
}
```

Para obtener más información, consulte Mover un nombre de dominio alternativo a una distribución diferente en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte VerifyDnsConfiguration en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon CloudSearch que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar situaciones comunes usando la AWS Command Line Interface con Amazon CloudSearch.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`upload-documents`

En el siguiente ejemplo de código, se muestra cómo utilizar `upload-documents`.

AWS CLI

Con el siguiente comando `upload-documents`, se carga un lote de documentos JSON en un dominio de Amazon CloudSearch:

```
aws cloudsearchdomain upload-documents --endpoint-url https://doc-my-
domain.us-west-1.cloudsearch.amazonaws.com --content-type application/json --
documents document-batch.json
```

Salida:

```
{
  "status": "success",
  "adds": 5000,
  "deletes": 0
}
```

- Para obtener información sobre la API, consulte UploadDocuments en la Referencia de comandos de la AWS CLI.

Ejemplos de CloudTrail que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar situaciones comunes usando la AWS Command Line Interface con CloudTrail.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-tags`.

AWS CLI

Adición de etiquetas al registro de seguimiento

En el siguiente comando `add-tags`, se añaden etiquetas para `Trail1`:

```
aws cloudtrail add-tags --resource-id arn:aws:cloudtrail:us-
east-1:123456789012:trail/Trail1 --tags-
list Key=name,Value=Alice Key=location,Value=us
```

- Para obtener información sobre la API, consulte AddTags en la Referencia de comandos de la AWS CLI.

`create-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-subscription`.

AWS CLI

Creación y configuración de recursos de AWS para un registro de seguimiento

El siguiente comando `create-subscription` crea un nuevo bucket de S3 y un tema de SNS para `Trail1`.

```
aws cloudtrail create-subscription \
    --name Trail1 \
    --s3-new-bucket amzn-s3-demo-bucket \
    --sns-new-topic my-topic
```

Salida:

```
Setting up new S3 bucket amzn-s3-demo-bucket...
Setting up new SNS topic my-topic...
Creating/updating CloudTrail configuration...
CloudTrail configuration:
    {
        "trailList": [
            {
                "IncludeGlobalServiceEvents": true,
                "Name": "Trail1",
                "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/
Trail1",
                "LogFileValidationEnabled": false,
                "IsMultiRegionTrail": false,
                "S3BucketName": "amzn-s3-demo-bucket",
```

```
                "SnsTopicName": "my-topic",
                "HomeRegion": "us-east-1"
            }
        ],
        "ResponseMetadata": {
        "HTTPStatusCode": 200,
        "RequestId": "f39e51f6-c615-11e5-85bd-d35ca21ee3e2"
        }
    }
Starting CloudTrail service...
Logs will be delivered to my-bucket
```

- Para obtener información sobre la API, consulte CreateSubscription en la Referencia de comandos de la AWS CLI.

`create-trail`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-trail`.

AWS CLI

Creación de un registro de seguimiento

En el siguiente ejemplo de `create-trail`, se crea un registro de seguimiento multirregional denominado `Trail1` y se especifica un bucket de S3.

```
aws cloudtrail create-trail \
    --name Trail1 \
    --s3-bucket-name amzn-s3-demo-bucket \
    --is-multi-region-trail
```

Salida:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Trail1",
    "TrailARN": "arn:aws:cloudtrail:us-west-2:123456789012:trail/Trail1",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

- Para obtener información sobre la API, consulte CreateTrail en la Referencia de comandos de la AWS CLI.

`delete-trail`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-trail`.

AWS CLI

Eliminación de un registro de seguimiento

En el siguiente comando `delete-trail`, se elimina un registro de seguimiento denominado `Trail1`:

```
aws cloudtrail delete-trail --name Trail1
```

- Para obtener información sobre la API, consulte DeleteTrail en la Referencia de comandos de la AWS CLI.

`describe-trails`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-trails`.

AWS CLI

Descripción de un registro de seguimiento

En el siguiente ejemplo de `describe-trails`, se devuelve el valor establecido para `Trail1` y `Trail2`.

```
aws cloudtrail describe-trails \
    --trail-name-list Trail1 Trail2
```

Salida:

```
{
    "trailList": [
        {
            "IncludeGlobalServiceEvents": true,
            "Name": "Trail1",
```

```
            "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/Trail1",
            "LogFileValidationEnabled": false,
            "IsMultiRegionTrail": false,
            "S3BucketName": "amzn-s3-demo-bucket",
            "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/
CloudTrail_CloudWatchLogs_Role",
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:CloudTrail:*",
            "SnsTopicName": "my-topic",
            "HomeRegion": "us-east-1"
        },
        {
            "IncludeGlobalServiceEvents": true,
            "Name": "Trail2",
            "S3KeyPrefix": "my-prefix",
            "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/Trail2",
            "LogFileValidationEnabled": false,
            "IsMultiRegionTrail": false,
            "S3BucketName": "amzn-s3-demo-bucket2",
            "KmsKeyId": "arn:aws:kms:us-
east-1:123456789012:key/4c5ae5ac-3c13-421e-8335-c7868ef6a769",
            "HomeRegion": "us-east-1"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeTrails en la Referencia de comandos de la AWS CLI.

`get-event-selectors`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-event-selectors`.

AWS CLI

Visualización de la configuración de los selectores de eventos de un registro de seguimiento

En el siguiente comando `get-event-selectors`, se obtiene la configuración de `Trail1`:

```
aws cloudtrail get-event-selectors --trail-name Trail1
```

Salida:

```
{
  "EventSelectors": [
      {
          "IncludeManagementEvents": true,
          "DataResources": [],
          "ReadWriteType": "All"
      }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/Trail1"
}
```

- Para obtener información sobre la API, consulte GetEventSelectors en la Referencia de comandos de la AWS CLI.

`get-trail-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-trail-status`.

AWS CLI

Obtención del estado de un registro de seguimiento

En el siguiente comando `get-trail-status`, se obtienen los detalles de entrega y registro de `Trail1`:

```
aws cloudtrail get-trail-status --name Trail1
```

Salida:

```
{
  "LatestNotificationTime": 1454022144.869,
  "LatestNotificationAttemptSucceeded": "2016-01-28T23:02:24Z",
  "LatestDeliveryAttemptTime": "2016-01-28T23:02:24Z",
  "LatestDeliveryTime": 1454022144.869,
  "TimeLoggingStarted": "2015-11-06T18:36:38Z",
  "LatestDeliveryAttemptSucceeded": "2016-01-28T23:02:24Z",
  "IsLogging": true,
  "LatestCloudWatchLogsDeliveryTime": 1454022144.918,
  "StartLoggingTime": 1446834998.695,
  "StopLoggingTime": 1446834996.933,
  "LatestNotificationAttemptTime": "2016-01-28T23:02:24Z",
```

```
  "TimeLoggingStopped": "2015-11-06T18:36:36Z"
}
```

- Para obtener información sobre la API, consulte GetTrailStatus en la Referencia de comandos de la AWS CLI.

`list-public-keys`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-public-keys`.

AWS CLI

Generación de una lista de todas las claves públicas de un registro de seguimiento

En el siguiente comando `list-public-keys`, se obtienen todas las claves públicas cuyas claves privadas se han utilizado para firmar archivos de resumen en el intervalo de tiempo especificado:

```
aws cloudtrail list-public-keys --start-time 2016-01-01T20:30:00.000Z
```

Salida:

```
{
  "PublicKeyList": [
      {
         "ValidityStartTime": 1453076702.0,
         "ValidityEndTime": 1455668702.0,
         "Value": "MIIBCgKCAQEAlSS3cl92HDycr/MTj0moOhas8habjrraXw+KzlWF0axSI2tcF
+3iJ9BKQAVSKxGwxwu3m0wG3J
+kUl1xboEcEPHYoIYMbgfSw7KGnuDKwkLzsQWhUJ0cIbOHASox1vv/5fNXkrHhGbDCHeVXm804c83nvHUEFYThr1PfyP
+4WGDk+BGH5m9iuiAKkipEHWmUl8/P7XpfpWQuk4h8g3pXZOrNXr08lbh4d39svj7UqdhvOXoBISp9t/
EXYuePGEtBdrKD9Dz+VHwyUPtBQvYr9BnkF88qBnaPNhS44rzwIDAQAB",
         "Fingerprint": "7f3f401420072e50a65a141430817ab3"
      }
  ]
}
```

- Para obtener detalles de la API, consulte ListPublicKeys en la Referencia de comandos de la AWS CLI.

`list-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags`.

AWS CLI

Generación de una lista de etiquetas de un registro de seguimiento

Con el siguiente comando `list-tags`, se genera una lista de las etiquetas de `Trail1` y`Trail2`:

```
aws cloudtrail list-tags --resource-id-list arn:aws:cloudtrail:us-
east-1:123456789012:trail/Trail1 arn:aws:cloudtrail:us-east-1:123456789012:trail/
Trail2
```

Salida:

```
{
 "ResourceTagList": [
     {
         "ResourceId": "arn:aws:cloudtrail:us-east-1:123456789012:trail/Trail1",
         "TagsList": [
             {
                 "Value": "Alice",
                 "Key": "name"
             },
             {
                 "Value": "us",
                 "Key": "location"
             }
         ]
     },
     {
         "ResourceId": "arn:aws:cloudtrail:us-east-1:123456789012:trail/Trail2",
         "TagsList": [
             {
                 "Value": "Bob",
                 "Key": "name"
             }
         ]
     }
  ]
}
```

- Para obtener más información sobre la API, consulte ListTags en la Referencia de comandos de la AWS CLI.

`lookup-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `lookup-events`.

AWS CLI

Búsqueda de los eventos de un registro de seguimiento

Con el siguiente comando `lookup-events`, se buscan los eventos de actividad de la API por el atributo `EventName`:

```
aws cloudtrail lookup-events --lookup-
attributes AttributeKey=EventName,AttributeValue=ConsoleLogin
```

Salida:

```
{
  "Events": [
     {
         "EventId": "654ccbc0-ba0d-486a-9076-dbf7274677a7",
         "Username": "my-session-name",
         "EventTime": "2021-11-18T09:41:02-08:00",
         "CloudTrailEvent": "{\"eventVersion\":\"1.02\",\"userIdentity\":{\"type\":
\"AssumedRole\",\"principalId\":\"AROAJIKPFTA72SWU4L7T4:my-session-name\",\"arn\":
\"arn:aws:sts::123456789012:assumed-role/my-role/my-session-name\",\"accountId\":
\"123456789012\",\"sessionContext\":{\"attributes\":{\"mfaAuthenticated\":\"false
\",\"creationDate\":\"2016-01-26T21:42:12Z\"},\"sessionIssuer\":{\"type\":\"Role\",
\"principalId\":\"AROAJIKPFTA72SWU4L7T4\",\"arn\":\"arn:aws:iam::123456789012:role/
my-role\",\"accountId\":\"123456789012\",\"userName\":\"my-role\"}}},\"eventTime
\":\"2016-01-26T21:42:12Z\",\"eventSource\":\"signin.amazonaws.com\",\"eventName\":
\"ConsoleLogin\",\"awsRegion\":\"us-east-1\",\"sourceIPAddress\":\"72.21.198.70\",
\"userAgent\":\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/47.0.2526.111 Safari/537.36\",\"requestParameters
\":null,\"responseElements\":{\"ConsoleLogin\":\"Success\"},\"additionalEventData\":
{\"MobileVersion\":\"No\",\"MFAUsed\":\"No\"},\"eventID\":\"654ccbc0-ba0d-486a-9076-
dbf7274677a7\",\"eventType\":\"AwsConsoleSignIn\",\"recipientAccountId\":
\"123456789012\"}",
         "EventName": "ConsoleLogin",
         "Resources": []
```

```
        }
    ]
}
```

- Para obtener información sobre la API, consulte LookupEvents en la Referencia de comandos de la AWS CLI.

`put-event-selectors`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-event-selectors`.

AWS CLI

Ejemplo 1: cómo configurar un registro de seguimiento para registrar eventos de administración y eventos de datos mediante selectores de eventos avanzados

Puede añadir selectores de eventos avanzados y condiciones para los selectores de eventos avanzados; hasta un máximo de 500 valores para todas las condiciones y selectores de un registro de seguimiento. Puede utilizar los selectores de eventos avanzados para registrar todos los tipos de eventos de datos disponibles. Puede utilizar selectores de eventos avanzados o selectores de eventos básicos, pero no ambos. Si aplica selectores de eventos avanzados a un registro de seguimiento, se sobrescriben todos los selectores de eventos básicos existentes.

En el siguiente ejemplo de `put-event-selectors`, se crea un selector de eventos avanzado de un registro de seguimiento denominado `myTrail` para registrar todos los eventos de administración, registrar las llamadas a la API PutObject y DeleteObject de S3 para todos los bucket de S3, excepto uno, registrar las llamadas a la API de datos para una función de Lambda denominada `myFunction` y registrar las llamadas a la API de publicación en un tema de SNS denominado `myTopic`.

```
aws cloudtrail put-event-selectors \
    --trail-name myTrail \
    --advanced-event-selectors '[{"Name": "Log all management events",
 "FieldSelectors": [{ "Field": "eventCategory", "Equals": ["Management"] }] },
{"Name": "Log PutObject and DeleteObject events for all but one
 bucket","FieldSelectors": [{ "Field": "eventCategory", "Equals": ["Data"] },
{ "Field": "resources.type", "Equals": ["AWS::S3::Object"] },{ "Field":
 "eventName", "Equals": ["PutObject","DeleteObject"] },{ "Field": "resources.ARN",
 "NotStartsWith": ["arn:aws:s3:::amzn-s3-demo-bucket/"] }]},{"Name": "Log
 data events for a specific Lambda function","FieldSelectors": [{ "Field":
```

```
 "eventCategory", "Equals": ["Data"] },{ "Field": "resources.type",
 "Equals": ["AWS::Lambda::Function"] },{ "Field": "resources.ARN", "Equals":
 ["arn:aws:lambda:us-east-1:123456789012:function:myFunction"] }]},{"Name":
 "Log all Publish API calls on a specific SNS topic","FieldSelectors":
 [{ "Field": "eventCategory", "Equals": ["Data"] },{ "Field": "resources.type",
 "Equals": ["AWS::SNS::Topic"] },{ "Field": "eventName", "Equals":
 ["Publish"] },{ "Field": "resources.ARN", "Equals": ["arn:aws:sns:us-
east-1:123456789012:myTopic.fifo"] }]}]'
```

Salida:

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/myTrail",
    "AdvancedEventSelectors": [
        {
            "Name": "Log all management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        },
        {
            "Name": "Log PutObject and DeleteObject events for all but one bucket",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "eventName",
                    "Equals": [
```

```
                    "PutObject",
                    "DeleteObject"
                ]
            },
            {
                "Field": "resources.ARN",
                "NotStartsWith": [
                    "arn:aws:s3:::amzn-s3-demo-bucket/"
                ]
            }
        ]
    },
    {
        "Name": "Log data events for a specific Lambda function",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": [
                    "Data"
                ]
            },
            {
                "Field": "resources.type",
                "Equals": [
                    "AWS::Lambda::Function"
                ]
            },
            {
                "Field": "resources.ARN",
                "Equals": [
                    "arn:aws:lambda:us-east-1:123456789012:function:myFunction"
                ]
            }
        ]
    },
    {
        "Name": "Log all Publish API calls on a specific SNS topic",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": [
                    "Data"
                ]
            },
```

```
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::SNS::Topic"
                    ]
                },
                {
                    "Field": "eventName",
                    "Equals": [
                        "Publish"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "Equals": [
                        "arn:aws:sns:us-east-1:123456789012:myTopic.fifo"
                    ]
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Log events by using advanced event selectors en la Guía del usuario de AWS CloudTrail.

Ejemplo 2: cómo configurar selectores de eventos para un registro de seguimiento con objeto de registrar todos los eventos de administración y los eventos de datos

Puede configurar hasta cinco selectores de eventos para un registro de seguimiento y hasta 250 recursos de datos para un registro de seguimiento. Los selectores de eventos también se conocen como selectores de eventos básicos. Puede usar selectores de eventos para registrar eventos de administración y eventos de datos para objetos de S3, funciones de Lambda y tablas de DynnamoDB. Para registrar eventos de datos de otros tipos de recursos, debe utilizar selectores de eventos avanzados.

En el siguiente ejemplo de `put-event-selectors`, se crea un selector de eventos para que un registro de seguimiento denominado `TrailName` incluya todos los eventos de administración, eventos de datos para dos combinaciones de bucket/prefijo de Amazon S3 y eventos de datos para una sola función de AWS Lambda denominada `hello-world-python-function`.

```
aws cloudtrail put-event-selectors \
```

```
    --trail-name TrailName \
    --event-selectors '[{"ReadWriteType": "All","IncludeManagementEvents":
 true,"DataResources": [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::amzn-
s3-demo-bucket/prefix","arn:aws:s3:::amzn-s3-demo-bucket2/prefix2"]},
{"Type": "AWS::Lambda::Function","Values": ["arn:aws:lambda:us-
west-2:999999999999:function:hello-world-python-function"]}]}]'
```

Salida:

```
{
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::amzn-s3-demo-bucket/prefix",
                        "arn:aws:s3:::amzn-s3-demo-bucket2/prefix2"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda:us-west-2:123456789012:function:hello-world-
python-function"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para obtener más información, consulte Log events by using basic event selectors en la Guía del usuario de AWS CloudTrail.

Ejemplo 3: cómo configurar los selectores de eventos de un registro de seguimiento para que registre los eventos de administración, todos los eventos de datos de S3 en los objetos de S3 y todos los eventos de datos de Lambda en las funciones de la cuenta

En el siguiente ejemplo de `put-event-selectors`, se crea un selector de eventos para un registro de seguimiento denominado `TrailName2` que incluye todos los eventos de administración, así como todos los eventos de datos de todos los buckets de Amazon S3 y las funciones de AWS Lambda de la cuenta de AWS.

```
aws cloudtrail put-event-selectors \
    --trail-name TrailName2 \
    --event-selectors '[{"ReadWriteType": "All","IncludeManagementEvents":
 true,"DataResources": [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3"]},
{"Type": "AWS::Lambda::Function","Values": ["arn:aws:lambda"]}]}]'
```

Salida:

```
{
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName2"
}
```

Para obtener más información, consulte Log events by using basic event selectors en la Guía del usuario de AWS CloudTrail.

- Para obtener información sobre la API, consulte PutEventSelectors en la Referencia de comandos de la AWS CLI.

`remove-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-tags`.

AWS CLI

Eliminación de etiquetas de un registro de seguimiento

En el siguiente comando `remove-tags`, se eliminan las etiquetas especificadas para `Trail1`:

```
aws cloudtrail remove-tags --resource-id arn:aws:cloudtrail:us-
east-1:123456789012:trail/Trail1 --tags-list Key=name Key=location
```

- Para obtener información sobre la API, consulte RemoveTags en la Referencia de comandos de la AWS CLI.

`start-logging`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-logging`.

AWS CLI

Inicio del registro de un registro de seguimiento

En el siguiente comando `start-logging`, se activa el registro de `Trail1`:

```
aws cloudtrail start-logging --name Trail1
```

- Para obtener más información sobre la API, consulte StartLogging en la Referencia de comandos de la AWS CLI.

`stop-logging`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-logging`.

AWS CLI

Detención del registro de un registro de seguimiento

Con el siguiente comando `stop-logging`, se desactiva el registro de `Trail1`:

```
aws cloudtrail stop-logging --name Trail1
```

- Para obtener detalles de la API, consulte StopLogging en la Referencia de comandos de AWS CLI.

`update-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-subscription`.

AWS CLI

Actualización de los ajustes de configuración de un registro de seguimiento

En el siguiente ejemplo de `update-subscription`, se actualiza el registro de seguimiento para que especifique un nuevo bucket de S3 y un tema de SNS.

```
aws cloudtrail update-subscription \
    --name Trail1 \
    --s3-new-bucket amzn-s3-demo-bucket \
    --sns-new-topic my-topic-new
```

Salida:

```
Setting up new S3 bucket amzn-s3-demo-bucket...
Setting up new SNS topic my-topic-new...
Creating/updating CloudTrail configuration...
CloudTrail configuration:
{
    "trailList": [
        {
            "IncludeGlobalServiceEvents": true,
            "Name": "Trail1",
            "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/Trail1",
            "LogFileValidationEnabled": false,
            "IsMultiRegionTrail": false,
            "S3BucketName": "amzn-s3-demo-bucket",
            "SnsTopicName": "my-topic-new",
            "HomeRegion": "us-east-1"
        }
    ],
    "ResponseMetadata": {
        "HTTPStatusCode": 200,
        "RequestId": "31126f8a-c616-11e5-9cc6-2fd637936879"
    }
```

```
}
```

- Para obtener detalles sobre la API, consulte UpdateSubscription en la Referencia de comandos de la AWS CLI.

`update-trail`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-trail`.

AWS CLI

Actualización de un registro de seguimiento

En el siguiente ejemplo de `update-trail`, se actualiza un registro de seguimiento de manera que utilice un bucket existente para la entrega del registro.

```
aws cloudtrail update-trail \
    --name Trail1 \
    --s3-bucket-name amzn-s3-demo-bucket
```

Salida:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Trail1",
    "TrailARN": "arn:aws:cloudtrail:us-west-2:123456789012:trail/Trail1",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

- Para obtener información sobre la API, consulte UpdateTrail en la Referencia de comandos de la AWS CLI.

`validate-logs`

En el siguiente ejemplo de código, se muestra cómo utilizar `validate-logs`.

AWS CLI

Validación de un archivo de registro

En el siguiente comando de `validate-logs`, se validan los registros de `Trail1`:

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-1:123456789012:trail/Trail1 --start-time 20160129T19:00:00Z
```

Salida:

```
Validating log files for trail arn:aws:cloudtrail:us-east-1:123456789012:trail/
Trail1 between 2016-01-29T19:00:00Z and 2016-01-29T22:15:43Z
Results requested for 2016-01-29T19:00:00Z to 2016-01-29T22:15:43Z
Results found for 2016-01-29T19:24:57Z to 2016-01-29T21:24:57Z:
3/3 digest files valid
15/15 log files valid
```

- Para obtener información sobre la API, consulte ValidateLogs en la Referencia de comandos de la AWS CLI.

Ejemplos de CloudWatch que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con CloudWatch.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`delete-alarms`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-alarms`.

AWS CLI

Eliminación de una alarma

En el siguiente ejemplo, se utiliza el comando `delete-alarms` para eliminar la alarma de Amazon CloudWatch denominada “mialarma”:

```
aws cloudwatch delete-alarms --alarm-names myalarm
```

Salida:

```
This command returns to the prompt if successful.
```

- Para obtener información de la API, consulte DeleteAlarms en la Referencia de comandos de AWS CLI.

`delete-anomaly-detector`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-anomaly-detector`.

AWS CLI

Eliminación de un modelo de detección de anomalías especificado

En el siguiente ejemplo de `delete-anomaly-detector`, se elimina un modelo de detector de anomalías de la cuenta especificada.

```
aws cloudwatch delete-anomaly-detector \
    --namespace AWS/Logs \
    --metric-name IncomingBytes \
    --stat SampleCount
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de un modelo de detección de anomalías en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DeleteAnomalyDetector en la Referencia de comandos de la AWS CLI.

`delete-dashboards`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-dashboards`.

AWS CLI

Eliminación de paneles especificados

En el siguiente ejemplo de `delete-dashboards`, se eliminan dos paneles denominados `Dashboard-A` y `Dashboard-B` de la cuenta especificada.

```
aws cloudwatch delete-dashboards \
    --dashboard-names Dashboard-A Dashboard-B
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Paneles de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DeleteDashboards en la Referencia de comandos de la AWS CLI.

`delete-insight-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-insight-rules`.

AWS CLI

Eliminación de las reglas de Información de colaboradores especificadas

En el siguiente ejemplo de `delete-insight-rules`, se eliminan dos reglas de Información de colaboradores denominadas `Rule-A` y `Rule-B` en la cuenta especificada.

```
aws cloudwatch delete-insight-rules \
    --rule-names Rule-A Rule-B
```

Salida:

```
{
    "Failures": []
}
```

Para obtener más información, consulte Uso de Información de colaboradores para analizar datos de alta cardinalidad en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DeleteInsightRules en la Referencia de comandos de la AWS CLI.

`delete-metric-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-metric-stream`.

AWS CLI

Eliminación de un flujo de métricas específico

En el siguiente ejemplo de `delete-metric-stream`, se elimina el flujo métrico denominado `QuickPartial-gSCKv0` en la cuenta especificada.

```
aws cloudwatch delete-metric-stream \
    --name QuickPartial-gSCKv0
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de flujos métricos en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DeleteMetricStream en la Referencia de comandos de la AWS CLI.

`describe-alarm-history`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-alarm-history`.

AWS CLI

Recuperación del historial de una alarma

En el siguiente ejemplo, se utiliza el comando `describe-alarm-history` para recuperar el historial de la alarma de Amazon CloudWatch denominada “mialarma”:

```
aws cloudwatch describe-alarm-history --alarm-name "myalarm" --history-item-
type StateUpdate
```

Salida:

```
{
    "AlarmHistoryItems": [
        {
            "Timestamp": "2014-04-09T18:59:06.442Z",
            "HistoryItemType": "StateUpdate",
            "AlarmName": "myalarm",
            "HistoryData": "{\"version\":\"1.0\",\"oldState\":{\"stateValue\":
\"ALARM\",\"stateReason\":\"testing purposes\"},\"newState\":{\"stateValue\":\"OK
\",\"stateReason\":\"Threshold Crossed: 2 datapoints were not greater than the
 threshold (70.0). The most recent datapoints: [38.958, 40.292].\",\"stateReasonData
\":{\"version\":\"1.0\",\"queryDate\":\"2014-04-09T18:59:06.419+0000\",\"startDate
\":\"2014-04-09T18:44:00.000+0000\",\"statistic\":\"Average\",\"period\":300,
\"recentDatapoints\":[38.958,40.292],\"threshold\":70.0}}}",
            "HistorySummary": "Alarm updated from ALARM to OK"
        },
        {
            "Timestamp": "2014-04-09T18:59:05.805Z",
            "HistoryItemType": "StateUpdate",
            "AlarmName": "myalarm",
            "HistoryData": "{\"version\":\"1.0\",\"oldState\":{\"stateValue
\":\"OK\",\"stateReason\":\"Threshold Crossed: 2 datapoints were
 not greater than the threshold (70.0). The most recent datapoints:
 [38.839999999999996, 39.714].\",\"stateReasonData\":{\"version\":
\"1.0\",\"queryDate\":\"2014-03-11T22:45:41.569+0000\",\"startDate\":
\"2014-03-11T22:30:00.000+0000\",\"statistic\":\"Average\",\"period\":300,
\"recentDatapoints\":[38.839999999999996,39.714],\"threshold\":70.0}},\"newState\":
{\"stateValue\":\"ALARM\",\"stateReason\":\"testing purposes\"}}",
            "HistorySummary": "Alarm updated from OK to ALARM"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeAlarmHistory en la Referencia de comandos de la AWS CLI.

`describe-alarms-for-metric`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-alarms-for-metric`.

AWS CLI

Visualización de información sobre las alarmas asociadas a una métrica

En el siguiente ejemplo, se utiliza el comando `describe-alarms-for-metric` para mostrar información sobre las alarmas asociadas a la métrica CPUUtilization de Amazon EC2 y a la instancia con el ID i-0c986c72.:

```
aws cloudwatch describe-alarms-for-metric --metric-name CPUUtilization --
namespace AWS/EC2 --dimensions Name=InstanceId,Value=i-0c986c72
```

Salida:

```
{
    "MetricAlarms": [
        {
            "EvaluationPeriods": 10,
            "AlarmArn": "arn:aws:cloudwatch:us-
east-1:111122223333:alarm:myHighCpuAlarm2",
            "StateUpdatedTimestamp": "2013-10-30T03:03:51.479Z",
            "AlarmConfigurationUpdatedTimestamp": "2013-10-30T03:03:50.865Z",
            "ComparisonOperator": "GreaterThanOrEqualToThreshold",
            "AlarmActions": [
                "arn:aws:sns:us-east-1:111122223333:NotifyMe"
            ],
            "Namespace": "AWS/EC2",
            "AlarmDescription": "CPU usage exceeds 70 percent",
            "StateReasonData": "{\"version\":\"1.0\",\"queryDate\":
\"2013-10-30T03:03:51.479+0000\",\"startDate\":\"2013-10-30T02:08:00.000+0000\",
\"statistic\":\"Average\",\"period\":300,\"recentDatapoints\":
[40.698,39.612,42.432,39.796,38.816,42.28,42.854,40.088,40.760000000000005,41.316],
\"threshold\":70.0}",
            "Period": 300,
            "StateValue": "OK",
            "Threshold": 70.0,
            "AlarmName": "myHighCpuAlarm2",
            "Dimensions": [
                {
                    "Name": "InstanceId",
                    "Value": "i-0c986c72"
                }
            ],
            "Statistic": "Average",
```

```
            "StateReason": "Threshold Crossed: 10 datapoints were not greater than
 or equal to the threshold (70.0). The most recent datapoints: [40.760000000000005,
 41.316].",
            "InsufficientDataActions": [],
            "OKActions": [],
            "ActionsEnabled": true,
            "MetricName": "CPUUtilization"
        },
        {
            "EvaluationPeriods": 2,
            "AlarmArn": "arn:aws:cloudwatch:us-
east-1:111122223333:alarm:myHighCpuAlarm",
            "StateUpdatedTimestamp": "2014-04-09T18:59:06.442Z",
            "AlarmConfigurationUpdatedTimestamp": "2014-04-09T22:26:05.958Z",
            "ComparisonOperator": "GreaterThanThreshold",
            "AlarmActions": [
                "arn:aws:sns:us-east-1:111122223333:HighCPUAlarm"
            ],
            "Namespace": "AWS/EC2",
            "AlarmDescription": "CPU usage exceeds 70 percent",
            "StateReasonData": "{\"version\":\"1.0\",\"queryDate\":
\"2014-04-09T18:59:06.419+0000\",\"startDate\":\"2014-04-09T18:44:00.000+0000\",
\"statistic\":\"Average\",\"period\":300,\"recentDatapoints\":[38.958,40.292],
\"threshold\":70.0}",
            "Period": 300,
            "StateValue": "OK",
            "Threshold": 70.0,
            "AlarmName": "myHighCpuAlarm",
            "Dimensions": [
                {
                    "Name": "InstanceId",
                    "Value": "i-0c986c72"
                }
            ],
            "Statistic": "Average",
            "StateReason": "Threshold Crossed: 2 datapoints were not greater than
 the threshold (70.0). The most recent datapoints: [38.958, 40.292].",
            "InsufficientDataActions": [],
            "OKActions": [],
            "ActionsEnabled": false,
            "MetricName": "CPUUtilization"
        }
    ]
```

```
}
```

- Para obtener información sobre la API, consulte DescribeAlarmsForMetric en la Referencia de comandos de la AWS CLI.

`describe-alarms`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-alarms`.

AWS CLI

Visualización de información acerca de una alarma

En el siguiente ejemplo, se utiliza el comando `describe-alarms` para proporcionar información sobre la alarma denominada “mialarma”:

```
aws cloudwatch describe-alarms --alarm-names "myalarm"
```

Salida:

```
{
    "MetricAlarms": [
        {
            "EvaluationPeriods": 2,
            "AlarmArn": "arn:aws:cloudwatch:us-east-1:123456789012:alarm:myalarm",
            "StateUpdatedTimestamp": "2014-04-09T18:59:06.442Z",
            "AlarmConfigurationUpdatedTimestamp": "2012-12-27T00:49:54.032Z",
            "ComparisonOperator": "GreaterThanThreshold",
            "AlarmActions": [
                "arn:aws:sns:us-east-1:123456789012:myHighCpuAlarm"
            ],
            "Namespace": "AWS/EC2",
            "AlarmDescription": "CPU usage exceeds 70 percent",
            "StateReasonData": "{\"version\":\"1.0\",\"queryDate\":
\"2014-04-09T18:59:06.419+0000\",\"startDate\":\"2014-04-09T18:44:00.000+0000\",
\"statistic\":\"Average\",\"period\":300,\"recentDatapoints\":[38.958,40.292],
\"threshold\":70.0}",
            "Period": 300,
            "StateValue": "OK",
            "Threshold": 70.0,
            "AlarmName": "myalarm",
            "Dimensions": [
```

```
                {
                    "Name": "InstanceId",
                    "Value": "i-0c986c72"
                }
            ],
            "Statistic": "Average",
            "StateReason": "Threshold Crossed: 2 datapoints were not greater than
 the threshold (70.0). The most recent datapoints: [38.958, 40.292].",
            "InsufficientDataActions": [],
            "OKActions": [],
            "ActionsEnabled": true,
            "MetricName": "CPUUtilization"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeAlarms en la Referencia de comandos de la AWS CLI.

`describe-anomaly-detectors`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-anomaly-detectors`.

AWS CLI

Recuperación de una lista de modelos de detección de anomalías

En el siguiente ejemplo de `describe-anomaly-detectors` se muestra información sobre los modelos de detectores de anomalías que están asociados al espacio de nombres de `AWS/Logs` en la cuenta especificada.

```
aws cloudwatch describe-anomaly-detectors \
    --namespace AWS/Logs
```

Salida:

```
{
    "AnomalyDetectors": [
        {
            "Namespace": "AWS/Logs",
            "MetricName": "IncomingBytes",
            "Dimensions": [],
```

```
            "Stat": "SampleCount",
            "Configuration": {
                "ExcludedTimeRanges": []
            },
            "StateValue": "TRAINED",
            "SingleMetricAnomalyDetector": {
                "AccountId": "123456789012",
                "Namespace": "AWS/Logs",
                "MetricName": "IncomingBytes",
                "Dimensions": [],
                "Stat": "SampleCount"
            }
        },
        {
            "Namespace": "AWS/Logs",
            "MetricName": "IncomingBytes",
            "Dimensions": [
                {
                    "Name": "LogGroupName",
                    "Value": "demo"
                }
            ],
            "Stat": "Average",
            "Configuration": {
                "ExcludedTimeRanges": []
            },
            "StateValue": "PENDING_TRAINING",
            "SingleMetricAnomalyDetector": {
                "AccountId": "123456789012",
                "Namespace": "AWS/Logs",
                "MetricName": "IncomingBytes",
                "Dimensions": [
                    {
                        "Name": "LogGroupName",
                        "Value": "demo"
                    }
                ],
                "Stat": "Average"
            }
        }
    ]
}
```

Para obtener más información, consulte Uso de detección de anomalías de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DescribeAnomalyDetectors en la Referencia de comandos de la AWS CLI.

`describe-insight-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-insight-rules`.

AWS CLI

Recuperación de una lista de reglas de Información de colaboradores

En el siguiente ejemplo de `describe-insight-rules`, se muestran todas las reglas de Información de colaboradores en la cuenta especificada.

```
aws cloudwatch describe-insight-rules
```

Salida:

```
{
    "InsightRules": [
        {
            "Name": "Rule-A",
            "State": "ENABLED",
            "Schema": "CloudWatchLogRule/1",
            "Definition": "{\n\t\"AggregateOn\": \"Count\",\n\t\"Contribution\":
 {\n\t\t\"Filters\": [],\n\t\t\"Keys\": [\n\t\t\t\"$.requestId\"\n\t\t]\n\t},\n
\t\"LogFormat\": \"JSON\",\n\t\"Schema\": {\n\t\t\"Name\": \"CloudWatchLogRule
\",\n\t\t\"Version\": 1\n\t},\n\t\"LogGroupARNs\": [\n\t\t\"arn:aws:logs:us-
east-1:123456789012:log-group:demo\"\n\t]\n}",
            "ManagedRule": false
        },
        {
            "Name": "Rule-B",
            "State": "ENABLED",
            "Schema": "CloudWatchLogRule/1",
            "Definition": "{\n\t\"AggregateOn\": \"Count\",\n\t\"Contribution\":
 {\n\t\t\"Filters\": [],\n\t\t\"Keys\": [\n\t\t\t\"$.requestId\"\n\t\t]\n\t},\n
\t\"LogFormat\": \"JSON\",\n\t\"Schema\": {\n\t\t\"Name\": \"CloudWatchLogRule
\",\n\t\t\"Version\": 1\n\t},\n\t\"LogGroupARNs\": [\n\t\t\"arn:aws:logs:us-
east-1:123456789012:log-group:demo-1\"\n\t]\n}",
```

```
            "ManagedRule": false
        }
    ]
}
```

Para obtener más información, consulte Uso de Información de colaboradores para analizar datos de alta cardinalidad en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DescribeInsightRules en la Referencia de comandos de la AWS CLI.

`disable-alarm-actions`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-alarm-actions`.

AWS CLI

Desactivación de acciones en una alarma

En el siguiente ejemplo, se utiliza el comando `disable-alarm-actions` para deshabilitar todas las acciones de la alarma denominada mialarma:

```
aws cloudwatch disable-alarm-actions --alarm-names myalarm
```

Este comando vuelve a la petición si se ejecuta correctamente.

- Para obtener información sobre la API, consulte DisableAlarmActions en la Referencia de comandos de la AWS CLI.

`disable-insight-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-insight-rules`.

AWS CLI

Desactivación de las reglas de Información de colaboradores especificadas

En el siguiente ejemplo de `disable-insight-rules`, se desactivan dos reglas de Información de colaboradores denominadas `Rule-A` y `Rule-B` en la cuenta especificada.

```
aws cloudwatch disable-insight-rules \
```

```
    --rule-names Rule-A Rule-B
```

Salida:

```
{
    "Failures": []
}
```

Para obtener más información, consulte Uso de Información de colaboradores para analizar datos de alta cardinalidad en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DisableInsightRules en la Referencia de comandos de la AWS CLI.

`enable-alarm-actions`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-alarm-actions`.

AWS CLI

Activación de todas las acciones de una alarma

En el siguiente ejemplo, se utiliza el comando `enable-alarm-actions` para activar todas las acciones de la alarma denominada myalarm.:

```
aws cloudwatch enable-alarm-actions --alarm-names myalarm
```

Este comando vuelve a la petición si se ejecuta correctamente.

- Para obtener información sobre las API, consulte EnableAlarmActions en la Referencia de comandos de la AWS CLI.

`enable-insight-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-insight-rules`.

AWS CLI

Habilitación de las reglas de Información de colaboradores especificadas

En el siguiente ejemplo de `enable-insight-rules`, se habilitan dos reglas de Información de colaboradores denominadas `Rule-A` y `Rule-B` en la cuenta especificada.

```
aws cloudwatch enable-insight-rules \
    --rule-names Rule-A Rule-B
```

Salida:

```
{
    "Failures": []
}
```

Para obtener más información, consulte Uso de Información de colaboradores para analizar datos de alta cardinalidad en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte EnableInsightRules en la Referencia de comandos de la AWS CLI.

`get-dashboard`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-dashboard`.

AWS CLI

Recuperación de información sobre un panel

En el siguiente ejemplo de `get-dashboard` se muestra información acerca del panel denominado `Dashboard-A` en la cuenta especificada.

```
aws cloudwatch get-dashboard \
    --dashboard-name Dashboard-A
```

Salida:

```
{
    "DashboardArn": "arn:aws:cloudwatch::123456789012:dashboard/Dashboard-A",
    "DashboardBody": "{\"widgets\":[{\"type\":\"metric\",\"x\":0,\"y\":0,\"width
\":6,\"height\":6,\"properties\":{\"view\":\"timeSeries\",\"stacked\":false,
\"metrics\":[[\"AWS/EC2\",\"NetworkIn\",\"InstanceId\",\"i-0131f062232ade043\"],[\".
\",\"NetworkOut\",\".\",\".\"]],\"region\":\"us-east-1\"}}]}",
    "DashboardName": "Dashboard-A"
}
```

Para obtener más información, consulte Paneles de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetDashboard en la Referencia de comandos de la AWS CLI.

`get-insight-rule-report`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-insight-rule-report`.

AWS CLI

Recuperación de datos de serie temporal recopilados por una regla de Información de colaboradores

En el siguiente ejemplo de `get-insight-rule-report`, se devuelven los datos de serie temporal recopilados por una regla de Información de colaboradores.

```
aws cloudwatch get-insight-rule-report \
    --rule-name Rule-A \
    --start-time 2024-10-13T20:15:00Z \
    --end-time 2024-10-13T20:30:00Z \
    --period 300
```

Salida:

```
{
    "KeyLabels": [
        "PartitionKey"
    ],
    "AggregationStatistic": "Sum",
    "AggregateValue": 0.5,
    "ApproximateUniqueCount": 1,
    "Contributors": [
        {
            "Keys": [
                "RequestID"
            ],
            "ApproximateAggregateValue": 0.5,
            "Datapoints": [
                {
                    "Timestamp": "2024-10-13T21:00:00+00:00",
```

```
                    "ApproximateValue": 0.5
                }
            ]
        }
    ],
    "RuleAttributes": []
}
```

Para obtener más información, consulte Uso de Información de colaboradores para analizar datos de alta cardinalidad en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetInsightRuleReport en la Referencia de comandos de la AWS CLI.

`get-metric-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-metric-data`.

AWS CLI

Ejemplo 1: Obtención del promedio total de IOPS de la instancia de EC2 especificada mediante una expresión matemática

En el siguiente ejemplo de `get-metric-data`, se recuperan los valores de las métricas de CloudWatch para la instancia de EC2 con InstanceID `i-abcdef` mediante una expresión matemática de métricas que combina las métricas `EBSReadOps` y `EBSWriteOps`.

```
aws cloudwatch get-metric-data \
    --metric-data-queries file://file.json \
    --start-time 2024-09-29T22:10:00Z \
    --end-time 2024-09-29T22:15:00Z
```

Contenido de `file.json`:

```
[
    {
        "Id": "m3",
        "Expression": "(m1+m2)/300",
        "Label": "Avg Total IOPS"
    },
    {
```

```
        "Id": "m1",
        "MetricStat": {
            "Metric": {
                "Namespace": "AWS/EC2",
                "MetricName": "EBSReadOps",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "i-abcdef"
                    }
                ]
            },
            "Period": 300,
            "Stat": "Sum",
            "Unit": "Count"
        },
        "ReturnData": false
    },
    {
        "Id": "m2",
        "MetricStat": {
            "Metric": {
                "Namespace": "AWS/EC2",
                "MetricName": "EBSWriteOps",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "i-abcdef"
                    }
                ]
            },
            "Period": 300,
            "Stat": "Sum",
            "Unit": "Count"
        },
        "ReturnData": false
    }
]
```

Salida:

```
{
    "MetricDataResults": [
```

```
        {
            "Id": "m3",
            "Label": "Avg Total IOPS",
            "Timestamps": [
                "2024-09-29T22:10:00+00:00"
            ],
            "Values": [
                96.85
            ],
            "StatusCode": "Complete"
        }
    ],
    "Messages": []
}
```

Ejemplo 2: Supervisión de los cargos de AWS estimados mediante las métricas de facturación de CloudWatch

En el siguiente ejemplo de `get-metric-data`, se recupera la métrica `EstimatedCharges` de CloudWatch del espacio de nombres AWS/Billing.

```
aws cloudwatch get-metric-data \
    --metric-data-queries '[{"Id":"m1","MetricStat":{"Metric":
{"Namespace":"AWS/Billing","MetricName":"EstimatedCharges","Dimensions":
[{"Name":"Currency","Value":"USD"}]},"Period":21600,"Stat":"Maximum"}}]' \
    --start-time 2024-09-26T12:00:00Z \
    --end-time 2024-09-26T18:00:00Z \
    --region us-east-1
```

Salida:

```
{
    "MetricDataResults": [
        {
            "Id": "m1",
            "Label": "EstimatedCharges",
            "Timestamps": [
                "2024-09-26T12:00:00+00:00"
            ],
            "Values": [
                542.38
            ],
            "StatusCode": "Complete"
```

```
        }
    ],
    "Messages": []
}
```

Para obtener más información, consulte Uso de expresiones matemáticas con métricas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetMetricData en la Referencia de comandos de la AWS CLI.

`get-metric-statistics`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-metric-statistics`.

AWS CLI

Obtención de la utilización de la CPU por cada instancia de EC

En el siguiente ejemplo, se utiliza el comando `get-metric-statistics` para obtener la utilización de la CPU para una instancia de EC2 con el ID i-abcdef.

```
aws cloudwatch get-metric-statistics --metric-name CPUUtilization --start-
time 2014-04-08T23:18:00Z --end-time 2014-04-09T23:18:00Z --period 3600 --
namespace AWS/EC2 --statistics Maximum --dimensions Name=InstanceId,Value=i-abcdef
```

Salida:

```
{
    "Datapoints": [
        {
            "Timestamp": "2014-04-09T11:18:00Z",
            "Maximum": 44.79,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T20:18:00Z",
            "Maximum": 47.92,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T19:18:00Z",
            "Maximum": 50.85,
```

```
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T09:18:00Z",
            "Maximum": 47.92,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T03:18:00Z",
            "Maximum": 76.84,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T21:18:00Z",
            "Maximum": 48.96,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T14:18:00Z",
            "Maximum": 47.92,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T08:18:00Z",
            "Maximum": 47.92,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T16:18:00Z",
            "Maximum": 45.55,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T06:18:00Z",
            "Maximum": 47.92,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T13:18:00Z",
            "Maximum": 45.08,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T05:18:00Z",
```

```
            "Maximum": 47.92,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T18:18:00Z",
            "Maximum": 46.88,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T17:18:00Z",
            "Maximum": 52.08,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T07:18:00Z",
            "Maximum": 47.92,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T02:18:00Z",
            "Maximum": 51.23,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T12:18:00Z",
            "Maximum": 47.67,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-08T23:18:00Z",
            "Maximum": 46.88,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T10:18:00Z",
            "Maximum": 51.91,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T04:18:00Z",
            "Maximum": 47.13,
            "Unit": "Percent"
        },
        {
```

```
            "Timestamp": "2014-04-09T15:18:00Z",
            "Maximum": 48.96,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T00:18:00Z",
            "Maximum": 48.16,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2014-04-09T01:18:00Z",
            "Maximum": 49.18,
            "Unit": "Percent"
        }
    ],
    "Label": "CPUUtilization"
}
```

Especificación de varias dimensiones

En el siguiente ejemplo, se ilustra cómo especificar varias dimensiones. Cada dimensión se especifica mediante un par nombre/valor, con una coma entre el nombre y el valor. Cuando existen varias dimensiones se separan con un espacio. Si una métrica incluye varias dimensiones, debe especificar un valor para cada dimensión definida.

Para ver más ejemplos del uso del comando `get-metric-statistics`, consulte Obtener estadísticas para una métrica en la Guía para desarrolladores de Amazon CloudWatch.

```
aws cloudwatch get-metric-statistics --metric-name Buffers --namespace MyNameSpace
 --dimensions Name=InstanceID,Value=i-abcdef Name=InstanceType,Value=m1.small --
start-time 2016-10-15T04:00:00Z --end-time 2016-10-19T07:00:00Z --statistics Average
 --period 60
```

- Para obtener información sobre la API, consulte GetMetricStatistics en la Referencia de comandos de la AWS CLI.

`get-metric-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-metric-stream`.

AWS CLI

Recuperación de información sobre un flujo métrico

En el siguiente ejemplo de `get-metric-stream`, se muestra información acerca del flujo métrico denominado `QuickFull-GuaFbs` en la cuenta especificada.

```
aws cloudwatch get-metric-stream \
    --name QuickFull-GuaFbs
```

Salida:

```
{
    "Arn": "arn:aws:cloudwatch:us-east-1:123456789012:metric-stream/QuickFull-
GuaFbs",
    "Name": "QuickFull-GuaFbs",
    "FirehoseArn": "arn:aws:firehose:us-east-1:123456789012:deliverystream/
MetricStreams-QuickFull-GuaFbs-WnySbECG",
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/MetricStreams-
FirehosePutRecords-JN10W9B3",
    "State": "running",
    "CreationDate": "2024-10-11T18:48:59.187000+00:00",
    "LastUpdateDate": "2024-10-11T18:48:59.187000+00:00",
    "OutputFormat": "json",
    "IncludeLinkedAccountsMetrics": false
}
```

Para obtener más información, consulte Uso de flujos métricos en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetMetricStream en la Referencia de comandos de la AWS CLI.

`get-metric-widget-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-metric-widget-image`.

AWS CLI

Recuperación de un gráfico de instantáneas de CPUUtilization

En el siguiente ejemplo de `get-metric-widget-image`, se recupera un gráfico de instantáneas de la métrica `CPUUtilization` de la instancia de EC2 con el ID `i-abcde` y se guarda la imagen recuperada como archivo denominado “image.png” en la máquina local.

```
aws cloudwatch get-metric-widget-image \
    --metric-widget '{"metrics":[["AWS/EC2","CPUUtilization","InstanceId","i-abcde"]]}' \
    --output-format png \
    --output text | base64 --decode > image.png
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte GetMetricWidgetImage en la Referencia de comandos de la AWS CLI.

`list-dashboards`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-dashboards`.

AWS CLI

Recuperación de una lista de paneles

En el siguiente ejemplo de `list-dashboards`, se enumeran todos los paneles de la cuenta especificada.

```
aws cloudwatch list-dashboards
```

Salida:

```
{
    "DashboardEntries": [
        {
            "DashboardName": "Dashboard-A",
            "DashboardArn": "arn:aws:cloudwatch::123456789012:dashboard/Dashboard-A",
            "LastModified": "2024-10-11T18:40:11+00:00",
            "Size": 271
        },
        {
            "DashboardName": "Dashboard-B",
```

```
            "DashboardArn": "arn:aws:cloudwatch::123456789012:dashboard/Dashboard-
B",
            "LastModified": "2024-10-11T18:44:41+00:00",
            "Size": 522
        }
    ]
}
```

Para obtener más información, consulte Paneles de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener detalles sobre la API, consulte ListDashboards en la Referencia de comandos de la AWS CLI.

`list-metric-streams`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-metric-streams`.

AWS CLI

Recuperación de una lista de flujos métricos

En el siguiente ejemplo de `list-metric-streams`, se muestran todos los flujos métricos de la cuenta especificada.

```
aws cloudwatch list-metric-streams
```

Salida:

```
{
    "Entries": [
        {
            "Arn": "arn:aws:cloudwatch:us-east-1:123456789012:metric-stream/
QuickFull-GuaFbs",
            "CreationDate": "2024-10-11T18:48:59.187000+00:00",
            "LastUpdateDate": "2024-10-11T18:48:59.187000+00:00",
            "Name": "QuickFull-GuaFbs",
            "FirehoseArn": "arn:aws:firehose:us-east-1:123456789012:deliverystream/
MetricStreams-QuickFull-GuaFbs-WnySbECG",
            "State": "running",
            "OutputFormat": "json"
        }
    ]
```

```
}
```

Para obtener más información, consulte Uso de flujos métricos en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListMetricStreams en la Referencia de comandos de la AWS CLI.

`list-metrics`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-metrics`.

AWS CLI

Creación de una lista de las métricas de Amazon SNS

En el siguiente ejemplo de `list-metrics`, se muestran las métricas de Amazon SNS.

```
aws cloudwatch list-metrics \
    --namespace "AWS/SNS"
```

Salida:

```
{
    "Metrics": [
        {
            "Namespace": "AWS/SNS",
            "Dimensions": [
                {
                    "Name": "TopicName",
                    "Value": "NotifyMe"
                }
            ],
            "MetricName": "PublishSize"
        },
        {
            "Namespace": "AWS/SNS",
            "Dimensions": [
                {
                    "Name": "TopicName",
                    "Value": "CFO"
                }
            ],
```

```
            "MetricName": "PublishSize"
        },
        {
            "Namespace": "AWS/SNS",
            "Dimensions": [
                {
                    "Name": "TopicName",
                    "Value": "NotifyMe"
                }
            ],
            "MetricName": "NumberOfNotificationsFailed"
        },
        {
            "Namespace": "AWS/SNS",
            "Dimensions": [
                {
                    "Name": "TopicName",
                    "Value": "NotifyMe"
                }
            ],
            "MetricName": "NumberOfNotificationsDelivered"
        },
        {
            "Namespace": "AWS/SNS",
            "Dimensions": [
                {
                    "Name": "TopicName",
                    "Value": "NotifyMe"
                }
            ],
            "MetricName": "NumberOfMessagesPublished"
        },
        {
            "Namespace": "AWS/SNS",
            "Dimensions": [
                {
                    "Name": "TopicName",
                    "Value": "CFO"
                }
            ],
            "MetricName": "NumberOfMessagesPublished"
        },
        {
            "Namespace": "AWS/SNS",
```

```
            "Dimensions": [
                {
                    "Name": "TopicName",
                    "Value": "CFO"
                }
            ],
            "MetricName": "NumberOfNotificationsDelivered"
        },
        {
            "Namespace": "AWS/SNS",
            "Dimensions": [
                {
                    "Name": "TopicName",
                    "Value": "CFO"
                }
            ],
            "MetricName": "NumberOfNotificationsFailed"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListMetrics en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Muestra de las etiquetas asociadas a una alarma existente*

En el siguiente ejemplo de `list-tags-for-resource`, se muestran todas las etiquetas asociadas a una alarma denominada demo en la cuenta especificada.

```
aws cloudwatch list-tags-for-resource \
    --resource-arn arn:aws:cloudwatch:us-east-1:123456789012:alarm:demo
```

Salida:

```
{
```

```
    "Tags": [
        {
            "Key": "stack",
            "Value": "Production"
        },
        {
            "Key": "team",
            "Value": "Devops"
        }
    ]
}
```

Para obtener más información, consulte Alarmas y etiquetado en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-anomaly-detector`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-anomaly-detector`.

AWS CLI

Creación de un modelo de detección de anomalías

En el siguiente ejemplo de `put-anomaly-detector`, se crea un modelo de detección de anomalías para una métrica de CloudWatch.

```
aws cloudwatch put-anomaly-detector \
    --namespace AWS/Logs \
    --metric-name IncomingBytes \
    --stat SampleCount
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de detección de anomalías de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte PutAnomalyDetector en la Referencia de comandos de la AWS CLI.

`put-composite-alarm`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-composite-alarm`.

AWS CLI

Creación de una alarma compuesta de CloudWatch

En el siguiente ejemplo de `put-composite-alarm`, se crea una alarma compuesta denominada `ProdAlarm` en la cuenta especificada.

```
aws cloudwatch put-composite-alarm \
    --alarm-name ProdAlarm \
    --alarm-rule "ALARM(CPUUtilizationTooHigh) AND ALARM(MemUsageTooHigh)" \
    --alarm-actions arn:aws:sns:us-east-1:123456789012:demo \
    --actions-enabled
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación de una alarma compuesta en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte PutCompositeAlarm en la Referencia de comandos de la AWS CLI.

`put-dashboard`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-dashboard`.

AWS CLI

Para crear un panel

En el siguiente ejemplo de `put-dashboard`, se crea un panel denominado `Dashboard-A` en la cuenta especificada.

```
aws cloudwatch put-dashboard \
    --dashboard-name Dashboard-A \
    --dashboard-body '{"widgets":
[{"height":6,"width":6,"y":0,"x":0,"type":"metric","properties":
{"view":"timeSeries","stacked":false,"metrics":
```

```
[["Namespace","CPUUtilization","Environment","Prod","Type","App"]],"region":"us-east-1"}}]}'
```

Salida:

```
{
    "DashboardValidationMessages": []
}
```

Para obtener más información, consulte Creación de un panel de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información acerca de la API, consulte PutDashboard en la Referencia de comandos de la AWS CLI.

`put-insight-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-insight-rule`.

AWS CLI

Creación de una regla de Información de colaboradores

En el siguiente ejemplo de `put-insight-rule`, se crea una regla de Información de colaboradores denominada `VPCFlowLogsContributorInsights` en la cuenta especificada.

```
aws cloudwatch put-insight-rule \
    --rule-name VPCFlowLogsContributorInsights \
    --rule-definition file://insight-rule.json \
    --rule-state ENABLED
```

Contenido de `insight-rule.json`:

```
{
    "Schema": {
        "Name": "CloudWatchLogRule",
        "Version": 1
    },
    "AggregateOn": "Count",
    "Contribution": {
        "Filters": [],
        "Keys": [
```

```
            "tcp-flag"
        ]
    },
    "LogFormat": "CLF",
    "LogGroupNames": [
        "/vpc/flowlogs/*"
    ],
    "Fields": {
        "23": "tcp-flag"
    }
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación de una regla de Información de colaboradores en CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información acerca de la API, consulte PutInsightRule en la Referencia de comandos de la AWS CLI.

`put-metric-alarm`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-metric-alarm`.

AWS CLI

Envío de un mensaje por correo electrónico de Amazon Simple Notification Service cuando el uso de la CPU supere el 70 por ciento

El siguiente ejemplo usa el comando `put-metric-alarm` para enviar un mensaje por correo electrónico de Amazon Simple Notification Service cuando el uso de la CPU supere el 70 por ciento:

```
aws cloudwatch put-metric-alarm --alarm-name cpu-mon --alarm-description "Alarm
 when CPU exceeds 70 percent" --metric-name CPUUtilization --namespace AWS/
EC2 --statistic Average --period 300 --threshold 70 --comparison-
operator GreaterThanThreshold  --dimensions "Name=InstanceId,Value=i-12345678" --
evaluation-periods 2 --alarm-actions arn:aws:sns:us-east-1:111122223333:MyTopic --
unit Percent
```

Este comando vuelve a la petición si se ejecuta correctamente. Si existe una alarma con el mismo nombre, la alarma nueva la sobrescribirá.

Especificación de varias dimensiones

En el siguiente ejemplo, se ilustra cómo especificar varias dimensiones. Cada dimensión se especifica mediante un par nombre/valor, con una coma entre el nombre y el valor. Cuando existen varias dimensiones se separan con un espacio:

```
aws cloudwatch put-metric-alarm --alarm-name "Default_Test_Alarm3" --alarm-
description "The default example alarm" --namespace "CW EXAMPLE METRICS"
 --metric-name Default_Test --statistic Average --period 60 --evaluation-
periods 3 --threshold 50 --comparison-operator GreaterThanOrEqualToThreshold --
dimensions Name=key1,Value=value1 Name=key2,Value=value2
```

- Para obtener información sobre la API, consulte PutMetricAlarm en la Referencia de comandos de la AWS CLI.

`put-metric-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-metric-data`.

AWS CLI

Publicación de métricas personalizadas en Amazon CloudWatch

En el siguiente ejemplo, se utiliza el comando `put-metric-data` para publicar una métrica personalizada en Amazon CloudWatch:

```
aws cloudwatch put-metric-data --namespace "Usage Metrics" --metric-data file://
metric.json
```

Los valores de la métrica en sí se almacenan en el archivo JSON, `metric.json`.

A continuación, se muestra el contenido de ese archivo:

```
[
  {
    "MetricName": "New Posts",
    "Timestamp": "Wednesday, June 12, 2013 8:28:20 PM",
    "Value": 0.50,
    "Unit": "Count"
  }
]
```

Para obtener más información, consulte Publicación de métricas personalizadas en la Guía para desarrolladores de Amazon CloudWatch.

Cómo especificar varias dimensiones

En el siguiente ejemplo, se ilustra cómo especificar varias dimensiones. Cada dimensión se especifica con un par Nombre=Valor. Cuando existen varias dimensiones se separan con una coma:

```
aws cloudwatch put-metric-data --metric-name Buffers --
namespace MyNameSpace --unit Bytes --value 231434333 --
dimensions InstanceID=1-23456789,InstanceType=m1.small
```

- Para obtener información sobre la API, consulte PutMetricData en la Referencia de comandos de la AWS CLI.

`put-metric-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-metric-stream`.

AWS CLI

Creación de un flujo métrico

En el siguiente ejemplo de `put-metric-stream`, se crea un flujo métrico denominado `QuickFull-GuaFb` en la cuenta especificada.

```
aws cloudwatch put-metric-stream \
    --name QuickFull-GuaFbs \
    --firehose-arn arn:aws:firehose:us-east-1:123456789012:deliverystream/
MetricStreams-QuickFull-GuaFbs-WnySbECG \
    --role-arn arn:aws:iam::123456789012:role/service-role/MetricStreams-
FirehosePutRecords-JN10W9B3 \
    --output-format json \
    --no-include-linked-accounts-metrics
```

Salida:

```
{
    "Arn": "arn:aws:cloudwatch:us-east-1:123456789012:metric-stream/QuickFull-
GuaFbs"
```

```
}
```

Para obtener más información, consulte Configuración de un flujo métrico en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte PutMetricStream en la Referencia de comandos de la AWS CLI.

`set-alarm-state`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-alarm-state`.

AWS CLI

Cambio temporal del estado de una alarma

En el siguiente ejemplo, se utiliza el comando `set-alarm-state` para cambiar temporalmente el estado de una alarma de Amazon CloudWatch denominada mialarma y configurarla con el estado ALARMA para realizar pruebas:

```
aws cloudwatch set-alarm-state --alarm-name "myalarm" --state-value ALARM --state-
reason "testing purposes"
```

Este comando vuelve a la petición si se ejecuta correctamente.

- Para obtener información sobre la API, consulte SetAlarmState en la Referencia de comandos de la AWS CLI.

`start-metric-streams`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-metric-streams`.

AWS CLI

Inicio de un flujo métrico específico

En el siguiente ejemplo de `start-metric-streams`, se inicia el flujo métrico denominado `QuickFull-GuaFbs` en la cuenta especificada.

```
aws cloudwatch start-metric-streams \
    --names QuickFull-GuaFbs
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de flujos métricos en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte StartMetricStreams en la Referencia de comandos de la AWS CLI.

`stop-metric-streams`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-metric-streams`.

AWS CLI

Detención de un flujo métrico específico

En el siguiente ejemplo de `stop-metric-streams`, se detiene el flujo métrico denominado `QuickFull-GuaFbs` en la cuenta especificada.

```
aws cloudwatch stop-metric-streams \
    --names QuickFull-GuaFbs
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de flujos métricos en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte StopMetricStreams en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Agregación de una o varias etiquetas a un recurso especificado

En el siguiente ejemplo de `tag-resource`, se agregan 2 etiquetas a la alarma de Cloudwatch denominada `demo` en la cuenta especificada.

```
aws cloudwatch tag-resource \
    --resource-arn arn:aws:cloudwatch:us-east-1:123456789012:alarm:demo \
```

```
    --tags Key=stack,Value=Production Key=team,Value=Devops
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de los recursos de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de una o varias etiquetas del recurso especificado

En el siguiente ejemplo de `untag-resource`, se eliminan 2 etiquetas de la alarma de Cloudwatch denominada `demo` en la cuenta especificada.

```
aws cloudwatch untag-resource \
    --resource-arn arn:aws:cloudwatch:us-east-1:123456789012:alarm:demo \
    --tag-keys stack team
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de los recursos de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

Ejemplos de registros de CloudWatch que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con registros de CloudWatch.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-log-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-log-group`.

AWS CLI

El siguiente comando crea un grupo de registro denominado `my-logs`:

```
aws logs create-log-group --log-group-name my-logs
```

- Para obtener información sobre la API, consulte CreateLogGroup en la Referencia de comandos de la AWS CLI.

`create-log-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-log-stream`.

AWS CLI

El siguiente comando crea un flujo de registro denominado `20150601` en el grupo de registro `my-logs`:

```
aws logs create-log-stream --log-group-name my-logs --log-stream-name 20150601
```

- Para obtener información sobre la API, consulte CreateLogStream en la Referencia de comandos de la AWS CLI.

`delete-log-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-log-group`.

AWS CLI

El siguiente comando elimina un grupo de registro denominado `my-logs`:

```
aws logs delete-log-group --log-group-name my-logs
```

- Para obtener información sobre la API, consulte DeleteLogGroup en la Referencia de comandos de la AWS CLI.

`delete-log-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-log-stream`.

AWS CLI

El siguiente comando elimina un flujo de registro denominado `20150531` de un grupo de registro denominado `my-logs`:

```
aws logs delete-log-stream --log-group-name my-logs --log-stream-name 20150531
```

- Para obtener información sobre la API, consulte DeleteLogStream en la Referencia de comandos de la AWS CLI.

`delete-retention-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-retention-policy`.

AWS CLI

El siguiente comando elimina la política de retención que se aplicó anteriormente a un grupo de registro denominado `my-logs`:

```
aws logs delete-retention-policy --log-group-name my-logs
```

- Para obtener información sobre la API, consulte DeleteRetentionPolicy en la Referencia de comandos de la AWS CLI.

`describe-log-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-log-groups`.

AWS CLI

El siguiente comando describe un grupo de registro denominado `my-logs`:

```
aws logs describe-log-groups --log-group-name-prefix my-logs
```

Salida:

```
{
    "logGroups": [
        {
            "storedBytes": 0,
            "metricFilterCount": 0,
            "creationTime": 1433189500783,
            "logGroupName": "my-logs",
            "retentionInDays": 5,
            "arn": "arn:aws:logs:us-west-2:0123456789012:log-group:my-logs:*"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeLogGroups en la Referencia de comandos de la AWS CLI.

`describe-log-streams`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-log-streams`.

AWS CLI

El siguiente comando muestra todos los flujos de registro que comienzan con el prefijo `2015` del grupo de registro `my-logs`:

```
aws logs describe-log-streams --log-group-name my-logs --log-stream-name-prefix 2015
```

Salida:

```
{
    "logStreams": [
        {
            "creationTime": 1433189871774,
```

```
            "arn": "arn:aws:logs:us-west-2:0123456789012:log-group:my-logs:log-
stream:20150531",
            "logStreamName": "20150531",
            "storedBytes": 0
        },
        {
            "creationTime": 1433189873898,
            "arn": "arn:aws:logs:us-west-2:0123456789012:log-group:my-logs:log-
stream:20150601",
            "logStreamName": "20150601",
            "storedBytes": 0
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeLogStreams en la Referencia de comandos de la AWS CLI.

`get-log-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-log-events`.

AWS CLI

El siguiente comando recupera eventos de registro de un flujo de registro denominado `20150601` en el grupo de registro `my-logs`:

```
aws logs get-log-events --log-group-name my-logs --log-stream-name 20150601
```

Salida:

```
{
    "nextForwardToken":
 "f/31961209122447488583055879464742346735121166569214640130",
    "events": [
        {
            "ingestionTime": 1433190494190,
            "timestamp": 1433190184356,
            "message": "Example Event 1"
        },
        {
            "ingestionTime": 1433190516679,
```

```
            "timestamp": 1433190184356,
            "message": "Example Event 1"
        },
        {
            "ingestionTime": 1433190494190,
            "timestamp": 1433190184358,
            "message": "Example Event 2"
        }
    ],
    "nextBackwardToken":
 "b/31961209122358285602261756944988674324553373268216709120"
}
```

- Para obtener información sobre la API, consulte GetLogEvents en la Referencia de comandos de la AWS CLI.

`put-log-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-log-events`.

AWS CLI

El siguiente comando incluye eventos de registro en un flujo de registro denominado `20150601` en el grupo de registro `my-logs`:

```
aws logs put-log-events --log-group-name my-logs --log-stream-name 20150601 --log-
events file://events
```

Salida:

```
{
    "nextSequenceToken": "49542672486831074009579604567656788214806863282469607346"
}
```

En el ejemplo anterior, se lee una matriz JSON de eventos de un archivo denominado `events` en el directorio actual:

```
[
  {
    "timestamp": 1433190184356,
    "message": "Example Event 1"
```

```
  },
  {
    "timestamp": 1433190184358,
    "message": "Example Event 2"
  },
  {
    "timestamp": 1433190184360,
    "message": "Example Event 3"
  }
]
```

Cada llamada posterior requiere que el siguiente token de secuencia, proporcionado por la llamada anterior, se especifique con la opción de token de secuencia:

```
aws logs put-log-events --log-group-name my-logs --log-
stream-name 20150601 --log-events file://events2 --sequence-
token "49542672486831074009579604567656788214806863282469607346"
```

Salida:

```
{
    "nextSequenceToken": "49542672486831074009579604567900991230369019956308219826"
}
```

- Para obtener información acerca de la API, consulte PutLogEvents en la Referencia de comandos de la AWS CLI.

`put-retention-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-retention-policy`.

AWS CLI

El siguiente comando agrega una política de retención de 5 días a un grupo de registro denominado `my-logs`:

```
aws logs put-retention-policy --log-group-name my-logs --retention-in-days 5
```

- Para obtener información sobre la API, consulte PutRetentionPolicy en la Referencia de comandos de la AWS CLI.

Ejemplos de Monitor de red de CloudWatch que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios comunes mediante la AWS Command Line Interface con Monitor de red de CloudWatch.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-monitor`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-monitor`.

AWS CLI

Ejemplo 1: crear un monitor de red con un período de agregación

En el siguiente ejemplo de `create-monitor` se crea un monitor llamado `Example_NetworkMonitor` con `aggregationPeriod` establecido en `30` segundos. El `state` inicial del monitor será `INACTIVE` porque no tiene sondas asociadas. El estado cambia a `ACTIVE` solo cuando se agregan sondas. Puede utilizar los comandos update-monitor o create-probe para añadir sondas a este monitor.

```
aws networkmonitor create-monitor \
     --monitor-name Example_NetworkMonitor \
     --aggregation-period 30
```

Salida:

```
{
    "monitorArn": "arn:aws:networkmonitor:region:111122223333:monitor/
Example_NetworkMonitor",
```

```
    "monitorName": "Example_NetworkMonitor",
    "state": "INACTIVE",
    "aggregationPeriod": 30,
    "tags": {}
}
```

Para obtener más información, consulte Funcionamiento de Amazon CloudWatch Network Monitor en la Guía del usuario de Amazon CloudWatch.

Ejemplo 2: crear un monitor de red con una sonda utilizando TCP y que también incluya etiquetas

El siguiente ejemplo de `create-monitor` crea un monitor llamado `Example_NetworkMonitor`. El comando también crea una sonda que usa el protocolo `ICMP` e incluye etiquetas. Dado que no se pasa `aggregationPeriod` en la solicitud, se establece `60` segundos como valor predeterminado. El `state` del monitor con la sonda será `PENDING` hasta que el monitor sea `ACTIVE`. Esto puede tardar varios minutos, momento en el cual `state` cambiará a `ACTIVE` y ya podrá empezar a ver métricas de CloudWatch.

```
aws networkmonitor create-monitor \
    --monitor-name Example_NetworkMonitor \
    --probes sourceArn=arn:aws:ec2:region:111122223333:subnet/subnet-
id,destination=10.0.0.100,destinationPort=80,protocol=TCP,packetSize=56,probeTags={Name=Prob
 \
    --tags Monitor=Monitor1
```

Salida:

```
{
    "monitorArn": "arn:aws:networkmonitor:region111122223333:monitor/
Example_NetworkMonitor",
    "monitorName": "Example_NetworkMonitor",
    "state": "PENDING",
    "aggregationPeriod": 60,
    "tags": {
        "Monitor": "Monitor1"
    }
}
```

Para obtener más información, consulte Funcionamiento de Amazon CloudWatch Network Monitor en la Guía del usuario de Amazon CloudWatch.

Ejemplo 3: crear un monitor de red con una sonda utilizando ICMP y que también incluya etiquetas

En el siguiente ejemplo de `create-monitor` se crea un monitor llamado `Example_NetworkMonitor` con un `aggregationPeriod` de `30` segundos. El comando también crea una sonda que usa el protocolo `ICMP` e incluye etiquetas. Dado que no se pasa `aggregationPeriod` en la solicitud, se establece `60` segundos como valor predeterminado. El `state` del monitor con la sonda será `PENDING` hasta que el monitor sea `ACTIVE`. Esto puede tardar varios minutos, momento en el cual `state` cambiará a `ACTIVE` y ya podrá empezar a ver métricas de CloudWatch.

```
aws networkmonitor create-monitor \
     --monitor-name Example_NetworkMonitor \
     --aggregation-period 30 \
     --probes sourceArn=arn:aws:ec2:region111122223333:subnet/subnet-
id,destination=10.0.0.100,protocol=ICMP,packetSize=56,probeTags={Name=Probe1} \
     --tags Monitor=Monitor1
```

Salida:

```
{
    "monitorArn": "arn:aws:networkmonitor:region:111122223333:monitor/
Example_NetworkMonitor",
    "monitorName": "Example_NetworkMonitor",
    "state": "PENDING",
    "aggregationPeriod": 30,
    "tags": {
        "Monitor": "Monitor1"
    }
}
```

Para obtener más información, consulte Funcionamiento de Amazon CloudWatch Network Monitor en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte CreateMonitor en la Referencia de comandos de la AWS CLI.

`create-probe`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-probe`.

AWS CLI

Ejemplo 1: crear una sonda que utilice TCP y añadirla a un monitor de red

En el siguiente ejemplo de `create-probe` se crea una sonda que utiliza el `protocol` `TCP` y añade la sonda a un monitor llamado `Example_NetworkMonitor`. Una vez creado, el `state` del monitor con la sonda será `PENDING` hasta que el monitor sea `ACTIVE`. Esto puede tardar varios minutos, momento en el cual el estado cambiará a `ACTIVE` y ya podrá empezar a ver métricas de CloudWatch.

```
aws networkmonitor create-probe \
    --monitor-name Example_NetworkMonitor \
    --probe sourceArn=arn:aws:ec2:region:111122223333:subnet/subnet-
id,destination=10.0.0.100,destinationPort=80,protocol=TCP,packetSize=56,tags={Name=Probe1}
```

Salida:

```
{
    "probeId": "probe-12345",
    "probeArn": "arn:aws:networkmonitor:region:111122223333:probe/probe-12345",
    "destination": "10.0.0.100",
    "destinationPort": 80,
    "packetSize": 56,
    "addressFamily": "IPV4",
    "vpcId": "vpc-12345",
    "state": "PENDING",
    "createdAt": "2024-03-29T12:41:57.314000-04:00",
    "modifiedAt": "2024-03-29T12:41:57.314000-04:00",
    "tags": {
        "Name": "Probe1"
    }
}
```

Ejemplo 2: crear una sonda que utilice sondeo con ICMP y añadirla a un monitor de red

En el siguiente ejemplo de `create-probe` se crea una sonda que utiliza el `protocol` `ICMP` y añade la sonda a un monitor llamado `Example_NetworkMonitor`. Una vez creado, el `state` del monitor con la sonda será `PENDING` hasta que el monitor sea `ACTIVE`. Esto puede tardar varios minutos, momento en el cual el estado cambiará a `ACTIVE` y ya podrá empezar a ver métricas de CloudWatch.

```
aws networkmonitor create-probe \
    --monitor-name Example_NetworkMonitor \
    --probe sourceArn=arn:aws:ec2:region:012345678910:subnet/subnet-
id,destination=10.0.0.100,protocol=ICMP,packetSize=56,tags={Name=Probe1}
```

Salida:

```
{
    "probeId": "probe-12345",
    "probeArn": "arn:aws:networkmonitor:region:111122223333:probe/probe-12345",
    "destination": "10.0.0.100",
    "packetSize": 56,
    "addressFamily": "IPV4",
    "vpcId": "vpc-12345",
    "state": "PENDING",
    "createdAt": "2024-03-29T12:44:02.452000-04:00",
    "modifiedAt": "2024-03-29T12:44:02.452000-04:00",
    "tags": {
        "Name": "Probe1"
    }
}
```

Para obtener más información, consulte Funcionamiento de Amazon CloudWatch Network Monitor en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte CreateProbe en la Referencia de comandos de la AWS CLI.

`delete-monitor`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-monitor`.

AWS CLI

Para eliminar un monitor

En el siguiente ejemplo de `delete-monitor` se elimina un monitor llamado `Example_NetworkMonitor`.

```
aws networkmonitor delete-monitor \
    --monitor-name Example_NetworkMonitor
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Funcionamiento de Amazon CloudWatch Network Monitor en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DeleteMonitor en la Referencia de comandos de AWS CLI.

`delete-probe`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-probe`.

AWS CLI

Para eliminar una sonda

En el siguiente ejemplo de `delete-probe` se elimina una sonda con el ID `probe-12345` de un monitor de red llamado `Example_NetworkMonitor`.

```
aws networkmonitor delete-probe \
    --monitor-name Example_NetworkMonitor \
    --probe-id probe-12345
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Funcionamiento de Amazon CloudWatch Network Monitor en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DeleteProbe en la Referencia de comandos de la AWS CLI.

`get-monitor`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-monitor`.

AWS CLI

Para obtener información del monitor

En el siguiente ejemplo de `get-monitor` se obtiene información sobre un monitor llamado `Example_NetworkMonitor`.

```
aws networkmonitor get-monitor \
    --monitor-name Example_NetworkMonitor
```

Salida:

```
{
    "monitorArn": "arn:aws:networkmonitor:region:012345678910:monitor/
Example_NetworkMonitor",
    "monitorName": "Example_NetworkMonitor",
    "state": "ACTIVE",
    "aggregationPeriod": 60,
    "tags": {},
    "probes": [],
    "createdAt": "2024-04-01T17:58:07.211000-04:00",
    "modifiedAt": "2024-04-01T17:58:07.211000-04:00"
}
```

Para obtener más información, consulte Funcionamiento de Amazon CloudWatch Network Monitor en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetMonitor en la Referencia de comandos de la AWS CLI.

`get-probe`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-probe`.

AWS CLI

Para ver los detalles de sondas

En el siguiente ejemplo de `get-probe` se devuelven detalles sobre una sonda con el `probeID` `probe-12345` que está asociado a un monitor llamado `Example_NetworkMonitor`.

```
aws networkmonitor get-probe \
    --monitor-name Example_NetworkMonitor \
    --probe-id probe-12345
```

Salida:

```
{
```

```
    "probeId": "probe-12345",
    "probeArn": "arn:aws:networkmonitor:region:012345678910:probe/probe-12345",
    "sourceArn": "arn:aws:ec2:region:012345678910:subnet/subnet-12345",
    "destination": "10.0.0.100",
    "destinationPort": 80,
    "protocol": "TCP",
    "packetSize": 56,
    "addressFamily": "IPV4",
    "vpcId": "vpc-12345",
    "state": "ACTIVE",
    "createdAt": "2024-03-29T12:41:57.314000-04:00",
    "modifiedAt": "2024-03-29T12:42:28.610000-04:00",
    "tags": {
        "Name": "Probe1"
    }
}
```

Para obtener más información, consulte Funcionamiento de Amazon CloudWatch Network Monitor en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetProbe en la Referencia de comandos de la AWS CLI.

`list-monitors`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-monitors`.

AWS CLI

Ejemplo 1: enumerar todos los monitores (solo único)

En el siguiente ejemplo de `list-monitors` se devuelve una lista de un solo monitor. El `state` del monitor es `ACTIVE` y tiene un `aggregationPeriod` de 60 segundos.

```
aws networkmonitor list-monitors
```

Salida:

```
{
    "monitors": [{
            "monitorArn": "arn:aws:networkmonitor:region:012345678910:monitor/
Example_NetworkMonitor",
```

```
            "monitorName": "Example_NetworkMonitor",
            "state": "ACTIVE",
            "aggregationPeriod": 60,
            "tags": {
                "Monitor": "Monitor1"
            }
        }
    ]
}
```

Para obtener más información, consulte Funcionamiento de Amazon CloudWatch Network Monitor en la Guía del usuario de Amazon CloudWatch.

Ejemplo 2: enumerar todos los monitores (varios monitores)

En el siguiente ejemplo de `list-monitors` se devuelve una lista de tres monitores. El `state` de un monitor es `ACTIVE` y genera métricas de CloudWatch. Los estados de los otros dos monitores son `INACTIVE` y no generan métricas de CloudWatch. Los tres monitores utilizan un `aggregationPeriod` de 60 segundos.

```
aws networkmonitor list-monitors
```

Salida:

```
{
    "monitors": [
        {
            "monitorArn": "arn:aws:networkmonitor:us-east-1:111122223333:monitor/
Example_NetworkMonitor",
            "monitorName": "Example_NetworkMonitor",
            "state": "INACTIVE",
            "aggregationPeriod": 60,
            "tags": {}
        },
        {
            "monitorArn": "arn:aws:networkmonitor:us-east-1:111122223333:monitor/
Example_NetworkMonitor2",
            "monitorName": "Example_NetworkMonitor2",
            "state": "ACTIVE",
            "aggregationPeriod": 60,
            "tags": {
                "Monitor": "Monitor1"
```

```
            }
        },
        {
            "monitorArn": "arn:aws:networkmonitor:us-east-1:111122223333:monitor/
TestNetworkMonitor_CLI",
            "monitorName": "TestNetworkMonitor_CLI",
            "state": "INACTIVE",
            "aggregationPeriod": 60,
            "tags": {}
        }
    ]
}
```

Para obtener más información, consulte Funcionamiento de Amazon CloudWatch Network Monitor en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListMonitors en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un recurso

En el siguiente ejemplo de `list-tags-for-resource` se devuelve una lista de las etiquetas de un monitor llamado `Example_NetworkMonitor`.

```
aws networkmonitor list-tags-for-resource \
    --resource-arn arn:aws:networkmonitor:region:012345678910:monitor/
Example_NetworkMonitor
```

Salida:

```
{
    "tags": {
        "Environment": "Dev",
        "Application": "PetStore"
    }
}
```

Para obtener más información, consulte Funcionamiento de Amazon CloudWatch Network Monitor en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para etiquetar un recurso

En el siguiente ejemplo de `tag-resource` se etiqueta un monitor llamado `Example_NetworkMonitor` con etiquetas `Environment=Dev` y `Application=PetStore`.

```
aws networkmonitor tag-resource \
    --resource-arn arn:aws:networkmonitor:region:012345678910:monitor/
Example_NetworkMonitor \
    --tags Environment=Dev,Application=PetStore
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Funcionamiento de Amazon CloudWatch Network Monitor en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para retirar la etiqueta de un recurso

En el siguiente ejemplo de `untag-resource` se elimina un parámetro `tag-keys` con el par clave-valor de `Environment Application` de su asociación con un monitor llamado `Example_NetworkMonitor`.

```
aws networkmonitor untag-resource \
    --resource-arn arn:aws:networkmonitor:region:012345678910:monitor/
Example_NetworkMonitor \
    --tag-keys Environment Application
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Funcionamiento de Amazon CloudWatch Network Monitor en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-monitor

En el siguiente ejemplo de código, se muestra cómo utilizar `update-monitor`.

AWS CLI

Para actualizar un monitor

En el siguiente ejemplo de `update-monitor` se cambia el `aggregationPeriod` de un monitor de `60` segundos a `30` segundos.

```
aws networkmonitor update-monitor \
    --monitor-name Example_NetworkMonitor \
    --aggregation-period 30
```

Salida:

```
{
    "monitorArn": "arn:aws:networkmonitor:region:012345678910:monitor/
Example_NetworkMonitor",
    "monitorName": "Example_NetworkMonitor",
    "state": "PENDING",
    "aggregationPeriod": 30,
    "tags": {
        "Monitor": "Monitor1"
    }
}
```

Para obtener más información, consulte Funcionamiento de Amazon CloudWatch Network Monitor en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte UpdateMonitor en la Referencia de comandos de la AWS CLI.

`update-probe`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-probe`.

AWS CLI

Para actualizar una sonda

En el siguiente ejemplo de `update-probe` se actualiza la dirección IP de `destination` original de una sonda y también se actualiza el `packetSize` a `60`.

```
aws networkmonitor update-probe \
    --monitor-name Example_NetworkMonitor \
    --probe-id probe-12345 \
    --destination 10.0.0.150 \
    --packet-size 60
```

Salida:

```
{
    "probeId": "probe-12345",
    "probeArn": "arn:aws:networkmonitor:region:012345678910:probe/probe-12345",
    "sourceArn": "arn:aws:ec2:region:012345678910:subnet/subnet-12345",
    "destination": "10.0.0.150",
    "destinationPort": 80,
    "protocol": "TCP",
    "packetSize": 60,
    "addressFamily": "IPV4",
    "vpcId": "vpc-12345",
    "state": "PENDING",
    "createdAt": "2024-03-29T12:41:57.314000-04:00",
    "modifiedAt": "2024-03-29T13:52:23.115000-04:00",
    "tags": {
        "Name": "Probe1"
    }
}
```

Para obtener más información, consulte Funcionamiento de Amazon CloudWatch Network Monitor en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte UpdateProbe en la Referencia de comandos de la AWS CLI.

Ejemplos de CloudWatch Observability Access Monitor que utilizan AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios comunes mediante la AWS Command Line Interface con CloudWatch Observability Access Monitor.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-link`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-link`.

AWS CLI

Para crear un enlace

En el siguiente ejemplo de `create-link`, se crea un enlace entre una cuenta de origen y un receptor que ha creado en una cuenta de supervisión.

```
aws oam create-link \
    --label-template sourceAccount \
    --resource-types AWS::CloudWatch::Metric \
    --sink-identifier arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-example12345
```

Salida:

```
{
    "Arn": "arn:aws:oam:us-east-2:123456789111:link/a1b2c3d4-5678-90ab-cdef-
example11111",
    "Id": "a1b2c3d4-5678-90ab-cdef-example11111",
    "Label": "sourceAccount",
    "LabelTemplate": "sourceAccount",
    "ResourceTypes": [
        "AWS::CloudWatch::Metric"
    ],
    "SinkArn": "arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-
example12345",
    "Tags": {}
}
```

Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte CreateLink en la Referencia de comandos de la AWS CLI.

`create-sink`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-sink`.

AWS CLI

Creación de un receptor

En el siguiente ejemplo de `create-sink`, se crea un receptor en la cuenta actual para que pueda utilizarse como cuenta de supervisión en la observabilidad entre cuentas de CloudWatch.

```
aws oam create-sink \
    --name DemoSink
```

Salida:

```
{
    "Arn": "arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-
example12345",
```

```
    "Id": "a1b2c3d4-5678-90ab-cdef-example12345",
    "Name": "DemoSink",
    "Tags": {}
}
```

Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte CreateSink en la Referencia de comandos de la AWS CLI.

`delete-link`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-link`.

AWS CLI

Para eliminar un enlace

En el siguiente ejemplo de `delete-link`, se elimina un enlace entre un receptor de cuenta de supervisión y una cuenta de origen.

```
aws oam delete-link \
    --identifier arn:aws:oam:us-east-2:123456789111:link/a1b2c3d4-5678-90ab-cdef-example11111
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DeleteLink en la Referencia de comandos de la AWS CLI.

`delete-sink`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-sink`.

AWS CLI

Eliminación de un receptor

En el siguiente ejemplo de `delete-sink`, se elimina un receptor. Debe eliminar todos los enlaces a un receptor para poder eliminar ese receptor.

```
aws oam delete-sink \
    --identifier arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-example12345
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DeleteSink en la Referencia de comandos de la AWS CLI.

`get-link`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-link`.

AWS CLI

Devolución de la información completa sobre un enlace

En el siguiente ejemplo de `get-link`, se devuelve información completa sobre un enlace.

```
aws oam get-link \
    --identifier arn:aws:oam:us-east-2:123456789111:link/a1b2c3d4-5678-90ab-cdef-example11111
```

Salida:

```
{
    "Arn": "arn:aws:oam:us-east-2:123456789111:link/a1b2c3d4-5678-90ab-cdef-example11111",
    "Id": "a1b2c3d4-5678-90ab-cdef-example11111",
    "Label": "sourceAccount",
    "LabelTemplate": "sourceAccount",
    "ResourceTypes": [
        "AWS::CloudWatch::Metric"
    ],
    "SinkArn": "arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-example12345",
```

```
    "Tags": {}
}
```

Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetLink en la Referencia de comandos de la AWS CLI.

`get-sink-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-sink-policy`.

AWS CLI

Devolución de la política de receptor actual adjunta al receptor

En el siguiente ejemplo de `get-sink-policy`, se devuelve la política de receptor actual asociada al receptor.

```
aws oam get-sink-policy \
    --sink-identifier arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-example12345
```

Salida:

```
{
    "SinkArn": "arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-example12345",
    "SinkId": "a1b2c3d4-5678-90ab-cdef-example12345",
    "Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow\",\"Principal\":{\"AWS\":\"arn:aws:iam::123456789111:root\"},\"Action\":[\"oam:CreateLink\",\"oam:UpdateLink\"],\"Resource\":\"*\",\"Condition\":{\"ForAllValues:StringEquals\":{\"oam:ResourceTypes\":[\"AWS::Logs::LogGroup\",\"AWS::CloudWatch::Metric\",\"AWS::XRay::Trace\",\"AWS::ApplicationInsights::Application\"]}}}]}"
}
```

Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetSinkPolicy en la Referencia de comandos de la AWS CLI.

`get-sink`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-sink`.

AWS CLI

Devolución de la información completa sobre un receptor de cuenta de supervisión

En el siguiente ejemplo de `get-sink`, se devuelve información completa sobre un receptor de cuenta de supervisión.

```
aws oam get-sink \
    --identifier arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-example12345
```

Salida:

```
{
    "Arn": "arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-example12345",
    "Id": "a1b2c3d4-5678-90ab-cdef-example12345",
    "Name": "DemoSink",
    "Tags": {}
}
```

Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetSink en la Referencia de comandos de la AWS CLI.

`list-attached-links`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-attached-links`.

AWS CLI

Devolución de una lista de los enlaces de cuentas de origen que están vinculados a este receptor de cuentas de supervisión

En el siguiente ejemplo de `list-attached-links`, se devuelve una lista de los enlaces de cuentas de origen que están enlazados a este receptor de cuentas de supervisión.

```
aws oam list-attached-links \
    --sink-identifier arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-example12345
```

Salida:

```
{
    "Items": [{
        "Label": "Monitoring account",
        "LinkArn": "arn:aws:oam:us-east-2:123456789111:link/a1b2c3d4-5678-90ab-cdef-example11111",
        "ResourceTypes": [
            "AWS::ApplicationInsights::Application",
            "AWS::Logs::LogGroup",
            "AWS::CloudWatch::Metric",
            "AWS::XRay::Trace"
        ]
    }]
}
```

Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListAttachedLinks en la Referencia de comandos de la AWS CLI.

`list-links`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-links`.

AWS CLI

Devolución de una lista de enlaces para un receptor de cuentas de supervisión

En el siguiente ejemplo de `list-links`, se devuelve una lista de enlaces para un receptor de cuentas de supervisión. Ejecute esta operación en una cuenta de origen para devolver una lista de enlaces a los receptores de las cuentas de supervisión que tiene esta cuenta de origen.

```
aws oam list-links
```

Salida:

```
{
    "Items": [{
        "Arn": "arn:aws:oam:us-east-2:123456789111:link/a1b2c3d4-5678-90ab-cdef-
example11111",
        "Id": "a1b2c3d4-5678-90ab-cdef-example11111",
        "Label": "sourceAccount",
        "ResourceTypes": [
            "AWS::CloudWatch::Metric"
        ],
        "SinkArn": "arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-
example12345"
    }]
}
```

Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListLinks en la Referencia de comandos de la AWS CLI.

`list-sinks`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-sinks`.

AWS CLI

Para devolver la lista de receptores creada en la cuenta de supervisión

En el siguiente ejemplo de `list-sinks`, se devuelve una lista de receptores creada en la cuenta de supervisión. Ejecute esta operación en una cuenta de supervisión.

```
aws oam list-sinks
```

Salida:

```
{
    "Items": [
        {
            "Arn": "arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-
example12345",
            "Id": "a1b2c3d4-5678-90ab-cdef-example12345",
            "Name": "DemoSink"
        }
    ]
}
```

Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListSinks en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Muestra de las etiquetas asociadas a un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se muestran las etiquetas asociadas con un receptor.

```
aws oam list-tags-for-resource \
    --resource-arn arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-
example12345
```

Salida:

```
{
    "Tags": {
        "Team": "Devops"
    }
}
```

Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-sink-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-sink-policy`.

AWS CLI

Creación o actualización de la política de recursos

En el siguiente ejemplo de `put-sink-policy`, se crea la política de recursos que concede permisos a las cuentas de origen para que se vinculen al receptor de cuentas de supervisión.

```
aws oam put-sink-policy \
    --policy '{"Version":"2012-10-17",       "Statement":
[{"Effect":"Allow","Principal":{"AWS":"arn:aws:iam::123456789111:root"},"Action":
["oam:CreateLink","oam:UpdateLink"],"Resource":"*","Condition":
{"ForAllValues:StringEquals":{"oam:ResourceTypes":
["AWS::Logs::LogGroup","AWS::CloudWatch::Metric","AWS::XRay::Trace","AWS::ApplicationInsight
 \
    --sink-identifier arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-
cdef-example12345
```

Salida:

```
{
    "SinkArn": "arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-
example12345",
    "SinkId": "a1b2c3d4-5678-90ab-cdef-example12345",
    "Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":
\"Allow\",\"Principal\":{\"AWS\":\"arn:aws:iam::123456789111:root\"},
\"Action\":[\"oam:CreateLink\",\"oam:UpdateLink\"],\"Resource\":\"*\",
\"Condition\":{\"ForAllValues:StringEquals\":{\"oam:ResourceTypes\":
[\"AWS::Logs::LogGroup\",\"AWS::CloudWatch::Metric\",\"AWS::XRay::Trace\",
\"AWS::ApplicationInsights::Application\"]}}}]}"
}
```

Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte PutSinkPolicy en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Agregación de una o varias etiquetas al recurso especificado

En el siguiente ejemplo de `tag-resource`, se etiqueta un receptor `arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-example12345`.

```
aws oam tag-resource \
    --resource-arn arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-example12345 \
    --tags team=Devops
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de una o varias etiquetas del recurso especificado.

En el siguiente ejemplo de `untag-resource`, se elimina una etiqueta con la clave `team` del receptor `arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-example12345`.

```
aws oam untag-resource \
    --resource-arn arn:aws:oam:us-east-2:123456789012:sink/f3f42f60-
f0f2-425c-1234-12347bdd821f \
    --tag-keys team
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-link

En el siguiente ejemplo de código, se muestra cómo utilizar `update-link`.

AWS CLI

Cambio de los tipos de datos que se comparten desde una cuenta de origen a su receptor de cuentas de supervisión vinculado

En el siguiente ejemplo de `update-link`, se actualiza el enlace `arn:aws:oam:us-east-2:123456789111:link/0123e691-e7ef-43fa-1234-c57c837fced0` con los tipos de recursos `AWS::CloudWatch::Metric` y `AWS::Logs::LogGroup`.

```
aws oam update-link \
    --identifier arn:aws:oam:us-east-2:123456789111:link/a1b2c3d4-5678-90ab-cdef-
example11111 \
    --resource-types "AWS::CloudWatch::Metric" "AWS::Logs::LogGroup"
```

Salida:

```
{
    "Arn": "arn:aws:oam:us-east-2:123456789111:link/a1b2c3d4-5678-90ab-cdef-
example11111",
    "Id": "a1b2c3d4-5678-90ab-cdef-example11111",
    "Label": "sourceAccount",
    "LabelTemplate": "sourceAccount",
    "ResourceTypes": [
        "AWS::CloudWatch::Metric",
```

```
        "AWS::Logs::LogGroup"
    ],
    "SinkArn": "arn:aws:oam:us-east-2:123456789012:sink/a1b2c3d4-5678-90ab-cdef-
example12345",
    "Tags": {}
}
```

Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte UpdateLink en la Referencia de comandos de la AWS CLI.

Ejemplos del administrador de observabilidad de CloudWatch que utiliza AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios comunes mediante la AWS Command Line Interface con el administrador de observabilidad de CloudWatch.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`get-telemetry-evaluation-status-for-organization`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-telemetry-evaluation-status-for-organization`.

AWS CLI

Obtención del estado de incorporación de telemetría de la organización

En el siguiente ejemplo de `get-telemetry-evaluation-status-for-organization`, se devuelve el estado de incorporación actual de la característica de configuración de telemetría de la organización.

```
aws observabilityadmin get-telemetry-evaluation-status-for-organization
```

Salida:

```
{
    "Status": "RUNNING"
}
```

Para obtener más información, consulte Auditoría de las configuraciones de telemetría de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetTelemetryEvaluationStatusForOrganization en la Referencia de comandos de la AWS CLI.

`get-telemetry-evaluation-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-telemetry-evaluation-status`.

AWS CLI

Obtención del estado de incorporación de telemetría de la cuenta

En el siguiente ejemplo de `get-telemetry-evaluation-status`, se devuelve el estado de incorporación actual de la característica de configuración de telemetría de la cuenta especificada.

```
aws observabilityadmin get-telemetry-evaluation-status
```

Salida:

```
{
    "Status": "RUNNING"
}
```

Para obtener más información, consulte Auditoría de las configuraciones de telemetría de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetTelemetryEvaluationStatus en la Referencia de comandos de la AWS CLI.

`list-resource-telemetry-for-organization`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-telemetry-for-organization`.

AWS CLI

Recuperación de las configuraciones de telemetría de la organización

En el siguiente ejemplo de `list-resource-telemetry-for-organization`, se devuelve una lista de las configuraciones de telemetría de la organización para los recursos de AWS compatibles con la configuración de telemetría.

```
aws observabilityadmin list-resource-telemetry-for-organization \
    --resource-types  AWS::EC2::Instance
```

Salida:

```
{
    "TelemetryConfigurations": [
        {
            "AccountIdentifier": "111111111111",
            "TelemetryConfigurationState": {
                "Logs": "NotApplicable",
                "Metrics": "Disabled",
                "Traces": "NotApplicable"
            },
            "ResourceType": "AWS::EC2::Instance",
            "ResourceIdentifier": "i-a166400b",
            "ResourceTags": {
                "Name": "dev"
            },
            "LastUpdateTimeStamp": 1733168548521
        },
        {
            "AccountIdentifier": "222222222222",
            "TelemetryConfigurationState": {
                "Logs": "NotApplicable",
```

```
                "Metrics": "Disabled",
                "Traces": "NotApplicable"
            },
            "ResourceType": "AWS::EC2::Instance",
            "ResourceIdentifier": "i-b188560f",
            "ResourceTags": {
                "Name": "apache"
            },
            "LastUpdateTimeStamp": 1732744260182
        }
    ]
}
```

Para obtener más información, consulte Auditoría de las configuraciones de telemetría de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListResourceTelemetryForOrganization en la Referencia de comandos de la AWS CLI.

`list-resource-telemetry`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-telemetry`.

AWS CLI

Recuperación de las configuraciones de telemetría de la cuenta

En el siguiente ejemplo de `list-resource-telemetry`, se devuelve una lista de las configuraciones de telemetría para recursos de AWS compatibles con la configuración de telemetría de la cuenta especificada.

```
aws observabilityadmin list-resource-telemetry \
    --resource-types  AWS::EC2::Instance
```

Salida:

```
{
    "TelemetryConfigurations": [
        {
            "AccountIdentifier": "111111111111",
            "TelemetryConfigurationState": {
```

```
                "Logs": "NotApplicable",
                "Metrics": "Disabled",
                "Traces": "NotApplicable"
            },
            "ResourceType": "AWS::EC2::Instance",
            "ResourceIdentifier": "i-0e979d278b040f856",
            "ResourceTags": {
                "Name": "apache"
            },
            "LastUpdateTimeStamp": 1732744260182
        }
    ]
}
```

Para obtener más información, consulte Auditoría de las configuraciones de telemetría de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListResourceTelemetry en la Referencia de comandos de la AWS CLI.

`start-telemetry-evaluation-for-organization`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-telemetry-evaluation-for-organization`.

AWS CLI

Habilitación de la característica de configuración de telemetría

En el siguiente ejemplo de `start-telemetry-evaluation-for-organization`, se habilita la característica de configuración de telemetría de la organización.

```
aws observabilityadmin start-telemetry-evaluation-for-organization
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Turning on CloudWatch telemetry auditing en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte StartTelemetryEvaluationForOrganization en la Referencia de comandos de la AWS CLI.

`start-telemetry-evaluation`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-telemetry-evaluation`.

AWS CLI

Habilitación de la característica de configuración de telemetría

En el siguiente ejemplo de `start-telemetry-evaluation`, se habilita la característica de configuración de telemetría de la cuenta especificada.

```
aws observabilityadmin start-telemetry-evaluation
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Turning on CloudWatch telemetry auditing en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte StartTelemetryEvaluation en la Referencia de comandos de la AWS CLI.

`stop-telemetry-evaluation-for-organization`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-telemetry-evaluation-for-organization`.

AWS CLI

Desactivación de la característica de configuración de telemetría

En el siguiente ejemplo de `stop-telemetry-evaluation-for-organization`, se desactiva la característica de configuración de telemetría de la organización.

```
aws observabilityadmin stop-telemetry-evaluation-for-organization
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Desactivación de la auditoría de telemetría de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte StopTelemetryEvaluationForOrganization en la Referencia de comandos de la AWS CLI.

`stop-telemetry-evaluation`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-telemetry-evaluation`.

AWS CLI

Desactivación de la característica de configuración de telemetría

En el siguiente ejemplo de `stop-telemetry-evaluation`, se desactiva la característica de configuración de telemetría de la cuenta especificada.

```
aws observabilityadmin stop-telemetry-evaluation
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Desactivación de la auditoría de telemetría de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte StopTelemetryEvaluation en la Referencia de comandos de la AWS CLI.

Ejemplos de CloudWatch Synthetics con AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes mediante la AWS Command Line Interface con CloudWatch Synthetics.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-resource`.

AWS CLI

Asociación de un canario a un grupo

En el siguiente ejemplo de `associate-resource`, se asocia un canario a un grupo denominado `demo_group`.

```
aws synthetics associate-resource \
    --group-identifier demo_group \
    --resource-arn arn:aws:synthetics:us-east-1:123456789012:canary:demo_canary
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte AssociateResource en la Referencia de comandos de la AWS CLI.

`create-canary`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-canary`.

AWS CLI

Creación de un canario

En el siguiente ejemplo de `create-canary`, se crea un canario denominado `demo_canary`.

```
aws synthetics create-canary \
    --name demo_canary \
    --code '{"S3Bucket": "artifacts3bucket", "S3Key":"demo_canary.zip", "Handler":
 "index.lambda_handler"}' \
    --artifact-s3-location s3://amzn-s3-demo-bucket/demo_canary.zip \
    --execution-role-arn arn:aws:iam::123456789012:role/demo_canary_role \
    --schedule Expression="rate(10 minutes)" \
    --runtime-version syn-nodejs-puppeteer-9.1
```

Salida:

```
{
    "Canary": {
        "Id": "a1b2c3d4-5678-90ab-cdef-example11111",
```

```
        "Name": "demo_canary",
        "Code": {
            "Handler": "index.lambda_handler"
        },
        "ExecutionRoleArn": "arn:aws:iam::123456789012:role/demo_canary_role",
        "Schedule": {
            "Expression": "rate(10 minutes)",
            "DurationInSeconds": 0
        },
        "RunConfig": {
            "TimeoutInSeconds": 600,
            "MemoryInMB": 1000,
            "ActiveTracing": false
        },
        "SuccessRetentionPeriodInDays": 31,
        "FailureRetentionPeriodInDays": 31,
        "Status": {
            "State": "CREATING",
            "StateReasonCode": "CREATE_PENDING"
        },
        "Timeline": {
            "Created": "2024-10-15T19:03:08.826000+05:30",
            "LastModified": "2024-10-15T19:03:08.826000+05:30"
        },
        "ArtifactS3Location": "amzn-s3-demo-bucket/demo_canary.zip",
        "RuntimeVersion": "syn-nodejs-puppeteer-9.1",
        "Tags": {}
    }
}
```

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte CreateCanary en la Referencia de comandos de la AWS CLI.

`create-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-group`.

AWS CLI

Creación de un grupo

En el siguiente ejemplo de `create-group`, se crea un grupo llamado `demo_group`.

```
aws synthetics create-group \
    --name demo_group
```

Salida:

```
{
    "Group": {
        "Id": "example123",
        "Name": "demo_group",
        "Arn": "arn:aws:synthetics:us-east-1:123456789012:group:example123",
        "Tags": {},
        "CreatedTime": "2024-10-15T14:47:23.811000+05:30",
        "LastModifiedTime": "2024-10-15T14:47:23.811000+05:30"
    }
}
```

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte CreateGroup en la Referencia de comandos de la AWS CLI.

`delete-canary`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-canary`.

AWS CLI

Eliminación permanente de un canario

En el siguiente ejemplo de `delete-canary`, se elimina un canario denominado `demo_canary`.

```
aws synthetics delete-canary \
    --name demo_canary
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DeleteCanary en la Referencia de comandos de la AWS CLI.

`delete-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-group`.

AWS CLI

Para eliminar un grupo

En el siguiente ejemplo de `delete-group`, se elimina un grupo denominado `demo_group`.

```
aws synthetics delete-group \
    --group-identifier demo_group
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DeleteGroup en la Referencia de comandos de la AWS CLI.

`describe-canaries-last-run`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-canaries-last-run`.

AWS CLI

Visualización de la información de la ejecución más reciente de cada canario

En el siguiente ejemplo de `describe-canaries-last-run`, se devuelve la ejecución más reciente de cada canario que haya creado.

```
aws synthetics describe-canaries-last-run
```

Salida:

```
{
    "CanariesLastRun": [
        {
```

```
            "CanaryName": "demo_canary",
            "LastRun": {
                "Id": "a1b2c3d4-5678-90ab-cdef-example11111",
                "Name": "demo_canary",
                "Status": {
                    "State": "PASSED",
                    "StateReason": "",
                    "StateReasonCode": ""
                },
                "Timeline": {
                    "Started": "2024-10-15T19:20:39.691000+05:30",
                    "Completed": "2024-10-15T19:20:58.211000+05:30"
                },
                "ArtifactS3Location": "cw-syn-results-123456789012-us-east-1/canary/
us-east-1/demo_canary-abc-example1234/2024/10/15/13/50-39-690"
            }
        }
    ]
}
```

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DescribeCanariesLastRun en la Referencia de comandos de la AWS CLI.

`describe-canaries`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-canaries`.

AWS CLI

Inclusión de los canarios en la cuenta

En el siguiente ejemplo de `describe-canaries`, se muestran los detalles de los canarios de la cuenta.

```
aws synthetics describe-canaries
```

Salida:

```
{
    "Canaries": [
```

```
        {
            "Id": "a1b2c3d4-5678-90ab-cdef-example11111",
            "Name": "demo_canary",
            "Code": {
                "SourceLocationArn": "arn:aws:lambda:us-
east-1:123456789012:layer:cwsyn-demo_canary-a1b2c3d4-5678-90ab-cdef-
example11111b8:1",
                "Handler": "pageLoadBlueprint.handler"
            },
            "ExecutionRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudWatchSyntheticsRole-demo_canary-a12-a123bc456789",
            "Schedule": {
                "Expression": "rate(5 minutes)",
                "DurationInSeconds": 0
            },
            "RunConfig": {
                "TimeoutInSeconds": 300,
                "MemoryInMB": 1000,
                "ActiveTracing": false
            },
            "SuccessRetentionPeriodInDays": 31,
            "FailureRetentionPeriodInDays": 31,
            "Status": {
            "State": "RUNNING"
            },
            "Timeline": {
                "Created": "2024-10-15T18:55:15.168000+05:30",
                "LastModified": "2024-10-15T18:55:40.540000+05:30",
                "LastStarted": "2024-10-15T18:55:40.540000+05:30"
            },
            "ArtifactS3Location": "cw-syn-results-123456789012-us-east-1/canary/us-
east-1/demo_canary-a12-a123bc456789",
            "EngineArn": "arn:aws:lambda:us-east-1:123456789012:function:cwsyn-
demo_canary-a1b2c3d4-5678-90ab-cdef-example111118:1",
            "RuntimeVersion": "syn-nodejs-puppeteer-9.1",
            "Tags": {
                "blueprint": "heartbeat"
            }
        }
    ]
}
```

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DescribeCanaries en la Referencia de comandos de la AWS CLI.

`describe-runtime-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-runtime-versions`.

AWS CLI

Devolución de una lista de las versiones de tiempo de ejecución de canario de Synthetics

En el siguiente ejemplo de `describe-runtime-versions`, se devuelve la lista de versiones de tiempo de ejecución de canario de Synthetics.

```
aws synthetics describe-runtime-versions
```

Salida:

```
{
    "RuntimeVersions": [
        {
            "VersionName": "syn-nodejs-puppeteer-9.1",
            "Description": "Security fixes and bug fix for date range error in har.
 Dependencies: Node JS 20.x, Puppeteer-core 22.12.1, Chromium 126.0.6478.126",
            "ReleaseDate": "2024-10-02T05:30:00+05:30"
        },
        {
            "VersionName": "syn-nodejs-puppeteer-9.0",
            "Description": "Upgraded Chromium and Puppeteer. Dependencies: Node JS
 20.x, Puppeteer-core 22.12.1, Chromium 126.0.6478.126",
            "ReleaseDate": "2024-07-22T05:30:00+05:30"
        },
        {
            "VersionName": "syn-nodejs-puppeteer-8.0",
            "Description": "Upgraded Chromium and Puppeteer. Dependencies: Node JS
 20.x, Puppeteer-core 22.10.0, Chromium 125.0.6422.112",
            "ReleaseDate": "2024-06-21T05:30:00+05:30"
        },
        {
            "VersionName": "syn-nodejs-puppeteer-7.0",
```

```
            "Description": "Upgraded Chromium and Puppeteer. Dependencies: Node JS
18.x, Puppeteer-core 21.9.0, Chromium 121.0.6167.139",
            "ReleaseDate": "2024-03-08T05:30:00+05:30"
            },
        {
            "VersionName": "syn-nodejs-puppeteer-6.2",
            "Description": "Updated shared libraries for Chromium and added
ephemeral storage monitoring. Dependencies: Node JS 18.x, Puppeteer-core 19.7.0,
Chromium 111.0.5563.146",
            "ReleaseDate": "2024-02-02T05:30:00+05:30"
        },
        {
            "VersionName": "syn-nodejs-puppeteer-6.1",
            "Description": "Added puppeteer launch retry. Dependencies: Node JS
18.x, Puppeteer-core 19.7.0, Chromium 111.0.5563.146",
            "ReleaseDate": "2023-11-13T05:30:00+05:30",
            "DeprecationDate": "2024-03-08T13:30:00+05:30"
        },
        {
            "VersionName": "syn-nodejs-puppeteer-6.0",
            "Description": "Reduced X-Ray traces of a canary run, improved duration
metric and upgraded to NodeJS 18.x. Dependencies: Node JS 18.x, Puppeteer-core
19.7.0, Chromium 111.0.5563.146",
            "ReleaseDate": "2023-09-15T05:30:00+05:30",
            "DeprecationDate": "2024-03-08T13:30:00+05:30"
        },
        {
            "VersionName": "syn-nodejs-puppeteer-5.2",
            "Description": "Updated shared libraries for Chromium. Dependencies:
Node JS 16.x, Puppeteer-core 19.7.0, Chromium 111.0.5563.146",
            "ReleaseDate": "2024-02-01T05:30:00+05:30"
        },
        {
            "VersionName": "syn-nodejs-puppeteer-5.1",
            "Description": "Fixes a bug about missing request headers in har.
Dependencies: Node JS 16.x, Puppeteer-core 19.7.0, Chromium 111.0.5563.146",
            "ReleaseDate": "2023-08-09T05:30:00+05:30",
            "DeprecationDate": "2024-03-08T13:30:00+05:30"
        },
        {
            "VersionName": "syn-nodejs-puppeteer-5.0",
            "Description": "Upgraded Puppeteer and Chromium. Dependencies: Node JS
16.x, Puppeteer-core 19.7.0, Chromium 111.0.5563.146",
            "ReleaseDate": "2023-07-21T05:30:00+05:30",
```

```
            "DeprecationDate": "2024-03-08T13:30:00+05:30"
        },
        {
            "VersionName": "syn-nodejs-puppeteer-4.0",
            "Description": "Upgraded to NodeJS 16.x. Dependencies: Node JS 16.x,
 Puppeteer-core 5.5.0, Chromium 92.0.4512.0",
            "ReleaseDate": "2023-05-01T05:30:00+05:30",
            "DeprecationDate": "2024-03-08T13:30:00+05:30"
        }
    ]
}
```

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener detalles sobre la API, consulte DescribeRuntimeVersions en la Referencia de comandos de la AWS CLI.

`disassociate-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-resource`.

AWS CLI

Eliminación de un canario de un grupo

En el ejemplo siguiente de `disassociate-resource` se elimina un canario del grupo denominado `demo_group`.

```
aws synthetics disassociate-resource \
    --group-identifier demo_group \
    --resource-arn arn:aws:synthetics:us-east-1:123456789012:canary:demo_canary
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DisassociateResource en la Referencia de comandos de la AWS CLI.

`get-canary-runs`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-canary-runs`.

AWS CLI

Recuperación de una lista de ejecuciones de un canario específico

En el siguiente ejemplo de `get-canary-runs`, se devuelve una lista de las ejecuciones del canario denominado `demo_canary`.

```
aws synthetics get-canary-runs \
    --name demo_canary
```

Salida:

```
{
    "CanaryRuns": [
        {
            "Id": "a1b2c3d4-5678-90ab-cdef-example11111",
            "Name": "demo_canary",
            "Status": {
                "State": "PASSED",
                "StateReason": "",
                "StateReasonCode": ""
            },
            "Timeline": {
                "Started": "2024-10-16T10:38:57.013000+05:30",
                "Completed": "2024-10-16T10:39:25.793000+05:30"
            },
            "ArtifactS3Location": "cw-syn-results-123456789012-us-east-1/canary/us-
east-1/demo_canary-abc-example1234/2024/10/15/13/50-39-690"
        }
    ]
}
```

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetCanaryRuns en la Referencia de comandos de la AWS CLI.

`get-canary`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-canary`.

AWS CLI

Recuperación de la información completa sobre un canario

En el siguiente ejemplo de `get-canary`, se recupera información completa sobre un canario denominado `demo_canary`.

```
aws synthetics get-canary \
    --name demo_canary
```

Salida:

```
{
    "Canary": {
        "Id": "a1b2c3d4-5678-90ab-cdef-example11111",
        "Name": "demo_canary",
        "Code": {
            "SourceLocationArn": "arn:aws:lambda:us-east-1:123456789012:layer:cwsyn-
demo_canary-a1b2c3d4-5678-90ab-cdef-example111118:1",
            "Handler": "pageLoadBlueprint.handler"
        },
        "ExecutionRoleArn": "arn:aws:iam::123456789012:role/demo_canary_role",
        "Schedule": {
            "Expression": "rate(10 minutes)",
            "DurationInSeconds": 0
        },
        "RunConfig": {
            "TimeoutInSeconds": 300,
            "MemoryInMB": 1000,
            "ActiveTracing": false
        },
        "SuccessRetentionPeriodInDays": 31,
        "FailureRetentionPeriodInDays": 31,
        "Status": {
            "State": "RUNNING"
        },
        "Timeline": {
            "Created": "2024-10-15T18:55:15.168000+05:30",
            "LastModified": "2024-10-15T18:55:40.540000+05:30",
```

```
            "LastStarted": "2024-10-15T18:55:40.540000+05:30"
        },
        "ArtifactS3Location": "cw-syn-results-123456789012-us-east-1/canary/us-
east-1/demo_canary-a12-a123bc456789",
        "EngineArn": "arn:aws:lambda:us-east-1:123456789012:function:cwsyn-
demo_canary-a1b2c3d4-5678-90ab-cdef-example111118:1",
        "RuntimeVersion": "syn-nodejs-puppeteer-9.1",
        "Tags": {
            "blueprint": "heartbeat"
        }
    }
}
```

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener detalles sobre la API, consulte GetCanary en la Referencia de comandos de la AWS CLI.

`get-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-group`.

AWS CLI

Devolución de información sobre un grupo

En el siguiente ejemplo de `get-group`, se devuelve información sobre el grupo denominado `demo_group`.

```
aws synthetics get-group \
    --group-identifier demo_group
```

Salida:

```
{
    "Group": {
        "Id": "example123",
        "Name": "demo_group",
        "Arn": "arn:aws:synthetics:us-east-1:123456789012:group:example123",
        "Tags": {},
        "CreatedTime": "2024-10-15T14:47:23.811000+05:30",
```

```
        "LastModifiedTime": "2024-10-15T14:47:23.811000+05:30"
    }
}
```

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetGroup en la Referencia de comandos de la AWS CLI.

`list-associated-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-associated-groups`.

AWS CLI

Devolución de una lista de los grupos

En el siguiente ejemplo de `list-associated-groups`, se devuelve una lista de los grupos asociados al canario denominado `demo_canary`.

```
aws synthetics list-associated-groups \
    --resource-arn arn:aws:synthetics:us-east-1:123456789012:canary:demo_canary
```

Salida:

```
{
    "Groups": [
        {
            "Id": "example123",
            "Name": "demo_group",
            "Arn": "arn:aws:synthetics:us-east-1:123456789012:group:example123"
        }
    ]
}
```

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListAssociatedGroups en la Referencia de comandos de la AWS CLI.

`list-group-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-group-resources`.

AWS CLI

Devolución de una lista de los ARN de los canarios que están asociados al grupo especificado

En el siguiente ejemplo de `list-group-resources`, se devuelve una lista de los ARN de los canarios asociados al grupo denominado `demo_group`.

```
aws synthetics list-group-resources \
    --group-identifier demo_group
```

Salida:

```
{
    "Resources": [
        "arn:aws:synthetics:us-east-1:123456789012:canary:demo_canary"
    ]
}
```

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListGroupResources en la Referencia de comandos de la AWS CLI.

`list-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-groups`.

AWS CLI

Devolución de una lista de todos los grupos de la cuenta

En el siguiente ejemplo de `list-groups`, se devuelve una lista de todos los grupos en la cuenta.

```
aws synthetics list-groups
```

Salida:

```
{
    "Groups": [
        {
            "Id": "example123",
            "Name": "demo_group",
            "Arn": "arn:aws:synthetics:us-east-1:123456789012:group:example123"
        }
    ]
}
```

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListGroups en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Ejemplo 1: muestra de las etiquetas asociadas a un canario

En el siguiente ejemplo de `list-tags-for-resource`, se devuelven las etiquetas asociadas a un canario denominado `demo_canary`.

```
aws synthetics list-tags-for-resource \
    --resource-arn arn:aws:synthetics:us-east-1:123456789012:canary:demo_canary
```

Salida:

```
{
    "Tags": {
        "blueprint": "heartbeat"
    }
}
```

Ejemplo 2: muestra de las etiquetas asociadas a un grupo

En el siguiente ejemplo de `list-tags-for-resource`, se devuelven las etiquetas asociadas a un grupo denominado `demo_group`.

```
aws  synthetics list-tags-for-resource \
    --resource-arn arn:aws:synthetics:us-east-1:123456789012:group:example123
```

Salida:

```
{
    "Tags": {
        "team": "Devops"
    }
}
```

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`start-canary`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-canary`.

AWS CLI

Ejecución de un canario

En el siguiente ejemplo de `start-canary`, se ejecuta un canario denominado `demo_canary`.

```
aws synthetics start-canary \
    --name demo_canary
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte StartCanary en la Referencia de comandos de la AWS CLI.

`stop-canary`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-canary`.

AWS CLI

Detención de un canario

En el siguiente ejemplo de `stop-canary`, se detiene el canario denominado `demo_canary`.

```
aws synthetics stop-canary \
    --name demo_canary
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte StopCanary en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Ejemplo 1: asignación de una etiqueta al canario

En el siguiente ejemplo de `tag-resource`, se asigna una etiqueta al canario denominado `demo_canary`.

```
aws synthetics tag-resource \
    --resource-arn arn:aws:synthetics:us-east-1:123456789012:canary:demo_canary \
    --tags blueprint=heartbeat
```

Este comando no genera ninguna salida.

Ejemplo 2: asignación de una etiqueta al grupo

En el siguiente ejemplo de `tag-resource`, se asigna una etiqueta al grupo denominado `demo_group`.

```
aws synthetics tag-resource \
    --resource-arn arn:aws:synthetics:us-east-1:123456789012:group:example123 \
```

```
    --tags team=Devops
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Ejemplo 1: eliminación de una etiqueta del canario

En el siguiente ejemplo de `untag-resource`, se elimina una etiqueta del canario denominado `demo_canary`.

```
aws synthetics untag-resource \
    --resource-arn arn:aws:synthetics:us-east-1:123456789012:canary:demo_canary \
    --tag-keys blueprint
```

Este comando no genera ninguna salida.

Ejemplo 2: eliminación de una etiqueta del grupo

En el siguiente ejemplo de `untag-resource`, se asigna la eliminación de una etiqueta del grupo denominado `demo_group`.

```
aws synthetics untag-resource \
    --resource-arn arn:aws:synthetics:us-east-1:123456789012:group:example123 \
    --tag-keys team
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-canary`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-canary`.

AWS CLI

Actualización de un canario

En el siguiente ejemplo de `update-canary`, se actualiza la configuración de un canario denominado `demo_canary`.

```
aws synthetics update-canary \
    --name demo_canary \
    --schedule Expression="rate(15 minutes)"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Synthetic Monitoring (valores controlados) en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte UpdateCanary en la Referencia de comandos de la AWS CLI.

Ejemplos de CodeArtifact que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar situaciones comunes mediante la AWS Command Line Interface con CodeArtifact.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-external-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-external-connection`.

AWS CLI

Adición de una conexión externa a un repositorio

En el siguiente ejemplo de `associate-external-connection`, se agrega una conexión externa a npmjs.com a un repositorio denominado test-repo.

```
aws codeartifact associate-external-connection \
    --repository test-repo \
    --domain test-domain \
    --external-connection public:npmjs
```

Salida:

```
{
    "repository": {
        "name": "test-repo",
        "administratorAccount": "111122223333",
        "domainName": "test-domain",
        "domainOwner": "111122223333",
        "arn": "arn:aws:codeartifact:us-west-2:111122223333:repository/test-domain/
test-repo",
        "upstreams": [],
        "externalConnections": [
            {
                "externalConnectionName": "public:npmjs",
                "packageFormat": "npm",
                "status": "AVAILABLE"
            }
        ]
    }
}
```

Para obtener más información, consulte Add an external connection en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte AssociateExternalConnection en la Referencia de comandos de la AWS CLI.

`copy-package-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-package-versions`.

AWS CLI

Copia de versiones de un paquete de un repositorio a otro

En el siguiente ejemplo de `copy-package-versions`, se mueven las versiones 4.0.0 y 5.0.0 de un paquete denominado test-package de my-repo a test-repo.

```
aws codeartifact copy-package-versions \
    --domain test-domain \
    --source-repository my-repo \
    --destination-repository test-repo \
    --format npm \
    --package test-package \
    --versions '["4.0.0", "5.0.0"]'
```

Salida:

```
{
    "format": "npm",
    "package": "test-package",
    "versions": [
        {
        "version": "5.0.0",
        "revision": "REVISION-1-SAMPLE-6C81EFF7DA55CC",
        "status": "Published"
        },
        {
        "version": "4.0.0",
        "revision": "REVISION-2-SAMPLE-55C752BEE772FC",
        "status": "Published"
        }
    ]
}
```

Para obtener más información, consulte Copy packages between repositories en la Guía del usuario de AWS CodeArtifact.

- Para obtener detalles sobre la API, consulte CopyPackageVersions en la Referencia de comandos de la AWS CLI.

`create-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-domain`.

AWS CLI

Creación de un dominio

En el siguiente ejemplo de `create-domain`, se crea un dominio denominado test-domain.

```
aws codeartifact create-domain \
    --domain test-domain
```

Salida:

```
{
    "domain": {
        "name": "test-domain",
        "owner": "111122223333",
        "arn": "arn:aws:codeartifact:us-west-2:111122223333:domain/test-domain",
        "status": "Active",
        "createdTime": "2020-10-20T13:16:48.559000-04:00",
        "encryptionKey": "arn:aws:kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "repositoryCount": 0,
        "assetSizeBytes": 0
    }
}
```

Para obtener más información, consulte Create a domain en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte CreateDomain en la Referencia de comandos de la AWS CLI.

`create-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-repository`.

AWS CLI

Creación de un repositorio

En el siguiente ejemplo de `create-repository`, se crea un repositorio denominado test-repo dentro de un dominio denominado test-domain.

```
aws codeartifact create-repository \
    --domain test-domain \
    --domain-owner 111122223333 \
    --repository test-repo \
    --description "This is a test repository."
```

Salida:

```
{
    "repository": {
        "name": "test-repo",
        "administratorAccount": "111122223333",
        "domainName": "test-domain",
        "domainOwner": "111122223333",
        "arn": "arn:aws:codeartifact:us-west-2:111122223333:repository/test-domain/
test-repo",
        "description": "This is a test repository.",
        "upstreams": [],
        "externalConnections": []
    }
}
```

Para obtener más información, consulte Create a domain en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte CreateRepository en la Referencia de comandos de la AWS CLI.

`delete-domain-permissions-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-domain-permissions-policy`.

AWS CLI

Eliminación del documento de política de permisos de un dominio

En el siguiente ejemplo de `delete-domain-permissions-policy`, se elimina la política de permisos de un dominio denominado test-domain.

```
aws codeartifact delete-domain-permissions-policy \
    --domain test-domain
```

Salida:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "BasicDomainPolicy",
            "Action": [
                "codeartifact:GetDomainPermissionsPolicy",
                "codeartifact:ListRepositoriesInDomain",
                "codeartifact:GetAuthorizationToken",
                "codeartifact:CreateRepository"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            }
        }
    ]
}
```

Para obtener más información, consulte Delete a domain policy en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte DeleteDomainPermissionsPolicy en la Referencia de comandos de la AWS CLI.

`delete-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-domain`.

AWS CLI

Eliminación de un dominio

En el siguiente ejemplo de `delete-domain`, se elimina un dominio denominado `test-domain`.

```
aws codeartifact delete-domain \
    --domain test-domain
```

Salida:

```
{
    "domain": {
        "name": "test-domain",
        "owner": "417498243647",
        "arn": "arn:aws:codeartifact:us-west-2:417498243647:domain/test-domain",
        "status": "Deleted",
        "createdTime": "2020-10-20T13:16:48.559000-04:00",
        "encryptionKey": "arn:aws:kms:us-west-2:417498243647:key/c9fe2447-0795-4fda-
afbe-8464574ae162",
        "repositoryCount": 0,
        "assetSizeBytes": 0
    }
}
```

Para obtener más información, consulte Delete a domain en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte DeleteDomain en la Referencia de comandos de la AWS CLI.

`delete-package-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-package-versions`.

AWS CLI

Eliminación de versiones de un paquete

En el siguiente ejemplo de `delete-package-versions`, se elimina la versión 4.0.0 de un paquete denominado test-package.

```
aws codeartifact delete-package-versions \
    --domain test-domain \
    --repo test-repo \
    --format npm \
    --package test-package \
    --versions 4.0.0
```

Salida:

```
{
    "successfulVersions": {
        "4.0.0": {
            "revision": "Ciqe5/9yicvkJT13b5/LdLpCyE6fqA7poa9qp+FilPs=",
            "status": "Deleted"
        }
    },
    "failedVersions": {}
}
```

Para obtener más información, consulte Delete a package version en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte DeletePackageVersions en la Referencia de comandos de la AWS CLI.

`delete-repository-permissions-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-repository-permissions-policy`.

AWS CLI

Eliminación de una política de permisos de un repositorio

En el siguiente ejemplo de `delete-repository-permissions-policy`, se elimina la política de permisos de un repositorio denominado test-repo.

```
aws codeartifact delete-repository-permissions-policy \
```

```
    --domain test-domain \
    --repository test-repo
```

Salida:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "codeartifact:DescribePackageVersion",
                "codeartifact:DescribeRepository",
                "codeartifact:GetPackageVersionReadme",
                "codeartifact:GetRepositoryEndpoint",
                "codeartifact:ListPackages",
                "codeartifact:ListPackageVersions",
                "codeartifact:ListPackageVersionAssets",
                "codeartifact:ListPackageVersionDependencies",
                "codeartifact:ReadFromRepository"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener más información, consulte Delete a policy en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte DeleteRepositoryPermissionsPolicy en la Referencia de comandos de la AWS CLI.

`delete-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-repository`.

AWS CLI

Eliminación de un repositorio

En el siguiente ejemplo de `delete-repository`, se elimina un repositorio denominado `test-repo` de un dominio denominado `test-domain`.

```
aws codeartifact delete-repository \
    --domain test-domain \
    --repository test-repo
```

Salida:

```
{
    "repository": {
        "name": "test-repo",
        "administratorAccount": "111122223333",
        "domainName": "test-domain",
        "domainOwner": "111122223333",
        "arn": "arn:aws:codeartifact:us-west-2:111122223333:repository/test-domain/
test-repo",
        "description": "This is a test repository",
        "upstreams": [],
        "externalConnections": []
    }
}
```

Para obtener más información, consulte Delete a repository en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte DeleteRepository en la Referencia de comandos de la AWS CLI.

`describe-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-domain`.

AWS CLI

Para obtener información acerca de un dominio

En el siguiente ejemplo de `describe-domain`, se obtiene un objeto DomainDescription de un dominio denominado test-domain.

```
aws codeartifact describe-domain \
```

```
    --domain test-domain
```

Salida:

```
{
    "domain": {
        "name": "test-domain",
        "owner": "111122223333",
        "arn": "arn:aws:codeartifact:us-west-2:111122223333:domain/test-domain",
        "status": "Active",
        "createdTime": "2020-10-20T13:16:48.559000-04:00",
        "encryptionKey": "arn:aws:kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "repositoryCount": 2,
        "assetSizeBytes": 0,
        "s3BucketArn": "arn:aws:s3:::assets-111122223333-us-west-2"
    }
}
```

Para obtener más información, consulte Domain overview en la Guía del usuario de AWS CodeArtifact.

- Para obtener más información sobre la API, consulte DescribeDomain en la Referencia de comandos de la AWS CLI.

`describe-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-repository`.

AWS CLI

Obtención de información sobre un repositorio

En el siguiente ejemplo de `describe-repository`, se obtiene un objeto RepositoryDescription de un repositorio denominado test-repo.

```
aws codeartifact describe-repository \
    --domain test-domain \
    --repository test-repo
```

Salida:

```
{
    "repository": {
        "name": "test-repo",
        "administratorAccount": "111122223333",
        "domainName": "test-domain",
        "domainOwner": "111122223333",
        "arn": "arn:aws:codeartifact:us-west-2:111122223333:repository/test-domain/
test-repo",
        "description": "This is a test repository.",
        "upstreams": [],
        "externalConnections": []
    }
}
```

Para obtener más información, consulte Create a domain en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte DescribeRepository en la Referencia de comandos de la AWS CLI.

`disassociate-external-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-external-connection`.

AWS CLI

Eliminación de una conexión externa de un repositorio

En el siguiente ejemplo de `disassociate-external-connection`, se elimina una conexión externa a npmjs.com de un repositorio denominado test-repo.

```
aws codeartifact disassociate-external-connection \
    --repository test-repo \
    --domain test-domain \
    --external-connection public:npmjs
```

Salida:

```
{
    "repository": {
```

```
        "name": "test-repo",
        "administratorAccount": "111122223333",
        "domainName": "test-domain",
        "domainOwner": "111122223333",
        "arn": "arn:aws:codeartifact:us-west-2:111122223333:repository/test-domain/
test-repo",
        "upstreams": [],
        "externalConnections": []
    }
}
```

Para obtener más información, consulte Remove an external connection en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte DisassociateExternalConnection en la Referencia de comandos de la AWS CLI.

`dispose-package-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `dispose-package-versions`.

AWS CLI

Eliminación de los activos de la versión de un paquete y establecimiento del estado en Disposed

En el siguiente ejemplo de `dispose-package-versions`, se eliminan los activos de la versión 4.0.0 de test-package y se establece su estado en Disposed.

```
aws codeartifact dispose-package-versions \
    --domain test-domain \
    --repo test-repo \
    --format npm \
    --package test-package \
    --versions 4.0.0
```

Salida:

```
{
    "successfulVersions": {
        "4.0.0": {
            "revision": "Ciqe5/9yicvkJT13b5/LdLpCyE6fqA7poa9qp+FilPs=",
            "status": "Disposed"
```

```
        }
    },
    "failedVersions": {}
}
```

Para obtener más información, consulte Working with packages in CodeArtifact en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte DisposePackageVersions en la Referencia de comandos de la AWS CLI.

`get-authorization-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-authorization-token`.

AWS CLI

Obtención de un token de autorización

El siguiente ejemplo de `get-authorization-token`, se recupera un token de autorización de CodeArtifact.

```
aws codeartifact get-authorization-token \
    --domain test-domain \
    --query authorizationToken \
    --output text
```

Salida:

```
This command will return the authorization token. You can store the output in an
 environment variable when calling the command.
```

Para obtener más información, consulte Configure pip without the login command en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte GetAuthorizationToken en la Referencia de comandos de la AWS CLI.

`get-domain-permissions-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-domain-permissions-policy`.

AWS CLI

Obtención del documento de la política de permisos de un dominio

En el siguiente ejemplo de `get-domain-permissions-policy`, se obtiene la política de permisos adjunta a un dominio denominado test-domain.

```
aws codeartifact get-domain-permissions-policy \
    --domain test-domain
```

Salida:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "BasicDomainPolicy",
            "Action": [
                "codeartifact:GetDomainPermissionsPolicy",
                "codeartifact:ListRepositoriesInDomain",
                "codeartifact:GetAuthorizationToken",
                "codeartifact:CreateRepository"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            }
        }
    ]
}
```

Para obtener más información, consulte Read a domain policy en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte GetDomainPermissionsPolicy en la Referencia de comandos de la AWS CLI.

`get-package-version-asset`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-package-version-asset`.

AWS CLI

Obtención de un activo de una versión de paquete

En el siguiente ejemplo de `get-package-version-asset`, se recupera el activo `package.tgz` de la versión 4.0.0 de un paquete npm denominado test-package.

```
aws codeartifact get-package-version-asset \
    --domain test-domain \
    --repository test-repo \
    --format npm \
    --package test-package \
    --package-version 4.0.0 \
    --asset 'package.tgz' \
    outfileName
```

Salida:

```
The output for this command will also store the raw asset in the file provided in
 place of outfileName.

{
    "assetName": "package.tgz",
    "packageVersion": "4.0.0",
    "packageVersionRevision": "Ciqe5/9yicvkJT13b5/LdLpCyE6fqA7poa9qp+FilPs="
}
```

Para obtener más información, consulte List package version assets en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte GetPackageVersionAsset en la Referencia de comandos de la AWS CLI.

`get-package-version-readme`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-package-version-readme`.

AWS CLI

Obtención del archivo readme de una versión de paquete

En el siguiente ejemplo de `get-package-version-readme`, se obtiene el activo readme de la versión 4.0.0 de un paquete npm denominado test-package.

```
aws codeartifact get-package-version-readme \
    --domain test-domain \
    --repo test-repo \
    --format npm \
    --package test-package \
    --package-version 4.0.0
```

Salida:

```
{
    "format": "npm",
    "package": "test-package",
    "version": "4.0.0",
    "readme": "<div align=\"center\">\n   <a href=\https://github.com/test-package/
testpack\"> ... more content ... \n",
    "versionRevision": "Ciqe5/9yicvkJT13b5/LdLpCyE6fqA7poa9qp+FilPs="
}
```

Para obtener más información, consulte View package version readme file en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte GetPackageVersionReadme en la Referencia de comandos de la AWS CLI.

`get-repository-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-repository-endpoint`.

AWS CLI

Obtención del punto de conexión de la URL de un repositorio

En el siguiente ejemplo de `get-repository-endpoint`, se obtiene el punto de conexión npm del repositorio test-repo.

```
aws codeartifact get-repository-endpoint \
    --domain test-domain \
    --repository test-repo \
```

```
    --format npm
```

Salida:

```
{
    "repositoryEndpoint": "https://test-domain-111122223333.d.codeartifact.us-
west-2.amazonaws.com/npm/test-repo/"
}
```

Para obtener más información, consulte Connect to a repository en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte GetRepositoryEndpoint en la Referencia de comandos de la AWS CLI.

`get-repository-permissions-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-repository-permissions-policy`.

AWS CLI

Obtención del documento de la política de permisos de un repositorio

En el siguiente ejemplo de `get-repository-permissions-policy`, se obtiene la política de permisos adjunta a un repositorio denominado test-repo.

```
aws codeartifact get-repository-permissions-policy \
    --domain test-domain \
    --repository test-repo
```

Salida:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
```

```
                "codeartifact:DescribePackageVersion",
                "codeartifact:DescribeRepository",
                "codeartifact:GetPackageVersionReadme",
                "codeartifact:GetRepositoryEndpoint",
                "codeartifact:ListPackages",
                "codeartifact:ListPackageVersions",
                "codeartifact:ListPackageVersionAssets",
                "codeartifact:ListPackageVersionDependencies",
                "codeartifact:ReadFromRepository"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener más información, consulte Read a policy en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte GetRepositoryPermissionsPolicy en la Referencia de comandos de la AWS CLI.

`list-domains`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-domains`.

AWS CLI

Para enumerar dominios

En el siguiente ejemplo de `list-domains`, se obtiene un resumen de todos los dominios que pertenecen a la cuenta de AWS que realiza la llamada.

```
aws codeartifact list-domains
```

Salida:

```
{
    "domains": [
        {
            "name": "my-domain",
            "owner": "111122223333",
            "status": "Active",
```

```
            "encryptionKey": "arn:aws:kms:us-west-2:111122223333:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
        },
        {
            "name": "test-domain",
            "owner": "111122223333",
            "status": "Active",
            "encryptionKey": "arn:aws:kms:us-west-2:111122223333:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
        }
    ]
}
```

Para obtener más información, consulte Working with domains in CodeArtifact en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte ListDomains en la Referencia de comandos de la AWS CLI.

`list-package-version-assets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-package-version-assets`.

AWS CLI

Recuperación de los activos de una versión de paquete

En el siguiente ejemplo de `list-package-version-assets`, se recuperan los activos de la versión 4.0.0 de un paquete npm denominado test-package.

```
aws codeartifact list-package-version-assets \
    --domain test-domain \
    --repo test-repo \
    --format npm \
    --package test-package \
    --package-version 4.0.0
```

Salida:

```
{
    "format": "npm",
    "package": "test-package",
```

```
    "version": "4.0.0",
    "versionRevision": "Ciqe5/9yicvkJT13b5/LdLpCyE6fqA7poa9qp+FilPs=",
    "assets": [
        {
            "name": "package.tgz",
            "size": 316680,
            "hashes": {
                "MD5": "60078ec6d9e76b89fb55c860832742b2",
                "SHA-1": "b44a9b6297bcb698f1c51a3545a2b3b368d59c52",
                "SHA-256":
 "d2aa8c6afc3c8591765785a37d1c5acae482a8eb3ab9729ed28922692454f2e2",
                "SHA-512":
 "3e585d15c8a594e20d7de57b362ea81754c011acb2641a19f1b72c8531ea39825896bab344ae616a0a5a824cb9
            }
        }
    ]
}
```

Para obtener más información, consulte List package version assets en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte ListPackageVersionAssets en la Referencia de comandos de la AWS CLI.

`list-package-version-dependencies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-package-version-dependencies`.

AWS CLI

Recuperación de las dependencias de la versión de un paquete

En el siguiente ejemplo de `list-package-version-dependencies`, se recuperan las dependencias de la versión 4.0.0 de un paquete npm denominado test-package.

```
aws codeartifact list-package-version-dependencies \
    --domain test-domain \
    --repo test-repo \
    --format npm \
    --package test-package \
    --package-version 4.0.0
```

Salida:

```
{
    "format": "npm",
    "package": "test-package",
    "version": "4.0.0",
    "versionRevision": "Ciqe5/9yicvkJT13b5/LdLpCyE6fqA7poa9qp+FilPs=",
    "dependencies": [
        {
            "namespace": "testns",
            "package": "testdep1",
            "dependencyType": "regular",
            "versionRequirement": "1.8.5"
        },
        {
            "namespace": "testns",
            "package": "testdep2",
            "dependencyType": "regular",
            "versionRequirement": "1.8.5"
        }
    ]
}
```

Para obtener más información, consulte View and update package version details and dependencies en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte ListPackageVersionDependencies en la Referencia de comandos de la AWS CLI.

`list-package-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-package-versions`.

AWS CLI

Generación de una lista de las versiones de un paquete

En el siguiente ejemplo de `list-package-versions`, se genera una lista de las versiones de un paquete denominado `kind-of`.

```
aws codeartifact list-package-versions \
    --package kind-of \
    --domain test-domain \
```

```
    --repository test-repo \
    --format npm
```

Salida:

```
{
    "defaultDisplayVersion": "1.0.1",
    "format": "npm",
    "package": "kind-of",
    "versions": [
        {
            "version": "1.0.1",
            "revision": "REVISION-SAMPLE-1-C7F4S5E9B772FC",
            "status": "Published"
        },
        {
            "version": "1.0.0",
            "revision": "REVISION-SAMPLE-2-C752BEEF6D2CFC",
            "status": "Published"
        },
        {
            "version": "0.1.2",
            "revision": "REVISION-SAMPLE-3-654S65A5C5E1FC",
            "status": "Published"
        },
        {
            "version": "0.1.1",
            "revision": "REVISION-SAMPLE-1-C7F4S5E9B772FC"",
            "status": "Published"
        },
        {
            "version": "0.1.0",
            "revision": "REVISION-SAMPLE-4-AF669139B772FC",
            "status": "Published"
        }
    ]
}
```

Para obtener más información, consulte List package versions en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte ListPackageVersions en la Referencia de comandos de la AWS CLI.

`list-packages`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-packages`.

AWS CLI

Generación de una lista de los paquetes de un repositorio

En el siguiente ejemplo de `list-packages`, se genera una lista de los paquetes de un repositorio denominado `test-repo` en un dominio denominado `test-domain`.

```
aws codeartifact list-packages \
    --domain test-domain \
    --repository test-repo
```

Salida:

```
{
    "packages": [
        {
            "format": "npm",
            "package": "lodash"
        }
        {
            "format": "python",
            "package": "test-package"
        }
    ]
}
```

Para obtener más información, consulte List package names en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte ListPackages en la Referencia de comandos de la AWS CLI.

`list-repositories-in-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-repositories-in-domain`.

AWS CLI

Generación de una lista de los repositorios de un dominio

En el siguiente ejemplo de `list-repositories-in-domain`, se obtiene un resumen de todos los repositorios del dominio test-domain.

```
aws codeartifact list-repositories-in-domain \
    --domain test-domain
```

Salida:

```
{
    "repositories": [
        {
            "name": "test-repo",
            "administratorAccount": "111122223333",
            "domainName": "test-domain",
            "domainOwner": "111122223333",
            "arn": "arn:aws:codeartifact:us-west-2:111122223333:repository/test-
domain/test-repo",
            "description": "This is a test repository."
        },
        {
            "name": "test-repo2",
            "administratorAccount": "111122223333",
            "domainName": "test-domain",
            "domainOwner": "111122223333",
            "arn": "arn:aws:codeartifact:us-west-2:111122223333:repository/test-
domain/test-repo2",
            "description": "This is a test repository."
        }
    ]
}
```

Para obtener más información, consulte List repositories en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte ListRepositoriesInDomain en la Referencia de comandos de la AWS CLI.

`list-repositories`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-repositories`.

AWS CLI

Generación de una lista de repositorios

En el siguiente ejemplo de `list-repositories`, se obtiene un resumen de todos los repositorios de un dominio que pertenece a la cuenta de AWS que realiza la llamada.

```
aws codeartifact list-repositories
```

Salida:

```
{
    "repositories": [
        {
            "name": "npm-store",
            "administratorAccount": "111122223333",
            "domainName": "my-domain",
            "domainOwner": "111122223333",
            "arn": "arn:aws:codeartifact:us-west-2:111122223333:repository/my-
domain/npm-store",
            "description": "Provides npm artifacts from npm, Inc."
        },
        {
            "name": "target-repo",
            "administratorAccount": "111122223333",
            "domainName": "my-domain",
            "domainOwner": "111122223333",
            "arn": "arn:aws:codeartifact:us-west-2:111122223333:repository/my-
domain/target-repo",
            "description": "test target repo"
        },
        {
            "name": "test-repo2",
            "administratorAccount": "111122223333",
            "domainName": "test-domain",
            "domainOwner": "111122223333",
            "arn": "arn:aws:codeartifact:us-west-2:111122223333:repository/test-
domain/test-repo2",
            "description": "This is a test repository."
        }
    ]
}
```

Para obtener más información, consulte List repositories en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte ListRepositories en la Referencia de comandos de la AWS CLI.

`login`

En el siguiente ejemplo de código, se muestra cómo utilizar `login`.

AWS CLI

Configuración de la autenticación en el repositorio con el comando login

En el siguiente ejemplo de `login`, se configura el administrador de paquetes npm con un repositorio denominado test-repo dentro de un dominio denominado test-domain.

```
aws codeartifact login \
    --domain test-domain \
    --repository test-repo \
    --tool npm
```

Salida:

```
Successfully configured npm to use AWS CodeArtifact repository https://test-
domain-111122223333.d.codeartifact.us-west-2.amazonaws.com/npm/test-repo/
Login expires in 12 hours at 2020-11-12 01:53:16-05:00
```

Para obtener más información, consulte Getting started with the AWS CLI en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte Login en la Referencia de comandos de la AWS CLI.

`put-domain-permissions-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-domain-permissions-policy`.

AWS CLI

Para asociar una política de permisos a un dominio

En el siguiente ejemplo de `put-domain-permissions-policy`, se asocia una política de permisos definida en el archivo policy.json a un dominio denominado test-domain.

```
aws codeartifact put-domain-permissions-policy \
    --domain test-domain \
    --policy-document file://PATH/TO/policy.json
```

Salida:

```
{
    "policy": {
        "resourceArn": "arn:aws:codeartifact:region-id:111122223333:domain/test-
domain",
        "document": "{ ...policy document content...}",
        "revision": "MQlyyTQRASRU3HB58gBtSDHXG7Q3hvxxxxxxx="
    }
}
```

Para obtener más información, consulte Set a domain policy en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte PutDomainPermissionsPolicy en la Referencia de comandos de la AWS CLI.

`put-repository-permissions-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-repository-permissions-policy`.

AWS CLI

Para asociar una política de permisos a un repositorio

En el siguiente ejemplo de `put-repository-permissions-policy`, se asocia una política de permisos definida en el archivo policy.json a un repositorio denominado test-repo.

```
aws codeartifact put-repository-permissions-policy \
    --domain test-domain \
    --repository test-repo \
    --policy-document file://PATH/TO/policy.json
```

Salida:

```
{
    "policy": {
        "resourceArn": "arn:aws:codeartifact:region-id:111122223333:repository/test-
domain/test-repo",
        "document": "{ ...policy document content...}",
        "revision": "MQlyyTQRASRU3HB58gBtSDHXG7Q3hvxxxxxxx="
    }
}
```

Para obtener más información, consulte Set a policy en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte PutRepositoryPermissionsPolicy en la Referencia de comandos de la AWS CLI.

`update-package-versions-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-package-versions-status`.

AWS CLI

Actualización del estado de la versión de un paquete

En el siguiente ejemplo de `update-package-versions-status`, se actualiza el estado de la versión 4.0.0 del paquete test-package a Archived.

```
aws codeartifact update-package-versions-status \
    --domain test-domain \
    --repo test-repo \
    --format npm \
    --package test-package \
    --versions 4.0.0 \
    --target-status Archived
```

Salida:

```
{
    "successfulVersions": {
        "4.0.0": {
            "revision": "Ciqe5/9yicvkJT13b5/LdLpCyE6fqA7poa9qp+FilPs=",
            "status": "Archived"
```

```
        }
    },
    "failedVersions": {}
}
```

Para obtener más información, consulte Update package version status en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte UpdatePackageVersionsStatus en la Referencia de comandos de la AWS CLI.

`update-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-repository`.

AWS CLI

Actualización de un repositorio

En el siguiente ejemplo de `update-repository`, se actualiza la descripción de un repositorio denominado test-repo en un dominio denominado test-domain a “this is an updated description”.

```
aws codeartifact update-repository \
    --domain test-domain \
    --repository test-repo \
    --description "this is an updated description"
```

Salida:

```
{
    "repository": {
        "name": "test-repo",
        "administratorAccount": "111122223333",
        "domainName": "test-domain",
        "domainOwner": "111122223333",
        "arn": "arn:aws:codeartifact:us-west-2:111122223333:repository/test-domain/
test-repo",
        "description": "this is an updated description",
        "upstreams": [],
        "externalConnections": []
    }
}
```

Para obtener más información, consulte View or modify a repository configuration en la Guía del usuario de AWS CodeArtifact.

- Para obtener información sobre la API, consulte UpdateRepository en la Referencia de comandos de la AWS CLI.

Ejemplos de CodeBuild que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar situaciones comunes mediante la AWS Command Line Interface con CodeBuild.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`batch-delete-builds`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-delete-builds`.

AWS CLI

Eliminación de compilaciones en AWS CodeBuild.

En el siguiente ejemplo de `batch-delete-builds`, se eliminan las compilaciones de CodeBuild con los ID especificados.

```
aws codebuild batch-delete-builds --ids my-build-project-one:a1b2c3d4-5678-9012-abcd-11111EXAMPLE my-build-project-two:a1b2c3d4-5678-9012-abcd-22222EXAMPLE
```

Salida:

```
{
    "buildsNotDeleted": [
```

```
        {
            "id": "arn:aws:codebuild:us-west-2:123456789012:build/my-build-project-
one:a1b2c3d4-5678-9012-abcd-11111EXAMPLE",
            "statusCode": "BUILD_IN_PROGRESS"
        }
    ],
    "buildsDeleted": [
        "arn:aws:codebuild:us-west-2:123456789012:build/my-build-project-
two:a1b2c3d4-5678-9012-abcd-22222EXAMPLE"
    ]
}
```

Para obtener más información, consulte Delete Builds (AWS CLI) en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte BatchDeleteBuilds en la Referencia de comandos de la AWS CLI.

`batch-get-build-batches`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-build-batches`.

AWS CLI

Visualización de los detalles de las compilaciones en AWS CodeBuild.

En el siguiente ejemplo de `batch-get-build-batches`, se obtiene información sobre los lotes de compilación en CodeBuild con los ID especificados.

```
aws codebuild batch-get-build-batches \
    --ids codebuild-demo-project:e9c4f4df-3f43-41d2-ab3a-60fe2EXAMPLE
```

Salida:

```
{
    "buildBatches": [
        {
            "id": "codebuild-demo-project:e9c4f4df-3f43-41d2-ab3a-60fe2EXAMPLE",
            "arn": "arn:aws:codebuild:us-west-2:123456789012:build-batch/codebuild-
demo-project:e9c4f4df-3f43-41d2-ab3a-60fe2EXAMPLE",
            "startTime": "2020-11-03T21:52:20.775000+00:00",
            "endTime": "2020-11-03T21:56:59.784000+00:00",
            "currentPhase": "SUCCEEDED",
```

```
            "buildBatchStatus": "SUCCEEDED",
            "resolvedSourceVersion": "0a6546f68309560d08a310daac92314c4d378f6b",
            "projectName": "codebuild-demo-project",
            "phases": [
                {
                    "phaseType": "SUBMITTED",
                    "phaseStatus": "SUCCEEDED",
                    "startTime": "2020-11-03T21:52:20.775000+00:00",
                    "endTime": "2020-11-03T21:52:20.976000+00:00",
                    "durationInSeconds": 0
                },
                {
                    "phaseType": "DOWNLOAD_BATCHSPEC",
                    "phaseStatus": "SUCCEEDED",
                    "startTime": "2020-11-03T21:52:20.976000+00:00",
                    "endTime": "2020-11-03T21:52:57.401000+00:00",
                    "durationInSeconds": 36
                },
                {
                    "phaseType": "IN_PROGRESS",
                    "phaseStatus": "SUCCEEDED",
                    "startTime": "2020-11-03T21:52:57.401000+00:00",
                    "endTime": "2020-11-03T21:56:59.751000+00:00",
                    "durationInSeconds": 242
                },
                {
                    "phaseType": "COMBINE_ARTIFACTS",
                    "phaseStatus": "SUCCEEDED",
                    "startTime": "2020-11-03T21:56:59.751000+00:00",
                    "endTime": "2020-11-03T21:56:59.784000+00:00",
                    "durationInSeconds": 0
                },
                {
                    "phaseType": "SUCCEEDED",
                    "startTime": "2020-11-03T21:56:59.784000+00:00"
                }
            ],
            "source": {
                "type": "GITHUB",
                "location": "https://github.com/my-repo/codebuild-demo-project.git",
                "gitCloneDepth": 1,
                "gitSubmodulesConfig": {
                    "fetchSubmodules": false
                },
```

```
                "reportBuildStatus": false,
                "insecureSsl": false
            },
            "secondarySources": [],
            "secondarySourceVersions": [],
            "artifacts": {
                "location": ""
            },
            "secondaryArtifacts": [],
            "cache": {
                "type": "NO_CACHE"
            },
            "environment": {
                "type": "LINUX_CONTAINER",
                "image": "aws/codebuild/amazonlinux2-x86_64-standard:3.0",
                "computeType": "BUILD_GENERAL1_SMALL",
                "environmentVariables": [],
                "privilegedMode": false,
                "imagePullCredentialsType": "CODEBUILD"
            },
            "logConfig": {
                "cloudWatchLogs": {
                    "status": "ENABLED"
                },
                "s3Logs": {
                    "status": "DISABLED",
                    "encryptionDisabled": false
                }
            },
            "buildTimeoutInMinutes": 60,
            "queuedTimeoutInMinutes": 480,
            "complete": true,
            "initiator": "Strohm",
            "encryptionKey": "arn:aws:kms:us-west-2:123456789012:alias/aws/s3",
            "buildBatchNumber": 6,
            "buildBatchConfig": {
                "serviceRole": "arn:aws:iam::123456789012:role/service-role/
codebuild-demo-project",
                "restrictions": {
                    "maximumBuildsAllowed": 100
                },
                "timeoutInMins": 480
            },
            "buildGroups": [
```

```
                {
                    "identifier": "DOWNLOAD_SOURCE",
                    "ignoreFailure": false,
                    "currentBuildSummary": {
                        "arn": "arn:aws:codebuild:us-west-2:123456789012:build/
codebuild-demo-project:379737d8-bc35-48ec-97fd-776d27545315",
                        "requestedOn": "2020-11-03T21:52:21.394000+00:00",
                        "buildStatus": "SUCCEEDED",
                        "primaryArtifact": {
                            "type": "no_artifacts",
                            "identifier": "DOWNLOAD_SOURCE"
                        },
                        "secondaryArtifacts": []
                    }
                },
                {
                    "identifier": "linux_small",
                    "dependsOn": [],
                    "ignoreFailure": false,
                    "currentBuildSummary": {
                        "arn": "arn:aws:codebuild:us-west-2:123456789012:build/
codebuild-demo-project:dd785171-ed84-4bb6-8ede-ceeb86e54bdb",
                        "requestedOn": "2020-11-03T21:52:57.604000+00:00",
                        "buildStatus": "SUCCEEDED",
                        "primaryArtifact": {
                            "type": "no_artifacts",
                            "identifier": "linux_small"
                        },
                        "secondaryArtifacts": []
                    }
                },
                {
                    "identifier": "linux_medium",
                    "dependsOn": [
                        "linux_small"
                    ],
                    "ignoreFailure": false,
                    "currentBuildSummary": {
                        "arn": "arn:aws:codebuild:us-west-2:123456789012:build/
codebuild-demo-project:97cf7bd4-5313-4786-8243-4aef350a1267",
                        "requestedOn": "2020-11-03T21:54:18.474000+00:00",
                        "buildStatus": "SUCCEEDED",
                        "primaryArtifact": {
                            "type": "no_artifacts",
```

```
                            "identifier": "linux_medium"
                        },
                        "secondaryArtifacts": []
                    }
                },
                {
                    "identifier": "linux_large",
                    "dependsOn": [
                        "linux_medium"
                    ],
                    "ignoreFailure": false,
                    "currentBuildSummary": {
                        "arn": "arn:aws:codebuild:us-west-2:123456789012:build/
codebuild-demo-project:60a194cd-0d03-4337-9db1-d41476a17d27",
                        "requestedOn": "2020-11-03T21:55:39.203000+00:00",
                        "buildStatus": "SUCCEEDED",
                        "primaryArtifact": {
                            "type": "no_artifacts",
                            "identifier": "linux_large"
                        },
                        "secondaryArtifacts": []
                    }
                }
            ]
        }
    ],
    "buildBatchesNotFound": []
}
```

Para obtener más información, consulte Batch builds in AWS CodeBuild <https://docs.aws.amazon.com/codebuild/latest/userguide/batch-build.html>)__ en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte BatchGetBuildBatches en la Referencia de comandos de la AWS CLI.

`batch-get-builds`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-builds`.

AWS CLI

Visualización de los detalles de las compilaciones en AWS CodeBuild.

En el siguiente ejemplo de `batch-get-builds`, se obtiene información sobre las compilaciones en CodeBuild con los ID especificados.

```
aws codebuild batch-get-builds --ids codebuild-demo-project:e9c4f4df-3f43-41d2-ab3a-60fe2EXAMPLE codebuild-demo-project:815e755f-bade-4a7e-80f0-efe51EXAMPLE
```

Salida:

```
{
    "buildsNotFound": [],
    "builds": [
        {
            "artifacts": {
                "md5sum": "0e95edf915048a0c22efe6d139fff837",
                "location": "arn:aws:s3:::codepipeline-us-west-2-820783811474/
CodeBuild-Python-Pip/BuildArtif/6DJsqQa",
                "encryptionDisabled": false,
                "sha256sum":
 "cfa0df33a090966a737f64ae4fe498969fdc842a0c9aec540bf93c37ac0d05a2"
            },
            "logs": {
                "cloudWatchLogs": {
                    "status": "ENABLED"
                },
                "s3Logs": {
                    "status": "DISABLED"
                },
                "streamName": "46472baf-8f6b-43c2-9255-b3b963af2732",
                "groupName": "/aws/codebuild/codebuild-demo-project",
                "deepLink": "https://console.aws.amazon.com/cloudwatch/
home?region=us-west-2#logEvent:group=/aws/codebuild/codebuild-demo-
project;stream=46472baf-8f6b-43c2-9255-b3b963af2732"
            },
            "timeoutInMinutes": 60,
            "environment": {
                "privilegedMode": false,
                "computeType": "BUILD_GENERAL1_MEDIUM",
                "image": "aws/codebuild/windows-base:1.0",
                "environmentVariables": [],
                "type": "WINDOWS_CONTAINER"
            },
            "projectName": "codebuild-demo-project",
            "buildComplete": true,
```

```
            "source": {
                "gitCloneDepth": 1,
                "insecureSsl": false,
                "type": "CODEPIPELINE"
            },
            "buildStatus": "SUCCEEDED",
            "secondaryArtifacts": [],
            "phases": [
                {
                    "durationInSeconds": 0,
                    "startTime": 1548717462.122,
                    "phaseType": "SUBMITTED",
                    "endTime": 1548717462.484,
                    "phaseStatus": "SUCCEEDED"
                },
                {
                    "durationInSeconds": 0,
                    "startTime": 1548717462.484,
                    "phaseType": "QUEUED",
                    "endTime": 1548717462.775,
                    "phaseStatus": "SUCCEEDED"
                },
                {
                    "durationInSeconds": 34,
                    "endTime": 1548717496.909,
                    "contexts": [
                        {
                            "statusCode": "",
                            "message": ""
                        }
                    ],
                    "startTime": 1548717462.775,
                    "phaseType": "PROVISIONING",
                    "phaseStatus": "SUCCEEDED"
                },
                {
                    "durationInSeconds": 15,
                    "endTime": 1548717512.555,
                    "contexts": [
                        {
                            "statusCode": "",
                            "message": ""
                        }
                    ],
```

```
            "startTime": 1548717496.909,
            "phaseType": "DOWNLOAD_SOURCE",
            "phaseStatus": "SUCCEEDED"
        },
        {
            "durationInSeconds": 0,
            "endTime": 1548717512.734,
            "contexts": [
                {
                    "statusCode": "",
                    "message": ""
                }
            ],
            "startTime": 1548717512.555,
            "phaseType": "INSTALL",
            "phaseStatus": "SUCCEEDED"
        },
        {
            "durationInSeconds": 0,
            "endTime": 1548717512.924,
            "contexts": [
                {
                    "statusCode": "",
                    "message": ""
                }
            ],
            "startTime": 1548717512.734,
            "phaseType": "PRE_BUILD",
            "phaseStatus": "SUCCEEDED"
        },
        {
            "durationInSeconds": 9,
            "endTime": 1548717522.254,
            "contexts": [
                {
                    "statusCode": "",
                    "message": ""
                }
            ],
            "startTime": 1548717512.924,
            "phaseType": "BUILD",
            "phaseStatus": "SUCCEEDED"
        },
        {
```

```
                    "durationInSeconds": 3,
                    "endTime": 1548717525.498,
                    "contexts": [
                        {
                            "statusCode": "",
                            "message": ""
                        }
                    ],
                    "startTime": 1548717522.254,
                    "phaseType": "POST_BUILD",
                    "phaseStatus": "SUCCEEDED"
                },
                {
                    "durationInSeconds": 9,
                    "endTime": 1548717534.646,
                    "contexts": [
                        {
                            "statusCode": "",
                            "message": ""
                        }
                    ],
                    "startTime": 1548717525.498,
                    "phaseType": "UPLOAD_ARTIFACTS",
                    "phaseStatus": "SUCCEEDED"
                },
                {
                    "durationInSeconds": 2,
                    "endTime": 1548717536.846,
                    "contexts": [
                        {
                            "statusCode": "",
                            "message": ""
                        }
                    ],
                    "startTime": 1548717534.646,
                    "phaseType": "FINALIZING",
                    "phaseStatus": "SUCCEEDED"
                },
                {
                    "startTime": 1548717536.846,
                    "phaseType": "COMPLETED"
                }
            ],
            "startTime": 1548717462.122,
```

```
            "encryptionKey": "arn:aws:kms:us-west-2:123456789012:alias/aws/s3",
            "initiator": "codepipeline/CodeBuild-Pipeline",
            "secondarySources": [],
            "serviceRole": "arn:aws:iam::123456789012:role/service-role/my-
codebuild-service-role",
            "currentPhase": "COMPLETED",
            "id": "codebuild-demo-project:e9c4f4df-3f43-41d2-ab3a-60fe2EXAMPLE",
            "cache": {
                "type": "NO_CACHE"
            },
            "sourceVersion": "arn:aws:s3:::codepipeline-us-west-2-820783811474/
CodeBuild-Python-Pip/SourceArti/1TspnN3.zip",
            "endTime": 1548717536.846,
            "arn": "arn:aws:codebuild:us-west-2:123456789012:build/codebuild-demo-
project:e9c4f4df-3f43-41d2-ab3a-60fe2EXAMPLE",
            "queuedTimeoutInMinutes": 480,
            "resolvedSourceVersion": "f2194c1757bbdcb0f8f229254a4b3c8b27d43e0b"
        },
        {
            "artifacts": {
                "md5sum": "",
                "overrideArtifactName": false,
                "location": "arn:aws:s3:::my-artifacts/codebuild-demo-project",
                "encryptionDisabled": false,
                "sha256sum": ""
            },
            "logs": {
                "cloudWatchLogs": {
                    "status": "ENABLED"
                },
                "s3Logs": {
                    "status": "DISABLED"
                },
                "streamName": "4dea3ca4-20ec-4898-b22a-a9eb9292775d",
                "groupName": "/aws/codebuild/codebuild-demo-project",
                "deepLink": "https://console.aws.amazon.com/cloudwatch/
home?region=us-west-2#logEvent:group=/aws/codebuild/codebuild-demo-
project;stream=4dea3ca4-20ec-4898-b22a-a9eb9292775d"
            },
            "timeoutInMinutes": 60,
            "environment": {
                "privilegedMode": false,
                "computeType": "BUILD_GENERAL1_MEDIUM",
                "image": "aws/codebuild/windows-base:1.0",
```

```
            "environmentVariables": [],
            "type": "WINDOWS_CONTAINER"
        },
        "projectName": "codebuild-demo-project",
        "buildComplete": true,
        "source": {
            "gitCloneDepth": 1,
            "location": "https://github.com/my-repo/codebuild-demo-project.git",
            "insecureSsl": false,
            "reportBuildStatus": false,
            "type": "GITHUB"
        },
        "buildStatus": "SUCCEEDED",
        "secondaryArtifacts": [],
        "phases": [
            {
                "durationInSeconds": 0,
                "startTime": 1548716241.89,
                "phaseType": "SUBMITTED",
                "endTime": 1548716242.241,
                "phaseStatus": "SUCCEEDED"
            },
            {
                "durationInSeconds": 0,
                "startTime": 1548716242.241,
                "phaseType": "QUEUED",
                "endTime": 1548716242.536,
                "phaseStatus": "SUCCEEDED"
            },
            {
                "durationInSeconds": 33,
                "endTime": 1548716276.171,
                "contexts": [
                    {
                        "statusCode": "",
                        "message": ""
                    }
                ],
                "startTime": 1548716242.536,
                "phaseType": "PROVISIONING",
                "phaseStatus": "SUCCEEDED"
            },
            {
                "durationInSeconds": 15,
```

```
            "endTime": 1548716291.809,
            "contexts": [
                {
                    "statusCode": "",
                    "message": ""
                }
            ],
            "startTime": 1548716276.171,
            "phaseType": "DOWNLOAD_SOURCE",
            "phaseStatus": "SUCCEEDED"
        },
        {
            "durationInSeconds": 0,
            "endTime": 1548716291.993,
            "contexts": [
                {
                    "statusCode": "",
                    "message": ""
                }
            ],
            "startTime": 1548716291.809,
            "phaseType": "INSTALL",
            "phaseStatus": "SUCCEEDED"
        },
        {
            "durationInSeconds": 0,
            "endTime": 1548716292.191,
            "contexts": [
                {
                    "statusCode": "",
                    "message": ""
                }
            ],
            "startTime": 1548716291.993,
            "phaseType": "PRE_BUILD",
            "phaseStatus": "SUCCEEDED"
        },
        {
            "durationInSeconds": 9,
            "endTime": 1548716301.622,
            "contexts": [
                {
                    "statusCode": "",
                    "message": ""
```

```
                    }
                ],
                "startTime": 1548716292.191,
                "phaseType": "BUILD",
                "phaseStatus": "SUCCEEDED"
            },
            {
                "durationInSeconds": 3,
                "endTime": 1548716304.783,
                "contexts": [
                    {
                        "statusCode": "",
                        "message": ""
                    }
                ],
                "startTime": 1548716301.622,
                "phaseType": "POST_BUILD",
                "phaseStatus": "SUCCEEDED"
            },
            {
                "durationInSeconds": 8,
                "endTime": 1548716313.775,
                "contexts": [
                    {
                        "statusCode": "",
                        "message": ""
                    }
                ],
                "startTime": 1548716304.783,
                "phaseType": "UPLOAD_ARTIFACTS",
                "phaseStatus": "SUCCEEDED"
            },
            {
                "durationInSeconds": 2,
                "endTime": 1548716315.935,
                "contexts": [
                    {
                        "statusCode": "",
                        "message": ""
                    }
                ],
                "startTime": 1548716313.775,
                "phaseType": "FINALIZING",
                "phaseStatus": "SUCCEEDED"
```

```
                },
                {
                    "startTime": 1548716315.935,
                    "phaseType": "COMPLETED"
                }
            ],
            "startTime": 1548716241.89,
            "secondarySourceVersions": [],
            "initiator": "my-codebuild-project",
            "arn": "arn:aws:codebuild:us-west-2:123456789012:build/codebuild-demo-
project:815e755f-bade-4a7e-80f0-efe51EXAMPLE",
            "encryptionKey": "arn:aws:kms:us-west-2:123456789012:alias/aws/s3",
            "serviceRole": "arn:aws:iam::123456789012:role/service-role/my-
codebuild-service-role",
            "currentPhase": "COMPLETED",
            "id": "codebuild-demo-project:815e755f-bade-4a7e-80f0-efe51EXAMPLE",
            "cache": {
                "type": "NO_CACHE"
            },
            "endTime": 1548716315.935,
            "secondarySources": [],
            "queuedTimeoutInMinutes": 480,
            "resolvedSourceVersion": "f2194c1757bbdcb0f8f229254a4b3c8b27d43e0b"
        }
    ]
}
```

Para obtener más información, consulte View Build Details (AWS CLI) en la Guía del usuario de AWS CodeBuild.

- Para obtener información de la API, consulte BatchGetBuilds en la Referencia de comandos de la AWS CLI.

`batch-get-projects`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-projects`.

AWS CLI

Obtención de una lista de nombres de proyectos de compilación de AWS CodeBuild

En el siguiente ejemplo de `batch-get-projects` se obtiene una lista de proyectos de compilación de CodeBuild especificados por nombre.

```
aws codebuild batch-get-projects --names codebuild-demo-project codebuild-demo-
project2 my-other-demo-project
```

En el resultado anterior, la matriz `projectsNotFound` indica todos los nombres de proyectos de compilación que se han especificado, pero no se han encontrado. La matriz `projects` muestra los detalles de cada proyecto de compilación donde se encontró información.


```
{
    "projectsNotFound": [],
    "projects": [
        {
            "encryptionKey": "arn:aws:kms:us-west-2:123456789012:alias/aws/s3",
            "name": "codebuild-demo-project2",
            "queuedTimeoutInMinutes": 480,
            "timeoutInMinutes": 60,
            "source": {
                "buildspec": "version: 0.2\n\n#env:\n  #variables:\n     # key:
 \"value\"\n     # key: \"value\"\n  #parameter-store:\n     # key: \"value\"\n
  # key:\"value\"\n\nphases:\n  #install:\n    #commands:\n      # - command\n
  # - command\n  #pre_build:\n    #commands:\n      # - command\n      # - command
\n  build:\n    commands:\n      # - command\n      # - command\n  #post_build:\n
   #commands:\n      # - command\n      # - command\n#artifacts:\n  #files:\n    #
 - location\n    # - location\n  #name: $(date +%Y-%m-%d)\n  #discard-paths: yes\n
 #base-directory: location\n#cache:\n  #paths:\n    # - paths",
                "type": "NO_SOURCE",
                "insecureSsl": false,
                "gitCloneDepth": 1
            },
            "artifacts": {
                "type": "NO_ARTIFACTS"
            },
            "badge": {
                "badgeEnabled": false
            },
            "lastModified": 1540588091.108,
            "created": 1540588091.108,
            "arn": "arn:aws:codebuild:us-west-2:123456789012:project/test-for-
sample",
            "secondarySources": [],
            "secondaryArtifacts": [],
            "cache": {
                "type": "NO_CACHE"
```

```
            },
            "serviceRole": "arn:aws:iam::123456789012:role/service-role/my-test-
role",
            "environment": {
                "image": "aws/codebuild/java:openjdk-8",
                "privilegedMode": true,
                "type": "LINUX_CONTAINER",
                "computeType": "BUILD_GENERAL1_SMALL",
                "environmentVariables": []
            },
            "tags": []
        },
        {
            "encryptionKey": "arn:aws:kms:us-west-2:123456789012:alias/aws/s3",
            "name": "my-other-demo-project",
            "queuedTimeoutInMinutes": 480,
            "timeoutInMinutes": 60,
            "source": {
                "location": "https://github.com/iversonic/codedeploy-sample.git",
                "reportBuildStatus": false,
                "buildspec": "buildspec.yml",
                "insecureSsl": false,
                "gitCloneDepth": 1,
                "type": "GITHUB",
                "auth": {
                    "type": "OAUTH"
                }
            },
            "artifacts": {
                "type": "NO_ARTIFACTS"
            },
            "badge": {
                "badgeEnabled": false
            },
            "lastModified": 1523401711.73,
            "created": 1523401711.73,
            "arn": "arn:aws:codebuild:us-west-2:123456789012:project/Project2",
            "cache": {
                "type": "NO_CACHE"
            },
            "serviceRole": "arn:aws:iam::123456789012:role/service-role/codebuild-
Project2-service-role",
            "environment": {
                "image": "aws/codebuild/nodejs:4.4.7",
```

```
                "privilegedMode": false,
                "type": "LINUX_CONTAINER",
                "computeType": "BUILD_GENERAL1_SMALL",
                "environmentVariables": []
            },
            "tags": []
        }
    ]
}
```

Para obtener más información, consulte View a Build Project's Details (AWS CLI) en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre de la API, consulte BatchGetProjects en la Referencia de comandos de la AWS CLI

`batch-get-report-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-report-groups`.

AWS CLI

Obtención de información sobre uno o varios grupos de informes en AWS CodeBuild.

En el siguiente ejemplo de `batch-get-report-groups` se obtiene información sobre el grupo de informes con el ARN especificado.

```
aws codebuild batch-get-report-groups \
    --report-group-arns arn:aws:codebuild:<region-ID>:<user-ID>:report-group/
<report-group-name>
```

Salida:

```
{
    "reportGroups": [
        {
            "arn": "arn:aws:codebuild:<region-ID>:<user-ID>:report-group/<report-
group-name>",
            "name": "report-group-name",
            "type": "TEST",
            "exportConfig": {
                "exportConfigType": "NO_EXPORT"
            },
```

```
            "created": "2020-10-01T18:04:08.466000+00:00",
            "lastModified": "2020-10-01T18:04:08.466000+00:00",
            "tags": []
        }
    ],
    "reportGroupsNotFound": []
}
```

Para obtener más información, consulte Working with report groups en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte BatchGetReportGroups en la Referencia de comandos de la AWS CLI.

`batch-get-reports`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-reports`.

AWS CLI

Obtención de información sobre uno o varios informes en AWS CodeBuild.

En el siguiente ejemplo de `batch-get-reports` se obtiene información sobre los informes con los ARN especificados.

```
aws codebuild batch-get-reports \
    --report-arns arn:aws:codebuild:<region-ID>:<user-ID>:report/<report-group-name>:<report 1 ID> arn:aws:codebuild:<region-ID>:<user-ID>:report/<report-group-name>:<report 2 ID>
```

Salida:

```
{
    "reports": [
        {
            "arn": "arn:aws:codebuild:<region-ID>:<user-ID>:report/<report-group-name>:<report 1 ID>",
            "type": "TEST",
            "name": "<report-group-name>",
            "reportGroupArn": "arn:aws:codebuild:<region-ID>:<user-ID>:report-group/<report-group-name>",
            "executionId": "arn:aws:codebuild:<region-ID>:<user-ID>:build/test-reports:<ID>",
```

```
            "status": "FAILED",
            "created": "2020-10-01T11:25:22.531000-07:00",
            "expired": "2020-10-31T11:25:22-07:00",
            "exportConfig": {
                "exportConfigType": "NO_EXPORT"
            },
            "truncated": false,
            "testSummary": {
                "total": 28,
                "statusCounts": {
                    "ERROR": 5,
                    "FAILED": 1,
                    "SKIPPED": 4,
                    "SUCCEEDED": 18,
                    "UNKNOWN": 0
                },
                "durationInNanoSeconds": 94000000
            }
        },
        {
            "arn": "arn:aws:codebuild:<region-ID>:<user-ID>:report/<report-group-
name>:<report 2 ID>",
            "type": "TEST",
            "name": "<report-group-name>",
            "reportGroupArn": "arn:aws:codebuild:<region-ID>:<user-ID>:report-group/
<report-group-name>",
            "executionId": "arn:aws:codebuild:<region-ID>:<user-ID>:build/test-
reports:<ID>",
            "status": "FAILED",
            "created": "2020-10-01T11:13:05.816000-07:00",
            "expired": "2020-10-31T11:13:05-07:00",
            "exportConfig": {
                "exportConfigType": "NO_EXPORT"
            },
            "truncated": false,
            "testSummary": {
                "total": 28,
                "statusCounts": {
                    "ERROR": 5,
                    "FAILED": 1,
                    "SKIPPED": 4,
                    "SUCCEEDED": 18,
                    "UNKNOWN": 0
                },
```

```
                "durationInNanoSeconds": 94000000
            }
        }
    ],
    "reportsNotFound": []
}
```

Para obtener más información, consulte Working with reports en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte BatchGetReports en la Referencia de comandos de la AWS CLI.

`create-project`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-project`.

AWS CLI

Ejemplo 1: Creación de un proyecto de compilación de AWS CodeBuild

En el siguiente ejemplo `create-project` se crea un proyecto de compilación de CodeBuild con archivos de origen de un bucket de S3

```
aws codebuild create-project \
    --name "my-demo-project" \
    --source "{\"type\": \"S3\",\"location\": \"codebuild-us-west-2-123456789012-
input-bucket/my-source.zip\"}" \
    --artifacts {"\"type\": \"S3\",\"location\": \"codebuild-us-west-2-123456789012-
output-bucket\""} \
    --environment "{\"type\": \"LINUX_CONTAINER\",\"image\": \"aws/codebuild/
standard:1.0\",\"computeType\": \"BUILD_GENERAL1_SMALL\"}" \
    --service-role "arn:aws:iam::123456789012:role/service-role/my-codebuild-
service-role"
```

Salida:

```
{
    "project": {
        "arn": "arn:aws:codebuild:us-west-2:123456789012:project/my-demo-project",
        "name": "my-cli-demo-project",
        "encryptionKey": "arn:aws:kms:us-west-2:123456789012:alias/aws/s3",
```

```
        "serviceRole": "arn:aws:iam::123456789012:role/service-role/my-codebuild-
service-role",
        "lastModified": 1556839783.274,
        "badge": {
            "badgeEnabled": false
        },
        "queuedTimeoutInMinutes": 480,
        "environment": {
            "image": "aws/codebuild/standard:1.0",
            "computeType": "BUILD_GENERAL1_SMALL",
            "type": "LINUX_CONTAINER",
            "imagePullCredentialsType": "CODEBUILD",
            "privilegedMode": false,
            "environmentVariables": []
        },
        "artifacts": {
            "location": "codebuild-us-west-2-123456789012-output-bucket",
            "name": "my-cli-demo-project",
            "namespaceType": "NONE",
            "type": "S3",
            "packaging": "NONE",
            "encryptionDisabled": false
        },
        "source": {
            "type": "S3",
            "location": "codebuild-us-west-2-123456789012-input-bucket/my-
source.zip",
            "insecureSsl": false
        },
        "timeoutInMinutes": 60,
        "cache": {
            "type": "NO_CACHE"
        },
        "created": 1556839783.274
    }
}
```

Ejemplo 2: Creación de un proyecto de compilación de AWS CodeBuild utilizando un archivo de entrada JSON para los parámetros

En el siguiente ejemplo `create-project`, se crea un proyecto de compilación de CodeBuild pasando todos los parámetros necesarios a un archivo de entrada JSON. Cree la plantilla del archivo de entrada ejecutando el comando solo con `--generate-cli-skeleton parameter`.

```
aws codebuild create-project --cli-input-json file://create-project.json
```

El archivo JSON de entrada `create-project.json` contiene lo siguiente:

```
{
    "name": "codebuild-demo-project",
    "source": {
        "type": "S3",
        "location": "codebuild-region-ID-account-ID-input-bucket/MessageUtil.zip"
    },
    "artifacts": {
        "type": "S3",
        "location": "codebuild-region-ID-account-ID-output-bucket"
    },
    "environment": {
        "type": "LINUX_CONTAINER",
        "image": "aws/codebuild/standard:1.0",
        "computeType": "BUILD_GENERAL1_SMALL"
    },
    "serviceRole": "serviceIAMRole"
}
```

Salida:

```
{
    "project": {
        "name": "codebuild-demo-project",
        "serviceRole": "serviceIAMRole",
        "tags": [],
        "artifacts": {
            "packaging": "NONE",
            "type": "S3",
            "location": "codebuild-region-ID-account-ID-output-bucket",
            "name": "message-util.zip"
        },
        "lastModified": 1472661575.244,
        "timeoutInMinutes": 60,
        "created": 1472661575.244,
        "environment": {
            "computeType": "BUILD_GENERAL1_SMALL",
            "image": "aws/codebuild/standard:1.0",
            "type": "LINUX_CONTAINER",
```

```
            "environmentVariables": []
        },
        "source": {
            "type": "S3",
            "location": "codebuild-region-ID-account-ID-input-bucket/
MessageUtil.zip"
        },
        "encryptionKey": "arn:aws:kms:region-ID:account-ID:alias/aws/s3",
        "arn": "arn:aws:codebuild:region-ID:account-ID:project/codebuild-demo-
project"
    }
}
```

Para obtener más información, consulte Creación de un proyecto de compilación (AWS CLI) en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte CreateProject en la Referencia de comandos de la AWS CLI.

`create-report-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-report-group`.

AWS CLI

Creación de un grupo de informes en AWS CodeBuild

El siguiente ejemplo de `create-report-group`, crea un nuevo grupo de informes.

```
aws codebuild create-report-group \
    --cli-input-json file://create-report-group-source.json
```

Contenido de create-report-group-source.json:

```
{
    "name": "cli-created-report-group",
    "type": "TEST",
    "exportConfig": {
        "exportConfigType": "S3",
        "s3Destination": {
            "bucket": "amzn-s3-demo-bucket",
            "path": "",
            "packaging": "ZIP",
```

```
            "encryptionDisabled": true
        }
    }
}
```

Salida:

```
{
    "reportGroup": {
        "arn": "arn:aws:codebuild:<region-ID>:<user-ID>:report-group/cli-created-
report-group",
        "name": "cli-created-report-group",
        "type": "TEST",
        "exportConfig": {
            "exportConfigType": "S3",
            "s3Destination": {
                "bucket": "amzn-s3-demo-bucket",
                "path": "",
                "packaging": "ZIP",
                "encryptionDisabled": true
            }
        },
        "created": 1602020026.775,
        "lastModified": 1602020026.775
    }
}
```

Para obtener más información, consulte Working with report groups en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte CreateReportGroup en la Referencia de comandos de la AWS CLI.

`create-webhook`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-webhook`.

AWS CLI

Creación de filtros de webhook para un proyecto de AWS CodeBuild

En el siguiente ejemplo de `create-webhook`, se crea un webhook para un proyecto de CodeBuild denominado `my-project` y que tiene dos grupos de filtros. El primer grupo de

filtros especifica las solicitudes de extracción que se crean, actualizan o vuelven a abrirse en ramificaciones con nombres de referencia de Git que coinciden con la expresión regular `^refs/heads/master$` y las referencias de encabezado que coinciden con `^refs/heads/myBranch$`. El segundo grupo de filtros especifica solicitudes de inserción en ramificaciones con nombres de referencia de Git que no coinciden con la expresión regular `^refs/heads/myBranch$`.

```
aws codebuild create-webhook \
    --project-name my-project \
    --filter-groups "[[{\"type\":\"EVENT\",\"pattern\":\"PULL_REQUEST_CREATED,
 PULL_REQUEST_UPDATED, PULL_REQUEST_REOPENED\"},{\"type\":\"HEAD_REF\",\"pattern
\":\"^refs/heads/myBranch$\",\"excludeMatchedPattern\":true},{\"type\":\"BASE_REF
\",\"pattern\":\"^refs/heads/master$\",\"excludeMatchedPattern\":true}],[{\"type\":
\"EVENT\",\"pattern\":\"PUSH\"},{\"type\":\"HEAD_REF\",\"pattern\":\"^refs/heads/
myBranch$\",\"excludeMatchedPattern\":true}]]"
```

Salida:

```
{
    "webhook": {
        "payloadUrl": "https://codebuild.us-west-2.amazonaws.com/webhooks?
t=eyJlbmNyeXB0ZWREYXRhIjoiVVl5MGtoeGRwSzZFRXl2Wnh4bld1Z0tKZ291TVpQNEtFamQ3RDlDYWpRaGIreVFrdm
        "url": "https://api.github.com/repos/iversonic/codedeploy-sample/
hooks/105190656",
        "lastModifiedSecret": 1556311319.069,
        "filterGroups": [
            [
                {
                    "type": "EVENT",
                    "pattern": "PULL_REQUEST_CREATED, PULL_REQUEST_UPDATED,
 PULL_REQUEST_REOPENED",
                    "excludeMatchedPattern": false
                },
                {
                    "type": "HEAD_REF",
                    "pattern": "refs/heads/myBranch$",
                    "excludeMatchedPattern": true
                },
                {
                    "type": "BASE_REF",
                    "pattern": "refs/heads/master$",
                    "excludeMatchedPattern": true
                }
```

```
            ],
            [
                {
                    "type": "EVENT",
                    "pattern": "PUSH",
                    "excludeMatchedPattern": false
                },
                {
                    "type": "HEAD_REF",
                    "pattern": "refs/heads/myBranch$",
                    "excludeMatchedPattern": true
                }
            ]
        ]
    }
}
```

Para obtener más información, consulte Filter GitHub Webhook Events (SDK) en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte CreateWebhook en la Referencia de comandos de la AWS CLI.

`delete-build-batch`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-build-batch`.

AWS CLI

Eliminación de una compilación por lotes en AWS CodeBuild

En el siguiente ejemplo de `delete-build-batch` se elimina la compilación por lotes especificada.

```
aws codebuild delete-build-batch \
    --id <project-name>:<batch-ID>
```

Salida:

```
{
    "statusCode": "BATCH_DELETED",
    "buildsDeleted": [
```

```
        "arn:aws:codebuild:<region-ID>:<account-ID>:build/<project-name>:<build-
ID>",
        "arn:aws:codebuild:<region-ID>:<account-ID>:build/<project-name>:<build-
ID>",
        "arn:aws:codebuild:<region-ID>:<account-ID>:build/<project-name>:<build-
ID>",
        "arn:aws:codebuild:<region-ID>:<account-ID>:build/<project-name>:<build-ID>"
    ],
    "buildsNotDeleted": []
}
```

Para obtener más información, consulte Batch builds in AWS CodeBuild en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte DeleteBuildBatch en la Referencia de comandos de la AWS CLI.

`delete-project`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-project`.

AWS CLI

Eliminación de un proyecto de compilación de AWS CodeBuild

En el siguiente ejemplo de `delete-project`, se elimina el proyecto de compilación de CodeBuild especificado.

```
aws codebuild delete-project --name my-project
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Delete a Build Project (AWS CLI) en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte DeleteProject en la Referencia de comandos de la AWS CLI.

`delete-report-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-report-group`.

AWS CLI

Eliminación de un grupo de informes en AWS CodeBuild

En el siguiente ejemplo de `delete-report-group`, se elimina el grupo de informes con el ARN especificado.

```
aws codebuild delete-report-group \
    --arn arn:aws:codebuild:<region-ID>:<user-ID>:report-group/<report-group-name>
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with report groups en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte DeleteReportGroup en la Referencia de comandos de la AWS CLI.

`delete-report`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-report`.

AWS CLI

Eliminación de un informe en AWS CodeBuild

En el siguiente ejemplo de `delete-report`, se elimina el informe especificado.

```
aws codebuild delete-report \
    --arn arn:aws:codebuild:<region-ID>:<account-ID>:report/<report-group-
name>:<report-ID>
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with reports en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte DeleteReport en la Referencia de comandos de la AWS CLI.

`delete-source-credentials`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-source-credentials`.

AWS CLI

Para desconectar un proveedor de origen y eliminar los tokens de acceso

En el siguiente ejemplo de `delete-source-credentials`, se desconecta un proveedor de origen y se eliminan los tokens. El ARN de las credenciales de origen utilizadas para conectarse al proveedor de origen determina las credenciales de origen en cuestión.

```
aws codebuild delete-source-credentials --arn arn-of-your-credentials
```

Salida:

```
{
    "arn": "arn:aws:codebuild:your-region:your-account-id:token/your-server-type"
}
```

Para obtener más información, consulte Connect Source Providers with Access Tokens (CLI) en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte DeleteSourceCredentials en la Referencia de comandos de la AWS CLI.

`delete-webhook`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-webhook`.

AWS CLI

Eliminación de un filtro de webhook de un proyecto de AWS CodeBuild

En el siguiente ejemplo de `delete-webhook`, se elimina un webhook del proyecto de CodeBuild especificado.

```
aws codebuild delete-webhook --project-name my-project
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Stop Running Builds Automatically (AWS CLI) en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte DeleteWebhook en la Referencia de comandos de AWS CLI.

`describe-code-coverages`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-code-coverages`.

AWS CLI

Obtención de información detallada sobre los resultados de las pruebas de cobertura de código en AWS CodeBuild

En el siguiente ejemplo de `describe-code-coverages`, se obtiene información sobre los resultados de las pruebas de cobertura de código del informe especificado.

```
aws codebuild describe-code-coverages \
    --report-arn arn:aws:codebuild:<region-ID>:<account-ID>:report/<report-group-name>:<report-ID>
```

Salida:

```
{
    "codeCoverages": [
        {
            "id": "20a0adcc-db13-4b66-804b-ecaf9f852855",
            "reportARN": "arn:aws:codebuild:<region-ID>:972506530580:report/<report-group-name>:<report-ID>",
            "filePath": "<source-file-1-path>",
            "lineCoveragePercentage": 83.33,
            "linesCovered": 5,
            "linesMissed": 1,
            "branchCoveragePercentage": 50.0,
            "branchesCovered": 1,
            "branchesMissed": 1,
            "expired": "2020-11-20T21:22:45+00:00"
        },
        {
            "id": "0887162d-bf57-4cf1-a164-e432373d1a83",
            "reportARN": "arn:aws:codebuild:<region-ID>:972506530580:report/<report-group-name>:<report-ID>",
```

```
            "filePath": "<source-file-2-path>",
            "lineCoveragePercentage": 90.9,
            "linesCovered": 10,
            "linesMissed": 1,
            "branchCoveragePercentage": 50.0,
            "branchesCovered": 1,
            "branchesMissed": 1,
            "expired": "2020-11-20T21:22:45+00:00"
        }
    ]
}
```

Para obtener más información, consulte Code coverage reports en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte DescribeCodeCoverages en la Referencia de comandos de la AWS CLI.

`describe-test-cases`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-test-cases`.

AWS CLI

Obtención de información detallada sobre los casos de prueba en AWS CodeBuild

En el siguiente ejemplo de `describe-test-cases`, se obtiene información sobre los casos de prueba del informe especificado.

```
aws codebuild describe-test-cases \
    --report-arn arn:aws:codebuild:<region-ID>:<account-ID>:report/<report-group-name>:<report-ID>
```

Salida:

```
{
    "testCases": [
        {
            "reportArn": "arn:aws:codebuild:<region-ID>:<account-ID>:report/<report-group-name>:<report-ID>",
            "testRawDataPath": "<test-report-path>",
            "prefix": "NUnit.Tests.Assemblies.MockTestFixture",
```

```
            "name": "NUnit.Tests.Assemblies.MockTestFixture.NotRunnableTest",
            "status": "ERROR",
            "durationInNanoSeconds": 0,
            "message": "No arguments were provided\n",
            "expired": "2020-11-20T17:52:10+00:00"
        },
        {
            "reportArn": "arn:aws:codebuild:<region-ID>:<account-ID>:report/<report-
group-name>:<report-ID>",
            "testRawDataPath": "<test-report-path>",
            "prefix": "NUnit.Tests.Assemblies.MockTestFixture",
            "name": "NUnit.Tests.Assemblies.MockTestFixture.TestWithException",
            "status": "ERROR",
            "durationInNanoSeconds": 0,
            "message": "System.ApplicationException : Intentional Exception
\nat NUnit.Tests.Assemblies.MockTestFixture.MethodThrowsException()\nat
 NUnit.Tests.Assemblies.MockTestFixture.TestWithException()\n\n",
            "expired": "2020-11-20T17:52:10+00:00"
        }
    ]
}
```

Para obtener más información, consulte Working with test reporting in AWS CodeBuild en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte DescribeTestCases en la Referencia de comandos de la AWS CLI.

`import-source-credentials`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-source-credentials`.

AWS CLI

Conexión de un usuario de AWS CodeBuild a un proveedor de origen importando las credenciales del proveedor de origen.

En el siguiente ejemplo de `import-source-credentials`, se importa un token para un repositorio de Bitbucket que utiliza BASIC_AUTH como tipo de autenticación.

```
aws codebuild import-source-credentials --server-type BITBUCKET --auth-
type BASIC_AUTH --token my-Bitbucket-password --username my-Bitbucket-username
```

Salida:

```
{
    "arn": "arn:aws:codebuild:us-west-2:123456789012:token/bitbucket"
}
```

Para obtener más información, consulte Connect Source Providers with Access Tokens (CLI) en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte ImportSourceCredentials en la Referencia de comandos de la AWS CLI.

`invalidate-project-cache`

En el siguiente ejemplo de código, se muestra cómo utilizar `invalidate-project-cache`.

AWS CLI

Restablecimiento de la caché de un proyecto de compilación de AWS CodeBuild

En el siguiente ejemplo de `invalidate-project-cache`, se restablece la caché del proyecto CodeBuild especificado.

```
aws codebuild invalidate-project-cache --project-name my-project
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Build Caching in CodeBuild en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte InvalidateProjectCache en la Referencia de comandos de la AWS CLI.

`list-build-batches-for-project`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-build-batches-for-project`.

AWS CLI

Generación de una lista de las compilaciones por lotes de un proyecto de compilación específico en AWS CodeBuild

En el siguiente ejemplo de `list-build-batches-for-project`, se genera una lista de las compilaciones por lotes de CodeBuild para el proyecto especificado.

```
aws codebuild list-build-batches-for-project \
    --project-name "<project-name>"
```

Salida:

```
{
    "ids": [
        "<project-name>:<batch-ID>",
        "<project-name>:<batch-ID>"
    ]
}
```

Para obtener más información, consulte Batch builds in AWS CodeBuild en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte ListBuildBatchesForProject en la Referencia de comandos de la AWS CLI.

`list-build-batches`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-build-batches`.

AWS CLI

Generación de una lista de compilaciones por lotes en AWS CodeBuild

En el siguiente ejemplo de `list-build-batches`, se genera una lista de las compilaciones por lotes de CodeBuild para la cuenta actual.

```
aws codebuild list-build-batches
```

Salida:

```
{
    "ids": [
        "<project-name>:<batch-ID>",
        "<project-name>:<batch-ID>"
```

```
    ]
}
```

Para obtener más información, consulte Batch builds in AWS CodeBuild <https://docs.aws.amazon.com/codebuild/latest/userguide/batch-build.html>)__ en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte ListBuildBatches en la Referencia de comandos de la AWS CLI.

`list-builds-for-project`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-builds-for-project`.

AWS CLI

Visualización de una lista de compilaciones de un proyecto de compilación de AWS CodeBuild

En el siguiente ejemplo de `list-builds-for-project`, se genera una lista de los ID de compilación en orden descendente para el proyecto de compilaciones de CodeBuild especificado.

```
aws codebuild list-builds-for-project --project-name codebuild-demo-project --sort-order DESCENDING
```

Salida:

```
{
    "ids": [
        "codebuild-demo-project:1a2b3c4d-5678-90ab-cdef-11111example",
        "codebuild-demo-project:1a2b3c4d-5678-90ab-cdef-22222example",
        "codebuild-demo-project:1a2b3c4d-5678-90ab-cdef-33333example",
        "codebuild-demo-project:1a2b3c4d-5678-90ab-cdef-44444example",
        "codebuild-demo-project:1a2b3c4d-5678-90ab-cdef-55555example"
    ]
}
```

Para obtener más información, consulte View a List of Build IDs for a Build Project (AWS CLI) en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte ListBuildsForProject en la Referencia de comandos de la AWS CLI.

`list-builds`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-builds`.

AWS CLI

Obtención de una lista de los ID de compilación de AWS CodeBuild

En el siguiente ejemplo de `list-builds` se obtiene una lista de los ID de CodeBuild ordenados de forma ascendente.

```
aws codebuild list-builds --sort-order ASCENDING
```

La salida incluye un valor `nextToken` que indica que hay más salidas disponibles.

```
{
    "nextToken": "4AEA6u7J...The full token has been omitted for
 brevity...MzY2OA==",
    "ids": [
        "codebuild-demo-project:815e755f-bade-4a7e-80f0-efe51EXAMPLE"
        "codebuild-demo-project:84a7f3d1-d40e-4956-b4cf-7a9d4EXAMPLE"
            ... The full list of build IDs has been omitted for brevity ...
        "codebuild-demo-project:931d0b72-bf6f-4040-a472-5c707EXAMPLE"
    ]
}
```

Vuelva a ejecutar este comando y proporcione el valor `nextToken` de la respuesta anterior como parámetro para obtener la siguiente parte de la salida. Repita el procedimiento hasta que no reciba ningún valor `nextToken` en la respuesta.

```
aws codebuild list-builds --sort-order ASCENDING --next-
token 4AEA6u7J...The full token has been omitted for brevity...MzY2OA==
```

Siguiente parte de la salida:

```
{
    "ids": [
        "codebuild-demo-project:49015049-21cf-4b50-9708-df115EXAMPLE",
        "codebuild-demo-project:543e7206-68a3-46d6-a4da-759abEXAMPLE",
            ... The full list of build IDs has been omitted for brevity ...
        "codebuild-demo-project:c282f198-4582-4b38-bdc0-26f96EXAMPLE"
    ]
```

```
}
```

Para obtener más información, consulte View a List of Build IDs (AWS CLI) en la Guía del usuario de AWS CodeBuild

- Para obtener información sobre la API, consulte ListBuilds en la Referencia de comandos de la AWS CLI.

`list-curated-environment-images`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-curated-environment-images`.

AWS CLI

Obtención de una lista con las imágenes de Docker administradas por AWS CodeBuild que puede utilizar en las compilaciones

El siguiente ejemplo de `list-curated-environment-images`, se muestran las imágenes de Docker administradas por CodeBuild que se pueden usar en las compilaciones.

```
aws codebuild list-curated-environment-images
```

Salida:

```
{
    "platforms": [
        {
            "platform": "AMAZON_LINUX",
            "languages": [
                {
                    "language": "JAVA",
                    "images": [
                        {
                            "description": "AWS ElasticBeanstalk - Java 7 Running on
 Amazon Linux 64bit v2.1.3",
                            "name": "aws/codebuild/eb-java-7-amazonlinux-64:2.1.3",
                            "versions": [
                                "aws/codebuild/eb-java-7-amazonlinux-64:2.1.3-1.0.0"
                            ]
                        },
                        {
```

```
                            "description": "AWS ElasticBeanstalk - Java 8 Running on
 Amazon Linux 64bit v2.1.3",
                            "name": "aws/codebuild/eb-java-8-amazonlinux-64:2.1.3",
                            "versions": [
                                "aws/codebuild/eb-java-8-amazonlinux-64:2.1.3-1.0.0"
                            ]
                        },
                        ... LIST TRUNCATED FOR BREVITY ...
                    ]
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Docker Images Provided by CodeBuild en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte ListCuratedEnvironmentImages en la Referencia de comandos de la AWS CLI.

`list-projects`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-projects`.

AWS CLI

Obtención de una lista de nombres de proyectos de compilación de AWS CodeBuild

En el siguiente ejemplo de `list-projects` se obtiene una lista de proyectos de compilación de CodeBuild ordenados por nombre de forma ascendente.

```
aws codebuild list-projects --sort-by NAME --sort-order ASCENDING
```

La salida incluye un valor `nextToken` que indica que hay más salidas disponibles.

```
{
    "nextToken": "Ci33ACF6...The full token has been omitted for brevity...U
+AkMx8=",
    "projects": [
        "codebuild-demo-project",
        "codebuild-demo-project2",
```

```
            ... The full list of build project names has been omitted for
 brevity ...
        "codebuild-demo-project99"
    ]
}
```

Vuelva a ejecutar este comando y proporcione el valor `nextToken` de la respuesta anterior como parámetro para obtener la siguiente parte de la salida. Repita el procedimiento hasta que no reciba ningún valor `nextToken` en la respuesta.

```
aws codebuild list-projects  --sort-by NAME --sort-order ASCENDING --next-
token Ci33ACF6...The full token has been omitted for brevity...U+AkMx8=

{
    "projects": [
        "codebuild-demo-project100",
        "codebuild-demo-project101",

  ... The full list of build project names has been omitted for brevity ...
        "codebuild-demo-project122"

  ]
}
```

Para obtener más información, consulte View a List of Build Project Names (AWS CLI) en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte ListProjects en la Referencia de comandos de la AWS CLI.

`list-report-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-report-groups`.

AWS CLI

Obtención de una lista de los ARN del grupo de informes en AWS CodeBuild

En el siguiente ejemplo de `list-report-groups`, se ofrecen los ARN del grupo de informes de la cuenta en la región.

```
aws codebuild list-report-groups
```

Salida:

```
{
    "reportGroups": [
        "arn:aws:codebuild:<region-ID>:<user-ID>:report-group/report-group-1",
        "arn:aws:codebuild:<region-ID>:<user-ID>:report-group/report-group-2",
        "arn:aws:codebuild:<region-ID>:<user-ID>:report-group/report-group-3"
    ]
}
```

Para obtener más información, consulte Working with report groups en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte ListReportGroups en la Referencia de comandos de la AWS CLI.

`list-reports-for-report-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-reports-for-report-group`.

AWS CLI

Obtención de una lista de los informes de un grupo de informes en AWS CodeBuild

En el siguiente ejemplo de `list-report-for-report-groups`, se ofrecen los informes del grupo de informes especificado de la cuenta en la región.

```
aws codebuild list-reports-for-report-group \
    --report-group-arn arn:aws:codebuild:<region-ID>:<user-ID>:report-group/<report-group-name>
```

Salida:

```
{
    "reports": [
        "arn:aws:codebuild:<region-ID>:<user-ID>:report/report-1",
        "arn:aws:codebuild:<region-ID>:<user-ID>:report/report-2",
        "arn:aws:codebuild:<region-ID>:<user-ID>:report/report-3"
    ]
}
```

Para obtener más información, consulte Working with report groups en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte ListReportsForReportGroup en la Referencia de comandos de la AWS CLI.

`list-reports`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-reports`.

AWS CLI

Obtención de una lista de los informes de la cuenta actual en AWS CodeBuild

En el siguiente ejemplo de `list-reports`, se ofrecen los ARN de los informes de la cuenta actual.

```
aws codebuild list-reports
```

Salida:

```
{
    "reports": [
        "arn:aws:codebuild:<region-ID>:<user-ID>:report/<report-group-name>:<report
 ID>",
        "arn:aws:codebuild:<region-ID>:<user-ID>:report/<report-group-name>:<report
 ID>",
        "arn:aws:codebuild:<region-ID>:<user-ID>:report/<report-group-name>:<report
 ID>"
    ]
}
```

Para obtener más información, consulte Working with reports en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte ListReports en la Referencia de comandos de la AWS CLI.

`list-shared-projects`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-shared-projects`.

AWS CLI

Generación de una lista de los proyectos compartidos en AWS CodeBuild

En el siguiente ejemplo de `list-shared-projects`, se genera una lista de los proyectos compartidos de CodeBuild que están disponibles para la cuenta actual.

```
aws codebuild list-shared-projects
```

Salida:

```
{
    "projects": [
        "arn:aws:codebuild:<region-ID>:<account-ID>:project/<shared-project-
name-1>",
        "arn:aws:codebuild:<region-ID>:<account-ID>:project/<shared-project-name-2>"
    ]
}
```

Para obtener más información, consulte Working with shared projects en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte ListSharedProjects en la Referencia de comandos de la AWS CLI.

`list-shared-report-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-shared-report-groups`.

AWS CLI

Obtención de una lista de los ARN del grupo de informes compartido en AWS CodeBuild

En el siguiente ejemplo de `list-shared-report-groups`, se ofrecen los ARN del grupo de informes de la cuenta en la región.

```
aws codebuild list-shared-report-groups
```

Salida:

```
{
    "reportGroups": [
```

```
        "arn:aws:codebuild:<region-ID>:<user-ID>:report-group/report-group-1",
        "arn:aws:codebuild:<region-ID>:<user-ID>:report-group/report-group-2",
        "arn:aws:codebuild:<region-ID>:<user-ID>:report-group/report-group-3"
    ]
}
```

Para obtener más información, consulte Working with report groups en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte ListSharedReportGroups en la Referencia de comandos de la AWS CLI.

`list-source-credentials`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-source-credentials`.

AWS CLI

Visualización de una lista de sourceCredentialsObjects

En el siguiente ejemplo de `list-source-credentials`, se genera una lista de tokens de una cuenta de AWS conectada a una cuenta de Bitbucket y a una cuenta de GitHub. Cada objeto `sourceCredentialsInfos` de la respuesta contiene información sobre las credenciales de origen conectadas.

```
aws codebuild list-source-credentials
```

Salida:

```
{
    "sourceCredentialsInfos": [
        {
            "serverType": "BITBUCKET",
            "arn": "arn:aws:codebuild:us-west-2:123456789012:token/bitbucket",
            "authType": "BASIC_AUTH"
        },
        {
            "serverType": "GITHUB",
            "arn": "arn:aws:codebuild:us-west-2:123456789012:token/github",
            "authType": "OAUTH"
        }
    ]
```

```
}
```

Para obtener más información, consulte Connect Source Providers with Access Tokens (CLI) en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte ListSourceCredentials en la Referencia de comandos de la AWS CLI.

`retry-build-batch`

En el siguiente ejemplo de código, se muestra cómo utilizar `retry-build-batch`.

AWS CLI

Reintento de una compilación por lotes fallida en AWS CodeBuild

En el siguiente ejemplo de `retry-build-batch`, se reinicia la compilación por lotes especificada.

```
aws codebuild retry-build-batch \
    --id <project-name>:<batch-ID>
```

Salida:

```
{
    "buildBatch": {
        "id": "<project-name>:<batch-ID>",
        "arn": "arn:aws:codebuild:<region-ID>:<account-ID>:build-batch/<project-
name>:<batch-ID>",
        "startTime": "2020-10-21T17:26:23.099000+00:00",
        "currentPhase": "SUBMITTED",
        "buildBatchStatus": "IN_PROGRESS",
        "resolvedSourceVersion": "3a9e11cb419e8fff14b03883dc4e64f6155aaa7e",
        "projectName": "<project-name>",
        "phases": [
            {
                "phaseType": "SUBMITTED",
                "phaseStatus": "SUCCEEDED",
                "startTime": "2020-10-21T17:26:23.099000+00:00",
                "endTime": "2020-10-21T17:26:23.457000+00:00",
                "durationInSeconds": 0
            },
            {
```

```
                "phaseType": "DOWNLOAD_BATCHSPEC",
                "phaseStatus": "SUCCEEDED",
                "startTime": "2020-10-21T17:26:23.457000+00:00",
                "endTime": "2020-10-21T17:26:54.902000+00:00",
                "durationInSeconds": 31
            },
            {
                "phaseType": "IN_PROGRESS",
                "phaseStatus": "CLIENT_ERROR",
                "startTime": "2020-10-21T17:26:54.902000+00:00",
                "endTime": "2020-10-21T17:28:16.060000+00:00",
                "durationInSeconds": 81
            },
            {
                "phaseType": "FAILED",
                "phaseStatus": "RETRY",
                "startTime": "2020-10-21T17:28:16.060000+00:00",
                "endTime": "2020-10-21T17:29:39.709000+00:00",
                "durationInSeconds": 83
            },
            {
                "phaseType": "SUBMITTED",
                "startTime": "2020-10-21T17:29:39.709000+00:00"
            }
        ],
        "source": {
            "type": "GITHUB",
            "location": "https://github.com/strohm-a/<project-name>-graph.git",
            "gitCloneDepth": 1,
            "gitSubmodulesConfig": {
                "fetchSubmodules": false
            },
            "reportBuildStatus": false,
            "insecureSsl": false
        },
        "secondarySources": [],
        "secondarySourceVersions": [],
        "artifacts": {
            "location": ""
        },
        "secondaryArtifacts": [],
        "cache": {
            "type": "NO_CACHE"
        },
```

```
        "environment": {
            "type": "LINUX_CONTAINER",
            "image": "aws/codebuild/amazonlinux2-x86_64-standard:3.0",
            "computeType": "BUILD_GENERAL1_SMALL",
            "environmentVariables": [],
            "privilegedMode": false,
            "imagePullCredentialsType": "CODEBUILD"
        },
        "logConfig": {
            "cloudWatchLogs": {
                "status": "ENABLED"
            },
            "s3Logs": {
                "status": "DISABLED",
                "encryptionDisabled": false
            }
        },
        "buildTimeoutInMinutes": 60,
        "queuedTimeoutInMinutes": 480,
        "complete": false,
        "initiator": "<username>",
        "encryptionKey": "arn:aws:kms:<region-ID>:<account-ID>:alias/aws/s3",
        "buildBatchNumber": 4,
        "buildBatchConfig": {
            "serviceRole": "arn:aws:iam::<account-ID>:role/service-role/<project-
name>",
            "restrictions": {
                "maximumBuildsAllowed": 100
            },
            "timeoutInMins": 480
        },
        "buildGroups": [
            {
                "identifier": "DOWNLOAD_SOURCE",
                "ignoreFailure": false,
                "currentBuildSummary": {
                    "arn": "arn:aws:codebuild:<region-ID>:<account-ID>:build/
<project-name>:<build-ID>",
                    "requestedOn": "2020-10-21T17:26:23.889000+00:00",
                    "buildStatus": "SUCCEEDED",
                    "primaryArtifact": {
                        "type": "no_artifacts",
                        "identifier": "DOWNLOAD_SOURCE"
                    },
```

```
                    "secondaryArtifacts": []
                }
            },
            {
                "identifier": "linux_small",
                "dependsOn": [],
                "ignoreFailure": false,
                "currentBuildSummary": {
                    "arn": "arn:aws:codebuild:<region-ID>:<account-ID>:build/
<project-name>:<build-ID>",
                    "requestedOn": "2020-10-21T17:26:55.115000+00:00",
                    "buildStatus": "FAILED",
                    "primaryArtifact": {
                        "type": "no_artifacts",
                        "identifier": "linux_small"
                    },
                    "secondaryArtifacts": []
                }
            },
            {
                "identifier": "linux_medium",
                "dependsOn": [
                    "linux_small"
                ],
                "ignoreFailure": false,
                "currentBuildSummary": {
                    "arn": "arn:aws:codebuild:<region-ID>:<account-ID>:build/
<project-name>:<build-ID>",
                    "requestedOn": "2020-10-21T17:26:54.594000+00:00",
                    "buildStatus": "STOPPED"
                }
            },
            {
                "identifier": "linux_large",
                "dependsOn": [
                    "linux_medium"
                ],
                "ignoreFailure": false,
                "currentBuildSummary": {
                    "arn": "arn:aws:codebuild:<region-ID>:<account-ID>:build/
<project-name>:<build-ID>",
                    "requestedOn": "2020-10-21T17:26:54.701000+00:00",
                    "buildStatus": "STOPPED"
                }
```

```
            }
        ]
    }
}
```

Para obtener más información, consulte Batch builds in AWS CodeBuild en la Guía del usuario de AWS CodeBuild.

- Para obtener detalles sobre la API, consulte RetryBuildBatch en la Referencia de comandos de la AWS CLI.

`retry-build`

En el siguiente ejemplo de código, se muestra cómo utilizar `retry-build`.

AWS CLI

Reintento de una compilación fallida en AWS CodeBuild

En el siguiente ejemplo de `retry-build`, se reinicia la compilación especificada.

```
aws codebuild retry-build \
    --id <project-name>:<build-ID>
```

Salida:

```
{
    "build": {
        "id": "<project-name>:<build-ID>",
        "arn": "arn:aws:codebuild:<region-ID>:<account-ID>:build/<project-
name>:<build-ID>",
        "buildNumber": 9,
        "startTime": "2020-10-21T17:51:38.161000+00:00",
        "currentPhase": "QUEUED",
        "buildStatus": "IN_PROGRESS",
        "projectName": "<project-name>",
        "phases": [
            {
                "phaseType": "SUBMITTED",
                "phaseStatus": "SUCCEEDED",
                "startTime": "2020-10-21T17:51:38.161000+00:00",
                "endTime": "2020-10-21T17:51:38.210000+00:00",
                "durationInSeconds": 0
```

```
            },
            {
                "phaseType": "QUEUED",
                "startTime": "2020-10-21T17:51:38.210000+00:00"
            }
        ],
        "source": {
            "type": "GITHUB",
            "location": "<GitHub-repo-URL>",
            "gitCloneDepth": 1,
            "gitSubmodulesConfig": {
                "fetchSubmodules": false
            },
            "reportBuildStatus": false,
            "insecureSsl": false
        },
        "secondarySources": [],
        "secondarySourceVersions": [],
        "artifacts": {
            "location": ""
        },
        "secondaryArtifacts": [],
        "cache": {
            "type": "NO_CACHE"
        },
        "environment": {
            "type": "LINUX_CONTAINER",
            "image": "aws/codebuild/amazonlinux2-x86_64-standard:3.0",
            "computeType": "BUILD_GENERAL1_SMALL",
            "environmentVariables": [],
            "privilegedMode": false,
            "imagePullCredentialsType": "CODEBUILD"
        },
        "serviceRole": "arn:aws:iam::<account-ID>:role/service-role/<service-role-
name>",
        "logs": {
            "deepLink": "https://console.aws.amazon.com/cloudwatch/home?
region=<region-ID>#logEvent:group=null;stream=null",
            "cloudWatchLogsArn": "arn:aws:logs:<region-ID>:<account-ID>:log-
group:null:log-stream:null",
            "cloudWatchLogs": {
                "status": "ENABLED"
            },
            "s3Logs": {
```

```
                "status": "DISABLED",
                "encryptionDisabled": false
            }
        },
        "timeoutInMinutes": 60,
        "queuedTimeoutInMinutes": 480,
        "buildComplete": false,
        "initiator": "<username>",
        "encryptionKey": "arn:aws:kms:<region-ID>:<account-ID>:alias/aws/s3"
    }
}
```

Para obtener más información, consulte Batch builds in AWS CodeBuild en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte RetryBuild en la Referencia de comandos de la AWS CLI.

`start-build-batch`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-build-batch`.

AWS CLI

Inicio de una compilación por lotes en AWS CodeBuild

En el siguiente ejemplo de `start-build-batch`, se inicia una compilación por lotes del proyecto especificado.

```
aws codebuild start-build-batch \
    --project-name <project-name>
```

Salida:

```
{
    "buildBatch": {
        "id": "<project-name>:<batch-ID>",
        "arn": "arn:aws:codebuild:<region-ID>:<account-ID>:build-batch/<project-
name>:<batch-ID>",
        "startTime": "2020-10-21T16:54:24.740000+00:00",
        "currentPhase": "SUBMITTED",
        "buildBatchStatus": "IN_PROGRESS",
        "projectName": "<project-name>",
```

```
        "source": {
            "type": "GITHUB",
            "location": "<GitHub-repo-URL>",
            "gitCloneDepth": 1,
            "gitSubmodulesConfig": {
                "fetchSubmodules": false
            },
            "reportBuildStatus": false,
            "insecureSsl": false
        },
        "secondarySources": [],
        "secondarySourceVersions": [],
        "artifacts": {
            "location": ""
        },
        "secondaryArtifacts": [],
        "cache": {
            "type": "NO_CACHE"
        },
        "environment": {
            "type": "LINUX_CONTAINER",
            "image": "aws/codebuild/amazonlinux2-x86_64-standard:3.0",
            "computeType": "BUILD_GENERAL1_SMALL",
            "environmentVariables": [],
            "privilegedMode": false,
            "imagePullCredentialsType": "CODEBUILD"
        },
        "logConfig": {
            "cloudWatchLogs": {
                "status": "ENABLED"
            },
            "s3Logs": {
                "status": "DISABLED",
                "encryptionDisabled": false
            }
        },
        "buildTimeoutInMinutes": 60,
        "queuedTimeoutInMinutes": 480,
        "complete": false,
        "initiator": "<username>",
        "encryptionKey": "arn:aws:kms:<region-ID>:<account-ID>:alias/aws/s3",
        "buildBatchNumber": 3,
        "buildBatchConfig": {
```

```
            "serviceRole": "arn:aws:iam::<account-ID>:role/service-role/<service-
role-name>",
            "restrictions": {
                "maximumBuildsAllowed": 100
            },
            "timeoutInMins": 480
        }
    }
}
```

Para obtener más información, consulte Batch builds in AWS CodeBuild en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte StartBuildBatch en la Referencia de comandos de la AWS CLI.

`start-build`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-build`.

AWS CLI

Inicio de la ejecución de una compilación de un proyecto de compilación de AWS CodeBuild

En el siguiente ejemplo de `start-build`, se inicia una compilación para el proyecto de CodeBuild especificado. La compilación anula tanto la configuración del proyecto para el número de minutos que se permite poner en cola la compilación antes de que se agote el tiempo de espera como la configuración de artefacto del proyecto.

```
aws codebuild start-build \
    --project-name "my-demo-project" \
    --queued-timeout-in-minutes-override 5 \
    --artifacts-override {"\"type\": \"S3\",\"location\": \"arn:aws:s3:::artifacts-
override\",\"overrideArtifactName\":true"}
```

Salida:

```
{
    "build": {
        "serviceRole": "arn:aws:iam::123456789012:role/service-role/my-codebuild-
service-role",
        "buildStatus": "IN_PROGRESS",
```

```
        "buildComplete": false,
        "projectName": "my-demo-project",
        "timeoutInMinutes": 60,
        "source": {
            "insecureSsl": false,
            "type": "S3",
            "location": "codebuild-us-west-2-123456789012-input-bucket/my-
source.zip"
        },
        "queuedTimeoutInMinutes": 5,
        "encryptionKey": "arn:aws:kms:us-west-2:123456789012:alias/aws/s3",
        "currentPhase": "QUEUED",
        "startTime": 1556905683.568,
        "environment": {
            "computeType": "BUILD_GENERAL1_MEDIUM",
            "environmentVariables": [],
            "type": "LINUX_CONTAINER",
            "privilegedMode": false,
            "image": "aws/codebuild/standard:1.0",
            "imagePullCredentialsType": "CODEBUILD"
        },
        "phases": [
            {
                "phaseStatus": "SUCCEEDED",
                "startTime": 1556905683.568,
                "phaseType": "SUBMITTED",
                "durationInSeconds": 0,
                "endTime": 1556905684.524
            },
            {
                "startTime": 1556905684.524,
                "phaseType": "QUEUED"
            }
        ],
        "logs": {
            "deepLink": "https://console.aws.amazon.com/cloudwatch/home?region=us-
west-2#logEvent:group=null;stream=null"
        },
        "artifacts": {
            "encryptionDisabled": false,
            "location": "arn:aws:s3:::artifacts-override/my-demo-project",
            "overrideArtifactName": true
        },
        "cache": {
```

```
            "type": "NO_CACHE"
        },
        "id": "my-demo-project::12345678-a1b2-c3d4-e5f6-11111EXAMPLE",
        "initiator": "my-aws-account-name",
        "arn": "arn:aws:codebuild:us-west-2:123456789012:build/my-demo-
project::12345678-a1b2-c3d4-e5f6-11111EXAMPLE"
    }
}
```

Para obtener más información, consulte Run a Build (AWS CLI) en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte StartBuild en la Referencia de comandos de la AWS CLI.

`stop-build-batch`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-build-batch`.

AWS CLI

Detención de una compilación por lotes en curso en AWS CodeBuild

En el siguiente ejemplo de `stop-build-batch`, se detiene la compilación por lotes especificada.

```
aws codebuild stop-build-batch \
    --id <project-name>:<batch-ID>
```

Salida:

```
{
    "buildBatch": {
        "id": "<project-name>:<batch-ID>",
        "arn": "arn:aws:codebuild:<region-ID>:<account-ID>:build-batch/<project-
name>:<batch-ID>",
        "startTime": "2020-10-21T16:54:24.740000+00:00",
        "endTime": "2020-10-21T16:56:05.152000+00:00",
        "currentPhase": "STOPPED",
        "buildBatchStatus": "STOPPED",
        "resolvedSourceVersion": "aef7744ed069c51098e15c360f4102cd2cd1ad64",
        "projectName": "<project-name>",
        "phases": [
```

```
            {
                "phaseType": "SUBMITTED",
                "phaseStatus": "SUCCEEDED",
                "startTime": "2020-10-21T16:54:24.740000+00:00",
                "endTime": "2020-10-21T16:54:25.039000+00:00",
                "durationInSeconds": 0
            },
            {
                "phaseType": "DOWNLOAD_BATCHSPEC",
                "phaseStatus": "SUCCEEDED",
                "startTime": "2020-10-21T16:54:25.039000+00:00",
                "endTime": "2020-10-21T16:54:56.583000+00:00",
                "durationInSeconds": 31
            },
            {
                "phaseType": "IN_PROGRESS",
                "phaseStatus": "STOPPED",
                "startTime": "2020-10-21T16:54:56.583000+00:00",
                "endTime": "2020-10-21T16:56:05.152000+00:00",
                "durationInSeconds": 68
            },
            {
                "phaseType": "STOPPED",
                "startTime": "2020-10-21T16:56:05.152000+00:00"
            }
        ],
        "source": {
            "type": "GITHUB",
            "location": "<GitHub-repo-URL>",
            "gitCloneDepth": 1,
            "gitSubmodulesConfig": {
                "fetchSubmodules": false
            },
            "reportBuildStatus": false,
            "insecureSsl": false
        },
        "secondarySources": [],
        "secondarySourceVersions": [],
        "artifacts": {
            "location": ""
        },
        "secondaryArtifacts": [],
        "cache": {
            "type": "NO_CACHE"
```

```
        },
        "environment": {
            "type": "LINUX_CONTAINER",
            "image": "aws/codebuild/amazonlinux2-x86_64-standard:3.0",
            "computeType": "BUILD_GENERAL1_SMALL",
            "environmentVariables": [],
            "privilegedMode": false,
            "imagePullCredentialsType": "CODEBUILD"
        },
        "logConfig": {
            "cloudWatchLogs": {
                "status": "ENABLED"
            },
            "s3Logs": {
                "status": "DISABLED",
                "encryptionDisabled": false
            }
        },
        "buildTimeoutInMinutes": 60,
        "queuedTimeoutInMinutes": 480,
        "complete": true,
        "initiator": "Strohm",
        "encryptionKey": "arn:aws:kms:<region-ID>:<account-ID>:alias/aws/s3",
        "buildBatchNumber": 3,
        "buildBatchConfig": {
            "serviceRole": "arn:aws:iam::<account-ID>:role/service-role/<project-
name>",
            "restrictions": {
                "maximumBuildsAllowed": 100
            },
            "timeoutInMins": 480
        },
        "buildGroups": [
            {
                "identifier": "DOWNLOAD_SOURCE",
                "ignoreFailure": false,
                "currentBuildSummary": {
                    "arn": "arn:aws:codebuild:<region-ID>:<account-ID>:build/
<project-name>:<build-ID>",
                    "requestedOn": "2020-10-21T16:54:25.468000+00:00",
                    "buildStatus": "SUCCEEDED",
                    "primaryArtifact": {
                        "type": "no_artifacts",
                        "identifier": "DOWNLOAD_SOURCE"
```

```
                    },
                    "secondaryArtifacts": []
                }
            },
            {
                "identifier": "linux_small",
                "dependsOn": [],
                "ignoreFailure": false,
                "currentBuildSummary": {
                    "arn": "arn:aws:codebuild:<region-ID>:<account-ID>:build/
<project-name>:<build-ID>",
                    "requestedOn": "2020-10-21T16:54:56.833000+00:00",
                    "buildStatus": "IN_PROGRESS"
                }
            },
            {
                "identifier": "linux_medium",
                "dependsOn": [
                    "linux_small"
                ],
                "ignoreFailure": false,
                "currentBuildSummary": {
                    "arn": "arn:aws:codebuild:<region-ID>:<account-ID>:build/
<project-name>:<build-ID>",
                    "requestedOn": "2020-10-21T16:54:56.211000+00:00",
                    "buildStatus": "PENDING"
                }
            },
            {
                "identifier": "linux_large",
                "dependsOn": [
                    "linux_medium"
                ],
                "ignoreFailure": false,
                "currentBuildSummary": {
                    "arn": "arn:aws:codebuild:<region-ID>:<account-ID>:build/
<project-name>:<build-ID>",
                    "requestedOn": "2020-10-21T16:54:56.330000+00:00",
                    "buildStatus": "PENDING"
                }
            }
        ]
    }
```

```
}
```

Para obtener más información, consulte Batch builds in AWS CodeBuild en la Guía del usuario de AWS CodeBuild.

- Para obtener información de la API, consulte StopBuildBatch en la Referencia de comandos de la AWS CLI.

`stop-build`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-build`.

AWS CLI

Detención de una compilación de un proyecto de compilación de AWS CodeBuild

En el siguiente ejemplo de `stop-build`, se detiene la compilación de CodeBuild especificada.

```
aws codebuild stop-build --id my-demo-project:12345678-a1b2-c3d4-e5f6-11111EXAMPLE
```

Salida:

```
{
    "build": {
        "startTime": 1556906956.318,
        "initiator": "my-aws-account-name",
        "projectName": "my-demo-project",
        "currentPhase": "COMPLETED",
        "cache": {
            "type": "NO_CACHE"
        },
        "source": {
            "insecureSsl": false,
            "location": "codebuild-us-west-2-123456789012-input-bucket/my-
source.zip",
            "type": "S3"
        },
        "id": "my-demo-project:1a2b3c4d-5678-90ab-cdef-11111EXAMPLE",
        "endTime": 1556906974.781,
        "phases": [
            {
                "durationInSeconds": 0,
                "phaseType": "SUBMITTED",
```

```
            "endTime": 1556906956.935,
            "phaseStatus": "SUCCEEDED",
            "startTime": 1556906956.318
        },
        {
            "durationInSeconds": 1,
            "phaseType": "QUEUED",
            "endTime": 1556906958.272,
            "phaseStatus": "SUCCEEDED",
            "startTime": 1556906956.935
        },
        {
            "phaseType": "PROVISIONING",
            "phaseStatus": "SUCCEEDED",
            "durationInSeconds": 14,
            "contexts": [
                {
                    "message": "",
                    "statusCode": ""
                }
            ],
            "endTime": 1556906972.847,
            "startTime": 1556906958.272
        },
        {
            "phaseType": "DOWNLOAD_SOURCE",
            "phaseStatus": "SUCCEEDED",
            "durationInSeconds": 0,
            "contexts": [
                    {
                    "message": "",
                    "statusCode": ""
                }
            ],
            "endTime": 1556906973.552,
            "startTime": 1556906972.847
        },
        {
            "phaseType": "INSTALL",
            "phaseStatus": "SUCCEEDED",
            "durationInSeconds": 0,
            "contexts": [
                {
                    "message": "",
```

```
                        "statusCode": ""
                    }
                ],
                "endTime": 1556906973.75,
                "startTime": 1556906973.552
            },
            {
                "phaseType": "PRE_BUILD",
                "phaseStatus": "SUCCEEDED",
                "durationInSeconds": 0,
                "contexts": [
                    {
                        "message": "",
                        "statusCode": ""
                    }
                ],
                "endTime": 1556906973.937,
                "startTime": 1556906973.75
            },
            {
                "durationInSeconds": 0,
                "phaseType": "BUILD",
                "endTime": 1556906974.781,
                "phaseStatus": "STOPPED",
                "startTime": 1556906973.937
            },
            {
                "phaseType": "COMPLETED",
                "startTime": 1556906974.781
            }
        ],
        "artifacts": {
            "location": "arn:aws:s3:::artifacts-override/my-demo-project",
            "encryptionDisabled": false,
            "overrideArtifactName": true
        },
        "buildComplete": true,
        "buildStatus": "STOPPED",
        "encryptionKey": "arn:aws:kms:us-west-2:123456789012:alias/aws/s3",
        "serviceRole": "arn:aws:iam::123456789012:role/service-role/my-codebuild-
service-role",
        "queuedTimeoutInMinutes": 5,
        "timeoutInMinutes": 60,
        "environment": {
```

```
            "type": "LINUX_CONTAINER",
            "environmentVariables": [],
            "computeType": "BUILD_GENERAL1_MEDIUM",
            "privilegedMode": false,
            "image": "aws/codebuild/standard:1.0",
            "imagePullCredentialsType": "CODEBUILD"
        },
        "logs": {
            "streamName": "1a2b3c4d-5678-90ab-cdef-11111EXAMPLE",
            "deepLink": "https://console.aws.amazon.com/cloudwatch/home?region=us-
west-2#logEvent:group=/aws/codebuild/my-demo-project;stream=1a2b3c4d-5678-90ab-
cdef-11111EXAMPLE",
            "groupName": "/aws/codebuild/my-demo-project"
        },
        "arn": "arn:aws:codebuild:us-west-2:123456789012:build/my-demo-
project:1a2b3c4d-5678-90ab-cdef-11111EXAMPLE"
    }
}
```

Para obtener más información, consulte Stop a Build (AWS CLI) en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte StopBuild en la Referencia de comandos de la AWS CLI.

`update-project`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-project`.

AWS CLI

Cambio de la configuración de un proyecto de compilación de AWS CodeBuild

En el siguiente ejemplo de `update-project`, se cambia la configuración del proyecto de compilación de CodeBuild especificado, denominado my-demo-project.

```
aws codebuild update-project --name "my-demo-project" \
    --description "This project is updated" \
    --source "{\"type\": \"S3\",\"location\": \"codebuild-us-west-2-123456789012-
input-bucket/my-source-2.zip\"}" \
    --artifacts {"\"type\": \"S3\",\"location\": \"codebuild-us-west-2-123456789012-
output-bucket-2\""} \
```

```
    --environment "{\"type\": \"LINUX_CONTAINER\",\"image\": \"aws/codebuild/
standard:1.0\",\"computeType\": \"BUILD_GENERAL1_MEDIUM\"}" \
    --service-role "arn:aws:iam::123456789012:role/service-role/my-codebuild-
service-role"
```

La salida muestra la configuración actualizada.

```
{
    "project": {
        "arn": "arn:aws:codebuild:us-west-2:123456789012:project/my-demo-project",
        "environment": {
            "privilegedMode": false,
            "environmentVariables": [],
            "type": "LINUX_CONTAINER",
            "image": "aws/codebuild/standard:1.0",
            "computeType": "BUILD_GENERAL1_MEDIUM",
            "imagePullCredentialsType": "CODEBUILD"
        },
        "queuedTimeoutInMinutes": 480,
        "description": "This project is updated",
        "artifacts": {
            "packaging": "NONE",
            "name": "my-demo-project",
            "type": "S3",
            "namespaceType": "NONE",
            "encryptionDisabled": false,
            "location": "codebuild-us-west-2-123456789012-output-bucket-2"
        },
        "encryptionKey": "arn:aws:kms:us-west-2:123456789012:alias/aws/s3",
        "badge": {
            "badgeEnabled": false
        },
        "serviceRole": "arn:aws:iam::123456789012:role/service-role/my-codebuild-
service-role",
        "lastModified": 1556840545.967,
        "tags": [],
        "timeoutInMinutes": 60,
        "created": 1556839783.274,
        "name": "my-demo-project",
        "cache": {
            "type": "NO_CACHE"
        },
        "source": {
```

```
            "type": "S3",
            "insecureSsl": false,
            "location": "codebuild-us-west-2-123456789012-input-bucket/my-
source-2.zip"
        }
    }
}
```

Para obtener más información, consulte Change a Build Project's Settings (AWS CLI) en la Guía del usuario de AWS CodeBuild

- Para obtener información sobre la API, consulte UpdateProject en la Referencia de comandos de la AWS CLI.

`update-report-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-report-group`.

AWS CLI

Actualización de un grupo de informes en AWS CodeBuild

En el siguiente ejemplo de `update-report-group`, se cambia el tipo de exportación del grupo de informes a NO_EXPORT.

```
aws codebuild update-report-group \
    --arn arn:aws:codebuild:<region-ID>:<user-ID>:report-group/cli-created-report-
group \
    --export-config="exportConfigType=NO_EXPORT"
```

Salida:

```
{
    "reportGroup": {
        "arn": "arn:aws:codebuild:<region-ID>:<user-ID>:report-group/cli-created-
report-group",
        "name": "cli-created-report-group",
        "type": "TEST",
        "exportConfig": {
            "exportConfigType": "NO_EXPORT"
        },
        "created": 1602020686.009,
```

```
        "lastModified": 1602021033.454,
        "tags": []
    }
}
```

Para obtener más información, consulte Working with report groups en la Guía del usuario de AWS CodeBuild.

- Para obtener información sobre la API, consulte UpdateReportGroup en la Referencia de comandos de la AWS CLI.

`update-webhook`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-webhook`.

AWS CLI

Actualización del webhook de un proyecto de AWS CodeBuild

En el siguiente ejemplo de `update-webhook`, se actualiza un webhook del proyecto de CodeBuild especificado con dos grupos de filtros. El parámetro `--rotate-secret` especifica que GitHub rota la clave secreta del proyecto cada vez que un cambio de código desencadena una compilación. El primer grupo de filtros especifica las solicitudes de extracción que se crean, actualizan o vuelven a abrirse en ramificaciones con nombres de referencia de Git que coinciden con la expresión regular `^refs/heads/master$` y las referencias de encabezado que coinciden con `^refs/heads/myBranch$`. El segundo grupo de filtros especifica solicitudes de inserción en ramificaciones con nombres de referencia de Git que no coinciden con la expresión regular `^refs/heads/myBranch$`.

```
aws codebuild update-webhook \
    --project-name Project2 \
    --rotate-secret \
    --filter-groups "[[{\"type\":\"EVENT\",\"pattern\":\"PULL_REQUEST_CREATED,
 PULL_REQUEST_UPDATED, PULL_REQUEST_REOPENED\"},{\"type\":\"HEAD_REF\",\"pattern
\":\"^refs/heads/myBranch$\",\"excludeMatchedPattern\":true},{\"type\":\"BASE_REF
\",\"pattern\":\"^refs/heads/master$\",\"excludeMatchedPattern\":true}],[{\"type\":
\"EVENT\",\"pattern\":\"PUSH\"},{\"type\":\"HEAD_REF\",\"pattern\":\"^refs/heads/
myBranch$\",\"excludeMatchedPattern\":true}]]"
```

Salida:

```
{
    "webhook": {
        "filterGroups": [
            [
                {
                    "pattern": "PULL_REQUEST_CREATED, PULL_REQUEST_UPDATED,
 PULL_REQUEST_REOPENED",
                    "type": "EVENT"
                },
                {
                    "excludeMatchedPattern": true,
                    "pattern": "refs/heads/myBranch$",
                    "type": "HEAD_REF"
                },
                {
                    "excludeMatchedPattern": true,
                    "pattern": "refs/heads/master$",
                    "type": "BASE_REF"
                }
            ],
            [
                {
                    "pattern": "PUSH",
                    "type": "EVENT"
                },
                {
                    "excludeMatchedPattern": true,
                    "pattern": "refs/heads/myBranch$",
                    "type": "HEAD_REF"
                }
            ]
        ],
        "lastModifiedSecret": 1556312220.133
    }
}
```

Para obtener más información, consulte Change a Build Project's Settings (AWS CLI) en la Guía del usuario de AWS CodeBuild

- Para obtener información sobre la API, consulte UpdateWebhook en la Referencia de comandos de la AWS CLI.

Ejemplos de CodeCommit que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar situaciones comunes mediante la AWS Command Line Interface con CodeCommit.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-approval-rule-template-with-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-approval-rule-template-with-repository`.

AWS CLI

Asociación de una plantilla de regla de aprobación con un repositorio

En el siguiente ejemplo de `associate-approval-rule-template-with-repository`, se asocia la plantilla de regla de aprobación especificada con un repositorio denominado `MyDemoRepo`.

```
aws codecommit associate-approval-rule-template-with-repository \
    --repository-name MyDemoRepo  \
    --approval-rule-template-name 2-approver-rule-for-main
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Asociar una plantilla de regla de aprobación con un repositorio en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte AssociateApprovalRuleTemplateWithRepository en la Referencia de comandos de la AWS CLI.

batch-associate-approval-rule-template-with-repositories

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-associate-approval-rule-template-with-repositories`.

AWS CLI

Asociación de una plantilla de regla de aprobación con varios repositorios en una sola operación

En el siguiente ejemplo de `batch-associate-approval-rule-template-with-repositories`, se asocia la plantilla de regla de aprobación especificada con los repositorios denominados `MyDemoRepo` y `MyOtherDemoRepo`.

Nota: Las plantillas de reglas de aprobación son específicas de la región de AWS en la que se crean. Solo se pueden asociar a los repositorios de dicha región de AWS.

```
aws codecommit batch-associate-approval-rule-template-with-repositories \
    --repository-names MyDemoRepo, MyOtherDemoRepo  \
    --approval-rule-template-name 2-approver-rule-for-main
```

Salida:

```
{
    "associatedRepositoryNames": [
        "MyDemoRepo",
        "MyOtherDemoRepo"
    ],
    "errors": []
}
```

Para obtener más información, consulte Asociar una plantilla de regla de aprobación con un repositorio en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte BatchAssociateApprovalRuleTemplateWithRepositories en la Referencia de comandos de la AWS CLI.

batch-describe-merge-conflicts

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-describe-merge-conflicts`.

AWS CLI

Obtención de información sobre los conflictos de combinación en todos los archivos o un subconjunto de archivos de una combinación de dos especificadores de confirmación

En el siguiente ejemplo de `batch-describe-merge-conflicts`, se determinan los conflictos de combinación al combinar una ramificación de origen denominada `feature-randomizationfeature` con una ramificación de destino denominada `main` utilizando la estrategia `THREE_WAY_MERGE` de un repositorio denominado `MyDemoRepo`.

```
aws codecommit batch-describe-merge-conflicts \
    --source-commit-specifier feature-randomizationfeature \
    --destination-commit-specifier main \
    --merge-option THREE_WAY_MERGE \
    --repository-name MyDemoRepo
```

Salida:

```
{
    "conflicts": [
        {
            "conflictMetadata": {
                "filePath": "readme.md",
                "fileSizes": {
                    "source": 139,
                    "destination": 230,
                    "base": 85
                },
                "fileModes": {
                    "source": "NORMAL",
                    "destination": "NORMAL",
                    "base": "NORMAL"
                },
                "objectTypes": {
                    "source": "FILE",
                    "destination": "FILE",
                    "base": "FILE"
                },
                "numberOfConflicts": 1,
                "isBinaryFile": {
                    "source": false,
                    "destination": false,
```

```
                    "base": false
                },
                "contentConflict": true,
                "fileModeConflict": false,
                "objectTypeConflict": false,
                "mergeOperations": {
                    "source": "M",
                    "destination": "M"
                }
            },
            "mergeHunks": [
                {
                    "isConflict": true,
                    "source": {
                        "startLine": 0,
                        "endLine": 3,
                        "hunkContent": "VGhpcyBpEXAMPLE=="
                    },
                    "destination": {
                        "startLine": 0,
                        "endLine": 1,
                        "hunkContent": "VXNlIHRoEXAMPLE="
                    }
                }
            ]
        }
    ],
    "errors": [],
    "destinationCommitId": "86958e0aEXAMPLE",
    "sourceCommitId": "6ccd57fdEXAMPLE",
    "baseCommitId": "767b6958EXAMPLE"
}
```

Para obtener más información, consulte Resolver conflictos en una solicitud de extracción en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte BatchDescribeMergeConflicts en la Referencia de comandos de la AWS CLI.

`batch-disassociate-approval-rule-template-from-repositories`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-disassociate-approval-rule-template-from-repositories`.

AWS CLI

Desasociación de una plantilla de regla de aprobación de varios repositorios en una única operación

En el siguiente ejemplo de `batch-disassociate-approval-rule-template-from-repositories`, se desasocia la plantilla de regla de aprobación especificada de los repositorios denominados `MyDemoRepo` y `MyOtherDemoRepo`.

```
aws codecommit batch-disassociate-approval-rule-template-from-repositories \
    --repository-names MyDemoRepo, MyOtherDemoRepo  \
    --approval-rule-template-name 1-approval-rule-for-all pull requests
```

Salida:

```
{
    "disassociatedRepositoryNames": [
        "MyDemoRepo",
        "MyOtherDemoRepo"
    ],
    "errors": []
}
```

Para obtener más información, consulte Desasociar una plantilla de regla de aprobación en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte BatchDisassociateApprovalRuleTemplateFromRepositories en la Referencia de comandos de la AWS CLI.

`batch-get-commits`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-commits`.

AWS CLI

Visualización de información acerca de varias confirmaciones

En el siguiente ejemplo de `batch-get-commits`, se muestran los detalles de las confirmaciones especificadas.

```
aws codecommit batch-get-commits  \
    --repository-name MyDemoRepo  \
    --commit-ids 317f8570EXAMPLE 4c925148EXAMPLE
```

Salida:


```
{
    "commits": [
      {
        "additionalData": "",
        "committer": {
            "date": "1508280564 -0800",
            "name": "Mary Major",
            "email": "mary_major@example.com"
        },
        "author": {
            "date": "1508280564 -0800",
            "name": "Mary Major",
            "email": "mary_major@example.com"
        },
        "commitId": "317f8570EXAMPLE",
        "treeId": "1f330709EXAMPLE",
        "parents": [
            "6e147360EXAMPLE"
        ],
        "message": "Change variable name and add new response element"
    },
    {
        "additionalData": "",
        "committer": {
            "date": "1508280542 -0800",
            "name": "Li Juan",
            "email": "li_juan@example.com"
        },
        "author": {
            "date": "1508280542 -0800",
            "name": "Li Juan",
            "email": "li_juan@example.com"
        },
        "commitId": "4c925148EXAMPLE",
        "treeId": "1f330709EXAMPLE",
        "parents": [
            "317f8570EXAMPLE"
```

```
        ],
        "message": "Added new class"
    }
}
```

Para obtener más información, consulte Consulta los detalles de la confirmación en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte BatchGetCommits en la Referencia de comandos de la AWS CLI.

`batch-get-repositories`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-repositories`.

AWS CLI

Visualización de información de varios repositorios

En este ejemplo, se muestra información sobre varios repositorios de AWS CodeCommit.

```
aws codecommit batch-get-repositories \
    --repository-names MyDemoRepo MyOtherDemoRepo
```

Salida:

```
{
    "repositoriesNotFound": [],
    "repositories": [
         {
            "creationDate": 1429203623.625,
            "defaultBranch": "main",
            "repositoryName": "MyDemoRepo",
            "cloneUrlSsh": "ssh://git-codecommit.us-east-2.amazonaws.com/v1/repos/
MyDemoRepo",
            "lastModifiedDate": 1430783812.0869999,
            "repositoryDescription": "My demonstration repository",
            "cloneUrlHttp": "https://codecommit.us-east-2.amazonaws.com/v1/repos/
MyDemoRepo",
            "repositoryId": "f7579e13-b83e-4027-aaef-650c0EXAMPLE",
            "Arn": "arn:aws:codecommit:us-east-2:111111111111:MyDemoRepo"
            "accountId": "111111111111"
        },
```

```
        {
            "creationDate": 1429203623.627,
            "defaultBranch": "main",
            "repositoryName": "MyOtherDemoRepo",
            "cloneUrlSsh": "ssh://git-codecommit.us-east-2.amazonaws.com/v1/repos/
MyOtherDemoRepo",
            "lastModifiedDate": 1430783812.0889999,
            "repositoryDescription": "My other demonstration repository",
            "cloneUrlHttp": "https://codecommit.us-east-2.amazonaws.com/v1/repos/
MyOtherDemoRepo",
            "repositoryId": "cfc29ac4-b0cb-44dc-9990-f6f51EXAMPLE",
            "Arn": "arn:aws:codecommit:us-east-2:111111111111:MyOtherDemoRepo"
            "accountId": "111111111111"
        }
    ],
    "repositoriesNotFound": []
}
```

- Para obtener información sobre la API, consulte BatchGetRepositories en la Referencia de comandos de la AWS CLI.

`create-approval-rule-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-approval-rule-template`.

AWS CLI

Creación de una plantilla de regla de aprobación

En el siguiente ejemplo de `create-approval-rule-template`, se crea una plantilla de regla de aprobación denominada `2-approver-rule-for-main `` . The template requires two users who assume the role of ``CodeCommitReview` para aprobar cualquier solicitud de extracción antes de que se pueda combinar con la ramificación `main`.

```
aws codecommit create-approval-rule-template \
    --approval-rule-template-name 2-approver-rule-for-main \
    --approval-rule-template-description  "Requires two developers from the team to
 approve the pull request if the destination branch is main" \
    --approval-rule-template-content "{\"Version\": \"2018-11-08\",
\"DestinationReferences\": [\"refs/heads/main\"],\"Statements\": [{\"Type
\": \"Approvers\",\"NumberOfApprovalsNeeded\": 2,\"ApprovalPoolMembers\":
 [\"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}"
```

Salida:

```
{
    "approvalRuleTemplate": {
        "approvalRuleTemplateName": "2-approver-rule-for-main",
        "creationDate": 1571356106.936,
        "approvalRuleTemplateId": "dd8b17fe-EXAMPLE",
        "approvalRuleTemplateContent": "{\"Version\": \"2018-11-08\",
\"DestinationReferences\": [\"refs/heads/main\"],\"Statements\": [{\"Type
\": \"Approvers\",\"NumberOfApprovalsNeeded\": 2,\"ApprovalPoolMembers\":
 [\"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}",
        "lastModifiedUser": "arn:aws:iam::123456789012:user/Mary_Major",
        "approvalRuleTemplateDescription": "Requires two developers from the team to
 approve the pull request if the destination branch is main",
        "lastModifiedDate": 1571356106.936,
        "ruleContentSha256": "4711b576EXAMPLE"
    }
}
```

Para obtener más información, consulte Crear una plantilla de regla de aprobación en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte CreateApprovalRuleTemplate en la Referencia de comandos de la AWS CLI.

`create-branch`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-branch`.

AWS CLI

Creación de una ramificación

En este ejemplo, se crea una ramificación en un repositorio de AWS CodeCommit. Este comando devuelve resultados solo si hay errores.

Comando:

```
aws codecommit create-branch --repository-name MyDemoRepo --branch-name MyNewBranch
 --commit-id 317f8570EXAMPLE
```

Salida:

```
None.
```

- Para obtener información sobre la API, consulte CreateBranch en la Referencia de comandos de la AWS CLI.

`create-commit`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-commit`.

AWS CLI

Creación de una confirmación

En el siguiente ejemplo de `create-commit`, se muestra cómo crear una confirmación inicial para un repositorio que añada un archivo `readme.md` a un repositorio denominado `MyDemoRepo` en la ramificación `main`.

```
aws codecommit create-commit \
    --repository-name MyDemoRepo \
    --branch-name main \
    --put-files "filePath=readme.md,fileContent='Welcome to our team repository.'"
```

Salida:

```
{
    "filesAdded": [
        {
            "blobId": "5e1c309d-EXAMPLE",
            "absolutePath": "readme.md",
            "fileMode": "NORMAL"
        }
    ],
    "commitId": "4df8b524-EXAMPLE",
    "treeId": "55b57003-EXAMPLE",
    "filesDeleted": [],
    "filesUpdated": []
}
```

Para obtener más información, consulte Creación de una confirmación en AWS CodeCommit en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte CreateCommit en la Referencia de comandos de la AWS CLI.

`create-pull-request-approval-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-pull-request-approval-rule`.

AWS CLI

Creación de una regla de aprobación para una solicitud de extracción

En el ejemplo siguiente de `create-pull-request-approval-rule`, se crea una regla de aprobación denominada `Require two approved approvers` para una solicitud de extracción especificada. La regla especifica que se requieren dos aprobaciones de un grupo de aprobación. El grupo incluye a todos los usuarios que acceden a CodeCommit y asumen el rol de `CodeCommitReview` en la cuenta de AWS `123456789012`. También incluye un usuario de IAM o un usuario federado denominado `Nikhil_Jayashankar` en la misma cuenta de AWS.

```
aws codecommit create-pull-request-approval-rule  \
    --approval-rule-name "Require two approved approvers"  \
    --approval-rule-content "{\"Version\": \"2018-11-08\",\"Statements\":
 [{\"Type\": \"Approvers\",\"NumberOfApprovalsNeeded\": 2,\"ApprovalPoolMembers
\": [\"CodeCommitApprovers:123456789012:Nikhil_Jayashankar\",
 \"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}"
```

Salida:

```
{
    "approvalRule": {
        "approvalRuleName": "Require two approved approvers",
        "lastModifiedDate": 1570752871.932,
        "ruleContentSha256": "7c44e6ebEXAMPLE",
        "creationDate": 1570752871.932,
        "approvalRuleId": "aac33506-EXAMPLE",
        "approvalRuleContent": "{\"Version\": \"2018-11-08\",\"Statements\":
 [{\"Type\": \"Approvers\",\"NumberOfApprovalsNeeded\": 2,\"ApprovalPoolMembers
\": [\"CodeCommitApprovers:123456789012:Nikhil_Jayashankar\",
 \"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}",
        "lastModifiedUser": "arn:aws:iam::123456789012:user/Mary_Major"
    }
```

```
}
```

Para obtener más información, consulte Crear una regla de aprobación en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte CreatePullRequestApprovalRule en la Referencia de comandos de la AWS CLI.

`create-pull-request`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-pull-request`.

AWS CLI

Creación de una solicitud de extracción

En el siguiente ejemplo de `create-pull-request`, se crea una solicitud de extracción denominada Pronunciation difficulty analyzer (Analizador de dificultades de pronunciación) con la descripción Please review these changes by Tuesday (Revisar estos cambios antes del martes) que se dirige a la ramificación de origen jane-branch y se combina con la ramificación predeterminada main de un repositorio de AWS CodeCommit denominado MyDemoRepo.

```
aws codecommit create-pull-request \
    --title "My Pull Request" \
    --description "Please review these changes by Tuesday" \
    --client-request-token 123Example \
    --targets repositoryName=MyDemoRepo,sourceReference=MyNewBranch
```

Salida:

```
{
    "pullRequest": {
        "approvalRules": [
            {
                "approvalRuleContent": "{\"Version\": \"2018-11-08\",
\"DestinationReferences\": [\"refs/heads/main\"],\"Statements\": [{\"Type
\": \"Approvers\",\"NumberOfApprovalsNeeded\": 2,\"ApprovalPoolMembers\":
 [\"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}",
                "approvalRuleId": "dd8b17fe-EXAMPLE",
                "approvalRuleName": "2-approver-rule-for-main",
                "creationDate": 1571356106.936,
                "lastModifiedDate": 571356106.936,
```

```
                "lastModifiedUser": "arn:aws:iam::123456789012:user/Mary_Major",
                "originApprovalRuleTemplate": {
                    "approvalRuleTemplateId": "dd3d22fe-EXAMPLE",
                    "approvalRuleTemplateName": "2-approver-rule-for-main"
                },
                "ruleContentSha256": "4711b576EXAMPLE"
            }
        ],
        "authorArn": "arn:aws:iam::111111111111:user/Jane_Doe",
        "description": "Please review these changes by Tuesday",
        "title": "Pronunciation difficulty analyzer",
        "pullRequestTargets": [
            {
                "destinationCommit": "5d036259EXAMPLE",
                "destinationReference": "refs/heads/main",
                "repositoryName": "MyDemoRepo",
                "sourceCommit": "317f8570EXAMPLE",
                "sourceReference": "refs/heads/jane-branch",
                "mergeMetadata": {
                    "isMerged": false
                }
            }
        ],
        "lastActivityDate": 1508962823.285,
        "pullRequestId": "42",
        "clientRequestToken": "123Example",
        "pullRequestStatus": "OPEN",
        "creationDate": 1508962823.285
    }
}
```

- Para obtener información sobre la API, consulte CreatePullRequest en la Referencia de comandos de la AWS CLI.

`create-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-repository`.

AWS CLI

Creación de un repositorio

En este ejemplo, se crea un repositorio y se asocia a la cuenta de AWS del usuario.

Comando:

```
aws codecommit create-repository --repository-name MyDemoRepo --repository-
description "My demonstration repository"
```

Salida:

```
{
    "repositoryMetadata": {
        "repositoryName": "MyDemoRepo",
                "cloneUrlSsh": "ssh://git-codecommit.us-east-1.amazonaws.com/v1/
repos/MyDemoRepo",
                "lastModifiedDate": 1444766838.027,
        "repositoryDescription": "My demonstration repository",
                "cloneUrlHttp": "https://git-codecommit.us-east-1.amazonaws.com/v1/
repos/MyDemoRepo",
        "repositoryId": "f7579e13-b83e-4027-aaef-650c0EXAMPLE",
                "Arn": "arn:aws:codecommit:us-
east-1:111111111111EXAMPLE:MyDemoRepo",
        "accountId": "111111111111"
    }
}
```

- Para obtener información sobre la API, consulte CreateRepository en la Referencia de comandos de la AWS CLI.

`create-unreferenced-merge-commit`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-unreferenced-merge-commit`.

AWS CLI

Creación de una confirmación sin referencia que representa el resultado de combinar dos especificadores

En el siguiente ejemplo de `create-unreferenced-merge-commit`, se crea una confirmación que representa los resultados de una combinación entre una ramificación de origen denominada `bugfix-1234` con una ramificación de destino denominada `main` con la estrategia THREE_WAY_MERGE en un repositorio llamado `MyDemoRepo`.

```
aws codecommit create-unreferenced-merge-commit \
    --source-commit-specifier bugfix-1234 \
    --destination-commit-specifier main \
    --merge-option THREE_WAY_MERGE \
    --repository-name MyDemoRepo \
    --name "Maria Garcia" \
    --email "maria_garcia@example.com" \
    --commit-message "Testing the results of this merge."
```

Salida:

```
{
    "commitId": "4f178133EXAMPLE",
    "treeId": "389765daEXAMPLE"
}
```

Para obtener más información, consulte Resolver conflictos en una solicitud de extracción en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte CreateUnreferencedMergeCommit en la Referencia de comandos de la AWS CLI.

`credential-helper`

En el siguiente ejemplo de código, se muestra cómo utilizar `credential-helper`.

AWS CLI

Configuración del ayudante de credenciales incluido en la AWS CLI con AWS CodeCommit

La utilidad `credential-helper` no está diseñada para llamarla directamente desde la AWS CLI. Por el contrario, está pensada para usarse como parámetro con el comando `git config` al configurar el equipo local. Permite que Git use HTTPS y una versión con firma criptográfica de sus credenciales de usuario de IAM o del rol de la instancia de Amazon EC2 cada vez que Git requiera autenticarse con AWS para interactuar con los repositorios de CodeCommit.

```
git config --global credential.helper '!aws codecommit credential-helper $@'
git config --global credential.UseHttpPath true
```

Salida:

```
[credential]
    helper = !aws codecommit credential-helper $@
    UseHttpPath = true
```

Para obtener más información, consulte Configuración de AWS CodeCommit con otros métodos en la Guía del usuario de AWS CodeCommit. Revise el contenido detenidamente y, a continuación, siga los procedimientos descritos en uno de los siguientes temas: Para configurar conexiones HTTPS en Linux, macOS o Unix o Para configurar conexiones HTTPS en Windows en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte CredentialHelper en la Referencia de comandos de la AWS CLI.

`delete-approval-rule-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-approval-rule-template`.

AWS CLI

Eliminación de una plantilla de regla de aprobación

En el siguiente ejemplo de `delete-approval-rule-template`, se elimina la plantilla de regla de aprobación especificada.

```
aws codecommit delete-approval-rule-template  \
    --approval-rule-template-name 1-approver-for-all-pull-requests
```

Salida:

```
{
    "approvalRuleTemplateId": "41de97b7-EXAMPLE"
}
```

Para obtener más información, consulte Eliminar una plantilla de regla de aprobación en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte DeleteApprovalRuleTemplate en la Referencia de comandos de la AWS CLI.

`delete-branch`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-branch`.

AWS CLI

Eliminación de una ramificación

En este ejemplo se muestra cómo eliminar una ramificación en un repositorio de AWS CodeCommit.

Comando:

```
aws codecommit delete-branch --repository-name MyDemoRepo --branch-name MyNewBranch
```

Salida:

```
{
  "branch": {
      "commitId": "317f8570EXAMPLE",
      "branchName": "MyNewBranch"
  }
}
```

- Para obtener información sobre la API, consulte DeleteBranch en la Referencia de comandos de la AWS CLI.

`delete-comment-content`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-comment-content`.

AWS CLI

Eliminación del contenido de un comentario

Solo puede eliminar el contenido de un comentario que ha creado usted mismo. En este ejemplo, se muestra cómo eliminar el contenido de un comentario con el ID generado por el sistema `ff30b348EXAMPLEb9aa670f`.

```
aws codecommit delete-comment-content \
```

```
    --comment-id ff30b348EXAMPLEb9aa670f
```

Salida:

```
{
    "comment": {
        "creationDate": 1508369768.142,
        "deleted": true,
        "lastModifiedDate": 1508369842.278,
        "clientRequestToken": "123Example",
        "commentId": "ff30b348EXAMPLEb9aa670f",
        "authorArn": "arn:aws:iam::111111111111:user/Li_Juan",
        "callerReactions": [],
        "reactionCounts":
        {
            "CLAP" : 1
        }
    }
}
```

- Para obtener información sobre la API, consulte DeleteCommentContent en la Referencia de comandos de la AWS CLI.

`delete-file`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-file`.

AWS CLI

Eliminación de un archivo

En el siguiente ejemplo de `delete-file`, se muestra cómo eliminar un archivo denominado `README.md` de una ramificación denominada `main` con el ID de confirmación más reciente `c5709475EXAMPLE` en un repositorio denominado `MyDemoRepo`.

```
aws codecommit delete-file \
    --repository-name MyDemoRepo \
    --branch-name main \
    --file-path README.md \
    --parent-commit-id c5709475EXAMPLE
```

Salida:

```
{
    "blobId":"559b44fEXAMPLE",
    "commitId":"353cf655EXAMPLE",
    "filePath":"README.md",
    "treeId":"6bc824cEXAMPLE"
}
```

Para obtener más información, consulte Editar o eliminar un archivo en AWS CodeCommit en la guía Referencia de la API de AWS CodeCommit.

- Para obtener información sobre la API, consulte DeleteFile en la Referencia de comandos de la AWS CLI.

`delete-pull-request-approval-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-pull-request-approval-rule`.

AWS CLI

Eliminación de una regla de aprobación de una solicitud de extracción

En el siguiente ejemplo de `delete-pull-request-approval-rule`, se elimina una regla de aprobación denominada `My Approval Rule` de una solicitud de extracción especificada.

```
aws codecommit delete-pull-request-approval-rule  \
    --approval-rule-name "My Approval Rule"  \
    --pull-request-id 15
```

Salida:

```
{
    "approvalRuleId": "077d8e8a8-EXAMPLE"
}
```

Para obtener más información, consulte Editar o eliminar una regla de aprobación en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte DeletePullRequestApprovalRule en la Referencia de comandos de la AWS CLI.

`delete-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-repository`.

AWS CLI

Eliminación de un repositorio

En este ejemplo, se muestra cómo eliminar un repositorio de AWS CodeCommit.

Comando:

```
aws codecommit delete-repository --repository-name MyDemoRepo
```

Salida:

```
{
  "repositoryId": "f7579e13-b83e-4027-aaef-650c0EXAMPLE"
}
```

- Para obtener información sobre la API, consulte DeleteRepository en la Referencia de comandos de la AWS CLI.

`describe-merge-conflicts`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-merge-conflicts`.

AWS CLI

Obtención de información detallada sobre los conflictos de combinación

En el siguiente ejemplo de `describe-merge-conflicts`, se determinan los conflictos de combinación de un archivo denominado `readme.md` en las ramificaciones de origen y destino especificadas con la estrategia THREE_WAY_MERGE.

```
aws codecommit describe-merge-conflicts \
    --source-commit-specifier feature-randomizationfeature \
    --destination-commit-specifier main \
    --merge-option THREE_WAY_MERGE \
    --file-path readme.md \
    --repository-name MyDemoRepo
```

Salida:

```
{
    "conflictMetadata": {
        "filePath": "readme.md",
        "fileSizes": {
            "source": 139,
            "destination": 230,
            "base": 85
        },
        "fileModes": {
            "source": "NORMAL",
            "destination": "NORMAL",
            "base": "NORMAL"
        },
        "objectTypes": {
            "source": "FILE",
            "destination": "FILE",
            "base": "FILE"
        },
        "numberOfConflicts": 1,
        "isBinaryFile": {
            "source": false,
            "destination": false,
            "base": false
        },
        "contentConflict": true,
        "fileModeConflict": false,
        "objectTypeConflict": false,
        "mergeOperations": {
            "source": "M",
            "destination": "M"
        }
    },
    "mergeHunks": [
        {
            "isConflict": true,
            "source": {
                "startLine": 0,
                "endLine": 3,
                "hunkContent": "VGhpcyBpEXAMPLE="
            },
            "destination": {
                "startLine": 0,
```

```
                "endLine": 1,
                "hunkContent": "VXNlIHRoEXAMPLE="
            }
        }
    ],
    "destinationCommitId": "86958e0aEXAMPLE",
    "sourceCommitId": "6ccd57fdEXAMPLE",
    "baseCommitId": "767b69580EXAMPLE"
}
```

Para obtener más información, consulte Resolver conflictos en una solicitud de extracción en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte DescribeMergeConflicts en la Referencia de comandos de la AWS CLI.

`describe-pull-request-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-pull-request-events`.

AWS CLI

Visualización de los eventos de una solicitud de extracción

En el siguiente ejemplo de `describe-pull-request-events`, se recuperan los eventos de una solicitud de extracción con el ID 8.

```
aws codecommit describe-pull-request-events --pull-request-id 8
```

Salida:

```
{
    "pullRequestEvents": [
        {
            "pullRequestId": "8",
            "pullRequestEventType": "PULL_REQUEST_CREATED",
            "eventDate": 1510341779.53,
            "actor": "arn:aws:iam::111111111111:user/Zhang_Wei"
        },
        {
            "pullRequestStatusChangedEventMetadata": {
                "pullRequestStatus": "CLOSED"
            },
```

```
            "pullRequestId": "8",
            "pullRequestEventType": "PULL_REQUEST_STATUS_CHANGED",
            "eventDate": 1510341930.72,
            "actor": "arn:aws:iam::111111111111:user/Jane_Doe"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribePullRequestEvents en la Referencia de comandos de la AWS CLI.

`disassociate-approval-rule-template-from-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-approval-rule-template-from-repository`.

AWS CLI

Desasociación de una plantilla de regla de aprobación de un repositorio

En el siguiente ejemplo de `disassociate-approval-rule-template-from-repository`, se desasocia la plantilla de regla de aprobación especificada de un repositorio denominado `MyDemoRepo`.

```
aws codecommit disassociate-approval-rule-template-from-repository \
    --repository-name MyDemoRepo  \
    --approval-rule-template-name 1-approver-rule-for-all-pull-requests
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Desasociar una plantilla de regla de aprobación en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte DisassociateApprovalRuleTemplateFromRepository en la Referencia de comandos de la AWS CLI.

`evaluate-pull-request-approval-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `evaluate-pull-request-approval-rules`.

AWS CLI

Evaluación de si una solicitud de extracción cumple con todas las reglas de aprobación

En el siguiente ejemplo de `evaluate-pull-request-approval-rules`, se evalúa el estado de las reglas de aprobación de la solicitud de extracción especificada. En este ejemplo, no se cumple una regla de aprobación en la solicitud de extracción, por lo que el resultado del comando muestra `false` en el valor `approved`.

```
aws codecommit evaluate-pull-request-approval-rules \
    --pull-request-id 27  \
    --revision-id 9f29d167EXAMPLE
```

Salida:

```
{
    "evaluation": {
        "approved": false,
        "approvalRulesNotSatisfied": [
            "Require two approved approvers"
        ],
        "overridden": false,
        "approvalRulesSatisfied": []
    }
}
```

Para obtener más información, consulte Combinación de una solicitud de extracción en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte EvaluatePullRequestApprovalRules en la Referencia de comandos de la AWS CLI.

`get-approval-rule-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-approval-rule-template`.

AWS CLI

Obtención del contenido de una plantilla de regla de aprobación

En el siguiente ejemplo de `get-approval-rule-template`, se obtiene el contenido de una plantilla de regla de aprobación denominada `1-approver-rule-for-all-pull-requests`.

```
aws codecommit get-approval-rule-template \
    --approval-rule-template-name 1-approver-rule-for-all-pull-requests
```

Salida:

```
{
    "approvalRuleTemplate": {
        "approvalRuleTemplateContent": "{\"Version\": \"2018-11-08\",\"Statements\":
 [{\"Type\": \"Approvers\",\"NumberOfApprovalsNeeded\": 1,\"ApprovalPoolMembers\":
 [\"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}",
        "ruleContentSha256": "621181bbEXAMPLE",
        "lastModifiedDate": 1571356106.936,
        "creationDate": 1571356106.936,
        "approvalRuleTemplateName": "1-approver-rule-for-all-pull-requests",
        "lastModifiedUser": "arn:aws:iam::123456789012:user/Li_Juan",
        "approvalRuleTemplateId": "a29abb15-EXAMPLE",
        "approvalRuleTemplateDescription": "All pull requests must be approved by
 one developer on the team."
    }
}
```

Para obtener más información, consulte Administrar plantillas de reglas de aprobación en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte GetApprovalRuleTemplate en la Referencia de comandos de la AWS CLI.

`get-blob`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-blob`.

AWS CLI

Visualización de información sobre un objeto blob de Git

En el siguiente ejemplo de `get-blob`, se recupera información acerca de un blob de Git con el ID 2eb4af3bEXAMPLE de un repositorio de AWS CodeCommit denominado MyDemoRepo.

```
aws codecommit get-blob  --repository-name MyDemoRepo  --blob-id 2eb4af3bEXAMPLE
```

Salida:

```
{
    "content": "QSBCaW5hcnkgTGFyToEXAMPLE="
}
```

- Para obtener información sobre la API, consulte GetBlob en la Referencia de comandos de la AWS CLI.

`get-branch`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-branch`.

AWS CLI

Obtención de información sobre una ramificación

En este ejemplo, se obtiene información sobre una ramificación de un repositorio de AWS CodeCommit.

Comando:

```
aws codecommit get-branch --repository-name MyDemoRepo --branch-name MyNewBranch
```

Salida:

```
{
  "BranchInfo": {
        "commitID": "317f8570EXAMPLE",
                "branchName": "MyNewBranch"
  }
}
```

- Para obtener información sobre la API, consulte GetBranch en la Referencia de comandos de la AWS CLI.

`get-comment-reactions`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-comment-reactions`.

AWS CLI

Visualización de las reacciones con emojis a un comentario

En el siguiente ejemplo de `get-comment-reactions`, se genera una lista de todas las reacciones con emojis a un comentario con el ID `abcd1234EXAMPLEb5678efgh`. Si la fuente del intérprete de comandos admite la visualización de Emoji versión 1.0, en la salida de `emoji`, se mostrará el emoji.

```
aws codecommit get-comment-reactions \
    --comment-id abcd1234EXAMPLEb5678efgh
```

Salida:

```
{
    "reactionsForComment": {
        [
           {
               "reaction": {
                    "emoji:"??",
                    "shortCode": "thumbsup",
                    "unicode": "U+1F44D"
                },
                "users": [
                    "arn:aws:iam::123456789012:user/Li_Juan",
                    "arn:aws:iam::123456789012:user/Mary_Major",
                    "arn:aws:iam::123456789012:user/Jorge_Souza"
                ]
            },
            {
                "reaction": {
                    "emoji": "??",
                    "shortCode": "thumbsdown",
                    "unicode": "U+1F44E"
                },
                "users": [
                    "arn:aws:iam::123456789012:user/Nikhil_Jayashankar"
                ]
            },
            {
                "reaction": {
                    "emoji": "??",
                    "shortCode": "confused",
                    "unicode": "U+1F615"
                },
                "users": [
```

```
                    "arn:aws:iam::123456789012:user/Saanvi_Sarkar"
                ]
            }
        ]
    }
}
```

Para obtener más información, consulte Comenta una confirmación en AWS CodeCommit en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte GetCommentReactions en la Referencia de comandos de la AWS CLI.

`get-comment`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-comment`.

AWS CLI

Visualización de los detalles de un comentario

En este ejemplo, se muestra cómo ver los detalles de un comentario con el ID generado por el sistema `ff30b348EXAMPLEb9aa670f`.

```
aws codecommit get-comment \
    --comment-id ff30b348EXAMPLEb9aa670f
```

Salida:

```
{
    "comment": {
        "authorArn": "arn:aws:iam::111111111111:user/Li_Juan",
        "clientRequestToken": "123Example",
        "commentId": "ff30b348EXAMPLEb9aa670f",
        "content": "Whoops - I meant to add this comment to the line, but I don't
 see how to delete it.",
        "creationDate": 1508369768.142,
        "deleted": false,
        "commentId": "",
        "lastModifiedDate": 1508369842.278,
        "callerReactions": [],
```

```
        "reactionCounts":
        {
            "SMILE" : 6,
            "THUMBSUP" : 1
        }
    }
}
```

- Para obtener información sobre la API, consulte GetComment en la Referencia de comandos de la AWS CLI.

`get-comments-for-compared-commit`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-comments-for-compared-commit`.

AWS CLI

Visualización de los comentarios sobre una confirmación

En este ejemplo se muestra cómo ver los comentarios realizados en la comparación de dos confirmaciones en un repositorio denominado `MyDemoRepo`.

```
aws codecommit get-comments-for-compared-commit \
    --repository-name MyDemoRepo \
    --before-commit-ID 6e147360EXAMPLE \
    --after-commit-id 317f8570EXAMPLE
```

Salida:

```
{
    "commentsForComparedCommitData": [
        {
            "afterBlobId": "1f330709EXAMPLE",
            "afterCommitId": "317f8570EXAMPLE",
            "beforeBlobId": "80906a4cEXAMPLE",
            "beforeCommitId": "6e147360EXAMPLE",
            "comments": [
                {
                    "authorArn": "arn:aws:iam::111111111111:user/Li_Juan",
                    "clientRequestToken": "123Example",
```

```
                    "commentId": "ff30b348EXAMPLEb9aa670f",
                    "content": "Whoops - I meant to add this comment to the line,
 not the file, but I don't see how to delete it.",
                    "creationDate": 1508369768.142,
                    "deleted": false,
                    "CommentId": "123abc-EXAMPLE",
                    "lastModifiedDate": 1508369842.278,
                    "callerReactions": [],
                    "reactionCounts":
                    {
                        "SMILE" : 6,
                        "THUMBSUP" : 1
                    }
                },
                {
                    "authorArn": "arn:aws:iam::111111111111:user/Li_Juan",
                    "clientRequestToken": "123Example",
                    "commentId": "553b509bEXAMPLE56198325",
                    "content": "Can you add a test case for this?",
                    "creationDate": 1508369612.240,
                    "deleted": false,
                    "commentId": "456def-EXAMPLE",
                    "lastModifiedDate": 1508369612.240,
                    "callerReactions": [],
                    "reactionCounts":
                    {
                        "THUMBSUP" : 2
                    }
                }
            ],
            "location": {
                "filePath": "cl_sample.js",
                "filePosition": 1232,
                "relativeFileVersion": "after"
            },
            "repositoryName": "MyDemoRepo"
        }
    ],
    "nextToken": "exampleToken"
}
```

- Para obtener información sobre la API, consulte GetCommentsForComparedCommit en la Referencia de comandos de la AWS CLI.

`get-comments-for-pull-request`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-comments-for-pull-request`.

AWS CLI

Visualización de los comentarios de una solicitud de extracción

En este ejemplo, se muestra cómo ver los comentarios de una solicitud de extracción en un repositorio denominado `MyDemoRepo`.

```
aws codecommit get-comments-for-pull-request \
    --repository-name MyDemoRepo \
    --before-commit-ID 317f8570EXAMPLE \
    --after-commit-id 5d036259EXAMPLE
```

Salida:

```
{
    "commentsForPullRequestData": [
        {
            "afterBlobId": "1f330709EXAMPLE",
            "afterCommitId": "5d036259EXAMPLE",
            "beforeBlobId": "80906a4cEXAMPLE",
            "beforeCommitId": "317f8570EXAMPLE",
            "comments": [
                {
                    "authorArn": "arn:aws:iam::111111111111:user/Saanvi_Sarkar",
                    "clientRequestToken": "",
                    "commentId": "abcd1234EXAMPLEb5678efgh",
                    "content": "These don't appear to be used anywhere. Can we
 remove them?",
                    "creationDate": 1508369622.123,
                    "deleted": false,
                    "lastModifiedDate": 1508369622.123,
                    "callerReactions": [],
                    "reactionCounts":
                    {
                        "THUMBSUP" : 6,
                        "CONFUSED" : 1
                    }
                },
                {
```

```
                    "authorArn": "arn:aws:iam::111111111111:user/Li_Juan",
                    "clientRequestToken": "",
                    "commentId": "442b498bEXAMPLE5756813",
                    "content": "Good catch. I'll remove them.",
                    "creationDate": 1508369829.104,
                    "deleted": false,
                    "lastModifiedDate": 150836912.273,
                    "callerReactions": ["THUMBSUP"]
                    "reactionCounts":
                    {
                        "THUMBSUP" : 14
                    }
                }
            ],
            "location": {
                "filePath": "ahs_count.py",
                "filePosition": 367,
                "relativeFileVersion": "AFTER"
            },
            "repositoryName": "MyDemoRepo",
            "pullRequestId": "42"
        }
    ],
    "nextToken": "exampleToken"
}
```

- Para obtener información sobre la API, consulte GetCommentsForPullRequest en la Referencia de comandos de la AWS CLI.

`get-commit`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-commit`.

AWS CLI

Visualización de la información sobre una confirmación en un repositorio

En este ejemplo, se muestran detalles sobre una confirmación con el ID generado por el sistema 7e9fd3091thisisanexamplethisisanexample1 en un repositorio de AWS CodeCommit denominado MyDemoRepo.

Comando:

```
aws codecommit get-commit --repository-name MyDemoRepo --commit-
id 7e9fd3091thisisanexamplethisisanexample1
```

Salida:

```
{
  "commit": {
      "additionalData": "",
      "committer": {
          "date": "1484167798 -0800",
          "name": "Mary Major",
          "email": "mary_major@example.com"
      },
      "author": {
          "date": "1484167798 -0800",
          "name": "Mary Major",
          "email": "mary_major@example.com"
      },
      "treeId": "347a3408thisisanexampletreeidexample",
      "parents": [
          "7aa87a031thisisanexamplethisisanexample1"
      ],
      "message": "Fix incorrect variable name"
  }
}
```

- Para obtener información sobre la API, consulte GetCommit en la Referencia de comandos de la AWS CLI.

`get-differences`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-differences`.

AWS CLI

Obtención de información sobre las diferencias de un especificador de confirmación en un repositorio

En este ejemplo, se muestra información de metadatos de visualización acerca de los cambios entre dos especificadores de confirmación (ramificación, etiqueta, HEAD u otras referencias completas, como los ID de confirmación) en una carpeta con nombre cambiado del repositorio

de AWS CodeCommit denominado MyDemoRepo. En el ejemplo, se incluyen varias opciones que no son obligatorias, como --before-commit-specifier, --before-path y --afterpath, para ilustrar con más detalle cómo se pueden utilizar estas opciones para limitar los resultados. La respuesta incluye los permisos del modo de archivo.

Comando:

```
aws codecommit get-differences --repository-name MyDemoRepo --before-
commit-specifier 955bba12thisisanexamplethisisanexample --after-commit-
specifier 14a95463thisisanexamplethisisanexample --before-path tmp/example-folder --
after-path tmp/renamed-folder
```

Salida:

```
{
  "differences": [
      {
          "afterBlob": {
              "path": "blob.txt",
              "blobId": "2eb4af3b1thisisanexamplethisisanexample1",
              "mode": "100644"
          },
          "changeType": "M",
          "beforeBlob": {
              "path": "blob.txt",
              "blobId": "bf7fcf281thisisanexamplethisisanexample1",
              "mode": "100644"
          }
      }
  ]
}
```

- Para obtener información sobre la API, consulte GetDifferences en la Referencia de comandos de la AWS CLI.

`get-file`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-file`.

AWS CLI

Obtención del contenido codificado en base-64 de un archivo en un repositorio de AWS CodeCommit

En el siguiente ejemplo de `get-file`, se muestra cómo obtener el contenido codificado en base-64 de un archivo denominado `README.md` a partir de una ramificación denominada `main` en un repositorio llamado `MyDemoRepo`.

```
aws codecommit get-file \
    --repository-name MyDemoRepo \
    --commit-specifier main \
    --file-path README.md
```

Salida:

```
{
    "blobId":"559b44fEXAMPLE",
    "commitId":"c5709475EXAMPLE",
    "fileContent":"IyBQaHVzEXAMPLE",
    "filePath":"README.md",
    "fileMode":"NORMAL",
    "fileSize":1563
}
```

Para obtener más información, consulte GetFile en la guía Referencia de la API de AWS CodeCommit.

- Para obtener información sobre la API, consulte GetFile en la Referencia de comandos de la AWS CLI.

`get-folder`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-folder`.

AWS CLI

Obtención del contenido de una carpeta en un repositorio de AWS CodeCommit

En el siguiente ejemplo de `get-folder`, se muestra cómo obtener el contenido de una carpeta de nivel superior de un repositorio denominado `MyDemoRepo`.

```
aws codecommit get-folder --repository-name MyDemoRepo --folder-path ""
```

Salida:

```
{
    "commitId":"c5709475EXAMPLE",
    "files":[
        {
            "absolutePath":".gitignore",
            "blobId":"74094e8bEXAMPLE",
            "fileMode":"NORMAL",
            "relativePath":".gitignore"
        },
        {
            "absolutePath":"Gemfile",
            "blobId":"9ceb72f6EXAMPLE",
            "fileMode":"NORMAL",
            "relativePath":"Gemfile"
        },
        {
            "absolutePath":"Gemfile.lock",
            "blobId":"795c4a2aEXAMPLE",
            "fileMode":"NORMAL",
            "relativePath":"Gemfile.lock"
        },
        {
            "absolutePath":"LICENSE.txt",
            "blobId":"0c7932c8EXAMPLE",
            "fileMode":"NORMAL",
            "relativePath":"LICENSE.txt"
        },
        {
            "absolutePath":"README.md",
            "blobId":"559b44feEXAMPLE",
            "fileMode":"NORMAL",
            "relativePath":"README.md"
        }
    ],
    "folderPath":"",
    "subFolders":[
        {
            "absolutePath":"public",
            "relativePath":"public",
```

```
            "treeId":"d5e92ae3aEXAMPLE"
        },
        {
            "absolutePath":"tmp",
            "relativePath":"tmp",
            "treeId":"d564d0bcEXAMPLE"
        }
    ],
    "subModules":[],
    "symbolicLinks":[],
    "treeId":"7b3c4dadEXAMPLE"
}
```

Para obtener más información, consulte GetFolder en la guía Referencia de la API de AWS CodeCommit.

- Para obtener información sobre la API, consulte GetFolder en la Referencia de comandos de la AWS CLI.

`get-merge-commit`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-merge-commit`.

AWS CLI

Visualización de información sobre una confirmación de combinación

En el siguiente ejemplo de `get-merge-commit`, se muestra información sobre una confirmación de combinación de la ramificación de origen denominada `bugfix-bug1234` con una ramificación de destino denominada `main` en un repositorio denominado `MyDemoRepo`.

```
aws codecommit get-merge-commit \
    --source-commit-specifier bugfix-bug1234 \
    --destination-commit-specifier main \
    --repository-name MyDemoRepo
```

Salida:

```
{
    "sourceCommitId": "c5709475EXAMPLE",
    "destinationCommitId": "317f8570EXAMPLE",
```

```
    "baseCommitId": "fb12a539EXAMPLE",
    "mergeCommitId": "ffc4d608eEXAMPLE"
}
```

Para obtener más información, consulte Consulta los detalles de la confirmación en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte GetMergeCommit en la Referencia de comandos de la AWS CLI.

`get-merge-conflicts`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-merge-conflicts`.

AWS CLI

Visualización de si existen conflictos de combinación en una solicitud de extracción

En el siguiente ejemplo de `get-merge-conflicts`, se muestra si existen conflictos de combinación entre el extremo de una ramificación de origen denominada `feature-randomizationfeature` y una ramificación de destino denominada main en un repositorio llamado `MyDemoRepo`.

```
aws codecommit get-merge-conflicts \
    --repository-name MyDemoRepo \
    --source-commit-specifier feature-randomizationfeature \
    --destination-commit-specifier main \
    --merge-option THREE_WAY_MERGE
```

Salida:

```
{
    "mergeable": false,
    "destinationCommitId": "86958e0aEXAMPLE",
    "sourceCommitId": "6ccd57fdEXAMPLE",
    "baseCommitId": "767b6958EXAMPLE",
    "conflictMetadataList": [
        {
            "filePath": "readme.md",
            "fileSizes": {
                "source": 139,
```

```
                "destination": 230,
                "base": 85
            },
            "fileModes": {
                "source": "NORMAL",
                "destination": "NORMAL",
                "base": "NORMAL"
            },
            "objectTypes": {
                "source": "FILE",
                "destination": "FILE",
                "base": "FILE"
            },
            "numberOfConflicts": 1,
            "isBinaryFile": {
                "source": false,
                "destination": false,
                "base": false
            },
            "contentConflict": true,
            "fileModeConflict": false,
            "objectTypeConflict": false,
            "mergeOperations": {
                "source": "M",
                "destination": "M"
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetMergeConflicts en la Referencia de comandos de la AWS CLI.

`get-merge-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-merge-options`.

AWS CLI

Obtención de información sobre las opciones de combinación disponibles para combinar dos ramificaciones específicas

En el siguiente ejemplo de `get-merge-options`, se determinan las opciones de combinación disponibles para combinar una ramificación de origen denominada `bugfix-bug1234` con una ramificación de destino denominada `main` en un repositorio llamado `MyDemoRepo`.

```
aws codecommit get-merge-options \
    --source-commit-specifier bugfix-bug1234 \
    --destination-commit-specifier main \
    --repository-name MyDemoRepo
```

Salida:

```
{
    "mergeOptions": [
        "FAST_FORWARD_MERGE",
        "SQUASH_MERGE",
        "THREE_WAY_MERGE"
    ],
    "sourceCommitId": "18059494EXAMPLE",
    "destinationCommitId": "ffd3311dEXAMPLE",
    "baseCommitId": "ffd3311dEXAMPLE"
}
```

Para obtener más información, consulte Resolver conflictos en una solicitud de extracción en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte GetMergeOptions en la Referencia de comandos de la AWS CLI.

`get-pull-request-approval-states`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-pull-request-approval-states`.

AWS CLI

Visualización de aprobaciones en una solicitud de extracción

En el siguiente ejemplo de `get-pull-request-approval-states`, se obtienen las aprobaciones de una solicitud de extracción especificada.

```
aws codecommit get-pull-request-approval-states \
    --pull-request-id 8 \
```

```
    --revision-id 9f29d167EXAMPLE
```

Salida:

```
{
    "approvals": [
        {
            "userArn": "arn:aws:iam::123456789012:user/Mary_Major",
            "approvalState": "APPROVE"
        }
    ]
}
```

Para obtener más información, consulte Visualizar las solicitudes de extracción en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte GetPullRequestApprovalStates en la Referencia de comandos de la AWS CLI.

`get-pull-request-override-state`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-pull-request-override-state`.

AWS CLI

Obtención de información sobre el estado de anulación de una solicitud de extracción

En el siguiente ejemplo de `get-pull-request-override-state`, se obtiene el estado de anulación de una solicitud de extracción especificada. En este ejemplo, una usuaria llamada Mary Major ha anulado las reglas de aprobación de la solicitud de extracción, por lo que la salida es un valor de `true`.

```
aws codecommit get-pull-request-override-state \
    --pull-request-id 34  \
    --revision-id 9f29d167EXAMPLE
```

Salida:

```
{
    "overridden": true,
```

```
    "overrider": "arn:aws:iam::123456789012:user/Mary_Major"
}
```

Para obtener más información, consulte Anular reglas de aprobación en una solicitud de extracción en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte GetPullRequestOverrideState en la Referencia de comandos de la AWS CLI.

`get-pull-request`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-pull-request`.

AWS CLI

Visualización de detalles de una solicitud de extracción

En este ejemplo, se muestra cómo ver la información sobre una solicitud de extracción con el ID 27.

```
aws codecommit get-pull-request \
    --pull-request-id 27
```

Salida:

```
{
    "pullRequest": {
        "approvalRules": [
            {
                "approvalRuleContent": "{\"Version\": \"2018-11-08\",\"Statements\":
 [{\"Type\": \"Approvers\",\"NumberOfApprovalsNeeded\": 2,\"ApprovalPoolMembers\":
 [\"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}",
                "approvalRuleId": "dd8b17fe-EXAMPLE",
                "approvalRuleName": "2-approver-rule-for-main",
                "creationDate": 1571356106.936,
                "lastModifiedDate": 571356106.936,
                "lastModifiedUser": "arn:aws:iam::123456789012:user/Mary_Major",
                "ruleContentSha256": "4711b576EXAMPLE"
            }
        ],
        "lastActivityDate": 1562619583.565,
        "pullRequestTargets": [
            {
```

```
                "sourceCommit": "ca45e279EXAMPLE",
                "sourceReference": "refs/heads/bugfix-1234",
                "mergeBase": "a99f5ddbEXAMPLE",
                "destinationReference": "refs/heads/main",
                "mergeMetadata": {
                    "isMerged": false
                },
                "destinationCommit": "2abfc6beEXAMPLE",
                "repositoryName": "MyDemoRepo"
            }
        ],
        "revisionId": "e47def21EXAMPLE",
        "title": "Quick fix for bug 1234",
        "authorArn": "arn:aws:iam::123456789012:user/Nikhil_Jayashankar",
        "clientRequestToken": "d8d7612e-EXAMPLE",
        "creationDate": 1562619583.565,
        "pullRequestId": "27",
        "pullRequestStatus": "OPEN"
    }
}
```

- Para obtener información sobre la API, consulte GetPullRequest en la Referencia de comandos de la AWS CLI.

`get-repository-triggers`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-repository-triggers`.

AWS CLI

Obtención de información sobre los activadores de un repositorio

En este ejemplo, se muestran detalles sobre los activadores configurados para un repositorio de AWS CodeCommit denominado `MyDemoRepo`.

```
aws codecommit get-repository-triggers \
    --repository-name MyDemoRepo
```

Salida:

```
{
    "configurationId": "f7579e13-b83e-4027-aaef-650c0EXAMPLE",
```

```
    "triggers": [
        {
            "destinationArn": "arn:aws:sns:us-
east-1:111111111111:MyCodeCommitTopic",
            "branches": [
                "main",
                "preprod"
            ],
            "name": "MyFirstTrigger",
            "customData": "",
            "events": [
                "all"
            ]
        },
        {
            "destinationArn": "arn:aws:lambda:us-
east-1:111111111111:function:MyCodeCommitPythonFunction",
            "branches": [],
            "name": "MySecondTrigger",
            "customData": "EXAMPLE",
            "events": [
                "all"
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetRepositoryTriggers en la Referencia de comandos de la AWS CLI.

`get-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-repository`.

AWS CLI

Obtención de información sobre un repositorio

En este ejemplo, se muestra información sobre un repositorio de AWS CodeCommit.

```
aws codecommit get-repository \
    --repository-name MyDemoRepo
```

Salida:

```
{
    "repositoryMetadata": {
        "creationDate": 1429203623.625,
        "defaultBranch": "main",
        "repositoryName": "MyDemoRepo",
        "cloneUrlSsh": "ssh://git-codecommit.us-east-1.amazonaws.com/v1/repos/v1/
repos/MyDemoRepo",
        "lastModifiedDate": 1430783812.0869999,
        "repositoryDescription": "My demonstration repository",
        "cloneUrlHttp": "https://codecommit.us-east-1.amazonaws.com/v1/repos/
MyDemoRepo",
        "repositoryId": "f7579e13-b83e-4027-aaef-650c0EXAMPLE",
        "Arn": "arn:aws:codecommit:us-east-1:80398EXAMPLE:MyDemoRepo
        "accountId": "111111111111"
    }
}
```

- Para obtener información sobre la API, consulte GetRepository en la Referencia de comandos de la AWS CLI.

`list-approval-rule-templates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-approval-rule-templates`.

AWS CLI

Generación de una lista de todas las plantillas de reglas de aprobación de una región de AWS

En el siguiente ejemplo de `list-approval-rule-templates`, se genera una lista de todas las plantillas de regla de aprobación de la región especificada. Si no se especifica ninguna región de AWS como parámetro, el comando muestra las plantillas de reglas de aprobación de la región especificada en el perfil de la AWS CLI utilizado para ejecutar el comando.

```
aws codecommit list-approval-rule-templates \
    --region us-east-2
```

Salida:

```
{
    "approvalRuleTemplateNames": [
```

```
        "2-approver-rule-for-main",
        "1-approver-rule-for-all-pull-requests"
    ]
}
```

Para obtener más información, consulte Administrar plantillas de reglas de aprobación en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte ListApprovalRuleTemplates en la Referencia de comandos de la AWS CLI.

`list-associated-approval-rule-templates-for-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-associated-approval-rule-templates-for-repository`.

AWS CLI

Para enumerar todas las plantillas asociadas con un repositorio

En el siguiente ejemplo de `list-associated-approval-rule-templates-for-repository`, se genera una lista de todas las plantillas de regla de aprobación asociadas a un repositorio denominado `MyDemoRepo`.

```
aws codecommit list-associated-approval-rule-templates-for-repository \
    --repository-name MyDemoRepo
```

Salida:

```
{
  "approvalRuleTemplateNames": [
    "2-approver-rule-for-main",
    "1-approver-rule-for-all-pull-requests"
  ]
}
```

Para obtener más información, consulte Administrar plantillas de reglas de aprobación en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte ListAssociatedApprovalRuleTemplatesForRepository en la Referencia de comandos de la AWS CLI.

`list-branches`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-branches`.

AWS CLI

Visualización de una lista de los nombres de ramificaciones

En este ejemplo, se genera una lista de todos los nombres de ramificaciones en un repositorio de AWS CodeCommit.

```
aws codecommit list-branches \
    --repository-name MyDemoRepo
```

Salida:

```
{
    "branches": [
        "MyNewBranch",
        "main"
    ]
}
```

- Para obtener información sobre la API, consulte ListBranches en la Referencia de comandos de la AWS CLI.

`list-pull-requests`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-pull-requests`.

AWS CLI

Visualización de una lista de las solicitudes de extracción de un repositorio

En este ejemplo, se muestra cómo generar una lista de las solicitudes de extracción que ha creado un usuario de IAM cuyo ARN es arn:aws:iam::111111111111:user/Li_Juan y cuyo estado es CLOSED en un repositorio de AWS CodeCommit denominado MyDemoRepo:

```
aws codecommit list-pull-requests --author-arn arn:aws:iam::111111111111:user/
Li_Juan --pull-request-status CLOSED --repository-name MyDemoRepo
```

Salida:

```
{
 "nextToken": "",
 "pullRequestIds": ["2","12","16","22","23","35","30","39","47"]
}
```

- Para obtener información sobre la API, consulte ListPullRequests en la Referencia de comandos de la AWS CLI.

`list-repositories-for-approval-rule-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-repositories-for-approval-rule-template`.

AWS CLI

Para enumerar todos los repositorios asociados con una plantilla

En el siguiente ejemplo de `list-repositories-for-approval-rule-template`, se genera una lista de todos los repositorios asociados a una plantilla de regla de aprobación especificada.

```
aws codecommit list-repositories-for-approval-rule-template \
    --approval-rule-template-name 2-approver-rule-for-main
```

Salida:

```
{
    "repositoryNames": [
        "MyDemoRepo",
        "MyClonedRepo"
    ]
}
```

Para obtener más información, consulte Administrar plantillas de reglas de aprobación en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte ListRepositoriesForApprovalRuleTemplate en la Referencia de comandos de la AWS CLI.

`list-repositories`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-repositories`.

AWS CLI

Visualización de una lista de repositorios

En este ejemplo, se genera una lista de todos los repositorios de AWS CodeCommit asociados a la cuenta de AWS del usuario.

Comando:

```
aws codecommit list-repositories
```

Salida:

```
{
  "repositories": [
      {
         "repositoryName": "MyDemoRepo"
         "repositoryId": "f7579e13-b83e-4027-aaef-650c0EXAMPLE",
      },
      {
         "repositoryName": "MyOtherDemoRepo"
         "repositoryId": "cfc29ac4-b0cb-44dc-9990-f6f51EXAMPLE"
      }
  ]
}
```

- Para obtener información sobre la API, consulte ListRepositories en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Visualización de las etiquetas de AWS de un repositorio

En el siguiente ejemplo de `list-tags-for-resource`, se muestran las claves y los valores de las etiquetas del repositorio especificado.

```
aws codecommit list-tags-for-resource \
```

```
    --resource-arn arn:aws:codecommit:us-west-2:111111111111:MyDemoRepo
```

Salida:

```
{
    "tags": {
        "Status": "Secret",
        "Team": "Saanvi"
    }
}
```

Para obtener más información, consulte Visualización de etiquetas para un repositorio en la Guía del usuario de AWS CodeCommit.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`merge-branches-by-fast-forward`

En el siguiente ejemplo de código, se muestra cómo utilizar `merge-branches-by-fast-forward`.

AWS CLI

Combinación de dos ramificaciones mediante la estrategia de combinación de avance rápido

En el siguiente ejemplo de `merge-branches-by-fast-forward`, se combina la ramificación de origen especificada con la ramificación de destino especificada en un repositorio denominado `MyDemoRepo`.

```
aws codecommit merge-branches-by-fast-forward \
    --source-commit-specifier bugfix-bug1234 \
    --destination-commit-specifier bugfix-bug1233 \
    --repository-name MyDemoRepo
```

Salida:

```
{
    "commitId": "4f178133EXAMPLE",
    "treeId": "389765daEXAMPLE"
}
```

Para obtener más información, consulte Comparación y combinación de ramificaciones en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte MergeBranchesByFastForward en la Referencia de comandos de la AWS CLI.

`merge-branches-by-squash`

En el siguiente ejemplo de código, se muestra cómo utilizar `merge-branches-by-squash`.

AWS CLI

Combinación de dos ramificaciones mediante la estrategia de combinación de squash

En el siguiente ejemplo de `merge-branches-by-squash`, se combina la ramificación de origen especificada con la ramificación de destino especificada en un repositorio denominado `MyDemoRepo`.

```
aws codecommit merge-branches-by-squash \
    --source-commit-specifier bugfix-bug1234 \
    --destination-commit-specifier bugfix-bug1233 \
    --author-name "Maria Garcia" \
    --email "maria_garcia@example.com" \
    --commit-message "Merging two fix branches to prepare for a general patch." \
    --repository-name MyDemoRepo
```

Salida:

```
{
    "commitId": "4f178133EXAMPLE",
    "treeId": "389765daEXAMPLE"
}
```

Para obtener más información, consulte Comparación y combinación de ramificaciones en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte MergeBranchesBySquash en la Referencia de comandos de la AWS CLI.

`merge-branches-by-three-way`

En el siguiente ejemplo de código, se muestra cómo utilizar `merge-branches-by-three-way`.

AWS CLI

Combinación de dos ramificaciones mediante la estrategia de combinación de tres modos

En el siguiente ejemplo de `merge-branches-by-three-way`, se combina la ramificación de origen especificada con la ramificación de destino especificada en un repositorio denominado `MyDemoRepo`.

```
aws codecommit merge-branches-by-three-way \
    --source-commit-specifier main \
    --destination-commit-specifier bugfix-bug1234 \
    --author-name "Jorge Souza" --email "jorge_souza@example.com" \
    --commit-message "Merging changes from main to bugfix branch before additional
 testing." \
    --repository-name MyDemoRepo
```

Salida:

```
{
    "commitId": "4f178133EXAMPLE",
    "treeId": "389765daEXAMPLE"
}
```

Para obtener más información, consulte Comparación y combinación de ramificaciones en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte MergeBranchesByThreeWay en la Referencia de comandos de la AWS CLI.

`merge-pull-request-by-fast-forward`

En el siguiente ejemplo de código, se muestra cómo utilizar `merge-pull-request-by-fast-forward`.

AWS CLI

Combinación y cierre de una solicitud de extracción

En este ejemplo se muestra cómo combinar y cerrar una solicitud de extracción con el ID 47 y el ID de confirmación de origen 99132ab0EXAMPLE en un repositorio llamado `MyDemoRepo`.

```
aws codecommit merge-pull-request-by-fast-forward \
    --pull-request-id 47 \
    --source-commit-id 99132ab0EXAMPLE \
    --repository-name MyDemoRepo
```

Salida:

```
{
    "pullRequest": {
        "approvalRules": [
            {
                "approvalRuleContent": "{\"Version\": \"2018-11-08\",\"Statements\":
 [{\"Type\": \"Approvers\",\"NumberOfApprovalsNeeded\": 1,\"ApprovalPoolMembers\":
 [\"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}",
                "approvalRuleId": "dd8b17fe-EXAMPLE",
                "approvalRuleName": "I want one approver for this pull request",
                "creationDate": 1571356106.936,
                "lastModifiedDate": 571356106.936,
                "lastModifiedUser": "arn:aws:iam::123456789012:user/Mary_Major",
                "ruleContentSha256": "4711b576EXAMPLE"
            }
        ],
        "authorArn": "arn:aws:iam::123456789012:user/Li_Juan",
        "clientRequestToken": "",
        "creationDate": 1508530823.142,
        "description": "Review the latest changes and updates to the global
 variables",
        "lastActivityDate": 1508887223.155,
        "pullRequestId": "47",
        "pullRequestStatus": "CLOSED",
        "pullRequestTargets": [
            {
                "destinationCommit": "9f31c968EXAMPLE",
                "destinationReference": "refs/heads/main",
                "mergeMetadata": {
                    "isMerged": true,
                    "mergedBy": "arn:aws:iam::123456789012:user/Mary_Major"
                },
                "repositoryName": "MyDemoRepo",
                "sourceCommit": "99132ab0EXAMPLE",
                "sourceReference": "refs/heads/variables-branch"
            }
        ],
```

```
        "title": "Consolidation of global variables"
    }
}
```

Para obtener más información, consulte Combinación de una solicitud de extracción en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte MergePullRequestByFastForward en la Referencia de comandos de la AWS CLI.

`merge-pull-request-by-squash`

En el siguiente ejemplo de código, se muestra cómo utilizar `merge-pull-request-by-squash`.

AWS CLI

Combinación una solicitud de extracción mediante la estrategia de combinación de squash

En el siguiente ejemplo de `merge-pull-request-by-squash`, se combina y cierra la solicitud de extracción especificada mediante la estrategia de resolución de conflictos de ACCEPT_SOURCE en un repositorio denominado `MyDemoRepo`.

```
aws codecommit merge-pull-request-by-squash \
    --pull-request-id 47 \
    --source-commit-id 99132ab0EXAMPLE \
    --repository-name MyDemoRepo \
    --conflict-detail-level LINE_LEVEL \
    --conflict-resolution-strategy ACCEPT_SOURCE \
    --name "Jorge Souza" --email "jorge_souza@example.com" \
    --commit-message "Merging pull request 47 by squash and accepting source in
 merge conflicts"
```

Salida:

```
{
    "pullRequest": {
        "approvalRules": [
            {
                "approvalRuleContent": "{\"Version\": \"2018-11-08\",
\"DestinationReferences\": [\"refs/heads/main\"],\"Statements\": [{\"Type
\": \"Approvers\",\"NumberOfApprovalsNeeded\": 2,\"ApprovalPoolMembers\":
 [\"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}",
```

```
                "approvalRuleId": "dd8b17fe-EXAMPLE",
                "approvalRuleName": "2-approver-rule-for-main",
                "creationDate": 1571356106.936,
                "lastModifiedDate": 571356106.936,
                "lastModifiedUser": "arn:aws:iam::123456789012:user/Mary_Major",
                "originApprovalRuleTemplate": {
                    "approvalRuleTemplateId": "dd8b17fe-EXAMPLE",
                    "approvalRuleTemplateName": "2-approver-rule-for-main"
                },
                "ruleContentSha256": "4711b576EXAMPLE"
            }
        ],
        "authorArn": "arn:aws:iam::123456789012:user/Li_Juan",
        "clientRequestToken": "",
        "creationDate": 1508530823.142,
        "description": "Review the latest changes and updates to the global
 variables",
        "lastActivityDate": 1508887223.155,
        "pullRequestId": "47",
        "pullRequestStatus": "CLOSED",
        "pullRequestTargets": [
            {
                "destinationCommit": "9f31c968EXAMPLE",
                "destinationReference": "refs/heads/main",
                "mergeMetadata": {
                    "isMerged": true,
                    "mergedBy": "arn:aws:iam::123456789012:user/Mary_Major"
                },
                "repositoryName": "MyDemoRepo",
                "sourceCommit": "99132ab0EXAMPLE",
                "sourceReference": "refs/heads/variables-branch"
            }
        ],
        "title": "Consolidation of global variables"
    }
}
```

Para obtener más información, consulte Combinación de una solicitud de extracción en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte MergePullRequestBySquash en la Referencia de comandos de la AWS CLI.

merge-pull-request-by-three-way

En el siguiente ejemplo de código, se muestra cómo utilizar `merge-pull-request-by-three-way`.

AWS CLI

Combinación de una solicitud de extracción mediante la estrategia de combinación de tres modos

En el siguiente ejemplo de `merge-pull-request-by-three-way`, se combina y cierra la solicitud de extracción especificada con las opciones predeterminadas de detalles de conflicto y con la estrategia de resolución de conflictos en un repositorio denominado `MyDemoRepo`.

```
aws codecommit merge-pull-request-by-three-way \
    --pull-request-id 47 \
    --source-commit-id 99132ab0EXAMPLE \
    --repository-name MyDemoRepo \
    --name "Maria Garcia" \
    --email "maria_garcia@example.com" \
    --commit-message "Merging pull request 47 by three-way with default options"
```

Salida:

```
{
    "pullRequest": {
        "approvalRules": [
            {
                "approvalRuleContent": "{\"Version\": \"2018-11-08\",
\"DestinationReferences\": [\"refs/heads/main\"],\"Statements\": [{\"Type
\": \"Approvers\",\"NumberOfApprovalsNeeded\": 2,\"ApprovalPoolMembers\":
 [\"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}",
                "approvalRuleId": "dd8b17fe-EXAMPLE",
                "approvalRuleName": "2-approver-rule-for-main",
                "creationDate": 1571356106.936,
                "lastModifiedDate": 571356106.936,
                "lastModifiedUser": "arn:aws:iam::123456789012:user/Mary_Major",
                "originApprovalRuleTemplate": {
                    "approvalRuleTemplateId": "dd8b17fe-EXAMPLE",
                    "approvalRuleTemplateName": "2-approver-rule-for-main"
                },
                "ruleContentSha256": "4711b576EXAMPLE"
            }
        ],
```

```
        "authorArn": "arn:aws:iam::123456789012:user/Li_Juan",
        "clientRequestToken": "",
        "creationDate": 1508530823.142,
        "description": "Review the latest changes and updates to the global
 variables",
        "lastActivityDate": 1508887223.155,
        "pullRequestId": "47",
        "pullRequestStatus": "CLOSED",
        "pullRequestTargets": [
            {
                "destinationCommit": "9f31c968EXAMPLE",
                "destinationReference": "refs/heads/main",
                "mergeMetadata": {
                    "isMerged": true,
                    "mergedBy": "arn:aws:iam::123456789012:user/Mary_Major"
                },
                "repositoryName": "MyDemoRepo",
                "sourceCommit": "99132ab0EXAMPLE",
                "sourceReference": "refs/heads/variables-branch"
            }
        ],
        "title": "Consolidation of global variables"
    }
}
```

Para obtener más información, consulte Combinación de una solicitud de extracción en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte MergePullRequestByThreeWay en la Referencia de comandos de la AWS CLI.

`override-pull-request-approval-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `override-pull-request-approval-rules`.

AWS CLI

Para sustituir los requisitos de reglas de aprobación en una solicitud de extracción

En el siguiente ejemplo de `override-pull-request-approval-rules`, se anulan las reglas de aprobación de una solicitud de extracción especificada. Para, en lugar de ello, revocar una anulación, se define el valor de parámetro `--override-status` en `REVOKE`.

```
aws codecommit override-pull-request-approval-rules \
    --pull-request-id 34  \
    --revision-id 927df8d8EXAMPLE \
    --override-status OVERRIDE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Anular reglas de aprobación en una solicitud de extracción en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte OverridePullRequestApprovalRules en la Referencia de comandos de la AWS CLI.

`post-comment-for-compared-commit`

En el siguiente ejemplo de código, se muestra cómo utilizar `post-comment-for-compared-commit`.

AWS CLI

Creación de un comentario sobre una confirmación

En este ejemplo, se muestra cómo añadir el comentario `"Can you add a test case for this?"` al cambio del archivo `cl_sample.js` en la comparación de dos confirmaciones en un repositorio denominado `MyDemoRepo`.

```
aws codecommit post-comment-for-compared-commit \
    --repository-name MyDemoRepo \
    --before-commit-id 317f8570EXAMPLE \
    --after-commit-id 5d036259EXAMPLE \
    --client-request-token 123Example \
    --content "Can you add a test case for this?" \
    --location filePath=cl_sample.js,filePosition=1232,relativeFileVersion=AFTER
```

Salida:

```
{
    "afterBlobId": "1f330709EXAMPLE",
    "afterCommitId": "317f8570EXAMPLE",
    "beforeBlobId": "80906a4cEXAMPLE",
    "beforeCommitId": "6e147360EXAMPLE",
    "comment": {
```

```
        "authorArn": "arn:aws:iam::111111111111:user/Li_Juan",
        "clientRequestToken": "",
        "commentId": "553b509bEXAMPLE56198325",
        "content": "Can you add a test case for this?",
        "creationDate": 1508369612.203,
        "deleted": false,
        "commentId": "abc123-EXAMPLE",
        "lastModifiedDate": 1508369612.203,
        "callerReactions": [],
        "reactionCounts": []
    },
    "location": {
        "filePath": "cl_sample.js",
        "filePosition": 1232,
        "relativeFileVersion": "AFTER"
    ,
    "repositoryName": "MyDemoRepo"
    }
}
```

- Para obtener información sobre la API, consulte PostCommentForComparedCommit en la Referencia de comandos de la AWS CLI.

`post-comment-for-pull-request`

En el siguiente ejemplo de código, se muestra cómo utilizar `post-comment-for-pull-request`.

AWS CLI

Adición de un comentario a una solicitud de extracción

En el siguiente ejemplo de `post-comment-for-pull-request`, se añade el comentario These don't appear to be used anywhere. Can we remove them?" en el cambio realizado en el archivo `ahs_count.py` en una solicitud de extracción con el ID 47 en un repositorio denominado `MyDemoRepo`.

```
aws codecommit post-comment-for-pull-request \
    --pull-request-id "47" \
    --repository-name MyDemoRepo \
    --before-commit-id 317f8570EXAMPLE \
    --after-commit-id 5d036259EXAMPLE \
    --client-request-token 123Example \
```

```
    --content "These don't appear to be used anywhere. Can we remove them?" \
    --location filePath=ahs_count.py,filePosition=367,relativeFileVersion=AFTER
```

Salida:

```
{
     "afterBlobId": "1f330709EXAMPLE",
     "afterCommitId": "5d036259EXAMPLE",
     "beforeBlobId": "80906a4cEXAMPLE",
     "beforeCommitId": "317f8570EXAMPLE",
     "comment": {
            "authorArn": "arn:aws:iam::111111111111:user/Saanvi_Sarkar",
            "clientRequestToken": "123Example",
            "commentId": "abcd1234EXAMPLEb5678efgh",
            "content": "These don't appear to be used anywhere. Can we remove
 them?",
            "creationDate": 1508369622.123,
            "deleted": false,
            "CommentId": "",
            "lastModifiedDate": 1508369622.123,
            "callerReactions": [],
            "reactionCounts": []
        },
        "location": {
            "filePath": "ahs_count.py",
            "filePosition": 367,
            "relativeFileVersion": "AFTER"
         },
     "repositoryName": "MyDemoRepo",
     "pullRequestId": "47"
}
```

- Para obtener más información sobre la API, consulte PostCommentForPullRequest en la Referencia de comandos de la AWS CLI.

`post-comment-reply`

En el siguiente ejemplo de código, se muestra cómo utilizar `post-comment-reply`.

AWS CLI

Respuesta a un comentario en una confirmación o en una solicitud de extracción

En este ejemplo, se muestra cómo añadir la respuesta `"Good catch. I'll remove them."` a un comentario con el ID generado por el sistema `abcd1234EXAMPLEb5678efgh`.

```
aws codecommit post-comment-reply \
    --in-reply-to abcd1234EXAMPLEb5678efgh \
    --content "Good catch. I'll remove them." \
    --client-request-token 123Example
```

Salida:

```
{
    "comment": {
        "authorArn": "arn:aws:iam::111111111111:user/Li_Juan",
        "clientRequestToken": "123Example",
        "commentId": "442b498bEXAMPLE5756813",
        "content": "Good catch. I'll remove them.",
        "creationDate": 1508369829.136,
        "deleted": false,
        "CommentId": "abcd1234EXAMPLEb5678efgh",
        "lastModifiedDate": 150836912.221,
        "callerReactions": [],
        "reactionCounts": []
    }
}
```

- Para obtener información sobre la API, consulte PostCommentReply en la Referencia de comandos de la AWS CLI.

`put-comment-reaction`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-comment-reaction`.

AWS CLI

Respuesta a un comentario sobre una confirmación con un emoji

En el siguiente ejemplo de `put-comment-reaction`, se responde a un comentario con el ID `abcd1234EXAMPLEb5678efgh` con un valor de reacción de emoji de `:thumbsup:`.

```
aws codecommit put-comment-reaction \
    --comment-id abcd1234EXAMPLEb5678efgh \
```

```
    --reaction-value :thumbsup:
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Comenta una confirmación en AWS CodeCommit en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte PutCommentReaction en la Referencia de comandos de la AWS CLI.

`put-file`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-file`.

AWS CLI

Adición de un archivo a un repositorio

En el siguiente ejemplo de `put-file`, se añade un archivo denominado ExampleSolution.py a un repositorio llamado MyDemoRepo en una ramificación denominada feature-randomizationfeature cuya confirmación más reciente tiene un ID de 4c925148EXAMPLE.

```
aws codecommit put-file \
    --repository-name MyDemoRepo \
    --branch-name feature-randomizationfeature \
    --file-content file://MyDirectory/ExampleSolution.py \
    --file-path /solutions/ExampleSolution.py \
    --parent-commit-id 4c925148EXAMPLE \
    --name "Maria Garcia" \
    --email "maria_garcia@example.com" \
    --commit-message "I added a third randomization routine."
```

Salida:

```
{
    "blobId": "2eb4af3bEXAMPLE",
    "commitId": "317f8570EXAMPLE",
    "treeId": "347a3408EXAMPLE"
}
```

- Para obtener información sobre la API, consulte PutFile en la Referencia de comandos de la AWS CLI.

put-repository-triggers

En el siguiente ejemplo de código, se muestra cómo utilizar `put-repository-triggers`.

AWS CLI

Adición o actualización de un activador en un repositorio

En este ejemplo, se muestra cómo actualizar los activadores denominados MyFirstTrigger y MySecondTrigger mediante un archivo JSON ya creado (aquí denominado MyTriggers.json) que contiene la estructura de todos los activadores de un repositorio denominado MyDemoRepo. Para obtener información sobre cómo obtener el JSON de los activadores existentes, consulte el comando get-repository-triggers.

```
aws codecommit put-repository-triggers \
    --repository-name MyDemoRepo file://MyTriggers.json
```

Contenido de `MyTriggers.json`:

```
{
    "repositoryName": "MyDemoRepo",
    "triggers": [
        {
            "destinationArn": "arn:aws:sns:us-
east-1:80398EXAMPLE:MyCodeCommitTopic",
            "branches": [
                "main",
                "preprod"
            ],
            "name": "MyFirstTrigger",
            "customData": "",
            "events": [
                "all"
            ]
        },
        {
            "destinationArn": "arn:aws:lambda:us-
east-1:111111111111:function:MyCodeCommitPythonFunction",
            "branches": [],
            "name": "MySecondTrigger",
            "customData": "EXAMPLE",
            "events": [
```

```
                "all"
            ]
        }
    ]
}
```

Salida:

```
{
    "configurationId": "6fa51cd8-35c1-EXAMPLE"
}
```

- Para obtener información sobre la API, consulte PutRepositoryTriggers en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Adición de etiquetas de AWS a un repositorio ya existente

En el siguiente ejemplo de `tag-resource`, se añaden dos etiquetas al repositorio especificado.

```
aws codecommit tag-resource \
    --resource-arn arn:aws:codecommit:us-west-2:111111111111:MyDemoRepo \
    --tags Status=Secret,Team=Saanvi
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Añadir una etiqueta a un repositorio en la Guía del usuario de AWS CodeCommit.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`test-repository-triggers`

En el siguiente ejemplo de código, se muestra cómo utilizar `test-repository-triggers`.

AWS CLI

Prueba de los activadores en un repositorio

En este ejemplo, se muestra cómo probar un activador denominado MyFirstTrigger en un repositorio de AWS CodeCommit denominado MyDemoRepo. En este ejemplo, los eventos del repositorio activan notificaciones de un tema de Amazon Simple Notification Service (Amazon SNS).

Comando:

```
aws codecommit test-repository-triggers --repository-name MyDemoRepo
 --triggers name=MyFirstTrigger,destinationArn=arn:aws:sns:us-
east-1:111111111111:MyCodeCommitTopic,branches=mainline,preprod,events=all
```

Salida:

```
{
  "successfulExecutions": [
      "MyFirstTrigger"
  ],
  "failedExecutions": []
}
```

- Para obtener información sobre la API, consulte TestRepositoryTriggers en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de etiquetas de AWS de un repositorio

En el siguiente ejemplo de `untag-resource`, se elimina la etiqueta con la clave especificada del repositorio denominado `MyDemoRepo`.

```
aws codecommit untag-resource \
    --resource-arn arn:aws:codecommit:us-west-2:111111111111:MyDemoRepo \
    --tag-keys Status
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminar una etiqueta de un repositorio en la Guía del usuario de AWS CodeCommit.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-approval-rule-template-content

En el siguiente ejemplo de código, se muestra cómo utilizar `update-approval-rule-template-content`.

AWS CLI

Actualización del contenido de una plantilla de regla de aprobación

En este ejemplo de `update-approval-rule-template-content` se cambia el contenido de la plantilla de regla de aprobación especificada para redefinir el grupo de aprobación de manera que incluya a los usuarios que asuman el rol `CodeCommitReview`.

```
aws codecommit update-approval-rule-template-content \
    --approval-rule-template-name 1-approver-rule  \
    --new-rule-content "{\"Version\": \"2018-11-08\",\"DestinationReferences
\": [\"refs/heads/main\"],\"Statements\": [{\"Type\": \"Approvers
\",\"NumberOfApprovalsNeeded\": 2,\"ApprovalPoolMembers\":
 [\"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}"
```

Salida:

```
{
    "approvalRuleTemplate": {
        "creationDate": 1571352720.773,
        "approvalRuleTemplateDescription": "Requires 1 approval for all pull
 requests from the CodeCommitReview pool",
        "lastModifiedDate": 1571358728.41,
        "approvalRuleTemplateId": "41de97b7-EXAMPLE",
        "approvalRuleTemplateContent": "{\"Version\": \"2018-11-08\",\"Statements\":
 [{\"Type\": \"Approvers\",\"NumberOfApprovalsNeeded\": 1,\"ApprovalPoolMembers\":
 [\"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}",
        "approvalRuleTemplateName": "1-approver-rule-for-all-pull-requests",
        "ruleContentSha256": "2f6c21a5EXAMPLE",
```

```
        "lastModifiedUser": "arn:aws:iam::123456789012:user/Li_Juan"
    }
}
```

Para obtener más información, consulte Administrar plantillas de reglas de aprobación en la Guía del usuario de AWS CodeCommit.

- Para obtener detalles sobre la API, consulte UpdateApprovalRuleTemplateContent en la Referencia de comandos de la AWS CLI.

`update-approval-rule-template-description`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-approval-rule-template-description`.

AWS CLI

Actualización de la descripción de una plantilla de regla de aprobación

En el siguiente ejemplo de `update-approval-rule-template-description`, se cambia a `Requires 1 approval for all pull requests from the CodeCommitReview pool` la descripción de la plantilla de regla de aprobación especificada.

```
aws codecommit update-approval-rule-template-description \
    --approval-rule-template-name 1-approver-rule-for-all-pull-requests  \
    --approval-rule-template-description "Requires 1 approval for all pull requests
 from the CodeCommitReview pool"
```

Salida:

```
{
  "approvalRuleTemplate": {
    "creationDate": 1571352720.773,
    "approvalRuleTemplateDescription": "Requires 1 approval for all pull requests
 from the CodeCommitReview pool",
    "lastModifiedDate": 1571358728.41,
    "approvalRuleTemplateId": "41de97b7-EXAMPLE",
    "approvalRuleTemplateContent": "{\"Version\": \"2018-11-08\",\"Statements\":
 [{\"Type\": \"Approvers\",\"NumberOfApprovalsNeeded\": 1,\"ApprovalPoolMembers\":
 [\"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}",
    "approvalRuleTemplateName": "1-approver-rule-for-all-pull-requests",
    "ruleContentSha256": "2f6c21a5EXAMPLE",
```

```
    "lastModifiedUser": "arn:aws:iam::123456789012:user/Li_Juan"
  }
}
```

Para obtener más información, consulte Administrar plantillas de reglas de aprobación en la Guía del usuario de AWS CodeCommit.

- Para obtener información acerca de la API, consulte UpdateApprovalRuleTemplateDescription en la Referencia de comandos de la AWS CLI.

`update-approval-rule-template-name`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-approval-rule-template-name`.

AWS CLI

Actualización del nombre de una plantilla de regla de aprobación

En el siguiente ejemplo de `update-approval-rule-template-name`, se cambia el nombre de una plantilla de regla de aprobación de `1-approver-rule` a 1-approver-rule-for-all-pull-requests.

```
aws codecommit update-approval-rule-template-name \
    --old-approval-rule-template-name 1-approver-rule  \
    --new-approval-rule-template-name 1-approver-rule-for-all-pull-requests
```

Salida:

```
{
  "approvalRuleTemplate": {
    "approvalRuleTemplateName": "1-approver-rule-for-all-pull-requests",
    "lastModifiedDate": 1571358241.619,
    "approvalRuleTemplateId": "41de97b7-EXAMPLE",
    "approvalRuleTemplateContent": "{\"Version\": \"2018-11-08\",\"Statements\":
 [{\"Type\": \"Approvers\",\"NumberOfApprovalsNeeded\": 1,\"ApprovalPoolMembers\":
 [\"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}",
    "creationDate": 1571352720.773,
    "lastModifiedUser": "arn:aws:iam::123456789012:user/Mary_Major",
    "approvalRuleTemplateDescription": "All pull requests must be approved by one
 developer on the team.",
    "ruleContentSha256": "2f6c21a5cEXAMPLE"
```

```
  }
}
```

Para obtener más información, consulte Administrar plantillas de reglas de aprobación en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte UpdateApprovalRuleTemplateName en la Referencia de comandos de la AWS CLI.

`update-comment`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-comment`.

AWS CLI

Actualización de un comentario sobre una confirmación

En este ejemplo, se muestra cómo añadir el contenido `"Fixed as requested. I'll update the pull request."` a un comentario con un ID `442b498bEXAMPLE5756813`.

```
aws codecommit update-comment \
    --comment-id 442b498bEXAMPLE5756813 \
    --content "Fixed as requested. I'll update the pull request."
```

Salida:

```
{
    "comment": {
        "authorArn": "arn:aws:iam::111111111111:user/Li_Juan",
        "clientRequestToken": "",
        "commentId": "442b498bEXAMPLE5756813",
        "content": "Fixed as requested. I'll update the pull request.",
        "creationDate": 1508369929.783,
        "deleted": false,
        "lastModifiedDate": 1508369929.287,
        "callerReactions": [],
        "reactionCounts":
            {
                "THUMBSUP" : 2
            }
    }
}
```

- Para obtener información sobre la API, consulte UpdateComment en la Referencia de comandos de la AWS CLI.

`update-default-branch`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-default-branch`.

AWS CLI

Cambio de la ramificación predeterminada de un repositorio

En este ejemplo, se cambia la ramificación predeterminada de un repositorio de AWS CodeCommit. Este comando devuelve resultados solo si hay errores.

Comando:

```
aws codecommit update-default-branch --repository-name MyDemoRepo --default-branch-name MyNewBranch
```

Salida:

```
None.
```

- Para obtener información sobre la API, consulte UpdateDefaultBranch en la Referencia de comandos de la AWS CLI.

`update-pull-request-approval-rule-content`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-pull-request-approval-rule-content`.

AWS CLI

Edición de una regla de aprobación de una solicitud de extracción

En el siguiente ejemplo de `update-pull-request-approval-rule-content`, se actualiza la regla de aprobación especificada de manera que se requiera la aprobación de un usuario de un grupo de aprobación que incluya a cualquier usuario de IAM de la cuenta de AWS `123456789012`.

```
aws codecommit update-pull-request-approval-rule-content \
    --pull-request-id 27  \
    --approval-rule-name "Require two approved approvers" \
    --approval-rule-content "{Version: 2018-11-08, Statements: [{Type:
 \"Approvers\", NumberOfApprovalsNeeded: 1, ApprovalPoolMembers:
[\"CodeCommitApprovers:123456789012:user/*\"]}]}"
```

Salida:

```
{
    "approvalRule": {
        "approvalRuleContent": "{Version: 2018-11-08, Statements:
 [{Type: \"Approvers\", NumberOfApprovalsNeeded: 1, ApprovalPoolMembers:
[\"CodeCommitApprovers:123456789012:user/*\"]}]}",
        "approvalRuleId": "aac33506-EXAMPLE",
        "originApprovalRuleTemplate": {},
        "creationDate": 1570752871.932,
        "lastModifiedDate": 1570754058.333,
        "approvalRuleName": Require two approved approvers",
        "lastModifiedUser": "arn:aws:iam::123456789012:user/Mary_Major",
        "ruleContentSha256": "cd93921cEXAMPLE",
    }
}
```

Para obtener más información, consulte Editar o eliminar una regla de aprobación en la Guía del usuario de AWS CodeCommit.

- Para obtener información acerca de la API, consulte UpdatePullRequestApprovalRuleContent en la Referencia de comandos de la AWS CLI.

`update-pull-request-approval-state`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-pull-request-approval-state`.

AWS CLI

Aprobación o revocación de la aprobación de una solicitud de extracción

En el siguiente ejemplo de `update-pull-request-approval-state`, se aprueba una solicitud de extracción con el ID 27 y el ID de revisión `9f29d167EXAMPLE`. Si, en su lugar, desea revocar la aprobación, defina el valor del parámetro `--approval-state` en `REVOKE`.

```
aws codecommit update-pull-request-approval-state \
    --pull-request-id 27  \
    --revision-id 9f29d167EXAMPLE  \
    --approval-state "APPROVE"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Revisión de una solicitud de extracción en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte UpdatePullRequestApprovalState en la Referencia de comandos de la AWS CLI.

update-pull-request-description

En el siguiente ejemplo de código, se muestra cómo utilizar `update-pull-request-description`.

AWS CLI

Cambio de la descripción de una solicitud de extracción

En este ejemplo se muestra cómo cambiar la descripción de una solicitud de extracción con el ID 47.

```
aws codecommit update-pull-request-description \
    --pull-request-id 47 \
    --description "Updated the pull request to remove unused global variable."
```

Salida:

```
{
    "pullRequest": {
        "authorArn": "arn:aws:iam::111111111111:user/Li_Juan",
        "clientRequestToken": "",
        "creationDate": 1508530823.155,
        "description": "Updated the pull request to remove unused global variable.",
        "lastActivityDate": 1508372423.204,
        "pullRequestId": "47",
        "pullRequestStatus": "OPEN",
        "pullRequestTargets": [
```

```
            {
                "destinationCommit": "9f31c968EXAMPLE",
                "destinationReference": "refs/heads/main",
                "mergeMetadata": {
                    "isMerged": false,
                },
                "repositoryName": "MyDemoRepo",
                "sourceCommit": "99132ab0EXAMPLE",
                "sourceReference": "refs/heads/variables-branch"
            }
        ],
        "title": "Consolidation of global variables"
    }
}
```

- Para obtener información sobre la API, consulte UpdatePullRequestDescription en la Referencia de comandos de la AWS CLI.

`update-pull-request-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-pull-request-status`.

AWS CLI

Cambio del estado de una solicitud de extracción

En este ejemplo, se muestra cómo cambiar el estado de una solicitud de extracción con el ID 42 a un estado de CLOSED en un repositorio de AWS CodeCommit denominado MyDemoRepo.

```
aws codecommit update-pull-request-status \
    --pull-request-id 42 \
    --pull-request-status CLOSED
```

Salida:

```
{
    "pullRequest": {
        "approvalRules": [
            {
                "approvalRuleContent": "{\"Version\": \"2018-11-08\",\"Statements\":
 [{\"Type\": \"Approvers\",\"NumberOfApprovalsNeeded\": 2,\"ApprovalPoolMembers\":
 [\"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}",
```

```
                "approvalRuleId": "dd8b17fe-EXAMPLE",
                "approvalRuleName": "2-approvers-needed-for-this-change",
                "creationDate": 1571356106.936,
                "lastModifiedDate": 571356106.936,
                "lastModifiedUser": "arn:aws:iam::123456789012:user/Mary_Major",
                "ruleContentSha256": "4711b576EXAMPLE"
            }
        ],
        "authorArn": "arn:aws:iam::123456789012:user/Li_Juan",
        "clientRequestToken": "",
        "creationDate": 1508530823.165,
        "description": "Updated the pull request to remove unused global variable.",
        "lastActivityDate": 1508372423.12,
        "pullRequestId": "47",
        "pullRequestStatus": "CLOSED",
        "pullRequestTargets": [
            {
                "destinationCommit": "9f31c968EXAMPLE",
                "destinationReference": "refs/heads/main",
                "mergeMetadata": {
                    "isMerged": false,
                },
                "repositoryName": "MyDemoRepo",
                "sourceCommit": "99132ab0EXAMPLE",
                "sourceReference": "refs/heads/variables-branch"
            }
        ],
        "title": "Consolidation of global variables"
    }
}
```

- Para obtener información sobre la API, consulte UpdatePullRequestStatus en la Referencia de comandos de la AWS CLI.

`update-pull-request-title`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-pull-request-title`.

AWS CLI

Cambio del título de una solicitud de extracción

En este ejemplo, se muestra cómo cambiar el título de una solicitud de extracción con el ID 47.

```
aws codecommit update-pull-request-title \
    --pull-request-id 47 \
    --title "Consolidation of global variables - updated review"
```

Salida:

```
{
    "pullRequest": {
        "approvalRules": [
            {
                "approvalRuleContent": "{\"Version\": \"2018-11-08\",
\"DestinationReferences\": [\"refs/heads/main\"],\"Statements\": [{\"Type
\": \"Approvers\",\"NumberOfApprovalsNeeded\": 2,\"ApprovalPoolMembers\":
 [\"arn:aws:sts::123456789012:assumed-role/CodeCommitReview/*\"]}]}",
                "approvalRuleId": "dd8b17fe-EXAMPLE",
                "approvalRuleName": "2-approver-rule-for-main",
                "creationDate": 1571356106.936,
                "lastModifiedDate": 571356106.936,
                "lastModifiedUser": "arn:aws:iam::123456789012:user/Mary_Major",
                "originApprovalRuleTemplate": {
                    "approvalRuleTemplateId": "dd8b26gr-EXAMPLE",
                    "approvalRuleTemplateName": "2-approver-rule-for-main"
                },
                "ruleContentSha256": "4711b576EXAMPLE"
            }
        ],
        "authorArn": "arn:aws:iam::123456789012:user/Li_Juan",
        "clientRequestToken": "",
        "creationDate": 1508530823.12,
        "description": "Review the latest changes and updates to the global
 variables. I have updated this request with some changes, including removing some
 unused variables.",
        "lastActivityDate": 1508372657.188,
        "pullRequestId": "47",
        "pullRequestStatus": "OPEN",
        "pullRequestTargets": [
            {
                "destinationCommit": "9f31c968EXAMPLE",
                "destinationReference": "refs/heads/main",
                "mergeMetadata": {
                    "isMerged": false,
                },
                "repositoryName": "MyDemoRepo",
```

```
                "sourceCommit": "99132ab0EXAMPLE",
                "sourceReference": "refs/heads/variables-branch"
            }
        ],
        "title": "Consolidation of global variables - updated review"
    }
}
```

- Para obtener información sobre la API, consulte UpdatePullRequestTitle en la Referencia de comandos de la AWS CLI.

`update-repository-description`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-repository-description`.

AWS CLI

Cambio de la descripción de un repositorio

En este ejemplo, se cambia la descripción de un repositorio de AWS CodeCommit. Este comando devuelve resultados solo si hay errores.

Comando:

```
aws codecommit update-repository-description --repository-name MyDemoRepo --
repository-description "This description was changed"
```

Salida:

```
None.
```

- Para obtener información sobre la API, consulte UpdateRepositoryDescription en la Referencia de comandos de la AWS CLI.

`update-repository-name`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-repository-name`.

AWS CLI

Cambio del nombre de un repositorio

En este ejemplo, se cambia el nombre de un repositorio de AWS CodeCommit. Este comando devuelve resultados solo si hay errores. Si cambia el nombre del repositorio de AWS CodeCommit, se cambiarán las URL SSH y HTTPS que los usuarios necesitan para conectarse al repositorio. Para que los usuarios puedan conectarse a este repositorio, tendrán que actualizar la configuración de la conexión. Además, puesto que el repositorio cambiará el ARN, al cambiar el nombre del repositorio, se invalidarán las políticas del usuario de IAM que confían en este ARN del repositorio.

Comando:

```
aws codecommit update-repository-name --old-name MyDemoRepo --new-
name MyRenamedDemoRepo
```

Salida:

```
None.
```

- Para obtener información sobre la API, consulte UpdateRepositoryName en la Referencia de comandos de la AWS CLI.

Ejemplos de CodeDeploy que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar situaciones comunes usando la AWS Command Line Interface con CodeDeploy.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-tags-to-on-premises-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-tags-to-on-premises-instances`.

AWS CLI

Adición de etiquetas a instancias en las instalaciones

En el siguiente ejemplo de `add-tags-to-on-premises-instances`, en AWS CodeDeploy se asocia la misma etiqueta de instancia en las instalaciones a dos instancias en las instalaciones. No se registran las instancias en las instalaciones con AWS CodeDeploy.

```
aws deploy add-tags-to-on-premises-instances \
    --instance-names AssetTag12010298EX AssetTag23121309EX \
    --tags Key=Name,Value=CodeDeployDemo-OnPrem
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte AddTagsToOnPremisesInstances en la Referencia de comandos de la AWS CLI.

`batch-get-application-revisions`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-application-revisions`.

AWS CLI

Obtención de información sobre las revisiones de la aplicación

En el siguiente ejemplo de `batch-get-application-revisions`, se obtiene información acerca de la revisión especificada almacenada en un repositorio de GitHub.

```
aws deploy batch-get-application-revisions \
    --application-name my-codedeploy-application \
    --revisions "[{\"gitHubLocation\": {\"commitId\":
 \"fa85936EXAMPLEa31736c051f10d77297EXAMPLE\",\"repository\": \"my-github-token/my-
repository\"},\"revisionType\": \"GitHub\"}]"
```

Salida:

```
{
    "revisions": [
        {
            "genericRevisionInfo": {
                "description": "Application revision registered by Deployment ID: d-
A1B2C3111",
                "lastUsedTime": 1556912355.884,
                "registerTime": 1556912355.884,
                "firstUsedTime": 1556912355.884,
                "deploymentGroups": []
            },
            "revisionLocation": {
                "revisionType": "GitHub",
                "gitHubLocation": {
                    "commitId": "fa85936EXAMPLEa31736c051f10d77297EXAMPLE",
                    "repository": "my-github-token/my-repository"
                }
            }
        }
    ],
    "applicationName": "my-codedeploy-application",
    "errorMessage": ""
}
```

Para obtener más información, consulte BatchGetApplicationRevisions en la Referencia de la API de AWS CodeDeploy.

- Para obtener información sobre la API, consulte BatchGetApplicationRevisions en la Referencia de comandos de la AWS CLI.

`batch-get-applications`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-applications`.

AWS CLI

Obtención de información sobre varias aplicaciones

En el siguiente ejemplo de `batch-get-applications`, se muestra información sobre varias aplicaciones asociadas a la cuenta de AWS del usuario.

```
aws deploy batch-get-applications --application-names WordPress_App MyOther_App
```

Salida:

```
{
    "applicationsInfo": [
        {
            "applicationName": "WordPress_App",
            "applicationId": "d9dd6993-f171-44fa-a811-211e4EXAMPLE",
            "createTime": 1407878168.078,
            "linkedToGitHub": false
        },
        {
            "applicationName": "MyOther_App",
            "applicationId": "8ca57519-31da-42b2-9194-8bb16EXAMPLE",
            "createTime": 1407453571.63,
            "linkedToGitHub": false
        }
    ]
}
```

- Para obtener información sobre la API, consulte BatchGetApplications en la Referencia de comandos de la AWS CLI.

`batch-get-deployment-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-deployment-groups`.

AWS CLI

Obtención de información sobre uno o varios grupos de implementación

En el siguiente ejemplo de `batch-get-deployment-groups`, se obtiene información sobre dos de los grupos de implementación que están asociados a la aplicación CodeDeploy especificada.

```
aws deploy batch-get-deployment-groups \
    --application-name my-codedeploy-application \
    --deployment-group-names "[\"my-deployment-group-1\",\"my-deployment-group-2\"]"
```

Salida:

```
{
    "deploymentGroupsInfo": [
        {
            "deploymentStyle": {
                "deploymentOption": "WITHOUT_TRAFFIC_CONTROL",
                "deploymentType": "IN_PLACE"
            },
            "autoRollbackConfiguration": {
                "enabled": false
            },
            "onPremisesTagSet": {
                "onPremisesTagSetList": []
            },
            "serviceRoleArn": "arn:aws:iam::123456789012:role/
CodeDeployServiceRole",
            "lastAttemptedDeployment": {
                "endTime": 1556912366.415,
                "status": "Failed",
                "createTime": 1556912355.884,
                "deploymentId": "d-A1B2C3111"
            },
            "autoScalingGroups": [],
            "deploymentGroupName": "my-deployment-group-1",
            "ec2TagSet": {
                "ec2TagSetList": [
                    [
                        {
                            "Type": "KEY_AND_VALUE",
                            "Value": "my-EC2-instance",
                            "Key": "Name"
                        }
                    ]
                ]
            },
            "deploymentGroupId": "a1b2c3d4-5678-90ab-cdef-11111example",
            "triggerConfigurations": [],
            "applicationName": "my-codedeploy-application",
            "computePlatform": "Server",
            "deploymentConfigName": "CodeDeployDefault.AllAtOnce"
        },
        {
            "deploymentStyle": {
                "deploymentOption": "WITHOUT_TRAFFIC_CONTROL",
```

```
                "deploymentType": "IN_PLACE"
            },
            "autoRollbackConfiguration": {
                "enabled": false
            },
            "onPremisesTagSet": {
                "onPremisesTagSetList": []
            },
            "serviceRoleArn": "arn:aws:iam::123456789012:role/
CodeDeployServiceRole",
            "autoScalingGroups": [],
            "deploymentGroupName": "my-deployment-group-2",
            "ec2TagSet": {
                "ec2TagSetList": [
                    [
                        {
                            "Type": "KEY_AND_VALUE",
                            "Value": "my-EC2-instance",
                            "Key": "Name"
                            }
                    ]
                ]
            },
            "deploymentGroupId": "a1b2c3d4-5678-90ab-cdef-22222example",
            "triggerConfigurations": [],
            "applicationName": "my-codedeploy-application",
            "computePlatform": "Server",
            "deploymentConfigName": "CodeDeployDefault.AllAtOnce"
        }
    ],
    "errorMessage": ""
}
```

Para obtener más información, consulte BatchGetDeploymentGroups en la Referencia de la API de AWS CodeDeploy.

- Para obtener información sobre la API, consulte BatchGetDeploymentGroups en la Referencia de comandos de la AWS CLI.

`batch-get-deployment-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-deployment-targets`.

AWS CLI

Obtención de los objetivos asociados a una implementación

En el siguiente ejemplo de `batch-get-deployment-targets`, se obtiene información sobre uno de los objetivos asociados a la implementación especificada.

```
aws deploy batch-get-deployment-targets \
    --deployment-id "d-1A2B3C4D5" \
    --target-ids "i-01a2b3c4d5e6f1111"
```

Salida:

```
{
    "deploymentTargets": [
        {
            "deploymentTargetType": "InstanceTarget",
            "instanceTarget": {
                "lifecycleEvents": [
                    {
                        "startTime": 1556918592.162,
                        "lifecycleEventName": "ApplicationStop",
                        "status": "Succeeded",
                        "endTime": 1556918592.247,
                        "diagnostics": {
                            "scriptName": "",
                            "errorCode": "Success",
                            "logTail": "",
                            "message": "Succeeded"
                        }
                    },
                    {
                        "startTime": 1556918593.193,
                        "lifecycleEventName": "DownloadBundle",
                        "status": "Succeeded",
                        "endTime": 1556918593.981,
                        "diagnostics": {
                            "scriptName": "",
                            "errorCode": "Success",
                            "logTail": "",
                            "message": "Succeeded"
                        }
                    },
```

```
                    {
                        "startTime": 1556918594.805,
                        "lifecycleEventName": "BeforeInstall",
                        "status": "Succeeded",
                        "endTime": 1556918681.807,
                        "diagnostics": {
                            "scriptName": "",
                            "errorCode": "Success",
                            "logTail": "",
                            "message": "Succeeded"
                        }
                    }
                ],
                "targetArn": "arn:aws:ec2:us-west-2:123456789012:instance/
i-01a2b3c4d5e6f1111",
                "deploymentId": "d-1A2B3C4D5",
                "lastUpdatedAt": 1556918687.504,
                "targetId": "i-01a2b3c4d5e6f1111",
                "status": "Succeeded"
            }
        }
    ]
}
```

Para obtener más información, consulte BatchGetDeploymentTargets en la Referencia de la API de AWS CodeDeploy.

- Para obtener información sobre la API, consulte BatchGetDeploymentTargets en la Referencia de comandos de la AWS CLI.

`batch-get-deployments`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-deployments`.

AWS CLI

Obtención de información sobre varias implementaciones

En el siguiente ejemplo de `batch-get-deployments`, se muestra información sobre varias implementaciones asociadas a la cuenta de AWS del usuario.

```
aws deploy batch-get-deployments --deployment-ids d-A1B2C3111 d-A1B2C3222
```

Salida:

```
{
    "deploymentsInfo": [
        {
            "applicationName": "WordPress_App",
            "status": "Failed",
            "deploymentOverview": {
                "Failed": 0,
                "InProgress": 0,
                "Skipped": 0,
                "Succeeded": 1,
                "Pending": 0
            },
            "deploymentConfigName": "CodeDeployDefault.OneAtATime",
            "creator": "user",
            "deploymentGroupName": "WordPress_DG",
            "revision": {
                "revisionType": "S3",
                "s3Location": {
                "bundleType": "zip",
                "version": "uTecLusEXAMPLEFXtfUcyfV8bEXAMPLE",
                "bucket": "amzn-s3-demo-bucket",
                "key": "WordPressApp.zip"
                }
            },
            "deploymentId": "d-A1B2C3111",
            "createTime": 1408480721.9,
            "completeTime": 1408480741.822
        },
        {
            "applicationName": "MyOther_App",
            "status": "Failed",
            "deploymentOverview": {
                "Failed": 1,
                "InProgress": 0,
                "Skipped": 0,
                "Succeeded": 0,
                "Pending": 0
            },
            "deploymentConfigName": "CodeDeployDefault.OneAtATime",
            "creator": "user",
            "errorInformation": {
```

```
                "message": "Deployment failed: Constraint default violated: No hosts
 succeeded.",
                "code": "HEALTH_CONSTRAINTS"
            },
            "deploymentGroupName": "MyOther_DG",
            "revision": {
                "revisionType": "S3",
                "s3Location": {
                "bundleType": "zip",
                "eTag": "\"dd56cfdEXAMPLE8e768f9d77fEXAMPLE\"",
                "bucket": "amzn-s3-demo-bucket",
                "key": "MyOtherApp.zip"
                }
            },
            "deploymentId": "d-A1B2C3222",
            "createTime": 1409764576.589,
            "completeTime": 1409764596.101
        }
    ]
}
```

- Para obtener información sobre la API, consulte BatchGetDeployments en la Referencia de comandos de la AWS CLI.

`batch-get-on-premises-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-on-premises-instances`.

AWS CLI

Obtención de información acerca de una o varias instancias en las instalaciones

En el siguiente ejemplo de `batch-get-on-premises-instances`, se obtiene información acerca de dos instancias en las instalaciones.

```
aws deploy batch-get-on-premises-instances --instance-
names AssetTag12010298EX AssetTag23121309EX
```

Salida:

```
{
```

```
    "instanceInfos": [
        {
            "iamUserArn": "arn:aws:iam::123456789012:user/AWS/CodeDeploy/
AssetTag12010298EX",
            "tags": [
                {
                    "Value": "CodeDeployDemo-OnPrem",
                    "Key": "Name"
                }
            ],
            "instanceName": "AssetTag12010298EX",
            "registerTime": 1425579465.228,
            "instanceArn": "arn:aws:codedeploy:us-west-2:123456789012:instance/
AssetTag12010298EX_4IwLNI2Alh"
        },
        {
            "iamUserArn": "arn:aws:iam::123456789012:user/AWS/CodeDeploy/
AssetTag23121309EX",
            "tags": [
                {
                    "Value": "CodeDeployDemo-OnPrem",
                    "Key": "Name"
                }
            ],
            "instanceName": "AssetTag23121309EX",
            "registerTime": 1425595585.988,
            "instanceArn": "arn:aws:codedeploy:us-west-2:80398EXAMPLE:instance/
AssetTag23121309EX_PomUy64Was"
        }
    ]
}
```

- Para obtener información sobre la API, consulte BatchGetOnPremisesInstances en la Referencia de comandos de la AWS CLI.

`continue-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `continue-deployment`.

AWS CLI

Inicio del enrutamiento del tráfico sin tener que esperar a que transcurra un tiempo de espera especificado

En el siguiente ejemplo de `continue-deployment`, se comienza a enrutar el tráfico de las instancias en el entorno original que están listas para empezar a transferir el tráfico a instancias en el entorno de sustitución.

```
aws deploy continue-deployment \
    --deployment-id "d-A1B2C3111" \
    --deployment-wait-type "READY_WAIT"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte ContinueDeployment en la Referencia de la API de AWS CodeDeploy.

- Para obtener detalles sobre la API, consulte ContinueDeployment en la Referencia de comandos de la AWS CLI.

`create-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-application`.

AWS CLI

Para crear una aplicación

En el siguiente ejemplo de `create-application`, se crea una aplicación y se asocia a la cuenta de AWS del usuario.

```
aws deploy create-application --application-name MyOther_App
```

Salida:

```
{
    "applicationId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
}
```

- Para obtener información sobre la API, consulte CreateApplication en la Referencia de comandos de la AWS CLI.

`create-deployment-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-deployment-config`.

AWS CLI

Creación de una configuración de implementación personalizada

En el siguiente ejemplo de `create-deployment-config`, se crea una configuración de implementación personalizada y se asocia a la cuenta de AWS del usuario.

```
aws deploy create-deployment-config \
    --deployment-config-name ThreeQuartersHealthy \
    --minimum-healthy-hosts type=FLEET_PERCENT,value=75
```

Salida:

```
{
    "deploymentConfigId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
}
```

- Para obtener información sobre la API, consulte CreateDeploymentConfig en la Referencia de comandos de la AWS CLI.

`create-deployment-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-deployment-group`.

AWS CLI

Creación de un grupo de implementación

En el siguiente ejemplo de `create-deployment-group`, se crea un grupo de implementación y se asocia a la aplicación especificada de la cuenta de AWS del usuario.

```
aws deploy create-deployment-group \
    --application-name WordPress_App \
    --auto-scaling-groups CodeDeployDemo-ASG \
    --deployment-config-name CodeDeployDefault.OneAtATime \
    --deployment-group-name WordPress_DG \
    --ec2-tag-filters Key=Name,Value=CodeDeployDemo,Type=KEY_AND_VALUE \
    --service-role-arn arn:aws:iam::123456789012:role/CodeDeployDemoRole
```

Salida:

```
{
```

```
    "deploymentGroupId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
}
```

- Para obtener información sobre la API, consulte CreateDeploymentGroup en la Referencia de comandos de la AWS CLI.

`create-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-deployment`.

AWS CLI

Ejemplo 1: cómo crear una implementación de CodeDeploy con la plataforma de informática de EC2/en las instalaciones

En el siguiente ejemplo de `create-deployment`, se crea una implementación y se asocia a la cuenta de AWS del usuario.

```
aws deploy create-deployment \
    --application-name WordPress_App \
    --deployment-config-name CodeDeployDefault.OneAtATime \
    --deployment-group-name WordPress_DG \
    --description "My demo deployment" \
    --s3-location bucket=amzn-s3-demo-
bucket,bundleType=zip,eTag=dd56cfdEXAMPLE8e768f9d77fEXAMPLE,key=WordPressApp.zip
```

Salida:

```
{
    "deploymentId": "d-A1B2C3111"
}
```

Ejemplo 2: cómo crear una implementación de CodeDeploy con la plataforma de informática de Amazon EC

En el siguiente ejemplo de `create-deployment`, se utilizan los dos archivos siguientes para implementar un servicio de Amazon ECS.

Contenido del archivo `create-deployment.json`:

```
{
```

```
    "applicationName": "ecs-deployment",
    "deploymentGroupName": "ecs-deployment-dg",
    "revision": {
        "revisionType": "S3",
        "s3Location": {
            "bucket": "ecs-deployment-bucket",
            "key": "appspec.yaml",
            "bundleType": "YAML"
        }
    }
}
```

Ese archivo, a su vez, obtiene el siguiente archivo `appspec.yaml` de un bucket de S3 denominado `ecs-deployment-bucket`.

```
version: 0.0
Resources:
  - TargetService:
      Type: AWS::ECS::Service
      Properties:
        TaskDefinition: "arn:aws:ecs:region:123456789012:task-definition/ecs-task-
def:2"
        LoadBalancerInfo:
          ContainerName: "sample-app"
          ContainerPort: 80
        PlatformVersion: "LATEST"
```

Comando:

```
aws deploy create-deployment \
    --cli-input-json file://create-deployment.json \
    --region us-east-1
```

Salida:

```
{
    "deploymentId": "d-1234ABCDE"
}
```

Para obtener más información, consulte CreateDeployment en la Referencia de la API de AWS CodeDeploy.

- Para obtener información sobre la API, consulte CreateDeployment en la Referencia de comandos de la AWS CLI.

`delete-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-application`.

AWS CLI

Para eliminar una aplicación de

En el siguiente `delete-application` ejemplo, se elimina la aplicación especificada que está asociada a la cuenta de AWS del usuario.

```
aws deploy delete-application --application-name WordPress_App
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteApplication en la Referencia de comandos de la AWS CLI.

`delete-deployment-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-deployment-config`.

AWS CLI

Eliminación de una configuración de implementación

En el siguiente ejemplo de `delete-deployment-config`, se elimina una configuración de implementación personalizada que está asociada a la cuenta de AWS del usuario.

```
aws deploy delete-deployment-config --deployment-config-name ThreeQuartersHealthy
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteDeploymentConfig en la Referencia de comandos de la AWS CLI.

`delete-deployment-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-deployment-group`.

AWS CLI

Eliminación de un grupo de implementación

En el siguiente ejemplo de `delete-deployment-group`, se elimina un grupo de implementación que está asociado a la aplicación especificada.

```
aws deploy delete-deployment-group \
    --application-name WordPress_App \
    --deployment-group-name WordPress_DG
```

Salida:

```
{
    "hooksNotCleanedUp": []
}
```

- Para obtener información sobre la API, consulte DeleteDeploymentGroup en la Referencia de comandos de la AWS CLI.

`delete-git-hub-account-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-git-hub-account-token`.

AWS CLI

Eliminación de una conexión de cuenta de GitHub

En el siguiente ejemplo de `delete-git-hub-account-token`, se elimina la conexión de la cuenta de GitHub especificada.

```
aws deploy delete-git-hub-account-token --token-name my-github-account
```

Salida:

```
{
    "tokenName": "my-github-account"
```

```
}
```

Para obtener más información, consulte DeleteGitHubAccountToken en la Referencia de la API de AWS CodeDeploy.

- Para obtener información sobre la API, consulte DeleteGitHubAccountToken en la Referencia de comandos de la AWS CLI.

`deregister-on-premises-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-on-premises-instance`.

AWS CLI

Anulación del registro de una instancia en las instalaciones

En el siguiente ejemplo de `deregister-on-premises-instance`, se anula el registro de una instancia en las instalaciones con AWS CodeDeploy, pero no se elimina el usuario de IAM asociado a la instancia ni se desasocian de la instancia en AWS CodeDeploy las etiquetas de la instancia en las instalaciones. Tampoco se desinstala el agente de AWS CodeDeploy de la instancia ni se elimina el archivo de configuración en las instalaciones de la instancia.

```
aws deploy deregister-on-premises-instance --instance-name AssetTag12010298EX
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeregisterOnPremisesInstance en la Referencia de comandos de la AWS CLI.

`deregister`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister`.

AWS CLI

Anulación del registro de una instancia en las instalaciones

En el siguiente ejemplo de `deregister`, se anula el registro de la instancia en las instalaciones con AWS CodeDeploy. No se elimina el usuario de IAM que está asociado a la instancia. En AWS CodeDeploy, se desasocian de la instancia las etiquetas en las instalaciones. No se desinstala

el agente de AWS CodeDeploy de la instancia ni se elimina el archivo de configuración en las instalaciones de la instancia.

```
aws deploy deregister \
    --instance-name AssetTag12010298EX \
    --no-delete-iam-user \
    --region us-west-2
```

Salida:

```
Retrieving on-premises instance information... DONE
IamUserArn: arn:aws:iam::80398EXAMPLE:user/AWS/CodeDeploy/AssetTag12010298EX
Tags: Key=Name,Value=CodeDeployDemo-OnPrem
Removing tags from the on-premises instance... DONE
Deregistering the on-premises instance... DONE
Run the following command on the on-premises instance to uninstall the codedeploy-
agent:
aws deploy uninstall
```

- Para obtener información sobre la API, consulte Deregister en la Referencia de comandos de la AWS CLI.

`get-application-revision`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-application-revision`.

AWS CLI

Obtención de información sobre una revisión de la aplicación

En el siguiente ejemplo de `get-application-revision`, se muestra información sobre una revisión de la aplicación asociada a la aplicación especificada.

```
aws deploy get-application-revision \
    --application-name WordPress_App \
    --s3-location bucket=amzn-s3-demo-
bucket,bundleType=zip,eTag=dd56cfdEXAMPLE8e768f9d77fEXAMPLE,key=WordPressApp.zip
```

Salida:

```
{
```

```
    "applicationName": "WordPress_App",
    "revisionInfo": {
        "description": "Application revision registered by Deployment ID: d-
A1B2C3111",
        "registerTime": 1411076520.009,
        "deploymentGroups": "WordPress_DG",
        "lastUsedTime": 1411076520.009,
        "firstUsedTime": 1411076520.009
    },
    "revision": {
        "revisionType": "S3",
        "s3Location": {
            "bundleType": "zip",
            "eTag": "dd56cfdEXAMPLE8e768f9d77fEXAMPLE",
            "bucket": "amzn-s3-demo-bucket",
            "key": "WordPressApp.zip"
        }
    }
}
```

- Para obtener información sobre la API, consulte GetApplicationRevision en la Referencia de comandos de la AWS CLI.

`get-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-application`.

AWS CLI

Obtención de información sobre una aplicación

En el siguiente ejemplo de `get-application`, se muestra información sobre una aplicación que está asociada a la cuenta de AWS del usuario.

```
aws deploy get-application --application-name WordPress_App
```

Salida:

```
{
    "application": {
        "applicationName": "WordPress_App",
        "applicationId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
```

```
        "createTime": 1407878168.078,
        "linkedToGitHub": false
    }
}
```

- Para obtener más información sobre la API, consulte GetApplication en la Referencia de comandos de la AWS CLI.

`get-deployment-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-deployment-config`.

AWS CLI

Obtención de información acerca de una configuración de implementación

En el siguiente ejemplo de `get-deployment-config`, se muestra información sobre una configuración de implementación que está asociada a la cuenta de AWS del usuario.

```
aws deploy get-deployment-config --deployment-config-name ThreeQuartersHealthy
```

Salida:

```
{
    "deploymentConfigInfo": {
        "deploymentConfigId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
        "minimumHealthyHosts": {
            "type": "FLEET_PERCENT",
            "value": 75
        },
        "createTime": 1411081164.379,
        "deploymentConfigName": "ThreeQuartersHealthy"
    }
}
```

- Para obtener información sobre la API, consulte GetDeploymentConfig en la Referencia de comandos de la AWS CLI.

`get-deployment-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-deployment-group`.

AWS CLI

Visualización de información acerca de un grupo de implementación

En el siguiente ejemplo de `get-deployment-group`, se muestra información sobre un grupo de implementación que está asociado a la aplicación especificada.

```
aws deploy get-deployment-group \
    --application-name WordPress_App \
    --deployment-group-name WordPress_DG
```

Salida:

```
{
    "deploymentGroupInfo": {
        "applicationName": "WordPress_App",
        "autoScalingGroups": [
            "CodeDeployDemo-ASG"
        ],
        "deploymentConfigName": "CodeDeployDefault.OneAtATime",
        "ec2TagFilters": [
            {
                "Type": "KEY_AND_VALUE",
                "Value": "CodeDeployDemo",
                "Key": "Name"
            }
        ],
        "deploymentGroupId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
        "serviceRoleArn": "arn:aws:iam::123456789012:role/CodeDeployDemoRole",
        "deploymentGroupName": "WordPress_DG"
    }
}
```

- Para obtener información sobre la API, consulte GetDeploymentGroup en la Referencia de comandos de la AWS CLI.

`get-deployment-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-deployment-instance`.

AWS CLI

Obtención de información acerca de una instancia de implementación

En el siguiente ejemplo de `get-deployment-instance`, se muestra información sobre una instancia de implementación que está asociada a la implementación especificada.

```
aws deploy get-deployment-instance --deployment-id d-QA4G4F9EX --instance-
id i-902e9fEX
```

Salida:

```
{
    "instanceSummary": {
        "instanceId": "arn:aws:ec2:us-east-1:80398EXAMPLE:instance/i-902e9fEX",
        "lifecycleEvents": [
            {
                "status": "Succeeded",
                "endTime": 1408480726.569,
                "startTime": 1408480726.437,
                "lifecycleEventName": "ApplicationStop"
            },
            {
                "status": "Succeeded",
                "endTime": 1408480728.016,
                "startTime": 1408480727.665,
                "lifecycleEventName": "DownloadBundle"
            },
            {
                "status": "Succeeded",
                "endTime": 1408480729.744,
                "startTime": 1408480729.125,
                "lifecycleEventName": "BeforeInstall"
            },
            {
                "status": "Succeeded",
                "endTime": 1408480730.979,
                "startTime": 1408480730.844,
                "lifecycleEventName": "Install"
            },
            {
                "status": "Failed",
                "endTime": 1408480732.603,
```

```
                "startTime": 1408480732.1,
                "lifecycleEventName": "AfterInstall"
            },
            {
                "status": "Skipped",
                "endTime": 1408480732.606,
                "lifecycleEventName": "ApplicationStart"
            },
            {
                "status": "Skipped",
                "endTime": 1408480732.606,
                "lifecycleEventName": "ValidateService"
            }
        ],
        "deploymentId": "d-QA4G4F9EX",
        "lastUpdatedAt": 1408480733.152,
        "status": "Failed"
    }
}
```

- Para obtener información sobre la API, consulte GetDeploymentInstance en la Referencia de comandos de la AWS CLI.

`get-deployment-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-deployment-target`.

AWS CLI

Obtención de información sobre un destino de implementación

En el siguiente ejemplo de `get-deployment-target`, se obtiene información sobre un destino de implementación que está asociado a la implementación especificada.

```
aws deploy get-deployment-target \
    --deployment-id "d-A1B2C3111" \
    --target-id "i-a1b2c3d4e5f611111"
```

Salida:

```
{
    "deploymentTarget": {
```

```
        "deploymentTargetType": "InstanceTarget",
        "instanceTarget": {
            "lastUpdatedAt": 1556918687.504,
            "targetId": "i-a1b2c3d4e5f611111",
            "targetArn": "arn:aws:ec2:us-west-2:123456789012:instance/i-
a1b2c3d4e5f611111",
            "status": "Succeeded",
            "lifecycleEvents": [
                {
                    "status": "Succeeded",
                    "diagnostics": {
                        "errorCode": "Success",
                        "message": "Succeeded",
                        "logTail": "",
                        "scriptName": ""
                    },
                    "lifecycleEventName": "ApplicationStop",
                    "startTime": 1556918592.162,
                    "endTime": 1556918592.247
                },
                {
                    "status": "Succeeded",
                    "diagnostics": {
                        "errorCode": "Success",
                        "message": "Succeeded",
                        "logTail": "",
                        "scriptName": ""
                    },
                    "lifecycleEventName": "DownloadBundle",
                    "startTime": 1556918593.193,
                    "endTime": 1556918593.981
                },
                {
                    "status": "Succeeded",
                    "diagnostics": {
                        "errorCode": "Success",
                        "message": "Succeeded",
                        "logTail": "",
                        "scriptName": ""
                    },
                    "lifecycleEventName": "BeforeInstall",
                    "startTime": 1556918594.805,
                    "endTime": 1556918681.807
                },
```

```
                {
                    "status": "Succeeded",
                    "diagnostics": {
                        "errorCode": "Success",
                        "message": "Succeeded",
                        "logTail": "",
                        "scriptName": ""
                    },
                    "lifecycleEventName": "Install",
                    "startTime": 1556918682.696,
                    "endTime": 1556918683.005
                },
                {
                    "status": "Succeeded",
                    "diagnostics": {
                        "errorCode": "Success",
                        "message": "Succeeded",
                        "logTail": "",
                        "scriptName": ""
                    },
                    "lifecycleEventName": "AfterInstall",
                    "startTime": 1556918684.135,
                    "endTime": 1556918684.216
                },
                {
                    "status": "Succeeded",
                    "diagnostics": {
                        "errorCode": "Success",
                        "message": "Succeeded",
                        "logTail": "",
                        "scriptName": ""
                    },
                    "lifecycleEventName": "ApplicationStart",
                    "startTime": 1556918685.211,
                    "endTime": 1556918685.295
                },
                {
                    "status": "Succeeded",
                    "diagnostics": {
                        "errorCode": "Success",
                        "message": "Succeeded",
                        "logTail": "",
                        "scriptName": ""
                    },
```

```
                    "lifecycleEventName": "ValidateService",
                    "startTime": 1556918686.65,
                    "endTime": 1556918686.747
                }
            ],
            "deploymentId": "d-A1B2C3111"
        }
    }
}
```

Para obtener más información, consulte GetDeploymentTarget en la Referencia de la API de AWS CodeDeploy.

- Para obtener información sobre la API, consulte GetDeploymentTarget en la Referencia de comandos de la AWS CLI.

`get-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-deployment`.

AWS CLI

Para obtener información acerca de una implementación

En el siguiente ejemplo de `get-deployment`, se muestra información sobre una implementación que está asociada a la cuenta de AWS del usuario.

```
aws deploy get-deployment --deployment-id d-A1B2C3123
```

Salida:

```
{
    "deploymentInfo": {
        "applicationName": "WordPress_App",
        "status": "Succeeded",
        "deploymentOverview": {
            "Failed": 0,
            "InProgress": 0,
            "Skipped": 0,
            "Succeeded": 1,
            "Pending": 0
        },
```

```
        "deploymentConfigName": "CodeDeployDefault.OneAtATime",
        "creator": "user",
        "description": "My WordPress app deployment",
        "revision": {
            "revisionType": "S3",
            "s3Location":  {
            "bundleType": "zip",
            "eTag": "\"dd56cfdEXAMPLE8e768f9d77fEXAMPLE\"",
            "bucket": "amzn-s3-demo-bucket",
            "key": "WordPressApp.zip"
            }
        },
        "deploymentId": "d-A1B2C3123",
        "deploymentGroupName": "WordPress_DG",
        "createTime": 1409764576.589,
        "completeTime": 1409764596.101,
        "ignoreApplicationStopFailures": false
    }
}
```

- Para obtener información sobre la API, consulte GetDeployment en la Referencia de comandos de la AWS CLI.

`get-on-premises-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-on-premises-instance`.

AWS CLI

Obtención de información sobre una instancia en las instalaciones

En el siguiente ejemplo de `get-on-premises-instance`, se obtiene información sobre la instancia en las instalaciones especificada.

```
aws deploy get-on-premises-instance --instance-name AssetTag12010298EX
```

Salida:

```
{
    "instanceInfo": {
    "iamUserArn": "arn:aws:iam::123456789012:user/AWS/CodeDeploy/
AssetTag12010298EX",
```

```
        "tags": [
        {
            "Value": "CodeDeployDemo-OnPrem",
            "Key": "Name"
        }
        ],
        "instanceName": "AssetTag12010298EX",
        "registerTime": 1425579465.228,
        "instanceArn": "arn:aws:codedeploy:us-east-1:123456789012:instance/
AssetTag12010298EX_4IwLNI2Alh"
    }
}
```

- Para obtener información sobre la API, consulte GetOnPremisesInstance en la Referencia de comandos de la AWS CLI.

`install`

En el siguiente ejemplo de código, se muestra cómo utilizar `install`.

AWS CLI

Instalación de una instancia en las instalaciones

En el siguiente ejemplo de `install`, se copia el archivo de configuración en las instalaciones desde la ubicación especificada en la instancia a la ubicación donde el agente de AWS CodeDeploy espera encontrarlo. También se instala y ejecuta el agente de AWS CodeDeploy en la instancia. No se crea ningún usuario de IAM, ni se registra la instancia en las instalaciones con AWS CodeDeploy, ni tampoco se asocia ninguna etiqueta de instancia en las instalaciones en AWS CodeDeploy para la instancia.

```
aws deploy install \
    --override-config \
    --config-file C:\temp\codedeploy.onpremises.yml \
    --region us-west-2 \
    --agent-installer s3://aws-codedeploy-us-west-2/latest/codedeploy-agent.msi
```

Salida:

```
Creating the on-premises instance configuration file... DONE
Installing the AWS CodeDeploy Agent... DONE
```

- Para obtener información sobre la API, consulte Install en la Referencia de comandos de la AWS CLI.

`list-application-revisions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-application-revisions`.

AWS CLI

Obtención de información sobre las revisiones de la aplicación

En el siguiente ejemplo de `list-application-revisions`, se muestra información sobre todas las revisiones de la aplicación que están asociadas a la aplicación especificada.

```
aws deploy list-application-revisions \
    --application-name WordPress_App \
    --s-3-bucket amzn-s3-demo-bucket \
    --deployed exclude \
    --s-3-key-prefix WordPress_ \
    --sort-by lastUsedTime \
    --sort-order descending
```

Salida:

```
{
    "revisions": [
        {
            "revisionType": "S3",
            "s3Location": {
                "version": "uTecLusvCB_JqHFXtfUcyfV8bEXAMPLE",
                "bucket": "amzn-s3-demo-bucket",
                "key": "WordPress_App.zip",
                "bundleType": "zip"
            }
        },
        {
            "revisionType": "S3",
            "s3Location": {
                "version": "tMk.UxgDpMEVb7V187ZM6wVAWEXAMPLE",
                "bucket": "amzn-s3-demo-bucket",
                "key": "WordPress_App_2-0.zip",
                "bundleType": "zip"
```

```
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListApplicationRevisions en la Referencia de comandos de la AWS CLI.

`list-applications`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-applications`.

AWS CLI

Obtención de información sobre las aplicaciones

En el siguiente ejemplo de `list-applications`, se muestra información sobre todas las aplicaciones asociadas a la cuenta de AWS del usuario.

```
aws deploy list-applications
```

Salida:

```
{
    "applications": [
        "WordPress_App",
        "MyOther_App"
    ]
}
```

- Para obtener más información sobre la API, consulte ListApplications en la Referencia de comandos de la AWS CLI.

`list-deployment-configs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-deployment-configs`.

AWS CLI

Obtención de información acerca de las configuraciones de implementación

En el siguiente ejemplo de `list-deployment-configs`, se muestra información sobre todas las configuraciones de implementación que están asociadas a la cuenta de AWS del usuario.

```
aws deploy list-deployment-configs
```

Salida:

```
{
    "deploymentConfigsList": [
        "ThreeQuartersHealthy",
        "CodeDeployDefault.AllAtOnce",
        "CodeDeployDefault.HalfAtATime",
        "CodeDeployDefault.OneAtATime"
    ]
}
```

- Para obtener información sobre la API, consulte ListDeploymentConfigs en la Referencia de comandos de la AWS CLI.

`list-deployment-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-deployment-groups`.

AWS CLI

Obtención de información acerca de los grupos de implementación

En el siguiente ejemplo de `list-deployment-groups`, se muestra información sobre todos los grupos de implementación que están asociados a la aplicación especificada.

```
aws deploy list-deployment-groups --application-name WordPress_App
```

Salida:

```
{
    "applicationName": "WordPress_App",
    "deploymentGroups": [
        "WordPress_DG",
        "WordPress_Beta_DG"
    ]
}
```

- Para obtener información sobre la API, consulte ListDeploymentGroups en la Referencia de comandos de la AWS CLI.

`list-deployment-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-deployment-instances`.

AWS CLI

Obtención de información acerca de instancias de implementación

En el siguiente ejemplo de `list-deployment-instances`, se muestra información sobre todas las instancias de implementación que están asociadas a la implementación especificada.

```
aws deploy list-deployment-instances \
    --deployment-id d-A1B2C3111 \
    --instance-status-filter Succeeded
```

Salida:

```
{
    "instancesList": [
        "i-EXAMPLE11",
        "i-EXAMPLE22"
    ]
}
```

- Para obtener información sobre la API, consulte ListDeploymentInstances en la Referencia de comandos de la AWS CLI.

`list-deployment-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-deployment-targets`.

AWS CLI

Obtención de una lista de ID de destino asociados a una implementación

En el siguiente ejemplo de `list-deployment-targets`, se obtiene una lista de los ID de destino asociados a las implementaciones que tienen el estado Failed o InProgress.

```
aws deploy list-deployment-targets \
    --deployment-id "d-A1B2C3111" \
    --target-filters "{\"TargetStatus\":[\"Failed\",\"InProgress\"]}"
```

Salida:

```
{
    "targetIds": [
        "i-0f1558aaf90e5f1f9"
    ]
}
```

Para obtener más información, consulte ListDeploymentTargets en la Referencia de la API de AWS CodeDeploy.

- Para obtener información sobre la API, consulte ListDeploymentTargets en la Referencia de comandos de la AWS CLI.

`list-deployments`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-deployments`.

AWS CLI

Obtención de información acerca de las implementaciones

En el siguiente ejemplo de `list-deployments`, se muestra información sobre todas las implementaciones que están asociadas al grupo de implementación.

```
aws deploy list-deployments \
    --application-name WordPress_App \
    --create-time-range start=2014-08-19T00:00:00,end=2014-08-20T00:00:00 \
    --deployment-group-name WordPress_DG \
    --include-only-statuses Failed
```

Salida:

```
{
    "deployments": [
        "d-EXAMPLE11",
        "d-EXAMPLE22",
```

```
        "d-EXAMPLE33"
    ]
}
```

- Para obtener más información sobre la API, consulte ListDeployments en Referencia de comandos de la AWS CLI.

`list-git-hub-account-token-names`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-git-hub-account-token-names`.

AWS CLI

Generación de una lista de nombres de las conexiones almacenadas en las cuentas de GitHub

En el siguiente ejemplo de `list-git-hub-account-token-names`, se muestran los nombres de las conexiones almacenadas en las cuentas de GitHub del usuario de AWS actual.

```
aws deploy list-git-hub-account-token-names
```

Salida:

```
{
    "tokenNameList": [
        "my-first-token",
        "my-second-token",
        "my-third-token"
    ]
}
```

Para obtener más información, consulte ListGitHubAccountTokenNames en la Referencia de la API de AWS CodeDeploy.

- Para obtener información sobre la API, consulte ListGitHubAccountTokenNames en la Referencia de comandos de la AWS CLI.

`list-on-premises-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-on-premises-instances`.

AWS CLI

Obtención de información acerca de una o varias instancias en las instalaciones

En el siguiente ejemplo de `list-on-premises-instances`, se obtiene una lista de los nombres de instancias en las instalaciones que están disponibles para las instancias registradas en AWS CodeDeploy y que también tienen la etiqueta de instancia en las instalaciones especificada, asociada a la instancia en AWS CodeDeploy.

```
aws deploy list-on-premises-instances \
    --registration-status Registered \
    --tag-filters Key=Name,Value=CodeDeployDemo-OnPrem,Type=KEY_AND_VALUE
```

Salida:

```
{
    "instanceNames": [
        "AssetTag12010298EX"
    ]
}
```

- Para obtener información sobre la API, consulte ListOnPremisesInstances en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un recurso (aplicación)

En el siguiente ejemplo de `list-tags-for-resource`, se muestran las etiquetas aplicadas a una aplicación denominada testApp en CodeDeploy.

```
aws deploy list-tags-for-resource \
    --resource-arn arn:aws:codedeploy:us-west-2:111122223333:application:testApp
```

Salida:

```
{
```

```
    "Tags": [
        {
            "Key": "Type",
            "Value": "testType"
        },
        {
            "Key": "Name",
            "Value": "testName"
        }
    ]
}
```

Para obtener más información, consulte Tagging instances for deployment groups in CodeDeploy en la Guía del usuario de AWS CodeDeploy.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`push`

En el siguiente ejemplo de código, se muestra cómo utilizar `push`.

AWS CLI

Agrupación e implementación de una revisión de aplicación compatible con AWS CodeDeploy en Amazon S3

En el siguiente ejemplo de `push`, se agrupa e implementa una revisión de la aplicación en Amazon S3 y, a continuación, se asocia la revisión de la aplicación a la aplicación especificada.

```
aws deploy push \
    --application-name WordPress_App \
    --description "This is my deployment" \
    --ignore-hidden-files \
    --s3-location s3://amzn-s3-demo-bucket/WordPressApp.zip \
    --source /tmp/MyLocalDeploymentFolder/
```

La salida describe cómo utilizar el comando `create-deployment` para crear una implementación que utilice la revisión de la aplicación cargada.

```
To deploy with this revision, run:
```

```
aws deploy create-deployment --application-name WordPress_App --
deployment-config-name <deployment-config-name> --deployment-group-
name <deployment-group-name> --s3-location bucket=amzn-s3-demo-
bucket,key=WordPressApp.zip,bundleType=zip,eTag="cecc9b8EXAMPLE50a6e71fdb88EXAMPLE",version=
```

- Para obtener información sobre la API, consulte Push en la Referencia de comandos de la AWS CLI.

`register-application-revision`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-application-revision`.

AWS CLI

Registro de información sobre una revisión de aplicación ya cargada

En el siguiente ejemplo de `register-application-revision`, se registra información sobre una revisión de aplicación ya cargada y almacenada en Amazon S3 con AWS CodeDeploy.

```
aws deploy register-application-revision \
    --application-name WordPress_App \
    --description "Revised WordPress application" \
    --s3-location bucket=amzn-s3-demo-
bucket,key=RevisedWordPressApp.zip,bundleType=zip,eTag=cecc9b8a08eac650a6e71fdb88EXAMPLE
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte RegisterApplicationRevision en la Referencia de comandos de la AWS CLI.

`register-on-premises-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-on-premises-instance`.

AWS CLI

Para registrar una instancia en las instalaciones

En el siguiente ejemplo de `register-on-premises-instance`, se registra una instancia en las instalaciones con AWS CodeDeploy. No se crea el usuario de IAM especificado ni se asocia en AWS CodeDeploy ninguna etiqueta de instancia en las instalaciones a la instancia registrada.

```
aws deploy register-on-premises-instance \
    --instance-name AssetTag12010298EX \
    --iam-user-arn arn:aws:iam::80398EXAMPLE:user/CodeDeployDemoUser-OnPrem
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte RegisterOnPremisesInstance en la Referencia de comandos de la AWS CLI.

`register`

En el siguiente ejemplo de código, se muestra cómo utilizar `register`.

AWS CLI

Para registrar una instancia en las instalaciones

En el siguiente ejemplo de `register`, se registra una instancia en las instalaciones con AWS CodeDeploy, se asocia en AWS CodeDeploy la etiqueta de instancia en las instalaciones especificada a la instancia registrada y se crea un archivo de configuración en las instalaciones que se puede copiar en la instancia. No se crea el usuario de IAM ni se instala el agente de AWS CodeDeploy en la instancia.

```
aws deploy register \
    --instance-name AssetTag12010298EX \
    --iam-user-arn arn:aws:iam::80398EXAMPLE:user/CodeDeployUser-OnPrem \
    --tags Key=Name,Value=CodeDeployDemo-OnPrem \
    --region us-west-2
```

Salida:

```
Registering the on-premises instance... DONE
Adding tags to the on-premises instance... DONE
Copy the on-premises configuration file named codedeploy.onpremises.yml to the on-
premises instance, and run the following command on the on-premises instance to
 install and configure the AWS CodeDeploy Agent:
aws deploy install --config-file codedeploy.onpremises.yml
```

- Para obtener información sobre la API, consulte Register en la Referencia de comandos de la AWS CLI.

`remove-tags-from-on-premises-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-tags-from-on-premises-instances`.

AWS CLI

Eliminación de etiquetas de una o más instancias en las instalaciones

En el siguiente ejemplo de `remove-tags-from-on-premises-instances`, se desasocian en AWS CodeDeploy las etiquetas en las instalaciones especificadas de las instancias en las instalaciones. No se anula el registro de las instancias en las instalaciones en AWS CodeDeploy, ni se desinstala el agente de AWS CodeDeploy de la instancia, ni tampoco se elimina el archivo de configuración en las instalaciones de las instancias ni los usuarios de IAM asociados a las instancias.

```
aws deploy remove-tags-from-on-premises-instances \
    --instance-names AssetTag12010298EX AssetTag23121309EX \
    --tags Key=Name,Value=CodeDeployDemo-OnPrem
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte RemoveTagsFromOnPremisesInstances en la Referencia de comandos de la AWS CLI.

`stop-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-deployment`.

AWS CLI

Reintento de detener una implementación

En el siguiente ejemplo de `stop-deployment`, se intenta detener una implementación en curso que está asociada a la cuenta de AWS del usuario.

aws deploy stop-deployment --deployment-id d-A1B2C3111

Salida:

```
{
```

```
    "status": "Succeeded",
    "statusMessage": "No more commands will be scheduled for execution in the
 deployment instances"
}
```

- Para obtener información sobre la API, consulte StopDeployment en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Etiquetado de un recurso (aplicación)

En el siguiente ejemplo de `tag-resource`, se agregan dos etiquetas con las claves Name y Type y los valores testName y testType a una aplicación denominada testApp en CodeDeploy.

```
aws deploy tag-resource \
    --resource-arn  arn:aws:codedeploy:us-west-2:111122223333:application:testApp \
    --tags Key=Name,Value=testName Key=Type,Value=testType
```

Si se ejecuta correctamente, este comando no genera ninguna salida.

Para obtener más información, consulte Tagging instances for deployment groups in CodeDeploy en la Guía del usuario de AWS CodeDeploy.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`uninstall`

En el siguiente ejemplo de código, se muestra cómo utilizar `uninstall`.

AWS CLI

Desinstalación de una instancia en las instalaciones

En el siguiente ejemplo de `uninstall`, se desinstala el agente AWS CodeDeploy de la instancia en las instalaciones y se elimina el archivo de configuración en las instalaciones de la instancia.

No se anula el registro de la instancia en AWS CodeDeploy, ni se desasocian de la instancia las etiquetas de la instancia en las instalaciones en AWS CodeDeploy, ni tampoco se elimina el usuario de IAM asociado a la instancia.

```
aws deploy uninstall
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte Uninstall en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de etiquetas de un recurso (aplicación)

En el siguiente ejemplo de `untag-resource`, se eliminan dos etiquetas con las claves Name y Type de una aplicación denominada testApp en CodeDeploy.

```
aws deploy untag-resource \
    --resource-arn  arn:aws:codedeploy:us-west-2:111122223333:application:testApp \
    --tag-keys Name Type
```

Si se ejecuta correctamente, este comando no genera ninguna salida.

Para obtener más información, consulte Tagging instances for deployment groups in CodeDeploy en la Guía del usuario de AWS CodeDeploy.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-application`.

AWS CLI

Cambio de los detalles de una aplicación

En el siguiente `update-application` ejemplo, se cambia el nombre de una aplicación que está asociada a la cuenta de AWS del usuario.

```
aws deploy update-application \
    --application-name WordPress_App \
    --new-application-name My_WordPress_App
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte UpdateApplication en la Referencia de comandos de la AWS CLI.

`update-deployment-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-deployment-group`.

AWS CLI

Cambio de la información acerca de un grupo de implementación

En el siguiente ejemplo de `update-deployment-group`, se cambia la configuración de un grupo de implementación que está asociado a la aplicación especificada.

```
aws deploy update-deployment-group \
    --application-name WordPress_App \
    --auto-scaling-groups My_CodeDeployDemo_ASG \
    --current-deployment-group-name WordPress_DG \
    --deployment-config-name CodeDeployDefault.AllAtOnce \
    --ec2-tag-filters Key=Name,Type=KEY_AND_VALUE,Value=My_CodeDeployDemo \
    --new-deployment-group-name My_WordPress_DepGroup \
    --service-role-arn arn:aws:iam::80398EXAMPLE:role/CodeDeployDemo-2
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte UpdateDeploymentGroup en la Referencia de comandos de la AWS CLI.

Ejemplos del Revisor de CodeGuru que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar situaciones comunes mediante la AWS Command Line Interface con el Revisor de CodeGuru.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-repository`.

AWS CLI

Ejemplo 1: cómo crear una asociación de repositorio de Bitbucket

En el ejemplo siguiente de `associate-repository`, se crea una asociación de repositorio mediante un repositorio de Bitbucket existente.

```
aws codeguru-reviewer associate-repository \
    --repository 'Bitbucket={Owner=sample-owner, Name=mySampleRepo,
 ConnectionArn=arn:aws:codestar-connections:us-west-2:123456789012:connection/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 }'
```

Salida:

```
{
    "RepositoryAssociation": {
        "ProviderType": "Bitbucket",
        "Name": "mySampleRepo",
        "LastUpdatedTimeStamp": 1596216896.979,
        "AssociationId": "association:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "CreatedTimeStamp": 1596216896.979,
        "ConnectionArn": "arn:aws:codestar-connections:us-
west-2:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "State": "Associating",
```

```
        "StateReason": "Pending Repository Association",
        "AssociationArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "Owner": "sample-owner"
    }
}
```

Para obtener más información, consulte Create a Bitbucket repository association in Amazon CodeGuru Reviewer en la Guía del usuario de Revisor de Amazon CodeGuru.

Ejemplo 2: cómo crear una asociación de repositorio de GitHub Enterprise

En el ejemplo siguiente de `associate-repository`, se crea una asociación de repositorio mediante un repositorio de GitHub Enterprise existente.

```
aws codeguru-reviewer associate-repository \
    --repository 'GitHubEnterpriseServer={Owner=sample-owner, Name=mySampleRepo,
 ConnectionArn=arn:aws:codestar-connections:us-west-2:123456789012:connection/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 }'
```

Salida:

```
{
    "RepositoryAssociation": {
        "ProviderType": "GitHubEnterpriseServer",
        "Name": "mySampleRepo",
        "LastUpdatedTimeStamp": 1596216896.979,
        "AssociationId": "association:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "CreatedTimeStamp": 1596216896.979,
        "ConnectionArn": "arn:aws:codestar-connections:us-
west-2:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "State": "Associating",
        "StateReason": "Pending Repository Association",
        "AssociationArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "Owner": "sample-owner"
    }
}
```

Para obtener más información, consulte Create a GitHub Enterprise Server repository association in Amazon CodeGuru Reviewer en la Guía del usuario de Revisor de Amazon CodeGuru.

Ejemplo 3: cómo crear una asociación de repositorio de AWS CodeCommit

En el ejemplo siguiente de `associate-repository`, se crea una asociación de repositorio mediante un repositorio de AWS CodeCommit existente.

```
aws codeguru-reviewer associate-repository \
    --repository CodeCommit={Name=mySampleRepo}
```

Salida:

```
{
    "RepositoryAssociation": {
        "AssociationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "Name": "My-ecs-beta-repo",
        "LastUpdatedTimeStamp": 1595634764.029,
        "ProviderType": "CodeCommit",
        "CreatedTimeStamp": 1595634764.029,
        "Owner": "544120495673",
        "State": "Associating",
        "StateReason": "Pending Repository Association",
        "AssociationArn": "arn:aws:codeguru-reviewer:us-
west-2:544120495673:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    }
}
```

Para obtener más información, consulte Create an AWS CodeCommit repository association in Amazon CodeGuru Reviewer en la Guía del usuario de Revisor de Amazon CodeGuru.

- Para obtener información sobre la API, consulte AssociateRepository en la Referencia de comandos de la AWS CLI.

`create-code-review`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-code-review`.

AWS CLI

Creación de una revisión de código

En el siguiente `create-code-review`, se crea una revisión del código en la ramificación `mainline` de un repositorio de AWS CodeCommit, que recibe el nombre de `my-repository-name`.

```
aws codeguru-reviewer create-code-review \
    --name my-code-review \
    --repository-association-arn arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --type '{"RepositoryAnalysis": {"RepositoryHead": {"BranchName": "mainline"}}}'
```

Salida:

```
{
    "CodeReview": {
        "Name": "my-code-review",
        "CodeReviewArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222:code-
review:RepositoryAnalysis-my-code-review",
        "RepositoryName": "my-repository-name",
        "Owner": "123456789012",
        "ProviderType": "CodeCommit",
        "State": "Pending",
        "StateReason": "CodeGuru Reviewer has received the request, and a code
 review is scheduled.",
        "CreatedTimeStamp": 1618873489.195,
        "LastUpdatedTimeStamp": 1618873489.195,
        "Type": "RepositoryAnalysis",
        "SourceCodeType": {
            "RepositoryHead": {
                "BranchName": "mainline"
            }
        },
        "AssociationArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    }
}
```

Para obtener más información, consulte Create code reviews in Amazon CodeGuru Reviewer en la Guía del usuario de Revisor de Amazon CodeGuru.

- Para obtener información sobre la API, consulte CreateCodeReview en la Referencia de comandos de la AWS CLI.

`describe-code-review`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-code-review`.

AWS CLI

Listado de detalles sobre una revisión de código

En el siguiente `describe-code-review`, se muestra información sobre una revisión del código en la ramificación mainline de un repositorio de AWS CodeCommit denominado my-repo-name.

```
aws codeguru-reviewer put-recommendation-feedback \
    --code-review-arn arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111:code-
review:RepositoryAnalysis-my-repository-name-branch-abcdefgh12345678 \
    --recommendation-
id 3be1b2e5d7ef6e298a06499379ee290c9c596cf688fdcadb08285ddb0dd390eb \
    --reactions ThumbsUp
```

Output

```
{
        "CodeReview": {
            "Name": "My-ecs-beta-repo-master-xs6di4kfd4j269dz",
            "CodeReviewArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222:code-
review:RepositoryAnalysis-my-repo-name",
            "RepositoryName": "My-ecs-beta-repo",
            "Owner": "123456789012",
            "ProviderType": "CodeCommit",
            "State": "Pending",
            "StateReason": "CodeGuru Reviewer is reviewing the source code.",
            "CreatedTimeStamp": 1618874226.226,
            "LastUpdatedTimeStamp": 1618874233.689,
            "Type": "RepositoryAnalysis",
            "SourceCodeType": {
                "RepositoryHead": {
                    "BranchName": "mainline"
                }
            },
            "AssociationArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
        }
    }
```

Para obtener más información, consulte View code review details en la Guía del usuario de Revisor de Amazon CodeGuru.

- Para obtener información sobre la API, consulte DescribeCodeReview en la Referencia de comandos de la AWS CLI.

`describe-recommendation-feedback`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-recommendation-feedback`.

AWS CLI

Visualización de información acerca de los comentarios sobre una recomendación

En el siguiente `describe-recommendation-feedback`, se muestra información acerca de los comentarios sobre una recomendación. Esta recomendación tiene una reacción ThumbsUp.

```
aws codeguru-reviewer describe-recommendation-feedback \
    --code-review-arn arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111:code-
review:RepositoryAnalysis-my-repository-name-branch-abcdefgh12345678 \
    --recommendation-
id 3be1b2e5d7ef6e298a06499379ee290c9c596cf688fdcadb08285ddb0dd390eb
```

Salida:

```
{
    "RecommendationFeedback": {
        "CodeReviewArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111:code-
review:RepositoryAnalysis-my-repository-name-branch-abcdefgh12345678",
        "RecommendationId":
 "3be1b2e5d7ef6e298a06499379ee290c9c596cf688fdcadb08285ddb0dd390eb",
        "Reactions": [
            "ThumbsUp"
        ],
        "UserId": "aws-user-id",
        "CreatedTimeStamp": 1618877070.313,
        "LastUpdatedTimeStamp": 1618877948.881
    }
}
```

Para obtener más información, consulte View recommendations and provide feedback y Step 4: Provide feedback en la Guía del usuario de Revisor de Amazon CodeGuru.

- Para obtener información sobre la API, consulte DescribeRecommendationFeedback en la Referencia de comandos de la AWS CLI.

`describe-repository-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-repository-association`.

AWS CLI

Ejemplo 1: cómo obtener información sobre una asociación de repositorio de GitHub

En el ejemplo siguiente de `describe-repository-association`, se muestra información sobre una asociación de repositorio que usa un repositorio de GitHub Enterprise y se encuentra en el estado `Associated`.

```
aws codeguru-reviewer describe-repository-association \
    --association-arn arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "RepositoryAssociation": {
        "AssociationId": "b822717e-0711-4e8a-bada-0e738289c75e",
        "Name": "mySampleRepo",
        "LastUpdatedTimeStamp": 1588102637.649,
        "ProviderType": "GitHub",
        "CreatedTimeStamp": 1588102615.636,
        "Owner": "sample-owner",
        "State": "Associated",
        "StateReason": "Pull Request Notification configuration successful",
        "AssociationArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    }
}
```

Para obtener más información, consulte Create a GitHub Enterprise Server repository association in Amazon CodeGuru Reviewer en la Guía del usuario de Revisor de Amazon CodeGuru.

Ejemplo 2: cómo obtener información sobre una asociación de repositorio fallida

En el ejemplo siguiente de `describe-repository-association`, se muestra información sobre una asociación de repositorio que usa un repositorio de GitHub Enterprise y se encuentra en el estado `Failed`.

```
aws codeguru-reviewer describe-repository-association \
    --association-arn arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "RepositoryAssociation": {
        "ProviderType": "GitHubEnterpriseServer",
        "Name": "mySampleRepo",
        "LastUpdatedTimeStamp": 1596217036.892,
        "AssociationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "CreatedTimeStamp": 1596216896.979,
        "ConnectionArn": "arn:aws:codestar-connections:us-
west-2:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "State": "Failed",
        "StateReason": "Failed, Please retry.",
        "AssociationArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
        "Owner": "sample-owner"
    }
}
```

Para obtener más información, consulte Create a GitHub Enterprise Server repository association in Amazon CodeGuru Reviewer en la Guía del usuario de Revisor de Amazon CodeGuru.

Ejemplo 3: cómo obtener información sobre una asociación de repositorio desasociada

En el ejemplo siguiente de `describe-repository-association`, se muestra información sobre una asociación de repositorio que usa un repositorio de GitHub Enterprise y se encuentra en el estado `Disassociating`.

```
aws codeguru-reviewer describe-repository-association \
    --association-arn arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "RepositoryAssociation": {
        "ProviderType": "GitHubEnterpriseServer",
        "Name": "mySampleRepo",
        "LastUpdatedTimeStamp": 1596217036.892,
        "AssociationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "CreatedTimeStamp": 1596216896.979,
        "ConnectionArn": "arn:aws:codestar-connections:us-
west-2:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "State": "Disassociating",
        "StateReason": "Source code access removal in progress",
        "AssociationArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
        "Owner": "sample-owner"
    }
}
```

Para obtener más información, consulte Create a GitHub Enterprise Server repository association in Amazon CodeGuru Reviewer en la Guía del usuario de Revisor de Amazon CodeGuru.

- Para obtener información sobre la API, consulte DescribeRepositoryAssociation en la Referencia de comandos de la AWS CLI.

`disassociate-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-repository`.

AWS CLI

Desasociación de una asociación de repositorio

En el siguiente `disassociate-repository`, se desasocia una asociación de repositorio mediante un repositorio de AWS CodeCommit.

```
aws codeguru-reviewer disassociate-repository \
    --association-arn arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "RepositoryAssociation": {
```

```
        "AssociationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "AssociationArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "Name": "my-repository",
        "Owner": "123456789012",
        "ProviderType": "CodeCommit",
        "State": "Disassociating",
        "LastUpdatedTimeStamp": 1618939174.759,
        "CreatedTimeStamp": 1595636947.096
    },
    "Tags": {
        "Status": "Secret",
        "Team": "Saanvi"
    }
}
```

Para obtener más información, consulte Disassociate a repository in CodeGuru Reviewer en la Guía del usuario de Revisor de Amazon CodeGuru.

- Para obtener información sobre la API, consulte DisassociateRepository en la Referencia de comandos de la AWS CLI.

`list-code-reviews`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-code-reviews`.

AWS CLI

Listado de las revisiones de código creadas en la cuenta de AWS en los últimos 90 días

En el siguiente ejemplo de `list-code-reviews`, se genera una lista de las revisiones de código creadas en los últimos 90 días mediante solicitudes de extracción.

```
aws codeguru-reviewer list-code-reviews \
    --type PullRequest
```

Salida:

```
{
    "CodeReviewSummaries": [
        {
            "LastUpdatedTimeStamp": 1588897288.054,
            "Name": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
            "ProviderType": "GitHub",
            "PullRequestId": "5",
            "MetricsSummary": {
                "MeteredLinesOfCodeCount": 24,
                "FindingsCount": 1
            },
            "CreatedTimeStamp": 1588897068.512,
            "State": "Completed",
            "CodeReviewArn": "arn:aws:codeguru-reviewer:us-west-2:123456789012:code-
review:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "Owner": "sample-owner",
            "RepositoryName": "sample-repository-name",
            "Type": "PullRequest"
        },
        {
            "LastUpdatedTimeStamp": 1588869793.263,
            "Name": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "ProviderType": "GitHub",
            "PullRequestId": "4",
            "MetricsSummary": {
                "MeteredLinesOfCodeCount": 29,
                "FindingsCount": 0
            },
            "CreatedTimeStamp": 1588869575.949,
            "State": "Completed",
            "CodeReviewArn": "arn:aws:codeguru-reviewer:us-west-2:123456789012:code-
review:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "Owner": "sample-owner",
            "RepositoryName": "sample-repository-name",
            "Type": "PullRequest"
        },
        {
            "LastUpdatedTimeStamp": 1588870511.211,
            "Name": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "ProviderType": "GitHub",
            "PullRequestId": "4",
            "MetricsSummary": {
                "MeteredLinesOfCodeCount": 2,
                "FindingsCount": 0
            },
            "CreatedTimeStamp": 1588870292.425,
            "State": "Completed",
            "CodeReviewArn": "arn:aws:codeguru-reviewer:us-west-2:123456789012:code-
review:a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
```

```
            "Owner": "sample-owner",
            "RepositoryName": "sample-repository-name",
            "Type": "PullRequest"
        },
        {
            "LastUpdatedTimeStamp": 1588118522.452,
            "Name": "a1b2c3d4-5678-90ab-cdef-EXAMPLE44444",
            "ProviderType": "GitHub",
            "PullRequestId": "3",
            "MetricsSummary": {
                "MeteredLinesOfCodeCount": 29,
                "FindingsCount": 0
            },
            "CreatedTimeStamp": 1588118301.131,
            "State": "Completed",
            "CodeReviewArn": "arn:aws:codeguru-reviewer:us-west-2:123456789012:code-
review:a1b2c3d4-5678-90ab-cdef-EXAMPLE44444",
            "Owner": "sample-owner",
            "RepositoryName": "sample-repository-name",
            "Type": "PullRequest"
        },
        {
            "LastUpdatedTimeStamp": 1588112205.207,
            "Name": "a1b2c3d4-5678-90ab-cdef-EXAMPLE55555",
            "ProviderType": "GitHub",
            "PullRequestId": "2",
            "MetricsSummary": {
                "MeteredLinesOfCodeCount": 25,
                "FindingsCount": 0
            },
            "CreatedTimeStamp": 1588111987.443,
            "State": "Completed",
            "CodeReviewArn": "arn:aws:codeguru-reviewer:us-west-2:123456789012:code-
review:a1b2c3d4-5678-90ab-cdef-EXAMPLE55555",
            "Owner": "sample-owner",
            "RepositoryName": "sample-repository-name",
            "Type": "PullRequest"
        },
        {
            "LastUpdatedTimeStamp": 1588104489.981,
            "Name": "a1b2c3d4-5678-90ab-cdef-EXAMPLE66666",
            "ProviderType": "GitHub",
            "PullRequestId": "1",
            "MetricsSummary": {
```

```
                "MeteredLinesOfCodeCount": 25,
                "FindingsCount": 0
            },
            "CreatedTimeStamp": 1588104270.223,
            "State": "Completed",
            "CodeReviewArn": "arn:aws:codeguru-reviewer:us-west-2:123456789012:code-
review:a1b2c3d4-5678-90ab-cdef-EXAMPLE66666",
            "Owner": "sample-owner",
            "RepositoryName": "sample-repository-name",
            "Type": "PullRequest"
        }
    ]
}
```

Para obtener más información, consulte View all code reviews en la Guía del usuario de Revisor de Amazon CodeGuru.

- Para obtener información sobre la API, consulte ListCodeReviews en la Referencia de comandos de la AWS CLI.

`list-recommendation-feedback`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-recommendation-feedback`.

AWS CLI

Listado de los comentarios de los clientes sobre una recomendación en un repositorio asociado

En el siguiente `list-recommendation-feedback`, se genera una lista de los comentarios de los clientes sobre todas las recomendaciones de una revisión de código. Esta revisión de código contiene un comentario, un ThumbsUp, de un cliente.

```
aws codeguru-reviewer list-recommendation-feedback \
    --code-review-arn arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111:code-
review:RepositoryAnalysis-my-repository-name-branch-abcdefgh12345678
```

Salida:

```
{
    "RecommendationFeedbackSummaries": [
        {
```

```
            "RecommendationId":
 "3be1b2e5d7ef6e298a06499379ee290c9c596cf688fdcadb08285ddb0dd390eb",
            "Reactions": [
                "ThumbsUp"
            ],
            "UserId": "aws-user-id"
        }
    ]
}
```

Para obtener más información, consulte Step 4: Provide feedback en la Guía del usuario de Revisor de Amazon CodeGuru.

- Para obtener información sobre la API, consulte ListRecommendationFeedback en la Referencia de comandos de la AWS CLI.

`list-recommendations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-recommendations`.

AWS CLI

Listado de las recomendaciones para una revisión de código completa

En el siguiente ejemplo de `list-recommendations`, se genera una lista de las recomendaciones para una revisión de código completa. Esta revisión del código tiene una recomendación.

```
aws codeguru-reviewer list-recommendations \
    --code-review-arn arn:aws:codeguru-reviewer:us-west-2:544120495673:code-
review:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "RecommendationSummaries": [
        {
            "Description": "\n\n**Problem**  \n You are using a `ConcurrentHashMap`,
 but your usage of `containsKey()` and `get()` may not be thread-safe at lines: **63
 and 64**. In between the check and the `get()` another thread can remove the key
 and the `get()` will return `null`. The remove that can remove the key is at line:
 **59**.\n\n**Fix**  \n Consider calling `get()`, checking instead of your current
```

```
 check if the returned object is `null`, and then using that object only, without
 calling `get()` again.\n\n**More info**  \n [View an example on GitHub](https://
github.com/apache/hadoop/blob/f16cf877e565084c66bc63605659b157c4394dc8/hadoop-tools/
hadoop-aws/src/main/java/org/apache/hadoop/fs/s3a/s3guard/S3Guard.java#L302-L304)
 (external link).",
            "RecommendationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "StartLine": 63,
            "EndLine": 64,
            "FilePath": "src/main/java/com/company/sample/application/
CreateOrderThread.java"
        }
    ]
}
```

Para obtener más información, consulte Step 4: Provide feedback en la Guía del usuario de Revisor de Amazon CodeGuru.

- Para obtener información sobre la API, consulte ListRecommendations en la Referencia de comandos de la AWS CLI.

`list-repository-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-repository-associations`.

AWS CLI

Listado de las asociaciones de repositorio en la cuenta de AWS

En el siguiente ejemplo de `list-repository-associations`, se genera una lista con los objetos de resumen de asociación de repositorio de la cuenta. Puede filtrar la lista obtenida por `ProviderType`, `Name`, `State` y `Owner`.

```
aws codeguru-reviewer list-repository-associations
```

Salida:

```
{
    "RepositoryAssociationSummaries": [
        {
            "LastUpdatedTimeStamp": 1595886609.616,
            "Name": "test",
            "AssociationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
            "Owner": "sample-owner",
            "State": "Associated",
            "AssociationArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "ProviderType": "Bitbucket"
        },
        {
            "LastUpdatedTimeStamp": 1595636969.035,
            "Name": "CodeDeploy-CodePipeline-ECS-Tutorial",
            "AssociationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "Owner": "123456789012",
            "State": "Associated",
            "AssociationArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "ProviderType": "CodeCommit"
        },
        {
            "LastUpdatedTimeStamp": 1595634785.983,
            "Name": "My-ecs-beta-repo",
            "AssociationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "Owner": "123456789012",
            "State": "Associated",
            "AssociationArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "ProviderType": "CodeCommit"
        },
        {
            "LastUpdatedTimeStamp": 1590712811.77,
            "Name": "MyTestCodeCommit",
            "AssociationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE44444",
            "Owner": "123456789012",
            "State": "Associated",
            "AssociationArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE44444",
            "ProviderType": "CodeCommit"
        },
        {
            "LastUpdatedTimeStamp": 1588102637.649,
            "Name": "aws-codeguru-profiler-sample-application",
            "AssociationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE55555",
            "Owner": "sample-owner",
            "State": "Associated",
            "AssociationArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE55555",
```

```
            "ProviderType": "GitHub"
        },
        {
            "LastUpdatedTimeStamp": 1588028233.995,
            "Name": "codeguru-profiler-demo-app",
            "AssociationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE66666",
            "Owner": "sample-owner",
            "State": "Associated",
            "AssociationArn": "arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE66666",
            "ProviderType": "GitHub"
        }
    ]
}
```

Para obtener más información, consulte View all repository associations in CodeGuru Reviewer en la Guía del usuario de Revisor de Amazon CodeGuru.

- Para obtener información sobre la API, consulte ListRepositoryAssociations en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Listado de las etiquetas de un repositorio asociado

En el siguiente `list-tags-for-resource`, se genera una lista de las etiquetas de un repositorio asociado. Este repositorio asociado tiene dos etiquetas.

```
aws codeguru-reviewer list-tags-for-resource \
    --resource-arn arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "Tags": {
        "Status": "Secret",
```

```
        "Team": "Saanvi"
    }
}
```

Para obtener más información, consulte View tags for a CodeGuru Reviewer associated repository (AWS CLI) en la Guía del usuario de Revisor de Amazon CodeGuru.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-recommendation-feedback`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-recommendation-feedback`.

AWS CLI

Adición de una recomendación a una revisión de código

En el siguiente `put-recommendation-feedback`, se incluye una recomendación ThumbsUp sobre una revisión de código.

```
aws codeguru-reviewer put-recommendation-feedback \
    --code-review-arn \arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111:code-
review:RepositoryAnalysis-my-repository-name-branch-abcdefgh12345678 \
    --recommendation-
id 3be1b2e5d7ef6e298a06499379ee290c9c596cf688fdcadb08285ddb0dd390eb \
    --reactions ThumbsUp
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Step 4: Provide feedback en la Guía del usuario de Revisor de Amazon CodeGuru.

- Para obtener información sobre la API, consulte PutRecommendationFeedback en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Adición de una etiqueta a un repositorio asociado

En el siguiente `tag-resource`, se genera una lista de las etiquetas de un repositorio asociado.

```
aws codeguru-reviewer tag-resource \
    --resource-arn arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --tags Status=Secret,Team=Saanvi
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Add a tag to a CodeGuru Reviewer associated repository (AWS CLI) y Add or update tags for a CodeGuru Reviewer associated repository (AWS CLI) en la Guía del usuario de Revisor de Amazon CodeGuru.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de etiqueta de un repositorio asociado

En el siguiente `untag-resource`, se eliminan dos etiquetas con las claves Secret y Team de un repositorio asociado.

```
aws codeguru-reviewer untag-resource \
    --resource-arn arn:aws:codeguru-reviewer:us-
west-2:123456789012:association:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --tag-keys Status Team
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Remove tags from a CodeGuru Reviewer associated repository (AWS CLI) en la Guía del usuario de Revisor de Amazon CodeGuru.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

Ejemplos de CodePipeline que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante la AWS Command Line Interface con CodePipeline.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`acknowledge-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `acknowledge-job`.

AWS CLI

Recuperación de información sobre un trabajo especificado

En este ejemplo, se devuelve información sobre un trabajo especificado, incluido el estado de ese trabajo, en su caso. Esto solo se usa para los procesos de trabajo y las acciones personalizadas. Para determinar el valor de nonce y el identificador del trabajo, utilice poll-for-jobs de AWS CodePipeline.

Comando:

```
aws codepipeline acknowledge-job --job-id f4f4ff82-2d11-EXAMPLE --nonce 3
```

Salida:

```
{
  "status": "InProgress"
}
```

- Para obtener detalles sobre la API, consulte AcknowledgeJob en la Referencia de comandos de la AWS CLI.

`create-custom-action-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-custom-action-type`.

AWS CLI

Creación de una acción personalizada

En este ejemplo, se crea una acción personalizada para AWS CodePipeline mediante un archivo JSON ya creado (aquí denominado MyCustomAction.json), que contiene la estructura de la acción personalizada. Para obtener más información sobre los requisitos para crear una acción personalizada, incluida la estructura del archivo, consulte la Guía del usuario de AWS CodePipeline.

```
aws codepipeline create-custom-action-type --cli-input-json file://
MyCustomAction.json
```

Contenido del archivo JSON `MyCustomAction.json`:

```
{
    "category": "Build",
    "provider": "MyJenkinsProviderName",
    "version": "1",
    "settings": {
        "entityUrlTemplate": "https://192.0.2.4/job/{Config:ProjectName}/",
        "executionUrlTemplate": "https://192.0.2.4/job/{Config:ProjectName}/
lastSuccessfulBuild/{ExternalExecutionId}/"
    },
    "configurationProperties": [
        {
            "name": "MyJenkinsExampleBuildProject",
            "required": true,
            "key": true,
            "secret": false,
            "queryable": false,
            "description": "The name of the build project must be provided when this
 action is added to the pipeline.",
            "type": "String"
        }
```

```
    ],
    "inputArtifactDetails": {
        "maximumCount": 1,
        "minimumCount": 0
    },
    "outputArtifactDetails": {
        "maximumCount": 1,
        "minimumCount": 0
    }
}
```

Este comando devuelve la estructura de la acción personalizada.

- Para obtener detalles sobre la API, consulte CreateCustomActionType en la Referencia de comandos de la AWS CLI.

`create-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-pipeline`.

AWS CLI

Creación de una canalización

En este ejemplo, se crea una canalización para AWS CodePipeline mediante un archivo JSON ya creado (aquí denominado MySecondPipeline.json), que contiene la estructura de la canalización. Para obtener más información sobre los requisitos para crear una canalización, incluida la estructura del archivo, consulte la Guía del usuario de AWS CodePipeline.

Comando:

```
aws codepipeline create-pipeline --cli-input-json file://MySecondPipeline.json
```

Contenidos de muestra del archivo JSON:

```
{
 "pipeline": {
  "roleArn": "arn:aws:iam::111111111111:role/AWS-CodePipeline-Service",
  "stages": [
    {
      "name": "Source",
      "actions": [
```

```
        {
          "inputArtifacts": [],
          "name": "Source",
          "actionTypeId": {
            "category": "Source",
            "owner": "AWS",
            "version": "1",
            "provider": "S3"
          },
          "outputArtifacts": [
            {
              "name": "MyApp"
            }
          ],
          "configuration": {
            "S3Bucket": "awscodepipeline-demo-bucket",
            "S3ObjectKey": "aws-codepipeline-s3-aws-codedeploy_linux.zip"
          },
          "runOrder": 1
        }
      ]
    },
    {
      "name": "Beta",
      "actions": [
        {
          "inputArtifacts": [
            {
              "name": "MyApp"
            }
          ],
          "name": "CodePipelineDemoFleet",
          "actionTypeId": {
            "category": "Deploy",
            "owner": "AWS",
            "version": "1",
            "provider": "CodeDeploy"
          },
          "outputArtifacts": [],
          "configuration": {
            "ApplicationName": "CodePipelineDemoApplication",
            "DeploymentGroupName": "CodePipelineDemoFleet"
          },
          "runOrder": 1
```

```
        }
      ]
    }
  ],
  "artifactStore": {
    "type": "S3",
    "location": "codepipeline-us-east-1-11EXAMPLE11"
  },
  "name": "MySecondPipeline",
  "version": 1
 }
}
```

Salida:

```
This command returns the structure of the pipeline.
```

- Para obtener detalles sobre la API, consulte CreatePipeline en la Referencia de comandos de la AWS CLI.

`delete-custom-action-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-custom-action-type`.

AWS CLI

Eliminación de una acción personalizada

En este ejemplo, se elimina una acción personalizada en AWS CodePipeline mediante un archivo JSON ya creado (aquí denominado DeleteMyCustomAction.json) que contiene el tipo de acción, el nombre del proveedor y el número de versión de la acción que se va a eliminar. Use el comando list-action-types para ver los valores correctos de la categoría, la versión y el proveedor.

Comando:

```
aws codepipeline delete-custom-action-type --cli-input-json file://
DeleteMyCustomAction.json
```

Contenidos de muestra del archivo JSON:

```
{
```

```
  "category": "Build",
  "version": "1",
  "provider": "MyJenkinsProviderName"
}
```

Salida:

```
None.
```

- Para obtener detalles sobre la API, consulte DeleteCustomActionType en la Referencia de comandos de la AWS CLI.

`delete-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-pipeline`.

AWS CLI

Para eliminar una canalización

En este ejemplo, se elimina una canalización llamada MySecondPipeline de AWS CodePipeline. Use el comando list-pipelines para ver una lista de todas las canalizaciones asociadas con su cuenta de AWS.

Comando:

```
aws codepipeline delete-pipeline --name MySecondPipeline
```

Salida:

```
None.
```

- Para obtener detalles sobre la API, consulte DeletePipeline en la Referencia de comandos de la AWS CLI.

`delete-webhook`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-webhook`.

AWS CLI

Eliminación de un webhook

En el siguiente ejemplo de `delete-webhook`, se elimina un webhook de una acción de origen de la versión 1 de GitHub. Debe usar el comando `deregister-webhook-with-third-party` para anular el registro del webhook antes de eliminarlo.

```
aws codepipeline delete-webhook \
    --name my-webhook
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Delete the webhook for your GitHub source en la Guía del usuario de AWS CodePipeline.

- Para obtener detalles sobre la API, consulte DeleteWebhook en la Referencia de comandos de AWS CLI.

`deregister-webhook-with-third-party`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-webhook-with-third-party`.

AWS CLI

Anulación del registro de un webhook

En el siguiente ejemplo de `deregister-webhook-with-third-party`, se elimina un webhook de una acción de origen de la versión 1 de GitHub. Debe anular el registro del webhook antes de eliminarlo.

```
aws codepipeline deregister-webhook-with-third-party \
    --webhook-name my-webhook
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Delete the webhook for your GitHub source en la Guía del usuario de AWS CodePipeline.

- Para obtener detalles sobre la API, consulte DeregisterWebhookWithThirdParty en la Referencia de comandos de la AWS CLI.

`disable-stage-transition`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-stage-transition`.

AWS CLI

Deshabilitación de la transición a una etapa de una canalización

En este ejemplo, se deshabilitan las transiciones a la fase beta de la canalización MyFirstPipeline en AWS CodePipeline.

Comando:

```
aws codepipeline disable-stage-transition --pipeline-name MyFirstPipeline --stage-name Beta  --transition-type Inbound
```

Salida:

```
None.
```

- Para obtener detalles sobre la API, consulte DisableStageTransition en la Referencia de comandos de la AWS CLI.

`enable-stage-transition`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-stage-transition`.

AWS CLI

Habilitación de una transición a una etapa de una canalización

En este ejemplo, se habilitan las transiciones a la fase beta de la canalización MyFirstPipeline en AWS CodePipeline.

Comando:

```
aws codepipeline enable-stage-transition --pipeline-name MyFirstPipeline --stage-name Beta  --transition-type Inbound
```

Salida:

```
None.
```

- Para obtener detalles sobre la API, consulte EnableStageTransition en la Referencia de comandos de la AWS CLI.

`get-job-details`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-job-details`.

AWS CLI

Obtención de detalles de un trabajo

En este ejemplo, se devuelve información sobre un trabajo cuyo identificador está representado por f4f4ff82-2d11-EXAMPLE. Este comando solo se usa para las acciones personalizadas. Cuando se llama a este comando, AWS CodePipeline devuelve las credenciales temporales del bucket de Amazon S3 que se usó para almacenar los artefactos de la canalización, si es necesario para la acción de personalización. Este comando también devolverá cualquier valor secreto definido para la acción en caso de haber definido alguno.

Comando:

```
aws codepipeline get-job-details --job-id f4f4ff82-2d11-EXAMPLE
```

Salida:

```
{
 "jobDetails": {
  "accountId": "111111111111",
  "data": {
    "actionConfiguration": {
      "__type": "ActionConfiguration",
      "configuration": {
        "ProjectName": "MyJenkinsExampleTestProject"
      }
    },
    "actionTypeId": {
      "__type": "ActionTypeId",
      "category": "Test",
      "owner": "Custom",
      "provider": "MyJenkinsProviderName",
      "version": "1"
    },
```

```
    "artifactCredentials": {
      "__type": "AWSSessionCredentials",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "secretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
      "sessionToken":
 "fICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwd
+a4GmWIWJ21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/
f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/
MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpEIbb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQ
+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs
    },
    "inputArtifacts": [
      {
        "__type": "Artifact",
        "location": {
          "s3Location": {
            "bucketName": "codepipeline-us-east-1-11EXAMPLE11",
            "objectKey": "MySecondPipeline/MyAppBuild/EXAMPLE"
          },
          "type": "S3"
        },
        "name": "MyAppBuild"
      }
    ],
    "outputArtifacts": [],
    "pipelineContext": {
      "__type": "PipelineContext",
      "action": {
        "name": "MyJenkinsTest-Action"
      },
      "pipelineName": "MySecondPipeline",
      "stage": {
        "name": "Testing"
      }
    }
  },
  "id": "f4f4ff82-2d11-EXAMPLE"
 }
}
```


- Para obtener detalles sobre la API, consulte GetJobDetails en la Referencia de comandos de la AWS CLI.

`get-pipeline-state`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-pipeline-state`.

AWS CLI

Obtención de información sobre el estado de una canalización

Este ejemplo devuelve el estado más reciente de una canalización denominada MyFirstPipeline.

Comando:

```
aws codepipeline get-pipeline-state --name MyFirstPipeline
```

Salida:

```
{
 "created": 1446137312.204,
 "pipelineName": "MyFirstPipeline",
 "pipelineVersion": 1,
 "stageStates": [
  {
    "actionStates": [
      {
        "actionName": "Source",
        "entityUrl": "https://console.aws.amazon.com/s3/home?#",
        "latestExecution": {
          "lastStatusChange": 1446137358.328,
          "status": "Succeeded"
        }
      }
    ],
    "stageName": "Source"
  },
  {
    "actionStates": [
      {
        "actionName": "CodePipelineDemoFleet",
        "entityUrl": "https://console.aws.amazon.com/codedeploy/home?#/applications/
CodePipelineDemoApplication/deployment-groups/CodePipelineDemoFleet",
        "latestExecution": {
          "externalExecutionId": "d-EXAMPLE",
          "externalExecutionUrl": "https://console.aws.amazon.com/codedeploy/home?#/
deployments/d-EXAMPLE",
```

```
            "lastStatusChange": 1446137493.131,
            "status": "Succeeded",
            "summary": "Deployment Succeeded"
          }
        }
      ],
      "inboundTransitionState": {
        "enabled": true
      },
      "stageName": "Beta"
    }
  ],
  "updated": 1446137312.204
}
```

- Para obtener detalles sobre la API, consulte GetPipelineState en la Referencia de comandos de la AWS CLI.

`get-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-pipeline`.

AWS CLI

Visualización de la estructura de una canalización

Este ejemplo devuelve la estructura más reciente de una canalización denominada MyFirstPipeline.

Comando:

```
aws codepipeline get-pipeline --name MyFirstPipeline
```

Salida:

```
{
  "pipeline": {
      "roleArn": "arn:aws:iam::111111111111:role/AWS-CodePipeline-Service",
      "stages": [
          {
              "name": "Source",
              "actions": [
```

```
                {
                    "inputArtifacts": [],
                    "name": "Source",
                    "actionTypeId": {
                        "category": "Source",
                        "owner": "AWS",
                        "version": "1",
                        "provider": "S3"
                    },
                    "outputArtifacts": [
                        {
                            "name": "MyApp"
                        }
                    ],
                    "configuration": {
                        "S3Bucket": "awscodepipeline-demo-bucket",
                        "S3ObjectKey": "aws-codepipeline-s3-aws-
codedeploy_linux.zip"
                    },
                    "runOrder": 1
                }
            ]
        },
        {
            "name": "Beta",
            "actions": [
                {
                    "inputArtifacts": [
                        {
                            "name": "MyApp"
                        }
                    ],
                    "name": "CodePipelineDemoFleet",
                    "actionTypeId": {
                        "category": "Deploy",
                        "owner": "AWS",
                        "version": "1",
                        "provider": "CodeDeploy"
                    },
                    "outputArtifacts": [],
                    "configuration": {
                        "ApplicationName": "CodePipelineDemoApplication",
                        "DeploymentGroupName": "CodePipelineDemoFleet"
                    },
```

```
                    "runOrder": 1
                }
            ]
        }
    ],
    "artifactStore": {
        "type": "S3",
        "location": "codepipeline-us-east-1-11EXAMPLE11"
    },
    "name": "MyFirstPipeline",
    "version": 1
  }
}
```

- Para obtener detalles sobre la API, consulte GetPipeline en la Referencia de comandos de la AWS CLI.

`list-action-executions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-action-executions`.

AWS CLI

Para enumerar las ejecuciones de acciones

En el siguiente ejemplo de `list-action-executions`, se ven los detalles de ejecución de las acciones de una canalización, como, por ejemplo, el ID de ejecución de la acción, los artefactos de entrada, los artefactos de salida, el resultado de la ejecución y el estado.

```
aws codepipeline list-action-executions \
    --pipeline-name myPipeline
```

Salida:

```
{
    "actionExecutionDetails": [
        {
            "pipelineExecutionId": "EXAMPLE0-adfc-488e-bf4c-1111111720d3",
            "actionExecutionId": "EXAMPLE4-2ee8-4853-bd6a-111111158148",
            "pipelineVersion": 12,
            "stageName": "Deploy",
            "actionName": "Deploy",
```

```
            "startTime": 1598572628.6,
            "lastUpdateTime": 1598572661.255,
            "status": "Succeeded",
            "input": {
                "actionTypeId": {
                    "category": "Deploy",
                    "owner": "AWS",
                    "provider": "CodeDeploy",
                    "version": "1"
                },
                "configuration": {
                    "ApplicationName": "my-application",
                    "DeploymentGroupName": "my-deployment-group"
                },
                "resolvedConfiguration": {
                    "ApplicationName": "my-application",
                    "DeploymentGroupName": "my-deployment-group"
                },
                "region": "us-east-1",
                "inputArtifacts": [
                    {
                        "name": "SourceArtifact",
                        "s3location": {
                            "bucket": "artifact-bucket",
                            "key": "myPipeline/SourceArti/key"
                        }
                    }
                ],
                "namespace": "DeployVariables"
            },
            "output": {
                "outputArtifacts": [],
                "executionResult": {
                    "externalExecutionId": "d-EXAMPLEE5",
                    "externalExecutionSummary": "Deployment Succeeded",
                    "externalExecutionUrl": "https://myaddress.com"
                },
                "outputVariables": {}
            }
        },
        {
            "pipelineExecutionId": "EXAMPLE0-adfc-488e-bf4c-1111111720d3",
            "actionExecutionId": "EXAMPLE5-abb4-4192-9031-11111113a7b0",
            "pipelineVersion": 12,
```

```
            "stageName": "Source",
            "actionName": "Source",
            "startTime": 1598572624.387,
            "lastUpdateTime": 1598572628.16,
            "status": "Succeeded",
            "input": {
                "actionTypeId": {
                    "category": "Source",
                    "owner": "AWS",
                    "provider": "CodeCommit",
                    "version": "1"
                },
                "configuration": {
                    "BranchName": "production",
                    "PollForSourceChanges": "false",
                    "RepositoryName": "my-repo"
                },
                "resolvedConfiguration": {
                    "BranchName": "production",
                    "PollForSourceChanges": "false",
                    "RepositoryName": "my-repo"
                },
                "region": "us-east-1",
                "inputArtifacts": [],
                "namespace": "SourceVariables"
            },
            "output": {
                "outputArtifacts": [
                    {
                        "name": "SourceArtifact",
                        "s3location": {
                            "bucket": "amzn-s3-demo-bucket",
                            "key": "myPipeline/SourceArti/key"
                        }
                    }
                ],
                "executionResult": {
                    "externalExecutionId":
"1111111ad99dcd35914c00b7fbea13995EXAMPLE",
                    "externalExecutionSummary": "Edited template.yml",
                    "externalExecutionUrl": "https://myaddress.com"
                },
                "outputVariables": {
                    "AuthorDate": "2020-05-08T17:45:43Z",
```

```
                    "BranchName": "production",
                    "CommitId": "EXAMPLEad99dcd35914c00b7fbea139951111111",
                    "CommitMessage": "Edited template.yml",
                    "CommitterDate": "2020-05-08T17:45:43Z",
                    "RepositoryName": "my-repo"
                }
            }
        },
. . . .
```

Para obtener más información, consulte View action executions (CLI) en la Guía del usuario de AWS CodePipeline.

- Para obtener detalles sobre la API, consulte ListActionExecutions en la Referencia de comandos de la AWS CLI.

`list-action-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-action-types`.

AWS CLI

Visualización de los tipos de acciones disponibles

Si se utiliza solo, el comando list-action-types devuelve la estructura de todas las acciones disponibles en la cuenta de AWS. En este ejemplo, se usa la opción --action-owner-filter para devolver solo las acciones personalizadas.

Comando:

```
aws codepipeline list-action-types --action-owner-filter Custom
```

Salida:

```
{
  "actionTypes": [
      {
          "inputArtifactDetails": {
              "maximumCount": 5,
              "minimumCount": 0
          },
          "actionConfigurationProperties": [
```

```
            {
                "secret": false,
                "required": true,
                "name": "MyJenkinsExampleBuildProject",
                "key": true,
                "queryable": true
            }
        ],
        "outputArtifactDetails": {
            "maximumCount": 5,
            "minimumCount": 0
        },
        "id": {
            "category": "Build",
            "owner": "Custom",
            "version": "1",
            "provider": "MyJenkinsProviderName"
        },
        "settings": {
            "entityUrlTemplate": "http://192.0.2.4/job/{Config:ProjectName}",
            "executionUrlTemplate": "http://192.0.2.4/job/{Config:ProjectName}/
{ExternalExecutionId}"
        }
    },
    {
        "inputArtifactDetails": {
            "maximumCount": 5,
            "minimumCount": 0
        },
        "actionConfigurationProperties": [
            {
                "secret": false,
                "required": true,
                "name": "MyJenkinsExampleTestProject",
                "key": true,
                "queryable": true
            }
        ],
        "outputArtifactDetails": {
            "maximumCount": 5,
            "minimumCount": 0
        },
        "id": {
            "category": "Test",
```

```
                "owner": "Custom",
                "version": "1",
                "provider": "MyJenkinsProviderName"
            },
            "settings": {
                "entityUrlTemplate": "http://192.0.2.4/job/{Config:ProjectName}",
                "executionUrlTemplate": "http://192.0.2.4/job/{Config:ProjectName}/
{ExternalExecutionId}"
            }
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte ListActionTypes en la Referencia de comandos de la AWS CLI.

`list-pipeline-executions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-pipeline-executions`.

AWS CLI

Visualización del historial de ejecución de una canalización

En el siguiente ejemplo de `list-pipeline-executions`, se muestra el historial de ejecución de una canalización de su cuenta de AWS.

```
aws codepipeline list-pipeline-executions \
    --pipeline-name MyPipeline
```

Salida:

```
{
    "pipelineExecutionSummaries": [
        {
            "lastUpdateTime": 1496380678.648,
            "pipelineExecutionId": "7cf7f7cb-3137-539g-j458-d7eu3EXAMPLE",
            "startTime": 1496380258.243,
            "status": "Succeeded"
        },
        {
```

```
            "lastUpdateTime": 1496591045.634,
            "pipelineExecutionId": "3137f7cb-8d494hj4-039j-d84l-d7eu3EXAMPLE",
            "startTime": 1496590401.222,
            "status": "Succeeded"
        },
        {
            "lastUpdateTime": 1496946071.6456,
            "pipelineExecutionId": "4992f7jf-7cf7-913k-k334-d7eu3EXAMPLE",
            "startTime": 1496945471.5645,
            "status": "Succeeded"
        }
    ]
}
```

Para obtener más información, consulte View execution history en la Guía del usuario de AWS CodePipeline.

- Para obtener detalles sobre la API, consulte ListPipelineExecutions en la Referencia de comandos de la AWS CLI.

`list-pipelines`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-pipelines`.

AWS CLI

Visualización de una lista de canalizaciones

En este ejemplo, se enumeran todas las canalizaciones de AWS CodePipeline asociadas a la cuenta del usuario de AWS.

Comando:

```
aws codepipeline list-pipelines
```

Salida:

```
{
  "pipelines": [
      {
          "updated": 1439504274.641,
```

```
            "version": 1,
            "name": "MyFirstPipeline",
            "created": 1439504274.641
        },
        {
            "updated": 1436461837.992,
            "version": 2,
            "name": "MySecondPipeline",
            "created": 1436460801.381
        }
        ]
}
```

- Para obtener detalles sobre la API, consulte ListPipelines en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar etiquetas

En el siguiente ejemplo de `list-tags-for-resource`, se recupera una lista de todas las etiquetas asociadas al recurso de canalización especificado.

```
aws codepipeline list-tags-for-resource \
    --resource-arn arn:aws:codepipeline:us-east-1:123456789012:MyPipeline
```

Salida:

```
{
    "tags": {
        "Project": "ProjectA",
        "IscontainerBased": "true"
    }
}
```

Para obtener más información, consulte View tags for a pipeline (CLI) en la Guía del usuario de AWS CodePipeline.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-webhooks`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-webhooks`.

AWS CLI

Para enumerar los webhooks

En el siguiente ejemplo de `list-webhooks`, se recupera una lista de todas las etiquetas asociadas al recurso de canalización especificado.

```
aws codepipeline list-webhooks \
    --endpoint-url "https://codepipeline.eu-central-1.amazonaws.com" \
    --region "eu-central-1"
```

Salida:

```
{
    "webhooks": [
        {
            "url": "https://webhooks.domain.com/
trigger111111111EXAMPLE1111111111111111": {
                "authenticationConfiguration": {
                    "SecretToken": "Secret"
                },
                "name": "my-webhook",
                "authentication": "GITHUB_HMAC",
                "targetPipeline": "my-Pipeline",
                "targetAction": "Source",
                "filters": [
                    {
                        "jsonPath": "$.ref",
                        "matchEquals": "refs/heads/{Branch}"
                    }
                ]
            },
            "arn": "arn:aws:codepipeline:eu-central-1:123456789012:webhook:my-
webhook"
        }
```

```
    ]
}
```

Para obtener más información, consulte List webhooks in your account en la Guía del usuario de AWS CodePipeline.

- Para obtener detalles sobre la API, consulte ListWebhooks en la Referencia de comandos de la AWS CLI.

`poll-for-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `poll-for-jobs`.

AWS CLI

Visualización de trabajos disponibles

En este ejemplo, se devuelve información sobre cualquier trabajo en el que pueda actuar un proceso de trabajo. En este ejemplo, se utiliza un archivo JSON predefinido (myActionTypeInfo.json) para proporcionar información sobre el tipo de acción para el cual el proceso de trabajo procesa los trabajos. Este comando solo se usa para las acciones personalizadas. Cuando se llama a este comando, AWS CodePipeline devuelve las credenciales temporales del bucket de Amazon S3 usado para almacenar los artefactos de la canalización. Este comando también devolverá cualquier valor secreto definido para la acción en caso de haber definido alguno.

Comando:

```
aws codepipeline poll-for-jobs --cli-input-json file://MyActionTypeInfo.json
```

Contenidos de muestra del archivo JSON:

```
{
  "actionTypeId": {
    "category": "Test",
    "owner": "Custom",
    "provider": "MyJenkinsProviderName",
    "version": "1"
  },
  "maxBatchSize": 5,
  "queryParam": {
```

```
      "ProjectName": "MyJenkinsTestProject"
  }
}
```

Salida:

```
{
 "jobs": [
  {
    "accountId": "111111111111",
    "data": {
      "actionConfiguration": {
        "__type": "ActionConfiguration",
        "configuration": {
          "ProjectName": "MyJenkinsExampleTestProject"
        }
      },
      "actionTypeId": {
        "__type": "ActionTypeId",
        "category": "Test",
        "owner": "Custom",
        "provider": "MyJenkinsProviderName",
        "version": "1"
      },
      "artifactCredentials": {
        "__type": "AWSSessionCredentials",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "secretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
        "sessionToken":
 "fICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwd
+a4GmWIWJ21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/
f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/
MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpEIbb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQ
+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs
      },
      "inputArtifacts": [
        {
          "__type": "Artifact",
          "location": {
            "s3Location": {
              "bucketName": "codepipeline-us-east-1-11EXAMPLE11",
              "objectKey": "MySecondPipeline/MyAppBuild/EXAMPLE"
            },
```

```
            "type": "S3"
          },
          "name": "MyAppBuild"
        }
      ],
      "outputArtifacts": [],
      "pipelineContext": {
        "__type": "PipelineContext",
        "action": {
          "name": "MyJenkinsTest-Action"
        },
        "pipelineName": "MySecondPipeline",
        "stage": {
          "name": "Testing"
        }
      }
    },
    "id": "ef66c259-64f9-EXAMPLE",
    "nonce": "3"
  }
 ]
}
```

- Para obtener detalles sobre la API, consulte PollForJobs en la Referencia de comandos de la AWS CLI.

`put-webhook`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-webhook`.

AWS CLI

Creación de un webhook

En el siguiente ejemplo de `put-webhook`, se crea un webhook de una acción de origen de la versión 1 de GitHub. Después de crear el webhook, debe usar el comando register-webhook-with-third-party para registrarlo.

```
aws codepipeline put-webhook \
    --cli-input-json file://webhook_json.json \
    --region "eu-central-1"
```

Contenido de `webhook_json.json`:

```
{
    "webhook": {
        "name": "my-webhook",
        "targetPipeline": "pipeline_name",
        "targetAction": "source_action_name",
        "filters": [
            {
                "jsonPath": "$.ref",
                "matchEquals": "refs/heads/{Branch}"
            }
        ],
        "authentication": "GITHUB_HMAC",
        "authenticationConfiguration": {
            "SecretToken": "secret"
        }
    }
}
```

Salida:

```
{
    "webhook": {
        "url": "https://webhooks.domain.com/
trigger111111111EXAMPLE11111111111111111",
        "definition": {
            "authenticationConfiguration": {
                "SecretToken": "secret"
            },
            "name": "my-webhook",
            "authentication": "GITHUB_HMAC",
            "targetPipeline": "pipeline_name",
            "targetAction": "Source",
            "filters": [
                {
                    "jsonPath": "$.ref",
                    "matchEquals": "refs/heads/{Branch}"
                }
            ]
        },
        "arn": "arn:aws:codepipeline:eu-central-1:123456789012:webhook:my-webhook"
    },
```

```
    "tags": [
        {
            "key": "Project",
            "value": "ProjectA"
        }
    ]
}
```

Para obtener más información, consulte Create a webhook for a GitHub source en la Guía del usuario de AWS CodePipeline.

- Para obtener detalles sobre la API, consulte PutWebhook en la Referencia de comandos de la AWS CLI.

`retry-stage-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `retry-stage-execution`.

AWS CLI

Reintento de acciones con errores

En el siguiente ejemplo de `retry-stage-execution`, se vuelve a intentar una etapa en la que se produjo un error en la acción.

```
aws codepipeline retry-stage-execution \
    --pipeline-name MyPipeline \
    --stage-name Deploy \
    --pipeline-execution-id b59babff-5f34-EXAMPLE \
    --retry-mode FAILED_ACTIONS
```

Salida:

```
{
    "pipelineExecutionId": "b59babff-5f34-EXAMPLE"
}
```

Para obtener más información, consulte Retry failed actions (CLI) en la Guía del usuario de AWS CodePipeline.

- Para obtener detalles sobre la API, consulte RetryStageExecution en la Referencia de comandos de la AWS CLI.

`start-pipeline-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-pipeline-execution`.

AWS CLI

Ejecución de la última revisión a través de una canalización

En este ejemplo, se ejecuta la última revisión presente en la fase de origen de una canalización a través de la canalización denominada MyFirstPipeline.

Comando:

```
aws codepipeline start-pipeline-execution --name MyFirstPipeline
```

Salida:

```
{
  "pipelineExecutionId": "3137f7cb-7cf7-EXAMPLE"
}
```

- Para obtener detalles sobre la API, consulte StartPipelineExecution en la Referencia de comandos de la AWS CLI.

`stop-pipeline-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-pipeline-execution`.

AWS CLI

Detención de la ejecución de una canalización

En el siguiente ejemplo de `stop-pipeline-execution`, se establece de forma predeterminada esperar hasta que finalicen las acciones en curso y, a continuación, se detiene la canalización. No puede elegir detener y esperar si la ejecución ya se encuentra en un estado Stopping (Deteniéndose). Puede optar por detener y abandonar una ejecución que ya se encuentra en un estado Stopping (Deteniéndose).

```
aws codepipeline stop-pipeline-execution \
    --pipeline-name MyFirstPipeline \
```

```
    --pipeline-execution-id d-EXAMPLE \
    --reason "Stopping pipeline after the build action is done"
```

Este comando no devuelve ningún resultado.

Para obtener más información, consulte Stop a pipeline execution (CLI) en la Guía del usuario de AWS CodePipeline.

- Para obtener detalles sobre la API, consulte StopPipelineExecution en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para etiquetar un recurso

En el siguiente ejemplo de `tag-resource`, se asocia un conjunto de etiquetas proporcionadas a una canalización. Use este comando para añadir o editar etiquetas.

```
aws codepipeline tag-resource \
    --resource-arn arn:aws:codepipeline:us-east-1:123456789012:MyPipeline \
    --tags key=Project,value=ProjectA key=IscontainerBased,value=true
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Add tags to a pipeline (CLI) en la Guía del usuario de AWS CodePipeline.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de etiquetas de AWS de un recurso de conexiones

En el siguiente ejemplo de `untag-resource`, se elimina una etiqueta de un recurso especificado.

```
aws codepipeline untag-resource \
    --resource-arn arn:aws:codepipeline:us-east-1:123456789012:MyPipeline \
    --tag-keys Project IscontainerBased
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Remove tags from a pipeline (CLI) en la Guía del usuario de AWS CodePipeline.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-pipeline`.

AWS CLI

Actualización de la estructura de una canalización

En este ejemplo, se usa el comando update-pipeline con el argumento --cli-input-json. En este ejemplo, se usa un archivo JSON predefinido (MyFirstPipeline.json) para actualizar la estructura de una canalización. AWS CodePipeline reconoce el nombre de la canalización contenido en el archivo JSON y, a continuación, aplica cualquier cambio en los campos modificados de la estructura de la canalización para actualizar esta última.

Utilice las siguientes pautas al crear el archivo JSON predefinido:

Si trabaja con una estructura de canalización recuperada mediante el comando get-pipeline, debe eliminar la sección de metadatos de la estructura de canalización del archivo JSON (las líneas metadata: { } y los campos created, pipelineARN y updated que contiene). El nombre de la canalización no se puede cambiar.

Comando:

```
aws codepipeline update-pipeline --cli-input-json file://MyFirstPipeline.json
```

Contenido del archivo JSON de muestra:

```
{
 "pipeline": {
  "roleArn": "arn:aws:iam::111111111111:role/AWS-CodePipeline-Service",
  "stages": [
    {
      "name": "Source",
      "actions": [
        {
          "inputArtifacts": [],
          "name": "Source",
          "actionTypeId": {
            "category": "Source",
            "owner": "AWS",
            "version": "1",
            "provider": "S3"
          },
          "outputArtifacts": [
            {
              "name": "MyApp"
            }
          ],
          "configuration": {
            "S3Bucket": "awscodepipeline-demo-bucket2",
            "S3ObjectKey": "aws-codepipeline-s3-aws-codedeploy_linux.zip"
          },
          "runOrder": 1
        }
      ]
    },
    {
      "name": "Beta",
      "actions": [
        {
          "inputArtifacts": [
            {
              "name": "MyApp"
            }
          ],
          "name": "CodePipelineDemoFleet",
          "actionTypeId": {
            "category": "Deploy",
            "owner": "AWS",
```

```
            "version": "1",
            "provider": "CodeDeploy"
          },
          "outputArtifacts": [],
          "configuration": {
            "ApplicationName": "CodePipelineDemoApplication",
            "DeploymentGroupName": "CodePipelineDemoFleet"
          },
          "runOrder": 1
        }
      ]
    }
  ],
  "artifactStore": {
    "type": "S3",
    "location": "codepipeline-us-east-1-11EXAMPLE11"
  },
  "name": "MyFirstPipeline",
  "version": 1
 }
}
```

Salida:

```
{
 "pipeline": {
  "artifactStore": {
    "location": "codepipeline-us-east-1-11EXAMPLE11",
    "type": "S3"
  },
  "name": "MyFirstPipeline",
  "roleArn": "arn:aws:iam::111111111111:role/AWS-CodePipeline-Service",
  "stages": [
    {
      "actions": [
        {
          "actionTypeId": {
            "__type": "ActionTypeId",
            "category": "Source",
            "owner": "AWS",
            "provider": "S3",
            "version": "1"
          },
```

```
          "configuration": {
            "S3Bucket": "awscodepipeline-demo-bucket2",
            "S3ObjectKey": "aws-codepipeline-s3-aws-codedeploy_linux.zip"
          },
          "inputArtifacts": [],
          "name": "Source",
          "outputArtifacts": [
            {
              "name": "MyApp"
            }
          ],
          "runOrder": 1
        }
      ],
      "name": "Source"
    },
    {
      "actions": [
        {
          "actionTypeId": {
            "__type": "ActionTypeId",
            "category": "Deploy",
            "owner": "AWS",
            "provider": "CodeDeploy",
            "version": "1"
          },
          "configuration": {
            "ApplicationName": "CodePipelineDemoApplication",
            "DeploymentGroupName": "CodePipelineDemoFleet"
          },
          "inputArtifacts": [
            {
              "name": "MyApp"
            }
          ],
          "name": "CodePipelineDemoFleet",
          "outputArtifacts": [],
          "runOrder": 1
        }
      ],
      "name": "Beta"
    }
  ],
  "version": 3
```

```
 }
}
```

- Para obtener detalles sobre la API, consulte UpdatePipeline en la Referencia de comandos de la AWS CLI.

Ejemplos de notificaciones de AWS CodeStar que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios comunes usando la AWS Command Line Interface para las notificaciones de AWS CodeStar.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-notification-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-notification-rule`.

AWS CLI

Creación de una regla de notificación

En el siguiente ejemplo de `create-notification-rule`, se usa un archivo JSON denominado `rule.json` para crear una regla de notificación con el nombre `MyNotificationRule` para un repositorio con el nombre `MyDemoRepo` en la cuenta de AWS especificada. Las notificaciones con el tipo de detalle `FULL` se envían al tema de Amazon SNS de destino especificado cuando se crean las ramificaciones y las etiquetas.

```
aws codestar-notifications create-notification-rule \
    --cli-input-json file://rule.json
```

Contenido de `rule.json`:

```
{
    "Name": "MyNotificationRule",
    "EventTypeIds": [
        "codecommit-repository-branches-and-tags-created"
    ],
    "Resource": "arn:aws:codecommit:us-east-1:123456789012:MyDemoRepo",
    "Targets": [
        {
            "TargetType": "SNS",
            "TargetAddress": "arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic"
        }
    ],
    "Status": "ENABLED",
    "DetailType": "FULL"
}
```

Salida:

```
{
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
}
```

Para obtener más información, consulte Create a Notification rule en la Guía del usuario de la Consola de herramientas para desarrolladores de AWS.

- Para obtener detalles sobre la API, consulte CreateNotificationRule en la Referencia de comandos de la AWS CLI.

`delete-notification-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-notification-rule`.

AWS CLI

Eliminación de una regla de notificación

En el siguiente ejemplo de `delete-notification-rule`, se elimina la regla de notificación especificada.

```
aws codestar-notifications delete-notification-rule \
    --arn arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE
```

Salida:

```
{
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
}
```

Para obtener más información, consulte Delete a Notification rule en la Guía del usuario de la Consola de herramientas para desarrolladores de AWS.

- Para obtener detalles sobre la API, consulte DeleteNotificationRule en la Referencia de comandos de la AWS CLI.

`delete-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-target`.

AWS CLI

Eliminación de un destino de regla de notificación

En el siguiente ejemplo de `delete-target`, se elimina el destino especificado de todas las reglas de notificación configuradas para utilizarlo como destino y, a continuación, eliminar el destino.

```
aws codestar-notifications  delete-target \
    --target-address arn:aws:sns:us-east-1:123456789012:MyNotificationTopic \
    --force-unsubscribe-all
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Delete a Notification Rule Target en la Guía del usuario de la Consola de herramientas para desarrolladores de AWS.

- Para obtener detalles sobre la API, consulte DeleteTarget en la Referencia de comandos de la AWS CLI.

`describe-notification-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-notification-rule`.

AWS CLI

Visualización de la información de una regla de notificación

En el siguiente ejemplo de `describe-notification-rule`, se recupera la información de la regla de notificación especificada.

```
aws codestar-notifications describe-notification-rule \
    --arn arn:aws:codestar-notifications:us-west-2:123456789012:notificationrule/
dc82df7a-EXAMPLE
```

Salida:

```
{
    "LastModifiedTimestamp": 1569199844.857,
    "EventTypes": [
        {
            "ServiceName": "CodeCommit",
            "EventTypeName": "Branches and tags: Created",
            "ResourceType": "Repository",
            "EventTypeId": "codecommit-repository-branches-and-tags-created"
        }
    ],
    "Status": "ENABLED",
    "DetailType": "FULL",
    "Resource": "arn:aws:codecommit:us-west-2:123456789012:MyDemoRepo",
    "Arn": "arn:aws:codestar-notifications:us-west-w:123456789012:notificationrule/
dc82df7a-EXAMPLE",
    "Targets": [
        {
            "TargetStatus": "ACTIVE",
            "TargetAddress": "arn:aws:sns:us-
west-2:123456789012:MyNotificationTopic",
            "TargetType": "SNS"
        }
    ],
    "Name": "MyNotificationRule",
    "CreatedTimestamp": 1569199844.857,
    "CreatedBy": "arn:aws:iam::123456789012:user/Mary_Major"
```

```
}
```

Para obtener más información, consulte View Notification Rules en la Guía del usuario de la Consola de herramientas para desarrolladores de AWS.

- Para obtener detalles sobre la API, consulte DescribeNotificationRule en la Referencia de comandos de la AWS CLI.

`list-event-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-event-types`.

AWS CLI

Obtención de una lista de tipos de eventos de una regla de notificación

En el siguiente ejemplo de `list-event-types`, se recupera una lista filtrada de todos los tipos de eventos de notificación disponibles para las aplicaciones de CodeDeploy. Si, por el contrario, no utiliza ningún filtro, el comando devuelve todos los tipos de eventos de notificación para todos los tipos de recursos.

```
aws codestar-notifications list-event-types \
    --filters Name=SERVICE_NAME,Value=CodeDeploy
```

Salida:

```
{
    "EventTypes": [
        {
            "EventTypeId": "codedeploy-application-deployment-succeeded",
            "ServiceName": "CodeDeploy",
            "EventTypeName": "Deployment: Succeeded",
            "ResourceType": "Application"
        },
        {
            "EventTypeId": "codedeploy-application-deployment-failed",
            "ServiceName": "CodeDeploy",
            "EventTypeName": "Deployment: Failed",
            "ResourceType": "Application"
        },
        {
            "EventTypeId": "codedeploy-application-deployment-started",
```

```
            "ServiceName": "CodeDeploy",
            "EventTypeName": "Deployment: Started",
            "ResourceType": "Application"
        }
    ]
}
```

Para obtener más información, consulte Create a Notification Rule en la Guía del usuario de la Consola de herramientas para desarrolladores de AWS.

- Para obtener detalles sobre la API, consulte ListEventTypes en la Referencia de comandos de la AWS CLI.

`list-notification-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-notification-rules`.

AWS CLI

Visualización de una lista de reglas de notificación

En el siguiente ejemplo de `list-notification-rules`, se recupera una lista de todas las reglas de notificación de la región de AWS especificada.

```
aws codestar-notifications list-notification-rules --region us-east-1
```

Salida:

```
{
    "NotificationRules": [
        {
            "Id": "dc82df7a-EXAMPLE",
            "Arn": "arn:aws:codestar-notifications:us-
east-1:123456789012:notificationrule/dc82df7a-EXAMPLE"
        },
        {
            "Id": "8d1f0983-EXAMPLE",
            "Arn": "arn:aws:codestar-notifications:us-
east-1:123456789012:notificationrule/8d1f0983-EXAMPLE"
        }
    ]
}
```

Para obtener más información, consulte View Notification Rules en la Guía del usuario de la Consola de herramientas para desarrolladores de AWS.

- Para obtener detalles sobre la API, consulte ListNotificationRules en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Obtención de una lista de etiquetas asociadas a una regla de notificación

El siguiente ejemplo de `list-tags-for-resource` recupera una lista de todas las etiquetas asociadas a la regla de notificación especificada. En este ejemplo, la regla de notificación actualmente no tiene ninguna etiqueta asociada.

```
aws codestar-notifications list-tags-for-resource \
    --arn arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
fe1efd35-EXAMPLE
```

Salida:

```
{
    "Tags": {}
}
```

Para obtener más información, consulte Create a Notification Rule en la Guía del usuario de la Consola de herramientas para desarrolladores de AWS.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-targets`.

AWS CLI

Visualización de una lista de destinos de reglas de notificación

En el siguiente ejemplo de `list-targets`, se recupera una lista de todos los destinos de las reglas de notificación de la región AWS especificada.

```
aws codestar-notifications list-targets \
    --region us-east-1
```

Salida:

```
{
    "Targets": [
        {
            "TargetAddress": "arn:aws:sns:us-
east-1:123456789012:MySNSTopicForNotificationRules",
            "TargetType": "SNS",
            "TargetStatus": "ACTIVE"
        },
        {
            "TargetAddress": "arn:aws:sns:us-
east-1:123456789012:MySNSTopicForNotificationsAboutMyDemoRepo",
            "TargetType": "SNS",
            "TargetStatus": "ACTIVE"
        }
    ]
}
```

Para obtener más información, consulte View Notification Rule Targets en la Guía del usuario de la Consola de herramientas para desarrolladores de AWS.

- Para obtener detalles sobre la API, consulte ListTargets en la Referencia de comandos de la AWS CLI.

`subscribe`

En el siguiente ejemplo de código, se muestra cómo utilizar `subscribe`.

AWS CLI

Adición de un destino a una regla de notificación

En el siguiente ejemplo de `subscribe`, se añade un tema de Amazon SNS como destino para la regla de notificación especificada.

```
aws codestar-notifications subscribe \
    --arn arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE \
    --target TargetType=SNS,TargetAddress=arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic
```

Salida:

```
{
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
}
```

Para obtener más información, consulte Add or Remove an Amazon SNS Topic as a Target for a Notification Rule en la Guía del usuario de la Consola de herramientas para desarrolladores de AWS.

- Para obtener detalles sobre la API, consulte Subscribe en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Adición de una etiqueta a una regla de notificación

En el siguiente ejemplo de `tag-resource`, se añade una etiqueta con el nombre de clave de `Team` y un valor de `Li_Juan` a la regla de notificación especificada.

```
aws codestar-notifications tag-resource \
    --arn arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
fe1efd35-EXAMPLE \
    --tags Team=Li_Juan
```

Salida:

```
{
    "Tags": {
```

```
        "Team": "Li_Juan"
    }
}
```

Para obtener más información, consulte Create a Notification Rule en la Guía del usuario de la Consola de herramientas para desarrolladores de AWS.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`unsubscribe`

En el siguiente ejemplo de código, se muestra cómo utilizar `unsubscribe`.

AWS CLI

Eliminación de un destino de una regla de notificación

En el siguiente ejemplo de `unsubscribe`, se elimina un tema de Amazon SNS como destino para la regla de notificación especificada.

```
aws codestar-notifications unsubscribe \
    --arn arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE \
    --target TargetType=SNS,TargetAddress=arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic
```

Salida:

```
{
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
    "TargetAddress": "arn:aws:sns:us-east-1:123456789012:MyNotificationTopic"
}
```

Para obtener más información, consulte Add or Remove an Amazon SNS Topic as a Target for a Notification Rule en la Guía del usuario de la Consola de herramientas para desarrolladores de AWS.

- Para obtener detalles sobre la API, consulte Unsubscribe en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de una etiqueta de una regla de notificación

En el siguiente ejemplo de `untag-resource`, se elimina la etiqueta con el nombre clave `Team` de la regla de notificación especificada.

```
aws codestar-notifications untag-resource \
    --arn arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
fe1efd35-EXAMPLE \
    --tag-keys Team
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Edit a Notification Rule en la Guía del usuario de la Consola de herramientas para desarrolladores de AWS.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-notification-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-notification-rule`.

AWS CLI

Actualización de una regla de notificación

En el siguiente ejemplo de `update-notification-rule`, se actualiza una regla de notificación denominada `MyNotificationRule` en la cuenta de AWS `123456789012` usando un archivo JSON denominado `update.json`.

```
aws codestar-notifications update-notification-rule \
    --cli-input-json file://update.json
```

Contenido de `update.json`:

```
{
```

```
    "Name": "MyUpdatedNotificationRule",
    "EventTypeIds": [
        "codecommit-repository-branches-and-tags-created"
    ],
    "Resource": "arn:aws:codecommit:us-east-1:123456789012:MyDemoRepo",
    "Targets": [
        {
            "TargetType": "SNS",
            "TargetAddress": "arn:aws:sns:us-
east-1:123456789012:MyNotificationTopic"
        }
    ],
    "Status": "ENABLED",
    "DetailType": "FULL"
}
```

Salida:

```
{
    "Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/
dc82df7a-EXAMPLE"
}
```

Para obtener más información, consulte Edit a notification rule en la Guía del usuario de la Consola de herramientas para desarrolladores de AWS.

- Para obtener detalles sobre la API, consulte UpdateNotificationRule en la Referencia de comandos de la AWS CLI.

Ejemplos de CodeConnections que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante AWS Command Line Interface con CodeConnections.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-connection`.

AWS CLI

Creación de una conexión

El siguiente ejemplo de `create-connection`, se muestra cómo crear una conexión a un repositorio externo. En este ejemplo, se crea una conexión en la que el proveedor externo es Bitbucket.

De forma predeterminada, las conexiones que se crean a través de la AWS CLI o de AWS CloudFormation tienen el estado Pendiente. Después de crear una conexión con la CLI o con AWS CloudFormation, utilice la consola para editar la conexión y cambiar su estado a Disponible.

```
aws codestar-connections create-connection \
    --provider-type Bitbucket \
    --connection-name MyConnection
```

Salida:

```
{
    "ConnectionArn": "arn:aws:codestar-connections:us-
east-1:123456789012:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f"
}
```

Para obtener más información, consulte Create a connection en la Guía del usuario de la consola de herramientas del desarrollador.

- Para obtener más información sobre la API, consulte CreateConnection en la Referencia de comandos de la AWS CLI.

`create-host`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-host`.

AWS CLI

Creación de un host

En el siguiente ejemplo de `create-host`, se muestra cómo crear un host para representar el punto de conexión de la infraestructura donde está instalado el proveedor externo. En este ejemplo, se crea un host en el que el proveedor externo instalado es GitHub Enterprise Server.

Un host creado mediante la AWS CLI está en estado Pendiente de forma predeterminada. Después de crear un host con la CLI, utilice la consola o la CLI para configurar el host de manera que su estado cambie a Disponible.

```
aws codestar-connections create-host \
    --name MyHost \
    --provider-type GitHubEnterpriseServer \
    --provider-endpoint "https://my-instance.dev"
```

Salida:

```
{
    "HostArn": "arn:aws:codestar-connections:us-east-1:123456789012:host/My-
Host-28aef605"
}
```

Para obtener más información, consulte Create a host (CLI) en la Guía del usuario de la consola de herramientas del desarrollador.

- Para obtener detalles sobre la API, consulte CreateHost en la Referencia de comandos de la AWS CLI.

`delete-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-connection`.

AWS CLI

Para eliminar una conexión

En el siguiente ejemplo de `delete-connection`, se muestra cómo eliminar una conexión.

```
aws codestar-connections delete-connection \
```

```
    --connection-arn arn:aws:codestar-connections:us-west-2:123456789012:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Delete a connection (CLI) en la Guía del usuario de la consola de herramientas del desarrollador.

- Para obtener detalles sobre la API, consulte DeleteConnection en la Referencia de comandos de la AWS CLI.

`delete-host`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-host`.

AWS CLI

Eliminación de un host

En el ejemplo siguiente de `delete-host`, se muestra cómo se elimina un host. Para poder eliminar un alojamiento, debe eliminar todas las conexiones asociadas al alojamiento.

```
aws codestar-connections delete-host \
    --host-arn "arn:aws:codestar-connections:us-east-1 :123456789012:host/My-
Host-28aef605"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Delete a host (CLI) en la Guía del usuario de la consola de herramientas del desarrollador.

- Para obtener detalles sobre la API, consulte DeleteHost en la Referencia de comandos de la AWS CLI.

`get-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-connection`.

AWS CLI

Obtención de información sobre una conexión

En el siguiente ejemplo de `get-connection`, se muestra información sobre una conexión.

```
aws codestar-connections get-connection \
    --connection-arn arn:aws:codestar-connections:us-east-1:123456789012:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f
```

Salida:

```
{
    "Connection": {
        "ConnectionName": "MyConnection",
        "ConnectionArn": "arn:aws:codestar-connections:us-east-1:123456789012:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
        "ProviderType": "Bitbucket",
        "OwnerAccountId": "123456789012",
        "ConnectionStatus": "AVAILABLE"
    }
}
```

Para obtener más información, consulte View connection details en la Guía del usuario de la consola de herramientas del desarrollador.

- Para obtener detalles sobre la API, consulte GetConnection en la Referencia de comandos de la AWS CLI.

`get-host`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-host`.

AWS CLI

Obtención de información acerca de un host

En el siguiente ejemplo de `get-host`, se muestra información sobre un host:

```
aws codestar-connections get-host \
    --host-arn arn:aws:codestar-connections:us-east-1:123456789012:host/MyHost-28aef605
```

Salida:

```
{
```

```
    "Name": "MyHost",
    "Status": "AVAILABLE",
    "ProviderType": "GitHubEnterpriseServer",
    "ProviderEndpoint": "https://test-instance-1.dev/"
}
```

Para obtener más información, consulte View host details (CLI) en la Guía del usuario de la consola de herramientas del desarrollador.

- Para obtener detalles sobre la API, consulte GetHost en la Referencia de comandos de la AWS CLI.

`list-connections`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-connections`.

AWS CLI

Para enumerar las conexiones

En el siguiente ejemplo de `list-connections`, se recupera una lista de todas las conexiones de su cuenta para el tipo de proveedor de Bitbucket:

```
aws codestar-connections list-connections \
--provider-type Bitbucket \
--max-results 5 \
--next-token: next-token
```

Salida:

```
{
    "Connections": [
        {
            "ConnectionName": "my-connection",
            "ProviderType": "Bitbucket",
            "Status": "PENDING",
            "ARN": "arn:aws:codestar-connections:us-east-1:123456789012:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
            "OwnerAccountId": "123456789012"
        },
        {
            "ConnectionName": "my-other-connection",
```

```
            "ProviderType": "Bitbucket",
            "Status": "AVAILABLE",
            "ARN": "arn:aws:codestar-connections:us-east-1:123456789012:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f",
            "OwnerAccountId": "123456789012"
        },
    ],
    "NextToken": "next-token"
}
```

Para obtener más información, consulte List connections (CLI) en la Guía del usuario de la consola de herramientas del desarrollador.

- Para obtener detalles sobre la API, consulte ListConnections en la Referencia de comandos de la AWS CLI.

`list-hosts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-hosts`.

AWS CLI

Para enumerar los hosts

En el siguiente ejemplo de `list-hosts`, se obtiene una lista de todos los hosts de su cuenta.

```
aws codestar-connections list-hosts
```

Salida:

```
{
    "Hosts": [
        {
            "Name": "My-Host",
            "HostArn": "arn:aws:codestar-connections:us-east-1:123456789012:host/My-
Host-28aef605",
            "ProviderType": "GitHubEnterpriseServer",
            "ProviderEndpoint": "https://my-instance.test.dev",
            "Status": "AVAILABLE"
        }
    ]
}
```

Para obtener más información, consulte List hosts (CLI) en la Guía del usuario de la consola de herramientas del desarrollador.

- Para obtener detalles sobre la API, consulte ListHosts en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar etiquetas

En el siguiente ejemplo de `list-tags-for-resource`, se recupera una lista de todas las etiquetas adjuntas al recurso de conexiones especificado.

```
aws codestar-connections list-tags-for-resource \
    --resource-arn arn:aws:codestar-connections:us-east-1:123456789012:connection/aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f
```

Salida:

```
{
    "Tags": [
        {
            "Key": "Project",
            "Value": "ProjectA"
        },
        {
            "Key": "ReadOnly",
            "Value": "true"
        }
    ]
}
```

Para obtener más información, consulte View tags for a connections resource en la Guía del usuario de la consola de herramientas del desarrollador.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para etiquetar un recurso

En el siguiente ejemplo de `tag-resource`, se asocia un conjunto de etiquetas proporcionadas a una conexión. Use este comando para añadir o editar etiquetas.

```
aws codestar-connections tag-resource \
    --resource-arn arn:aws:codestar-connections:us-east-1:123456789012:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f \
    --tags Key=Project,Value=ProjectA Key=IscontainerBased,Value=true
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Add tags to a connections resource en la Guía del usuario de la consola de herramientas del desarrollador.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de etiquetas de AWS de un recurso de conexiones

En el siguiente ejemplo de `untag-resource`, se elimina una etiqueta de un recurso especificado.

```
aws codestar-connections untag-resource \
    --resource-arn arn:aws:codestar-connections:us-east-1:123456789012:connection/
aEXAMPLE-8aad-4d5d-8878-dfcab0bc441f \
    --tag-keys Project ReadOnly
```

Salida:

```
{
    "Tags": []
}
```

Para obtener más información, consulte Remove tags from a connections resource en la Guía del usuario de la consola de herramientas del desarrollador.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

Ejemplos de identidades de Amazon Cognito que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo ejecutar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon Cognito Identity.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-identity-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-identity-pool`.

AWS CLI

Para crear un grupo de identidades con el proveedor de grupos de identidades de Cognito

En este ejemplo, se crea un grupo de identidades denominado MyIdentityPool. Tiene un proveedor de grupo de identidades de Cognito. No se permiten identidades no autenticadas.

Comando:

```
aws cognito-identity create-identity-pool --identity-pool-
name MyIdentityPool --no-allow-unauthenticated-identities --cognito-
identity-providers ProviderName="cognito-idp.us-west-2.amazonaws.com/us-
west-2_aaaaaaaaa",ClientId="3n4b5urk1ft4fl3mg5e62d9ado",ServerSideTokenCheck=false
```

Salida:

```
{
  "IdentityPoolId": "us-west-2:11111111-1111-1111-1111-111111111111",
  "IdentityPoolName": "MyIdentityPool",
  "AllowUnauthenticatedIdentities": false,
  "CognitoIdentityProviders": [
      {
          "ProviderName": "cognito-idp.us-west-2.amazonaws.com/us-west-2_111111111",
          "ClientId": "3n4b5urk1ft4fl3mg5e62d9ado",
          "ServerSideTokenCheck": false
      }
  ]
}
```

- Para obtener detalles sobre la API, consulte CreateIdentityPool en la Referencia de comandos de la AWS CLI.

`delete-identities`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-identities`.

AWS CLI

Para eliminar un grupo de identidades

En este ejemplo, se elimina un grupo de identidades.

Comando:

```
aws cognito-identity delete-identity-pool --identity-ids-to-delete "us-
west-2:11111111-1111-1111-1111-111111111111"
```

Salida:

```
{
```

```
  "UnprocessedIdentityIds": []
}
```

- Para obtener detalles sobre la API, consulte DeleteIdentities en la Referencia de comandos de la AWS CLI.

`delete-identity-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-identity-pool`.

AWS CLI

Para eliminar un grupo de identidades

En el siguiente ejemplo de `delete-identity-pool` se elimina el grupo de identidades especificado.

Comando:

```
aws cognito-identity delete-identity-pool \
    --identity-pool-id "us-west-2:11111111-1111-1111-1111-111111111111"
```

Este comando no genera ninguna salida.

- Para obtener detalles de la API, consulte DeleteIdentityPool en la Referencia de comandos de la AWS CLI.

`describe-identity-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-identity-pool`.

AWS CLI

Descripción de un grupo de identidades

En este ejemplo, se describe un grupo de identidades.

Comando:

```
aws cognito-identity describe-identity-pool --identity-pool-id "us-
west-2:11111111-1111-1111-1111-111111111111"
```

Salida:

```
{
  "IdentityPoolId": "us-west-2:11111111-1111-1111-1111-111111111111",
  "IdentityPoolName": "MyIdentityPool",
  "AllowUnauthenticatedIdentities": false,
  "CognitoIdentityProviders": [
      {
          "ProviderName": "cognito-idp.us-west-2.amazonaws.com/us-west-2_111111111",
          "ClientId": "3n4b5urk1ft4fl3mg5e62d9ado",
          "ServerSideTokenCheck": false
      }
  ]
}
```

- Para obtener detalles sobre la API, consulte DescribeIdentityPool en la Referencia de comandos de la AWS CLI.

`get-identity-pool-roles`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-identity-pool-roles`.

AWS CLI

Obtención de los roles del grupo de identidades

En este ejemplo, se obtienen los roles de grupos de identidades.

Comando:

```
aws cognito-identity get-identity-pool-roles --identity-pool-id "us-
west-2:11111111-1111-1111-1111-111111111111"
```

Salida:

```
{
  "IdentityPoolId": "us-west-2:11111111-1111-1111-1111-111111111111",
  "Roles": {
      "authenticated": "arn:aws:iam::111111111111:role/
Cognito_MyIdentityPoolAuth_Role",
      "unauthenticated": "arn:aws:iam::111111111111:role/
Cognito_MyIdentityPoolUnauth_Role"
```

```
  }
}
```

- Para obtener detalles sobre la API, consulte GetIdentityPoolRoles en la Referencia de comandos de la AWS CLI.

`list-identity-pools`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-identity-pools`.

AWS CLI

Para mostrar grupos de identidades

En este ejemplo, se muestran los grupos de identidades. Hay un máximo de 20 identidades en la lista.

Comando:

```
aws cognito-identity list-identity-pools --max-results 20
```

Salida:

```
{
  "IdentityPools": [
      {
          "IdentityPoolId": "us-west-2:11111111-1111-1111-1111-111111111111",
          "IdentityPoolName": "MyIdentityPool"
      },
      {
          "IdentityPoolId": "us-west-2:11111111-1111-1111-1111-111111111111",
          "IdentityPoolName": "AnotherIdentityPool"
      },
      {
          "IdentityPoolId": "us-west-2:11111111-1111-1111-1111-111111111111",
          "IdentityPoolName": "IdentityPoolRegionA"
      }
  ]
}
```

- Para obtener detalles sobre la API, consulte ListIdentityPools en la Referencia de comandos de la AWS CLI.

`set-identity-pool-roles`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-identity-pool-roles`.

AWS CLI

Establecimiento de los roles del grupo de identidades

En el siguiente ejemplo de `set-identity-pool-roles`, se establecen roles para un grupo de identidades.

```
aws cognito-identity set-identity-pool-roles \
    --identity-pool-id "us-west-2:11111111-1111-1111-1111-111111111111" \
    --roles authenticated="arn:aws:iam::111111111111:role/
Cognito_MyIdentityPoolAuth_Role"
```

- Para obtener detalles sobre la API, consulte SetIdentityPoolRoles en la Referencia de comandos de la AWS CLI.

`update-identity-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-identity-pool`.

AWS CLI

Actualización de un grupo de identidades

En este ejemplo, se actualiza un grupo de identidades. Establece el nombre como MyIdentityPool. Añade Cognito como un proveedor de identidades. No permite las identidades no autenticadas.

Comando:

```
aws cognito-identity update-identity-pool --identity-pool-id "us-
west-2:11111111-1111-1111-1111-111111111111" --identity-pool-
name "MyIdentityPool" --no-allow-unauthenticated-identities --cognito-
identity-providers ProviderName="cognito-idp.us-west-2.amazonaws.com/us-
west-2_111111111",ClientId="3n4b5urk1ft4fl3mg5e62d9ado",ServerSideTokenCheck=false
```

Salida:

```
{
```

```
  "IdentityPoolId": "us-west-2:11111111-1111-1111-1111-111111111111",
  "IdentityPoolName": "MyIdentityPool",
  "AllowUnauthenticatedIdentities": false,
  "CognitoIdentityProviders": [
      {
          "ProviderName": "cognito-idp.us-west-2.amazonaws.com/us-west-2_111111111",
          "ClientId": "3n4b5urk1ft4fl3mg5e62d9ado",
          "ServerSideTokenCheck": false
      }
  ]
}
```

- Para obtener detalles sobre la API, consulte UpdateIdentityPool en la Referencia de comandos de la AWS CLI.

Ejemplos del proveedor de identidades Amazon Cognito que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con el proveedor de identidades Amazon Cognito.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-custom-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-custom-attributes`.

AWS CLI

Adición de un atributo personalizado

Este ejemplo agrega un atributo personalizado CustomAttr1 a un grupo de usuarios. Es del tipo Cadena y debe tener entre 1 y 15 caracteres. No es obligatorio.

Comando:

```
aws cognito-idp add-custom-attributes --user-pool-id us-west-2_aaaaaaaaa --custom-
attributes
 Name="CustomAttr1",AttributeDataType="String",DeveloperOnlyAttribute=false,Required=false,S
```

- Para obtener detalles sobre la API, consulte AddCustomAttributes en la Referencia de comandos de la AWS CLI.

admin-add-user-to-group

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-add-user-to-group`.

AWS CLI

Adición de un usuario a un grupo

En este ejemplo, se agrega a la usuaria Jane al grupo MyGroup.

Comando:

```
aws cognito-idp admin-add-user-to-group --user-pool-id us-west-2_aaaaaaaaa --
username Jane --group-name MyGroup
```

- Para obtener detalles sobre la API, consulte AdminAddUserToGroup en la Referencia de comandos de la AWS CLI.

admin-confirm-sign-up

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-confirm-sign-up`.

AWS CLI

Confirmación del registro del usuario

En este ejemplo, se confirma el usuario jane@example.com.

Comando:

```
aws cognito-idp admin-confirm-sign-up --user-pool-id us-west-2_aaaaaaaaa --
username jane@example.com
```

- Para obtener detalles sobre la API, consulte AdminConfirmSignUp en la Referencia de comandos de la AWS CLI.

`admin-create-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-create-user`.

AWS CLI

Para crear un usuario

En el siguiente ejemplo `admin-create-user`, se crea un usuario con la dirección de correo electrónico y el número de teléfono especificados.

```
aws cognito-idp admin-create-user \
    --user-pool-id us-west-2_aaaaaaaaa \
    --username diego \
    --user-attributes Name=email,Value=diego@example.com
 Name=phone_number,Value="+15555551212" \
    --message-action SUPPRESS
```

Salida:

```
{
    "User": {
        "Username": "diego",
        "Attributes": [
            {
                "Name": "sub",
                "Value": "7325c1de-b05b-4f84-b321-9adc6e61f4a2"
            },
            {
                "Name": "phone_number",
                "Value": "+15555551212"
            },
            {
                "Name": "email",
                "Value": "diego@example.com"
```

```
            }
        ],
        "UserCreateDate": 1548099495.428,
        "UserLastModifiedDate": 1548099495.428,
        "Enabled": true,
        "UserStatus": "FORCE_CHANGE_PASSWORD"
    }
}
```

- Para obtener detalles sobre la API, consulte AdminCreateUser en la Referencia de comandos de la AWS CLI.

`admin-delete-user-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-delete-user-attributes`.

AWS CLI

Eliminación de un atributo de usuario

En este ejemplo, se elimina un atributo personalizado CustomAttr1 para el usuario diego@example.com.

Comando:

```
aws cognito-idp admin-delete-user-attributes --user-pool-id us-west-2_aaaaaaaaa --
username diego@example.com --user-attribute-names "custom:CustomAttr1"
```

- Para obtener detalles sobre la API, consulte AdminDeleteUserAttributes en la Referencia de comandos de la AWS CLI.

`admin-delete-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-delete-user`.

AWS CLI

Para eliminar un usuario

En este ejemplo se elimina un usuario.

Comando:

```
aws cognito-idp admin-delete-user --user-pool-id us-west-2_aaaaaaaaa --
username diego@example.com
```

- Para obtener detalles sobre la API, consulte AdminDeleteUser en la Referencia de comandos de la AWS CLI.

`admin-disable-provider-for-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-disable-provider-for-user`.

AWS CLI

Desvinculación de un usuario federado de un perfil de usuario local

En el siguiente ejemplo de `admin-disable-provider-for-user`, se desconecta a un usuario de Google de su perfil local vinculado.

```
aws cognito-idp admin-disable-provider-for-user \
    --user-pool-id us-west-2_EXAMPLE \
    --
user ProviderAttributeName=Cognito_Subject,ProviderAttributeValue=0000000000000000,ProviderN
```

Para obtener más información, consulte Vinculación de usuarios federados a un perfil de usuario existente en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte AdminDisableProviderForUser en la Referencia de comandos de la AWS CLI.

`admin-disable-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-disable-user`.

AWS CLI

Impedir que un usuario inicie sesión

En el siguiente ejemplo de `admin-disable-user`, se impide que el usuario `diego@example.com` inicie sesión.

```
aws cognito-idp admin-disable-user \
```

```
    --user-pool-id us-west-2_EXAMPLE \
    --username diego@example.com
```

Para obtener más información, consulte Administración de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte AdminDisableUser en la Referencia de comandos de AWS CLI.

`admin-enable-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-enable-user`.

AWS CLI

Habilitación del inicio de sesión de un usuario

En el siguiente ejemplo de `admin-enable-user`, se permite que el usuario diego@example.com inicie sesión.

```
aws cognito-idp admin-enable-user \
    --user-pool-id us-west-2_EXAMPLE \
    --username diego@example.com
```

Para obtener más información, consulte Administración de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte AdminEnableUser en la Referencia de comandos de la AWS CLI.

`admin-forget-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-forget-device`.

AWS CLI

Para olvidar un dispositivo

En este ejemplo, se olvida el nombre de usuario jane@example.com en el dispositivo

Comando:

```
aws cognito-idp admin-forget-device --user-pool-id us-west-2_aaaaaaaaa --
username jane@example.com --device-key us-west-2_abcd_1234-5678
```

- Para obtener detalles sobre la API, consulte AdminForgetDevice en la Referencia de comandos de la AWS CLI.

admin-get-device

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-get-device`.

AWS CLI

Obtención de un dispositivo

En el siguiente ejemplo de `admin-get-device`, se muestra un dispositivo para el usuario `diego`.

```
aws cognito-idp admin-get-device \
    --user-pool-id us-west-2_EXAMPLE \
    --username diego \
    --device-key us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "Device": {
        "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "DeviceAttributes": [
            {
                "Name": "device_status",
                "Value": "valid"
            },
            {
                "Name": "device_name",
                "Value": "MyDevice"
            },
            {
                "Name": "dev:device_arn",
                "Value": "arn:aws:cognito-idp:us-west-2:123456789012:owner/diego.us-
west-2_EXAMPLE/device/us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
```

```
            {
                "Name": "dev:device_owner",
                "Value": "diego.us-west-2_EXAMPLE"
            },
            {
                "Name": "last_ip_used",
                "Value": "192.0.2.1"
            },
            {
                "Name": "dev:device_remembered_status",
                "Value": "remembered"
            },
            {
                "Name": "dev:device_sdk",
                "Value": "aws-sdk"
            }
        ],
        "DeviceCreateDate": 1715100742.022,
        "DeviceLastModifiedDate": 1723233651.167,
        "DeviceLastAuthenticatedDate": 1715100742.0
    }
}
```

Para obtener más información, consulte Trabajo con dispositivos de usuario en el grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte AdminGetDevice en la Referencia de comandos de la AWS CLI.

`admin-get-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-get-user`.

AWS CLI

Para obtener un usuario

En este ejemplo se obtiene información sobre el nombre de usuario jane@example.com.

Comando:

```
aws cognito-idp admin-get-user --user-pool-id us-west-2_aaaaaaaaa --
username jane@example.com
```

Salida:

```
{
  "Username": "4320de44-2322-4620-999b-5e2e1c8df013",
  "Enabled": true,
  "UserStatus": "FORCE_CHANGE_PASSWORD",
  "UserCreateDate": 1548108509.537,
  "UserAttributes": [
      {
          "Name": "sub",
          "Value": "4320de44-2322-4620-999b-5e2e1c8df013"
      },
      {
          "Name": "email_verified",
          "Value": "true"
      },
      {
          "Name": "phone_number_verified",
          "Value": "true"
      },
      {
          "Name": "phone_number",
          "Value": "+01115551212"
      },
      {
          "Name": "email",
          "Value": "jane@example.com"
      }
  ],
  "UserLastModifiedDate": 1548108509.537
}
```

- Para obtener detalles de la API, consulte AdminGetUser en la Referencia de comandos de la AWS CLI.

`admin-initiate-auth`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-initiate-auth`.

AWS CLI

Inicio de sesión de un usuario como administrador

En el siguiente ejemplo de `admin-initiate-auth`, se inicia la sesión del usuario diego@example.com. Este ejemplo también incluye metadatos para la protección contra amenazas y ClientMetadata para los desencadenadores de Lambda. El usuario está configurado para MFA con TOTP y recibe el desafío de proporcionar un código desde la aplicación del autenticador antes de poder completar la autenticación.

```
aws cognito-idp admin-initiate-auth \
    --user-pool-id us-west-2_EXAMPLE \
    --client-id 1example23456789 \
    --auth-flow ADMIN_USER_PASSWORD_AUTH \
    --auth-parameters USERNAME=diego@example.com,PASSWORD="My@Example
$Password3!",SECRET_HASH=ExampleEncodedClientIdSecretAndUsername= \
    --context-data="{\"EncodedData\":\"abc123example\",\"HttpHeaders\":
[{\"headerName\":\"UserAgent\",\"headerValue\":\"Mozilla/5.0 (Windows NT 6.1;
 Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0\"}],\"IpAddress\":\"192.0.2.1\",
\"ServerName\":\"example.com\",\"ServerPath\":\"/login\"}" \
    --client-metadata="{\"MyExampleKey\": \"MyExampleValue\"}"
```

Salida:

```
{
    "ChallengeName": "SOFTWARE_TOKEN_MFA",
    "Session": "AYABeExample...",
    "ChallengeParameters": {
        "FRIENDLY_DEVICE_NAME": "MyAuthenticatorApp",
        "USER_ID_FOR_SRP": "diego@example.com"
    }
}
```

Para obtener más información, consulte Flujo de autenticación de administrador en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles de la API, consulte AdminInitiateAuth en la Referencia de comandos de la AWS CLI.

`admin-link-provider-for-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-link-provider-for-user`.

AWS CLI

Vinculación de un usuario local a un usuario federado

En el siguiente ejemplo de `admin-link-provider-for-user`, se vincula al usuario local Diego con un usuario que realizará un inicio de sesión federado con Google.

```
aws cognito-idp admin-link-provider-for-user \
    --user-pool-id us-west-2_EXAMPLE \
    --destination-user ProviderName=Cognito,ProviderAttributeValue=diego \
    --source-
user ProviderAttributeName=Cognito_Subject,ProviderAttributeValue=0000000000000000,ProviderN
```

Para obtener más información, consulte Vinculación de usuarios federados a un perfil de usuario existente en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte AdminLinkProviderForUser en la Referencia de comandos de la AWS CLI.

`admin-list-devices`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-list-devices`.

AWS CLI

Para enumerar todos los dispositivos de un usuario

En el siguiente ejemplo de `admin-list-devices`, se muestran dispositivos para el usuario Diego.

```
aws cognito-idp admin-list-devices \
    --user-pool-id us-west-2_EXAMPLE \
    --username diego \
    --limit 1
```

Salida:

```
{
    "Devices": [
        {
            "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "DeviceAttributes": [
                {
                    "Name": "device_status",
                    "Value": "valid"
```

```
                },
                {
                    "Name": "device_name",
                    "Value": "MyDevice"
                },
                {
                    "Name": "dev:device_arn",
                    "Value": "arn:aws:cognito-idp:us-west-2:123456789012:owner/
diego.us-west-2_EXAMPLE/device/us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                {
                    "Name": "dev:device_owner",
                    "Value": "diego.us-west-2_EXAMPLE"
                },
                {
                    "Name": "last_ip_used",
                    "Value": "192.0.2.1"
                },
                {
                    "Name": "dev:device_remembered_status",
                    "Value": "remembered"
                },
                {
                    "Name": "dev:device_sdk",
                    "Value": "aws-sdk"
                }
            ],
            "DeviceCreateDate": 1715100742.022,
            "DeviceLastModifiedDate": 1723233651.167,
            "DeviceLastAuthenticatedDate": 1715100742.0
        }
    ]
}
```

Para obtener más información, consulte Trabajo con dispositivos de usuario en el grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte AdminListDevices en la Referencia de comandos de la AWS CLI.

`admin-list-groups-for-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-list-groups-for-user`.

AWS CLI

Para enumerar los grupos de un usuario

En este ejemplo, se enumeran los grupos a los que pertenece el nombre de usuario jane@example.com.

Comando:

```
aws cognito-idp admin-list-groups-for-user --user-pool-id us-west-2_aaaaaaaaa --
username diego@example.com
```

Salida:

```
{
  "Groups": [
      {
          "Description": "Sample group",
          "Precedence": 1,
          "LastModifiedDate": 1548097827.125,
          "RoleArn": "arn:aws:iam::111111111111:role/SampleRole",
          "GroupName": "SampleGroup",
          "UserPoolId": "us-west-2_aaaaaaaaa",
          "CreationDate": 1548097827.125
      }
  ]
}
```

- Para obtener detalles sobre la API, consulte AdminListGroupsForUser en la Referencia de comandos de la AWS CLI.

`admin-list-user-auth-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-list-user-auth-events`.

AWS CLI

Para enumerar los eventos de autorización de un usuario

En el siguiente ejemplo de `admin-list-user-auth-events`, se muestra el evento de registro de actividad de usuario más reciente del usuario diego.

```
aws cognito-idp admin-list-user-auth-events \
    --user-pool-id us-west-2_ywDJHlIfU \
    --username brcotter+050123 \
    --max-results 1
```

Salida:

```
{
    "AuthEvents": [
        {
            "EventId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "EventType": "SignIn",
            "CreationDate": 1726694203.495,
            "EventResponse": "InProgress",
            "EventRisk": {
                "RiskDecision": "AccountTakeover",
                "RiskLevel": "Medium",
                "CompromisedCredentialsDetected": false
            },
            "ChallengeResponses": [
                {
                    "ChallengeName": "Password",
                    "ChallengeResponse": "Success"
                }
            ],
            "EventContextData": {
                "IpAddress": "192.0.2.1",
                "City": "Seattle",
                "Country": "United States"
            }
        }
    ],
    "NextToken": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222#2024-09-18T21:16:43.495Z"
}
```

Para obtener más información, consulte Visualización y exportación del historial de eventos de los usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte AdminListUserAuthEvents en la Referencia de comandos de la AWS CLI.

admin-remove-user-from-group

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-remove-user-from-group`.

AWS CLI

Eliminación de un usuario de un grupo

En este ejemplo, se elimina jane@example.com de SampleGroup.

Comando:

```
aws cognito-idp admin-remove-user-from-group --user-pool-id us-west-2_aaaaaaaaa --
username jane@example.com --group-name SampleGroup
```

- Para obtener detalles sobre la API, consulte AdminRemoveUserFromGroup en la Referencia de comandos de la AWS CLI.

admin-reset-user-password

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-reset-user-password`.

AWS CLI

Restablecimiento de una contraseña de usuario

En este ejemplo, se restablece la contraseña de diego@example.com.

Comando:

```
aws cognito-idp admin-reset-user-password --user-pool-id us-west-2_aaaaaaaaa --
username diego@example.com
```

- Para obtener detalles sobre la API, consulte AdminResetUserPassword en la Referencia de comandos de la AWS CLI.

admin-respond-to-auth-challenge

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-respond-to-auth-challenge`.

AWS CLI

Respuesta a un desafío de autenticación

Hay muchas maneras de responder a los diferentes desafíos de autenticación, en función del flujo de autenticación, la configuración del grupo de usuarios y los ajustes de los usuarios. En el siguiente ejemplo de `admin-respond-to-auth-challenge`, se proporciona un código MFA con TOTP para diego@example.com y se completa el inicio de sesión. Este grupo de usuarios tiene activada la función de recordar dispositivos, por lo que el resultado de la autenticación también devuelve una nueva clave de dispositivo.

```
aws cognito-idp admin-respond-to-auth-challenge \
    --user-pool-id us-west-2_EXAMPLE \
    --client-id 1example23456789 \
    --challenge-name SOFTWARE_TOKEN_MFA \
    --challenge-responses USERNAME=diego@example.com,SOFTWARE_TOKEN_MFA_CODE=000000
 \
    --session AYABeExample...
```

Salida:

```
{
    "ChallengeParameters": {},
    "AuthenticationResult": {
        "AccessToken": "eyJra456defEXAMPLE",
        "ExpiresIn": 3600,
        "TokenType": "Bearer",
        "RefreshToken": "eyJra123abcEXAMPLE",
        "IdToken": "eyJra789ghiEXAMPLE",
        "NewDeviceMetadata": {
            "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "DeviceGroupKey": "-ExAmPlE1"
        }
    }
}
```

Para obtener más información, consulte Flujo de autenticación de administrador en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte AdminRespondToAuthChallenge en Referencia de comandos de la AWS CLI.

`admin-set-user-mfa-preference`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-set-user-mfa-preference`.

AWS CLI

Configuración de la preferencia de MFA del usuario

En este ejemplo, se establece la preferencia de MFA mediante SMS para el nombre de usuario diego@example.com.

Comando:

```
aws cognito-idp admin-set-user-mfa-preference --user-pool-id us-west-2_aaaaaaaaa --
username diego@example.com --sms-mfa-settings Enabled=false,PreferredMfa=false
```

- Para obtener detalles sobre la API, consulte AdminSetUserMfaPreference en la Referencia de comandos de la AWS CLI.

`admin-set-user-password`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-set-user-password`.

AWS CLI

Configuración de una contraseña de usuario como administrador

En el siguiente ejemplo de `admin-set-user-password`, se establece de forma permanente la contraseña de diego@example.com.

```
aws cognito-idp admin-set-user-password \
    --user-pool-id us-west-2_EXAMPLE \
    --username diego@example.com \
    --password MyExamplePassword1! \
    --permanent
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Contraseñas, recuperación de contraseñas y políticas de contraseñas en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte AdminSetUserPassword en la Referencia de comandos de la AWS CLI.

`admin-set-user-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-set-user-settings`.

AWS CLI

Establecimiento de la configuración de usuario

En este ejemplo, se establece la preferencia de envío de la MFA para el nombre de usuario diego@example.com.

Comando:

```
aws cognito-idp admin-set-user-settings --user-pool-id us-west-2_aaaaaaaaa --
username diego@example.com --mfa-options DeliveryMedium=EMAIL
```

- Para obtener detalles sobre la API, consulte AdminSetUserSettings en la Referencia de comandos de la AWS CLI.

`admin-update-auth-event-feedback`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-update-auth-event-feedback`.

AWS CLI

Envío de comentarios sobre un evento de autorización

En este ejemplo, se establece el valor de los comentarios para un evento de autorización identificado por el identificador del evento como Válido.

Comando:

```
aws cognito-idp admin-update-auth-event-feedback --user-pool-id us-west-2_aaaaaaaaa
 --username diego@example.com --event-id c2c2cf89-c0d3-482d-aba6-99d78a5b0bfe --
feedback-value Valid
```

- Para obtener detalles sobre la API, consulte AdminUpdateAuthEventFeedback en la Referencia de comandos de la AWS CLI.

`admin-update-device-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-update-device-status`.

AWS CLI

Actualización del estado del dispositivo

En este ejemplo, se establece el estado de recuerdo del dispositivo identificado por la clave del dispositivo en not_remember.

Comando:

```
aws cognito-idp admin-update-device-status --user-pool-id us-west-2_aaaaaaaaa
 --username diego@example.com --device-key xxxx  --device-remembered-
status not_remembered
```

- Para obtener detalles sobre la API, consulte AdminUpdateDeviceStatus en la Referencia de comandos de la AWS CLI.

`admin-update-user-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-update-user-attributes`.

AWS CLI

Actualización de los atributos de usuario

En este ejemplo, se actualiza un atributo de usuario personalizado CustomAttr1 para el usuario diego@example.com.

Comando:

```
aws cognito-idp admin-update-user-attributes --user-pool-id us-
west-2_aaaaaaaaa --username diego@example.com --user-attributes
 Name="custom:CustomAttr1",Value="Purple"
```

- Para obtener detalles sobre la API, consulte AdminUpdateUserAttributes en la Referencia de comandos de la AWS CLI.

`admin-user-global-sign-out`

En el siguiente ejemplo de código, se muestra cómo utilizar `admin-user-global-sign-out`.

AWS CLI

Cierre de sesión de un usuario como administrador

En el siguiente ejemplo de `admin-user-global-sign-out`, se cierra la sesión del usuario diego@example.com.

```
aws cognito-idp admin-user-global-sign-out \
    --user-pool-id us-west-2_EXAMPLE \
    --username diego@example.com
```

Para obtener más información, consulte Autenticación con un grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte AdminUserGlobalSignOut en la Referencia de comandos de la AWS CLI.

`associate-software-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-software-token`.

AWS CLI

Generación de una clave secreta para una aplicación de autenticación MFA

En el siguiente ejemplo de `associate-software-token`, se genera una clave privada TOTP para un usuario que ha iniciado sesión y ha recibido un token de acceso. La clave privada resultante se puede ingresar manualmente en una aplicación de autenticación o las aplicaciones pueden renderizarla como un código QR que el usuario puede escanear.

```
aws cognito-idp associate-software-token \
    --access-token eyJra456defEXAMPLE
```

Salida:

```
{
    "SecretCode": "QWERTYUIOP123456EXAMPLE"
}
```

Para obtener más información, consulte MFA con token de software TOTP en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte AssociateSoftwareToken en la Referencia de comandos de la AWS CLI.

`change-password`

En el siguiente ejemplo de código, se muestra cómo utilizar `change-password`.

AWS CLI

Cambio de contraseña

En este ejemplo se cambia una contraseña.

Comando:

```
aws cognito-idp change-password --previous-password OldPassword --proposed-
password NewPassword --access-token ACCESS_TOKEN
```

- Para obtener información sobre la API, consulte ChangePassword en la Referencia de comandos de la AWS CLI.

`confirm-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `confirm-device`.

AWS CLI

Confirmación del dispositivo de un usuario

En el siguiente ejemplo de `confirm-device`, se agrega un nuevo dispositivo recordado para el usuario actual.

```
aws cognito-idp confirm-device \
   --access-token eyJra456defEXAMPLE \
   --device-key us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
   --device-secret-verifier-
config PasswordVerifier=TXlWZXJpZmllclN0cmluZw,Salt=TXlTUlBTYWx0
```

Salida:

```
{
     "UserConfirmationNecessary": false
}
```

Para obtener más información, consulte Trabajo con dispositivos de usuario en el grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información de la API, consulte ConfirmDevice en la Referencia de comandos de la AWS CLI.

`confirm-forgot-password`

En el siguiente ejemplo de código, se muestra cómo utilizar `confirm-forgot-password`.

AWS CLI

Confirmación de una contraseña olvidada

En este ejemplo, se confirma una contraseña olvidada del nombre de usuario diego@example.com.

Comando:

```
aws cognito-idp confirm-forgot-password --client-id 3n4b5urk1ft4fl3mg5e62d9ado --
username=diego@example.com --password PASSWORD --confirmation-code CONF_CODE
```

- Para obtener detalles sobre la API, consulte ConfirmForgotPassword en la Referencia de comandos de la AWS CLI.

`confirm-sign-up`

En el siguiente ejemplo de código, se muestra cómo utilizar `confirm-sign-up`.

AWS CLI

Para confirmar la inscripción

Este ejemplo confirma el registro del nombre de usuario diego@example.com.

Comando:

```
aws cognito-idp confirm-sign-up --client-id 3n4b5urk1ft4fl3mg5e62d9ado --
username=diego@example.com --confirmation-code CONF_CODE
```

- Para obtener detalles de la API, consulte ConfirmSignUp en la Referencia de comandos de la AWS CLI.

`create-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-group`.

AWS CLI

Creación de un grupo

En este ejemplo, se crea un grupo con una descripción.

Comando:

```
aws cognito-idp create-group --user-pool-id us-west-2_aaaaaaaaa --group-
name MyNewGroup --description "New group."
```

Salida:

```
{
  "Group": {
      "GroupName": "MyNewGroup",
      "UserPoolId": "us-west-2_aaaaaaaaa",
      "Description": "New group.",
      "LastModifiedDate": 1548270073.795,
      "CreationDate": 1548270073.795
  }
}
```

Creación de un grupo con un rol y una prioridad

En este ejemplo, se crea un grupo con una descripción. También incluye un rol y una prioridad.

Comando:

```
aws cognito-idp create-group --user-pool-id us-west-2_aaaaaaaaa --group-
name MyNewGroupWithRole --description "New group with a role." --role-
arn arn:aws:iam::111111111111:role/MyNewGroupRole --precedence 2
```

Salida:

```
{
  "Group": {
      "GroupName": "MyNewGroupWithRole",
      "UserPoolId": "us-west-2_aaaaaaaaa",
      "Description": "New group with a role.",
      "RoleArn": "arn:aws:iam::111111111111:role/MyNewGroupRole",
      "Precedence": 2,
      "LastModifiedDate": 1548270211.761,
      "CreationDate": 1548270211.761
  }
}
```

- Para obtener información sobre la API, consulte CreateGroup en la Referencia de comandos de la AWS CLI.

`create-identity-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-identity-provider`.

AWS CLI

Ejemplo 1: creación de un proveedor de identidades (IdP) SAML para un grupo de usuarios con una URL de metadatos

En el siguiente ejemplo de `create-identity-provider`, se crea un nuevo IdP de SAML con metadatos de una URL pública, una asignación de atributos y dos identificadores.

```
aws cognito-idp create-identity-provider \
```

```
    --user-pool-id us-west-2_EXAMPLE \
    --provider-name MySAML \
    --provider-type SAML \
    --provider-
details IDPInit=true,IDPSignout=true,EncryptedResponses=true,MetadataURL=https://
auth.example.com/sso/saml/metadata,RequestSigningAlgorithm=rsa-sha256 \
    --attribute-mapping email=emailaddress,phone_number=phone,custom:111=department
 \
    --idp-identifiers CorpSAML WestSAML
```

Salida:

```
{
    "IdentityProvider": {
        "UserPoolId": "us-west-2_EXAMPLE",
        "ProviderName": "MySAML",
        "ProviderType": "SAML",
        "ProviderDetails": {
            "ActiveEncryptionCertificate": "MIICvTCCAaEXAMPLE",
            "EncryptedResponses": "true",
            "IDPInit": "true",
            "IDPSignout": "true",
            "MetadataURL": "https://auth.example.com/sso/saml/metadata",
            "RequestSigningAlgorithm": "rsa-sha256",
            "SLORedirectBindingURI": "https://auth.example.com/slo/saml",
            "SSORedirectBindingURI": "https://auth.example.com/sso/saml"
        },
        "AttributeMapping": {
            "custom:111": "department",
            "emailaddress": "email",
            "phone": "phone_number"
        },
        "IdpIdentifiers": [
            "CorpSAML",
            "WestSAML"
        ],
        "LastModifiedDate": 1726853833.977,
        "CreationDate": 1726853833.977
    }
}
```

Para obtener más información, consulte Agregar inicio de sesión de grupo de usuarios a través de un tercero en la Guía para desarrolladores de Amazon Cognito.

Ejemplo 2: creación de un proveedor de identidades (IdP) SAML para un grupo de usuarios con un archivo de metadatos

En el siguiente ejemplo de `create-identity-provider`, se crea un nuevo IdP de SAML con metadatos de un archivo, una asignación de atributos y dos identificadores. La sintaxis del archivo puede diferir entre los sistemas operativos del parámetro `--provider-details`. Lo más sencillo es crear un archivo de entrada JSON para esta operación:

```
aws cognito-idp create-identity-provider \
    --cli-input-json file://.\SAML-identity-provider.json
```

Contenido de `SAML-identity-provider.json`:

```
{
    "AttributeMapping": {
        "email" : "idp_email",
        "email_verified" : "idp_email_verified"
    },
    "IdpIdentifiers": [ "platform" ],
    "ProviderDetails": {
        "MetadataFile": "<md:EntityDescriptor xmlns:md=
\"urn:oasis:names:tc:SAML:2.0:metadata\" entityID=\"http://www.example.com/
sso\"><md:IDPSSODescriptor WantAuthnRequestsSigned=\"false\"
 protocolSupportEnumeration=\"urn:oasis:names:tc:SAML:2.0:protocol
\"><md:KeyDescriptor use=\"signing\"><ds:KeyInfo xmlns:ds=\"http://
www.w3.org/2000/09/xmldsig#
\"><ds:X509Data><ds:X509Certificate>[IDP_CERTIFICATE_DATA]</ds:X509Certificate></
ds:X509Data></ds:KeyInfo></md:KeyDescriptor><md:SingleLogoutService
 Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST\" Location=
\"https://www.example.com/slo/saml\"/><md:SingleLogoutService
 Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect\" Location=\"https://www.example.com/slo/saml\"/
><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
md:NameIDFormat><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress</md:NameIDFormat><md:SingleSignOnService
 Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST\" Location=
\"https://www.example.com/sso/saml\"/><md:SingleSignOnService Binding=
\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect\" Location=\"https://
www.example.com/sso/saml\"/></md:IDPSSODescriptor></md:EntityDescriptor>",
        "IDPSignout" : "true",
        "RequestSigningAlgorithm" : "rsa-sha256",
        "EncryptedResponses" : "true",
```

```
        "IDPInit" : "true"
    },
    "ProviderName": "MySAML2",
    "ProviderType": "SAML",
    "UserPoolId": "us-west-2_EXAMPLE"
}
```

Salida:

```
{
    "IdentityProvider": {
        "UserPoolId": "us-west-2_EXAMPLE",
        "ProviderName": "MySAML2",
        "ProviderType": "SAML",
        "ProviderDetails": {
            "ActiveEncryptionCertificate":
 "[USER_POOL_ENCRYPTION_CERTIFICATE_DATA]",
            "EncryptedResponses": "true",
            "IDPInit": "true",
            "IDPSignout": "true",
            "MetadataFile": "<md:EntityDescriptor xmlns:md=
\"urn:oasis:names:tc:SAML:2.0:metadata\" entityID=\"http://www.example.com/
sso\"><md:IDPSSODescriptor WantAuthnRequestsSigned=\"false\"
 protocolSupportEnumeration=\"urn:oasis:names:tc:SAML:2.0:protocol
\"><md:KeyDescriptor use=\"signing\"><ds:KeyInfo xmlns:ds=\"http://
www.w3.org/2000/09/xmldsig#
\"><ds:X509Data><ds:X509Certificate>[IDP_CERTIFICATE_DATA]</ds:X509Certificate></
ds:X509Data></ds:KeyInfo></md:KeyDescriptor><md:SingleLogoutService
 Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST\" Location=
\"https://www.example.com/slo/saml\"/><md:SingleLogoutService
 Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect\" Location=\"https://www.example.com/slo/saml\"/
><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
md:NameIDFormat><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress</md:NameIDFormat><md:SingleSignOnService
 Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST\" Location=
\"https://www.example.com/sso/saml\"/><md:SingleSignOnService Binding=
\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect\" Location=\"https://
www.example.com/sso/saml\"/></md:IDPSSODescriptor></md:EntityDescriptor>",
            "RequestSigningAlgorithm": "rsa-sha256",
            "SLORedirectBindingURI": "https://www.example.com/slo/saml",
            "SSORedirectBindingURI": "https://www.example.com/sso/saml"
        },
```

```
        "AttributeMapping": {
            "email": "idp_email",
            "email_verified": "idp_email_verified"
        },
        "IdpIdentifiers": [
            "platform"
        ],
        "LastModifiedDate": 1726855290.731,
        "CreationDate": 1726855290.731
    }
}
```

Para obtener más información, consulte Agregar inicio de sesión de grupo de usuarios a través de un tercero en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte CreateIdentityProvider en la Referencia de comandos de la AWS CLI.

`create-resource-server`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-resource-server`.

AWS CLI

Para crear un cliente de un grupo de usuarios

En el siguiente ejemplo de `create-resource-server`, se crea un nuevo servidor de recursos con ámbitos personalizados.

```
aws cognito-idp create-resource-server \
    --user-pool-id us-west-2_EXAMPLE \
    --identifier solar-system-data \
    --name "Solar system object tracker" \
    --scopes ScopeName=sunproximity.read,ScopeDescription="Distance in AU from Sol"
 ScopeName=asteroids.add,ScopeDescription="Enter a new asteroid"
```

Salida:

```
{
    "ResourceServer": {
        "UserPoolId": "us-west-2_EXAMPLE",
        "Identifier": "solar-system-data",
```

```
        "Name": "Solar system object tracker",
        "Scopes": [
            {
                "ScopeName": "sunproximity.read",
                "ScopeDescription": "Distance in AU from Sol"
            },
            {
                "ScopeName": "asteroids.add",
                "ScopeDescription": "Enter a new asteroid"
            }
        ]
    }
}
```

Para obtener más información, consulte Ámbitos, M2M y API con servidores de recursos en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte CreateResourceServer en la Referencia de comandos de la AWS CLI.

`create-user-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-user-import-job`.

AWS CLI

Para crear un trabajo de importación de usuarios

En este ejemplo, se crea un trabajo de importación de usuarios denominado MyImportJob.

Para obtener más información sobre cómo importar usuarios, consulte la sección Importing Users into User Pools From a CSV File.

Comando:

```
aws cognito-idp create-user-import-job --user-pool-id us-west-2_aaaaaaaaa --
job-name MyImportJob --cloud-watch-logs-role-arn arn:aws:iam::111111111111:role/
CognitoCloudWatchLogsRole
```

Salida:

```
{
```

```
  "UserImportJob": {
      "JobName": "MyImportJob",
      "JobId": "import-qQ0DCt2fRh",
      "UserPoolId": "us-west-2_aaaaaaaaa",
      "PreSignedUrl": "PRE_SIGNED_URL",
      "CreationDate": 1548271795.471,
      "Status": "Created",
      "CloudWatchLogsRoleArn": "arn:aws:iam::111111111111:role/
CognitoCloudWatchLogsRole",
      "ImportedUsers": 0,
      "SkippedUsers": 0,
      "FailedUsers": 0
  }
}
```

Cargue el archivo .csv con curl mediante la URL prefirmada:

Comando:

```
curl -v -T "PATH_TO_CSV_FILE" -H "x-amz-server-side-encryption:aws:kms"
 "PRE_SIGNED_URL"
```

- Para obtener detalles sobre la API, consulte CreateUserImportJob en la Referencia de comandos de la AWS CLI.

`create-user-pool-client`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-user-pool-client`.

AWS CLI

Para crear un cliente de un grupo de usuarios

En el siguiente ejemplo de `create-user-pool-client`, se crea un nuevo cliente de grupo de usuarios con un secreto de cliente, atributos de lectura y escritura explícitos, inicio de sesión con flujos de nombre de usuario-contraseña y SRP, inicio de sesión con tres IdP, acceso a un subconjunto de ámbitos de OAuth, análisis de PinPoint y una validez de sesión de autenticación ampliada.

```
aws cognito-idp create-user-pool-client \
    --user-pool-id us-west-2_EXAMPLE \
```

```
    --client-name MyTestClient \
    --generate-secret \
    --refresh-token-validity 10 \
    --access-token-validity 60 \
    --id-token-validity 60 \
    --token-validity-units AccessToken=minutes,IdToken=minutes,RefreshToken=days \
    --read-attributes email phone_number email_verified phone_number_verified \
    --write-attributes email phone_number \
    --explicit-auth-
flows ALLOW_USER_PASSWORD_AUTH ALLOW_USER_SRP_AUTH ALLOW_REFRESH_TOKEN_AUTH \
    --supported-identity-providers Google Facebook MyOIDC \
    --callback-urls https://www.amazon.com https://example.com http://
localhost:8001 myapp://example \
    --allowed-o-auth-flows code implicit \
    --allowed-o-auth-scopes openid profile aws.cognito.signin.user.admin solar-
system-data/asteroids.add \
    --allowed-o-auth-flows-user-pool-client \
    --analytics-configuration ApplicationArn=arn:aws:mobiletargeting:us-
west-2:767671399759:apps/thisisanexamplepinpointapplicationid,UserDataShared=TRUE \
    --prevent-user-existence-errors ENABLED \
    --enable-token-revocation \
    --enable-propagate-additional-user-context-data \
    --auth-session-validity 4
```

Salida:

```
{
    "UserPoolClient": {
        "UserPoolId": "us-west-2_EXAMPLE",
        "ClientName": "MyTestClient",
        "ClientId": "123abc456defEXAMPLE",
        "ClientSecret": "this1234is5678my91011example1213client1415secret",
        "LastModifiedDate": 1726788459.464,
        "CreationDate": 1726788459.464,
        "RefreshTokenValidity": 10,
        "AccessTokenValidity": 60,
        "IdTokenValidity": 60,
        "TokenValidityUnits": {
            "AccessToken": "minutes",
            "IdToken": "minutes",
            "RefreshToken": "days"
        },
        "ReadAttributes": [
```

```
            "email_verified",
            "phone_number_verified",
            "phone_number",
            "email"
        ],
        "WriteAttributes": [
            "phone_number",
            "email"
        ],
        "ExplicitAuthFlows": [
            "ALLOW_USER_PASSWORD_AUTH",
            "ALLOW_USER_SRP_AUTH",
            "ALLOW_REFRESH_TOKEN_AUTH"
        ],
        "SupportedIdentityProviders": [
            "Google",
            "MyOIDC",
            "Facebook"
        ],
        "CallbackURLs": [
            "https://example.com",
            "https://www.amazon.com",
            "myapp://example",
            "http://localhost:8001"
        ],
        "AllowedOAuthFlows": [
            "implicit",
            "code"
        ],
        "AllowedOAuthScopes": [
            "aws.cognito.signin.user.admin",
            "openid",
            "profile",
            "solar-system-data/asteroids.add"
        ],
        "AllowedOAuthFlowsUserPoolClient": true,
        "AnalyticsConfiguration": {
            "ApplicationArn": "arn:aws:mobiletargeting:us-west-2:123456789012:apps/
thisisanexamplepinpointapplicationid",
            "RoleArn": "arn:aws:iam::123456789012:role/aws-service-role/cognito-
idp.amazonaws.com/AWSServiceRoleForAmazonCognitoIdp",
            "UserDataShared": true
        },
        "PreventUserExistenceErrors": "ENABLED",
```

```
        "EnableTokenRevocation": true,
        "EnablePropagateAdditionalUserContextData": true,
        "AuthSessionValidity": 4
    }
}
```

Para obtener más información, consulte Application-specific settings with app clients en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte CreateUserPoolClient en la Referencia de comandos de la AWS CLI.

`create-user-pool-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-user-pool-domain`.

AWS CLI

Ejemplo 1: creación de un dominio de grupo de usuarios

En el siguiente ejemplo de `create-user-pool-domain`, se crea un nombre de dominio personalizado.

```
aws cognito-idp create-user-pool-domain \
    --user-pool-id us-west-2_EXAMPLE \
    --domain auth.example.com \
    --custom-domain-config CertificateArn=arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

Salida:

```
{
    "CloudFrontDomain": "example1domain.cloudfront.net"
}
```

Para obtener más información, consulte Configuración de un dominio de grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

Ejemplo 2: creación de un dominio de grupo de usuarios

En el siguiente ejemplo de `create-user-pool-domain`, se crea un dominio nuevo con un prefijo que pertenece al servicio.

```
aws cognito-idp create-user-pool-domain \
    --user-pool-id us-west-2_EXAMPLE2 \
    --domain mydomainprefix
```

Para obtener más información, consulte Configuración de un dominio de grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte CreateUserPoolDomain en la Referencia de comandos de la AWS CLI.

`create-user-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-user-pool`.

AWS CLI

Para crear un grupo de usuarios con una configuración mínima

En este ejemplo, se crea un grupo de usuarios denominado MyUserPool con los valores predeterminados. No se requieren atributos ni clientes de aplicación. La MFA y la seguridad avanzada están deshabilitadas.

Comando:

```
aws cognito-idp create-user-pool --pool-name MyUserPool
```

Salida:

```
{
  "UserPool": {
      "SchemaAttributes": [
          {
              "Name": "sub",
              "StringAttributeConstraints": {
                  "MinLength": "1",
                  "MaxLength": "2048"
              },
              "DeveloperOnlyAttribute": false,
              "Required": true,
              "AttributeDataType": "String",
              "Mutable": false
          },
```

```
            {
                "Name": "name",
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                },
                "DeveloperOnlyAttribute": false,
                "Required": false,
                "AttributeDataType": "String",
                "Mutable": true
            },
            {
                "Name": "given_name",
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                },
                "DeveloperOnlyAttribute": false,
                "Required": false,
                "AttributeDataType": "String",
                "Mutable": true
            },
            {
                "Name": "family_name",
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                },
                "DeveloperOnlyAttribute": false,
                "Required": false,
                "AttributeDataType": "String",
                "Mutable": true
            },
            {
                "Name": "middle_name",
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                },
                "DeveloperOnlyAttribute": false,
                "Required": false,
                "AttributeDataType": "String",
                "Mutable": true
            },
```

```
            {
                "Name": "nickname",
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                },
                "DeveloperOnlyAttribute": false,
                "Required": false,
                "AttributeDataType": "String",
                "Mutable": true
            },
            {
                "Name": "preferred_username",
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                },
                "DeveloperOnlyAttribute": false,
                "Required": false,
                "AttributeDataType": "String",
                "Mutable": true
            },
            {
                "Name": "profile",
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                },
                "DeveloperOnlyAttribute": false,
                "Required": false,
                "AttributeDataType": "String",
                "Mutable": true
            },
            {
                "Name": "picture",
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                },
                "DeveloperOnlyAttribute": false,
                "Required": false,
                "AttributeDataType": "String",
                "Mutable": true
            },
```

```
            {
                "Name": "website",
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                },
                "DeveloperOnlyAttribute": false,
                "Required": false,
                "AttributeDataType": "String",
                "Mutable": true
            },
            {
                "Name": "email",
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                },
                "DeveloperOnlyAttribute": false,
                "Required": false,
                "AttributeDataType": "String",
                "Mutable": true
            },
            {
                "AttributeDataType": "Boolean",
                "DeveloperOnlyAttribute": false,
                "Required": false,
                "Name": "email_verified",
                "Mutable": true
            },
            {
                "Name": "gender",
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                },
                "DeveloperOnlyAttribute": false,
                "Required": false,
                "AttributeDataType": "String",
                "Mutable": true
            },
            {
                "Name": "birthdate",
                "StringAttributeConstraints": {
                    "MinLength": "10",
```

```
                "MaxLength": "10"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "zoneinfo",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "locale",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "phone_number",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "AttributeDataType": "Boolean",
            "DeveloperOnlyAttribute": false,
            "Required": false,
```

```
            "Name": "phone_number_verified",
            "Mutable": true
        },
        {
            "Name": "address",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "updated_at",
            "NumberAttributeConstraints": {
                "MinValue": "0"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "Number",
            "Mutable": true
        }
    ],
    "MfaConfiguration": "OFF",
    "Name": "MyUserPool",
    "LastModifiedDate": 1547833345.777,
    "AdminCreateUserConfig": {
        "UnusedAccountValidityDays": 7,
        "AllowAdminCreateUserOnly": false
    },
    "EmailConfiguration": {},
    "Policies": {
        "PasswordPolicy": {
            "RequireLowercase": true,
            "RequireSymbols": true,
            "RequireNumbers": true,
            "MinimumLength": 8,
            "RequireUppercase": true
        }
    },
    "CreationDate": 1547833345.777,
    "EstimatedNumberOfUsers": 0,
```

```
      "Id": "us-west-2_aaaaaaaaa",
      "LambdaConfig": {}
  }
}
```

Creación de un grupo de usuarios con dos atributos obligatorios

En este ejemplo, se crea un grupo de usuarios MyUserPool. El grupo está configurado para aceptar un correo electrónico como atributo de nombre de usuario. También establece la dirección de origen del correo electrónico en una dirección validada mediante Amazon Simple Email Service.

Comando:

```
aws cognito-idp create-user-pool --pool-name MyUserPool --username-
attributes "email" --email-configuration=SourceArn="arn:aws:ses:us-
east-1:111111111111:identity/
jane@example.com",ReplyToEmailAddress="jane@example.com"
```

Salida:

```
{
  "UserPool": {
      "SchemaAttributes": [
          {
              "Name": "sub",
              "StringAttributeConstraints": {
                  "MinLength": "1",
                  "MaxLength": "2048"
              },
              "DeveloperOnlyAttribute": false,
              "Required": true,
              "AttributeDataType": "String",
              "Mutable": false
          },
          {
              "Name": "name",
              "StringAttributeConstraints": {
                  "MinLength": "0",
                  "MaxLength": "2048"
              },
              "DeveloperOnlyAttribute": false,
              "Required": false,
```

```
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "given_name",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "family_name",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "middle_name",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "nickname",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
```

```
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "preferred_username",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "profile",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "picture",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "website",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
```

```
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "email",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "AttributeDataType": "Boolean",
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "Name": "email_verified",
            "Mutable": true
        },
        {
            "Name": "gender",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "birthdate",
            "StringAttributeConstraints": {
                "MinLength": "10",
                "MaxLength": "10"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
```

```
            "Name": "zoneinfo",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "locale",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "phone_number",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "AttributeDataType": "Boolean",
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "Name": "phone_number_verified",
            "Mutable": true
        },
        {
            "Name": "address",
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
```

```
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "String",
            "Mutable": true
        },
        {
            "Name": "updated_at",
            "NumberAttributeConstraints": {
                "MinValue": "0"
            },
            "DeveloperOnlyAttribute": false,
            "Required": false,
            "AttributeDataType": "Number",
            "Mutable": true
        }
    ],
    "MfaConfiguration": "OFF",
    "Name": "MyUserPool",
    "LastModifiedDate": 1547837788.189,
    "AdminCreateUserConfig": {
        "UnusedAccountValidityDays": 7,
        "AllowAdminCreateUserOnly": false
    },
    "EmailConfiguration": {
        "ReplyToEmailAddress": "jane@example.com",
        "SourceArn": "arn:aws:ses:us-east-1:111111111111:identity/
jane@example.com"
    },
    "Policies": {
        "PasswordPolicy": {
            "RequireLowercase": true,
            "RequireSymbols": true,
            "RequireNumbers": true,
            "MinimumLength": 8,
            "RequireUppercase": true
        }
    },
    "UsernameAttributes": [
        "email"
    ],
    "CreationDate": 1547837788.189,
    "EstimatedNumberOfUsers": 0,
    "Id": "us-west-2_aaaaaaaaa",
```

```
        "LambdaConfig": {}
    }
}
```

- Para obtener información sobre la API, consulte CreateUserPool en la Referencia de comandos de la AWS CLI.

`delete-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-group`.

AWS CLI

Para eliminar un grupo

En este ejemplo, se elimina un grupo.

Comando:

```
aws cognito-idp delete-group --user-pool-id us-west-2_aaaaaaaaa  --group-
name MyGroupName
```

- Para obtener información sobre la API, consulte DeleteGroup en la Referencia de comandos de la AWS CLI.

`delete-identity-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-identity-provider`.

AWS CLI

Eliminación de un proveedor de identidades

En este ejemplo, se elimina un proveedor de identidades.

Comando:

```
aws cognito-idp delete-identity-provider --user-pool-id us-west-2_aaaaaaaaa --
provider-name Facebook
```

- Para obtener detalles sobre la API, consulte DeleteIdentityProvider en la Referencia de comandos de la AWS CLI.

`delete-resource-server`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-resource-server`.

AWS CLI

Eliminación de un servidor de recursos

En este ejemplo, se elimina un servidor de recursos denominado weather.example.com.

Comando:

```
aws cognito-idp delete-resource-server --user-pool-id us-west-2_aaaaaaaaa --
identifier weather.example.com
```

- Para obtener detalles sobre la API, consulte DeleteResourceServer en la Referencia de comandos de la AWS CLI.

`delete-user-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-user-attributes`.

AWS CLI

Eliminación de un atributo de usuario

En el siguiente ejemplo de `delete-user-attributes`, se elimina el atributo personalizado “custom:attribute” del usuario que ha iniciado sesión actualmente.

```
aws cognito-idp delete-user-attributes \
    --access-token ACCESS_TOKEN \
    --user-attribute-names "custom:department"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Trabajo con atributos de usuario en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte DeleteUserAttributes en la Referencia de comandos de la AWS CLI.

`delete-user-pool-client`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-user-pool-client`.

AWS CLI

Eliminación de un cliente del grupo de usuarios

En este ejemplo, se elimina un cliente del grupo de usuarios.

Comando:

```
aws cognito-idp delete-user-pool-client --user-pool-id us-west-2_aaaaaaaaa --client-id 38fjsnc484p94kpqsnet7mpld0
```

- Para obtener detalles sobre la API, consulte DeleteUserPoolClient en la Referencia de comandos de la AWS CLI.

`delete-user-pool-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-user-pool-domain`.

AWS CLI

Eliminación de un dominio del grupo de usuarios

En el siguiente ejemplo `delete-user-pool-domain`, se elimina un dominio del grupo de usuarios denominado `my-domain`

```
aws cognito-idp delete-user-pool-domain \
    --user-pool-id us-west-2_aaaaaaaaa \
    --domain my-domain
```

- Para obtener detalles sobre la API, consulte DeleteUserPoolDomain en la Referencia de comandos de la AWS CLI.

`delete-user-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-user-pool`.

AWS CLI

Eliminación de un grupo de usuarios

En este ejemplo, se elimina un grupo de usuarios mediante el identificador del grupo de usuarios, us-west-2_aaaaaaaaa.

Comando:

```
aws cognito-idp delete-user-pool --user-pool-id us-west-2_aaaaaaaaa
```

- Para obtener detalles sobre la API, consulte DeleteUserPool en la Referencia de comandos de la AWS CLI.

`delete-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-user`.

AWS CLI

Para eliminar un usuario

En este ejemplo se elimina un usuario.

Comando:

```
aws cognito-idp delete-user --access-token ACCESS_TOKEN
```

- Para obtener información sobre la API, consulte DeleteUser en la Referencia de comandos de la AWS CLI.

`describe-identity-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-identity-provider`.

AWS CLI

Descripción de un proveedor de identidades

En este ejemplo, se describe un proveedor de identidades denominado Facebook.

Comando:

```
aws cognito-idp describe-identity-provider --user-pool-id us-west-2_aaaaaaaaa --
provider-name Facebook
```

Salida:

```
{
  "IdentityProvider": {
      "UserPoolId": "us-west-2_aaaaaaaaa",
      "ProviderName": "Facebook",
      "ProviderType": "Facebook",
      "ProviderDetails": {
          "attributes_url": "https://graph.facebook.com/me?fields=",
          "attributes_url_add_attributes": "true",
          "authorize_scopes": myscope",
          "authorize_url": "https://www.facebook.com/v2.9/dialog/oauth",
          "client_id": "11111",
          "client_secret": "11111",
          "token_request_method": "GET",
          "token_url": "https://graph.facebook.com/v2.9/oauth/access_token"
      },
      "AttributeMapping": {
          "username": "id"
      },
      "IdpIdentifiers": [],
      "LastModifiedDate": 1548105901.736,
      "CreationDate": 1548105901.736
  }
}
```

- Para obtener detalles sobre la API, consulte DescribeIdentityProvider en la Referencia de comandos de la AWS CLI.

`describe-resource-server`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-resource-server`.

AWS CLI

Descripción de un servidor de recursos

En este ejemplo, se describe el servidor de recursos denominado weather.example.com.

Comando:

```
aws cognito-idp describe-resource-server --user-pool-id us-west-2_aaaaaaaaa --
identifier weather.example.com
```

Salida:

```
{
  "ResourceServer": {
      "UserPoolId": "us-west-2_aaaaaaaaa",
      "Identifier": "weather.example.com",
      "Name": "Weather",
      "Scopes": [
          {
              "ScopeName": "weather.update",
              "ScopeDescription": "Update weather forecast"
          },
          {
              "ScopeName": "weather.read",
              "ScopeDescription": "Read weather forecasts"
          },
          {
              "ScopeName": "weather.delete",
              "ScopeDescription": "Delete a weather forecast"
          }
      ]
  }
}
```

- Para obtener detalles sobre la API, consulte DescribeResourceServer en la Referencia de comandos de la AWS CLI.

`describe-risk-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-risk-configuration`.

AWS CLI

Descripción de una configuración de riesgo

En este ejemplo, se describe la configuración de riesgo asociada al grupo us-west-2_aaaaaaaaa.

Comando:

```
aws cognito-idp describe-risk-configuration --user-pool-id us-west-2_aaaaaaaaa
```

Salida:

```
{
  "RiskConfiguration": {
      "UserPoolId": "us-west-2_aaaaaaaaa",
      "CompromisedCredentialsRiskConfiguration": {
          "EventFilter": [
              "SIGN_IN",
              "SIGN_UP",
              "PASSWORD_CHANGE"
          ],
          "Actions": {
              "EventAction": "BLOCK"
          }
      },
      "AccountTakeoverRiskConfiguration": {
          "NotifyConfiguration": {
              "From": "diego@example.com",
              "ReplyTo": "diego@example.com",
              "SourceArn": "arn:aws:ses:us-east-1:111111111111:identity/
diego@example.com",
              "BlockEmail": {
                  "Subject": "Blocked sign-in attempt",
                  "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML
 email context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We
 blocked an unrecognized sign-in to your account with this information:\n<ul>
\n<li>Time: {login-time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city},
 {country}</li>\n</ul>\nIf this sign-in was not by you, you should change your
 password and notify us by clicking on <a href={one-click-link-invalid}>this link</
a>\nIf this sign-in was by you, you can follow <a href={one-click-link-valid}>this
 link</a> to let us know</pre>\n</body>\n</html>",
                  "TextBody": "We blocked an unrecognized sign-in to your account
 with this information:\nTime: {login-time}\nDevice: {device-name}\nLocation:
 {city}, {country}\nIf this sign-in was not by you, you should change your password
 and notify us by clicking on {one-click-link-invalid}\nIf this sign-in was by you,
 you can follow {one-click-link-valid} to let us know"
              },
              "NoActionEmail": {
                  "Subject": "New sign-in attempt",
```

```
                    "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML
 email context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We
 observed an unrecognized sign-in to your account with this information:\n<ul>
\n<li>Time: {login-time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city},
 {country}</li>\n</ul>\nIf this sign-in was not by you, you should change your
 password and notify us by clicking on <a href={one-click-link-invalid}>this link</
a>\nIf this sign-in was by you, you can follow <a href={one-click-link-valid}>this
 link</a> to let us know</pre>\n</body>\n</html>",
                    "TextBody": "We observed an unrecognized sign-in to your account
 with this information:\nTime: {login-time}\nDevice: {device-name}\nLocation:
 {city}, {country}\nIf this sign-in was not by you, you should change your password
 and notify us by clicking on {one-click-link-invalid}\nIf this sign-in was by you,
 you can follow {one-click-link-valid} to let us know"
                },
                "MfaEmail": {
                    "Subject": "New sign-in attempt",
                    "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML email
 context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We required
 you to use multi-factor authentication for the following sign-in attempt:\n<ul>
\n<li>Time: {login-time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city},
 {country}</li>\n</ul>\nIf this sign-in was not by you, you should change your
 password and notify us by clicking on <a href={one-click-link-invalid}>this link</
a>\nIf this sign-in was by you, you can follow <a href={one-click-link-valid}>this
 link</a> to let us know</pre>\n</body>\n</html>",
                    "TextBody": "We required you to use multi-factor authentication
 for the following sign-in attempt:\nTime: {login-time}\nDevice: {device-
name}\nLocation: {city}, {country}\nIf this sign-in was not by you, you should
 change your password and notify us by clicking on {one-click-link-invalid}\nIf this
 sign-in was by you, you can follow {one-click-link-valid} to let us know"
                }
            },
            "Actions": {
                "LowAction": {
                    "Notify": true,
                    "EventAction": "NO_ACTION"
                },
                "MediumAction": {
                    "Notify": true,
                    "EventAction": "MFA_IF_CONFIGURED"
                },
                "HighAction": {
                    "Notify": true,
                    "EventAction": "MFA_IF_CONFIGURED"
                }
```

```
            }
        }
    }
}
```

- Para obtener detalles sobre la API, consulte DescribeRiskConfiguration en la Referencia de comandos de la AWS CLI.

`describe-user-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-user-import-job`.

AWS CLI

Descripción del trabajo de importación de usuarios

En este ejemplo, se describe un trabajo de introducción de usuarios.

Para obtener más información sobre cómo importar usuarios, consulte la sección Importing Users into User Pools From a CSV File.

Comando:

```
aws cognito-idp describe-user-import-job --user-pool-id us-west-2_aaaaaaaaa --job-id import-TZqNQvDRnW
```

Salida:

```
{
  "UserImportJob": {
      "JobName": "import-Test1",
      "JobId": "import-TZqNQvDRnW",
      "UserPoolId": "us-west-2_aaaaaaaaa",
      "PreSignedUrl": "PRE_SIGNED URL",
      "CreationDate": 1548271708.512,
      "Status": "Created",
      "CloudWatchLogsRoleArn": "arn:aws:iam::111111111111:role/
CognitoCloudWatchLogsRole",
      "ImportedUsers": 0,
      "SkippedUsers": 0,
      "FailedUsers": 0
  }
```

```
}
```

- Para obtener detalles sobre la API, consulte DescribeUserImportJob en la Referencia de comandos de la AWS CLI.

`describe-user-pool-client`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-user-pool-client`.

AWS CLI

Descripción de un cliente del grupo de usuarios

En este ejemplo, se describe a un cliente del grupo de usuarios.

Comando:

```
aws cognito-idp describe-user-pool-client --user-pool-id us-west-2_aaaaaaaaa --
client-id 38fjsnc484p94kpqsnet7mpld0
```

Salida:

```
{
  "UserPoolClient": {
      "UserPoolId": "us-west-2_aaaaaaaaa",
      "ClientName": "MyApp",
      "ClientId": "38fjsnc484p94kpqsnet7mpld0",
      "ClientSecret": "CLIENT_SECRET",
      "LastModifiedDate": 1548108676.163,
      "CreationDate": 1548108676.163,
      "RefreshTokenValidity": 30,
      "ReadAttributes": [
          "address",
          "birthdate",
          "custom:CustomAttr1",
          "custom:CustomAttr2",
          "email",
          "email_verified",
          "family_name",
          "gender",
          "given_name",
          "locale",
```

```
            "middle_name",
            "name",
            "nickname",
            "phone_number",
            "phone_number_verified",
            "picture",
            "preferred_username",
            "profile",
            "updated_at",
            "website",
            "zoneinfo"
        ],
        "WriteAttributes": [
            "address",
            "birthdate",
            "custom:CustomAttr1",
            "custom:CustomAttr2",
            "email",
            "family_name",
            "gender",
            "given_name",
            "locale",
            "middle_name",
            "name",
            "nickname",
            "phone_number",
            "picture",
            "preferred_username",
            "profile",
            "updated_at",
            "website",
            "zoneinfo"
        ],
        "ExplicitAuthFlows": [
            "ADMIN_NO_SRP_AUTH",
            "USER_PASSWORD_AUTH"
        ],
        "AllowedOAuthFlowsUserPoolClient": false
    }
}
```

- Para obtener detalles sobre la API, consulte DescribeUserPoolClient en la Referencia de comandos de la AWS CLI.

`describe-user-pool-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-user-pool-domain`.

AWS CLI

Descripción de un cliente del grupo de usuarios

En este ejemplo se describe un dominio del grupo de usuarios denominado my-domain.

Comando:

```
aws cognito-idp describe-user-pool-domain --domain my-domain
```

Salida:

```
{
  "DomainDescription": {
      "UserPoolId": "us-west-2_aaaaaaaaa",
      "AWSAccountId": "111111111111",
      "Domain": "my-domain",
      "S3Bucket": "aws-cognito-prod-pdx-assets",
      "CloudFrontDistribution": "aaaaaaaaaaaaa.cloudfront.net",
      "Version": "20190128175402",
      "Status": "ACTIVE",
      "CustomDomainConfig": {}
  }
}
```

- Para obtener detalles sobre la API, consulte DescribeUserPoolDomain en la Referencia de comandos de la AWS CLI.

`describe-user-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-user-pool`.

AWS CLI

Descripción de un grupo de usuarios

En el ejemplo siguiente, se describe un grupo de usuarios con el ID del grupo de usuarios us-west-2_EXAMPLE.

```
aws cognito-idp describe-user-pool \
    --user-pool-id us-west-2_EXAMPLE
```

Salida:

```
{
    "UserPool": {
        "Id": "us-west-2_EXAMPLE",
        "Name": "MyUserPool",
        "Policies": {
            "PasswordPolicy": {
                "MinimumLength": 8,
                "RequireUppercase": true,
                "RequireLowercase": true,
                "RequireNumbers": true,
                "RequireSymbols": true,
                "TemporaryPasswordValidityDays": 1
            }
        },
        "DeletionProtection": "ACTIVE",
        "LambdaConfig": {
            "PreSignUp": "arn:aws:lambda:us-
west-2:123456789012:function:MyPreSignUpFunction",
            "CustomMessage": "arn:aws:lambda:us-
west-2:123456789012:function:MyCustomMessageFunction",
            "PostConfirmation": "arn:aws:lambda:us-
west-2:123456789012:function:MyPostConfirmationFunction",
            "PreAuthentication": "arn:aws:lambda:us-
west-2:123456789012:function:MyPreAuthenticationFunction",
            "PostAuthentication": "arn:aws:lambda:us-
west-2:123456789012:function:MyPostAuthenticationFunction",
            "DefineAuthChallenge": "arn:aws:lambda:us-
west-2:123456789012:function:MyDefineAuthChallengeFunction",
            "CreateAuthChallenge": "arn:aws:lambda:us-
west-2:123456789012:function:MyCreateAuthChallengeFunction",
            "VerifyAuthChallengeResponse": "arn:aws:lambda:us-
west-2:123456789012:function:MyVerifyAuthChallengeFunction",
            "PreTokenGeneration": "arn:aws:lambda:us-
west-2:123456789012:function:MyPreTokenGenerationFunction",
            "UserMigration": "arn:aws:lambda:us-
west-2:123456789012:function:MyMigrateUserFunction",
            "PreTokenGenerationConfig": {
                "LambdaVersion": "V2_0",
```

```
                "LambdaArn": "arn:aws:lambda:us-
west-2:123456789012:function:MyPreTokenGenerationFunction"
            },
            "CustomSMSSender": {
                "LambdaVersion": "V1_0",
                "LambdaArn": "arn:aws:lambda:us-
west-2:123456789012:function:MyCustomSMSSenderFunction"
            },
            "CustomEmailSender": {
                "LambdaVersion": "V1_0",
                "LambdaArn": "arn:aws:lambda:us-
west-2:123456789012:function:MyCustomEmailSenderFunction"
            },
            "KMSKeyID": "arn:aws:kms:us-west-2:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"
        },
        "LastModifiedDate": 1726784814.598,
        "CreationDate": 1602103465.273,
        "SchemaAttributes": [
            {
                "Name": "sub",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": false,
                "Mutable": false,
                "Required": true,
                "StringAttributeConstraints": {
                    "MinLength": "1",
                    "MaxLength": "2048"
                }
            },
            {
                "Name": "name",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                }
            },
            {
                "Name": "given_name",
                "AttributeDataType": "String",
```

```
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                }
            },
            {
                "Name": "family_name",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                }
            },
            {
                "Name": "middle_name",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                }
            },
            {
                "Name": "nickname",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                }
            },
            {
                "Name": "preferred_username",
                "AttributeDataType": "String",
```

```
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                }
            },
            {
                "Name": "profile",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                }
            },
            {
                "Name": "picture",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                }
            },
            {
                "Name": "website",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                }
            },
            {
                "Name": "email",
                "AttributeDataType": "String",
```

```
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": true,
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                }
            },
            {
                "Name": "email_verified",
                "AttributeDataType": "Boolean",
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false
            },
            {
                "Name": "gender",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
                    "MinLength": "0",
                    "MaxLength": "2048"
                }
            },
            {
                "Name": "birthdate",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
                    "MinLength": "10",
                    "MaxLength": "10"
                }
            },
            {
                "Name": "zoneinfo",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
```

```
                "MinLength": "0",
                "MaxLength": "2048"
            }
        },
        {
            "Name": "locale",
            "AttributeDataType": "String",
            "DeveloperOnlyAttribute": false,
            "Mutable": true,
            "Required": false,
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            }
        },
        {
            "Name": "phone_number",
            "AttributeDataType": "String",
            "DeveloperOnlyAttribute": false,
            "Mutable": true,
            "Required": false,
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            }
        },
        {
            "Name": "phone_number_verified",
            "AttributeDataType": "Boolean",
            "DeveloperOnlyAttribute": false,
            "Mutable": true,
            "Required": false
        },
        {
            "Name": "address",
            "AttributeDataType": "String",
            "DeveloperOnlyAttribute": false,
            "Mutable": true,
            "Required": false,
            "StringAttributeConstraints": {
                "MinLength": "0",
                "MaxLength": "2048"
            }
        },
```

```
            {
                "Name": "updated_at",
                "AttributeDataType": "Number",
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "NumberAttributeConstraints": {
                    "MinValue": "0"
                }
            },
            {
                "Name": "identities",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {}
            },
            {
                "Name": "custom:111",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
                    "MinLength": "1",
                    "MaxLength": "256"
                }
            },
            {
                "Name": "dev:custom:222",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": true,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
                    "MinLength": "1",
                    "MaxLength": "421"
                }
            },
            {
                "Name": "custom:accesstoken",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": false,
```

```
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
                    "MaxLength": "2048"
                }
            },
            {
                "Name": "custom:idtoken",
                "AttributeDataType": "String",
                "DeveloperOnlyAttribute": false,
                "Mutable": true,
                "Required": false,
                "StringAttributeConstraints": {
                    "MaxLength": "2048"
                }
            }
        ],
        "AutoVerifiedAttributes": [
            "email"
        ],
        "SmsVerificationMessage": "Your verification code is {####}. ",
        "EmailVerificationMessage": "Your verification code is {####}. ",
        "EmailVerificationSubject": "Your verification code",
        "VerificationMessageTemplate": {
            "SmsMessage": "Your verification code is {####}. ",
            "EmailMessage": "Your verification code is {####}. ",
            "EmailSubject": "Your verification code",
            "EmailMessageByLink": "Please click the link below to verify your email
address. <b>{##Verify Your Email##}</b>\n this is from us-west-2_ywDJHlIfU",
            "EmailSubjectByLink": "Your verification link",
            "DefaultEmailOption": "CONFIRM_WITH_LINK"
        },
        "SmsAuthenticationMessage": "Your verification code is {####}. ",
        "UserAttributeUpdateSettings": {
            "AttributesRequireVerificationBeforeUpdate": []
        },
        "MfaConfiguration": "OPTIONAL",
        "DeviceConfiguration": {
            "ChallengeRequiredOnNewDevice": true,
            "DeviceOnlyRememberedOnUserPrompt": false
        },
        "EstimatedNumberOfUsers": 166,
        "EmailConfiguration": {
```

```
            "SourceArn": "arn:aws:ses:us-west-2:123456789012:identity/
admin@example.com",
            "EmailSendingAccount": "DEVELOPER"
        },
        "SmsConfiguration": {
            "SnsCallerArn": "arn:aws:iam::123456789012:role/service-role/userpool-
SMS-Role",
            "ExternalId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "SnsRegion": "us-west-2"
        },
        "UserPoolTags": {},
        "Domain": "myCustomDomain",
        "CustomDomain": "auth.example.com",
        "AdminCreateUserConfig": {
            "AllowAdminCreateUserOnly": false,
            "UnusedAccountValidityDays": 1,
            "InviteMessageTemplate": {
                "SMSMessage": "Your username is {username} and temporary password is
 {####}. ",
                "EmailMessage": "Your username is {username} and temporary password
 is {####}. ",
                "EmailSubject": "Your temporary password"
            }
        },
        "UserPoolAddOns": {
            "AdvancedSecurityMode": "ENFORCED",
            "AdvancedSecurityAdditionalFlows": {}
        },
        "Arn": "arn:aws:cognito-idp:us-west-2:123456789012:userpool/us-
west-2_EXAMPLE",
        "AccountRecoverySetting": {
            "RecoveryMechanisms": [
                {
                    "Priority": 1,
                    "Name": "verified_email"
                }
            ]
        }
    }
}
```

Para obtener más información, consulte Grupos de usuarios de Amazon Cognito en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte DescribeUserPool en la Referencia de comandos de la AWS CLI.

`forget-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `forget-device`.

AWS CLI

Para olvidar un dispositivo

En este ejemplo, se olvida un dispositivo.

Comando:

```
aws cognito-idp forget-device --device-key us-west-2_abcd_1234-5678
```

- Para obtener detalles sobre la API, consulte ForgetDevice en la Referencia de comandos de la AWS CLI.

`forgot-password`

En el siguiente ejemplo de código, se muestra cómo utilizar `forgot-password`.

AWS CLI

Cómo forzar el cambio de contraseña

En el siguiente ejemplo de `forgot-password`, se envía un mensaje a jane@example.com para cambiar la contraseña.

```
aws cognito-idp forgot-password --client-id 38fjsnc484p94kpqsnet7mpld0 --
username jane@example.com
```

Salida:

```
{
    "CodeDeliveryDetails": {
        "Destination": "j***@e***.com",
        "DeliveryMedium": "EMAIL",
        "AttributeName": "email"
```

```
    }
}
```

- Para obtener detalles sobre la API, consulte ForgotPassword en la Referencia de comandos de la AWS CLI.

`get-csv-header`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-csv-header`.

AWS CLI

Creación de un encabezado csv

En este ejemplo, se crea un encabezado csv.

Para obtener más información sobre cómo importar usuarios, consulte la sección Importing Users into User Pools From a CSV File.

Comando:

```
aws cognito-idp get-csv-header --user-pool-id us-west-2_aaaaaaaaa
```

Salida:

```
{
  "UserPoolId": "us-west-2_aaaaaaaaa",
  "CSVHeader": [
      "name",
      "given_name",
      "family_name",
      "middle_name",
      "nickname",
      "preferred_username",
      "profile",
      "picture",
      "website",
      "email",
      "email_verified",
      "gender",
      "birthdate",
      "zoneinfo",
      "locale",
```

```
      "phone_number",
      "phone_number_verified",
      "address",
      "updated_at",
      "cognito:mfa_enabled",
      "cognito:username"
  ]
}
```

... Importación de usuarios a grupos de usuarios desde un archivo CSV: https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-using-import-tool.html

- Para obtener detalles sobre la API, consulte GetCsvHeader en la Referencia de comandos de la AWS CLI.

`get-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-device`.

AWS CLI

Obtención de un dispositivo

En el siguiente ejemplo de `get-device`, se muestra un dispositivo para el usuario que ha iniciado sesión actualmente.

```
aws cognito-idp get-device \
    --access-token eyJra456defEXAMPLE \
    --device-key us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "Device": {
        "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "DeviceAttributes": [
            {
                "Name": "device_status",
                "Value": "valid"
            },
            {
                "Name": "device_name",
```

```
                "Value": "MyDevice"
            },
            {
                "Name": "dev:device_arn",
                "Value": "arn:aws:cognito-idp:us-west-2:123456789012:owner/diego.us-
west-2_EXAMPLE/device/us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            {
                "Name": "dev:device_owner",
                "Value": "diego.us-west-2_EXAMPLE"
            },
            {
                "Name": "last_ip_used",
                "Value": "192.0.2.1"
            },
            {
                "Name": "dev:device_remembered_status",
                "Value": "remembered"
            },
            {
                "Name": "dev:device_sdk",
                "Value": "aws-sdk"
            }
        ],
        "DeviceCreateDate": 1715100742.022,
        "DeviceLastModifiedDate": 1723233651.167,
        "DeviceLastAuthenticatedDate": 1715100742.0
    }
}
```

Para obtener más información, consulte Trabajo con dispositivos de usuario en el grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte GetDevice en la Referencia de comandos de la AWS CLI.

`get-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-group`.

AWS CLI

Obtención de información acerca de un grupo

En el siguiente ejemplo de `get-group`, se muestran las propiedades del grupo de usuarios denominado `MyGroup`. Este grupo tiene una prioridad y un rol de IAM asociado.

```
aws cognito-idp get-group \
    --user-pool-id us-west-2_EXAMPLE \
    --group-name MyGroup
```

Salida:

```
{
    "Group": {
        "GroupName": "MyGroup",
        "UserPoolId": "us-west-2_EXAMPLE",
        "RoleArn": "arn:aws:iam::123456789012:role/example-cognito-role",
        "Precedence": 7,
        "LastModifiedDate": 1697211218.305,
        "CreationDate": 1611685503.954
    }
}
```

Para obtener más información, consulte Adding groups to a user pool en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte GetGroup en la Referencia de comandos de la AWS CLI.

`get-identity-provider-by-identifier`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-identity-provider-by-identifier`.

AWS CLI

Obtención de la configuración de un proveedor de identidad a partir del identificador de IdP

En el siguiente ejemplo de `get-identity-provider-by-identifier`, se devuelve la configuración del proveedor de identidad con el identificador `mysso`.

```
aws cognito-idp get-identity-provider-by-identifier \
    --user-pool-id us-west-2_EXAMPLE \
    --idp-identifier mysso
```

Salida:

```
{
    "IdentityProvider": {
        "UserPoolId": "us-west-2_EXAMPLE",
        "ProviderName": "MYSAML",
        "ProviderType": "SAML",
        "ProviderDetails": {
            "ActiveEncryptionCertificate": "[Certificate contents]",
            "IDPSignout": "false",
            "MetadataURL": "https://auth.example.com/saml/metadata/",
            "SLORedirectBindingURI": "https://auth.example.com/saml/logout/",
            "SSORedirectBindingURI": "https://auth.example.com/saml/assertion/"
        },
        "AttributeMapping": {
            "email": "email"
        },
        "IdpIdentifiers": [
            "mysso",
            "mysamlsso"
        ],
        "LastModifiedDate": 1705616729.188,
        "CreationDate": 1643734622.919
    }
}
```

Para obtener más información, consulte Inicio de sesión de IdP de terceros en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte GetIdentityProviderByIdentifier en la Referencia de comandos de la AWS CLI.

`get-log-delivery-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-log-delivery-configuration`.

AWS CLI

Muestra de la configuración de entrega de registros

En el siguiente ejemplo de `get-log-delivery-configuration`, se muestra la configuración de exportación de registros del grupo de usuarios solicitado.

```
aws cognito-idp get-log-delivery-configuration \
    --user-pool-id us-west-2_EXAMPLE
```

Salida:

```
{
    "LogDeliveryConfiguration": {
        "UserPoolId": "us-west-2_EXAMPLE",
        "LogConfigurations": [
            {
                "LogLevel": "INFO",
                "EventSource": "userAuthEvents",
                "FirehoseConfiguration": {
                    "StreamArn": "arn:aws:firehose:us-
west-2:123456789012:deliverystream/my-test-deliverystream"
                }
            },
            {
                "LogLevel": "ERROR",
                "EventSource": "userNotification",
                "CloudWatchLogsConfiguration": {
                    "LogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:my-message-delivery-logs"
                }
            }
        ]
    }
}
```

Para obtener más información, consulte Exportación de registros del grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte GetLogDeliveryConfiguration en la Referencia de comandos de la AWS CLI.

`get-signing-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-signing-certificate`.

AWS CLI

Muestra del certificado de firma de SAML

En el siguiente ejemplo de `get-signing-certificate`, se muestra el certificado de firma SAML 2.0 para el grupo de usuarios solicitado.

```
aws cognito-idp get-signing-certificate \
    --user-pool-id us-west-2_EXAMPLE
```

Salida:

```
{
    "Certificate": "[Certificate content]"
}
```

Para obtener más información, consulte Firma y cifrado de SAML en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte GetSigningCertificate en la Referencia de comandos de la AWS CLI.

`get-ui-customization`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ui-customization`.

AWS CLI

Muestra de la configuración de personalización de la interfaz de usuario alojada clásica para un cliente de aplicación

En el siguiente ejemplo de `get-ui-customization`, se muestra la configuración de personalización de la interfaz de usuario alojada clásica para un cliente de aplicación que no hereda la configuración del grupo de usuarios.

```
aws cognito-idp get-ui-customization \
    --user-pool-id us-west-2_EXAMPLE \
    --client-id 1example23456789
```

Salida:

```
{
    "UICustomization": {
```

```
        "UserPoolId": "us-west-2_EXAMPLE",
        "ClientId": "1example23456789",
        "ImageUrl": "https://example.cloudfront.net/us-
west-2_EXAMPLE/1example23456789/20250115191928/assets/images/image.jpg",
        "CSS": "\n.logo-customizable {\n  max-width: 80%;\n  max-height: 30%;
\n}\n\n.banner-customizable {\n  padding: 25px 0px 25px 0px;\n  background-color:
 lightgray;\n}\n\n.label-customizable {\n  font-weight: 400;\n}\n\n.textDescription-
customizable {\n  padding-top: 100px;\n  padding-bottom: 10px;\n  display: block;
\n  font-size: 12px;\n}\n\n.idpDescription-customizable {\n  padding-top: 10px;\n
  padding-bottom: 10px;\n  display: block;\n  font-size: 16px;\n}\n\n.legalText-
customizable {\n  color: #747474;\n  font-size: 11px;\n}\n\n.submitButton-
customizable {\n  font-size: 14px;\n  font-weight: bold;\n  margin: 20px 0px
 10px 0px;\n  height: 50px;\n  width: 100%;\n  color: #fff;\n  background-color:
 #337ab7;\n}\n\n.submitButton-customizable:hover {\n  color: #fff;\n  background-
color: #286090;\n}\n\n.errorMessage-customizable {\n  padding: 5px;\n  font-size:
 12px;\n  width: 100%;\n  background: #F5F5F5;\n  border: 2px solid #D64958;\n
  color: #D64958;\n}\n\n.inputField-customizable {\n  width: 100%;\n  height:
 34px;\n  color: #555;\n  background-color: #fff;\n  border: 1px solid #ccc;\n}\n
\n.inputField-customizable:focus {\n  border-color: #66afe9;\n  outline: 0;\n}\n
\n.idpButton-customizable {\n  height: 40px;\n  width: 100%;\n  width: 100%;\n
 text-align: center;\n  margin-bottom: 15px;\n  color: #fff;\n  background-color:
 #5bc0de;\n  border-color: #46b8da;\n}\n\n.idpButton-customizable:hover {\n
 color: #fff;\n  background-color: #31b0d5;\n}\n\n.socialButton-customizable {\n
  border-radius: 2px;\n  height: 60px;\n  margin-bottom: 15px;\n  padding: 1px;
\n  text-align: left;\n  width: 100%;\n}\n\n.redirect-customizable {\n  text-
align: center;\n}\n\n.passwordCheck-notValid-customizable {\n  color: #DF3312;
\n}\n\n.passwordCheck-valid-customizable {\n  color: #19BF00;\n}\n\n.background-
customizable {\n  background-color: #fff;\n}\n",
        "CSSVersion": "20250115191928"
    }
}
```

Para obtener más información, consulte Marca de la interfaz de usuario alojada (clásica) en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte GetUiCustomization en la Referencia de comandos de la AWS CLI.

`get-user-attribute-verification-code`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-user-attribute-verification-code`.

AWS CLI

Envío de un código de verificación de atributo al usuario actual

En el siguiente ejemplo de `get-user-attribute-verification-code`, se envía un código de verificación de atributo a la dirección de correo electrónico del usuario que ha iniciado sesión actualmente.

```
aws cognito-idp get-user-attribute-verification-code \
    --access-token eyJra456defEXAMPLE \
    --attribute-name email
```

Salida:

```
{
    "CodeDeliveryDetails": {
        "Destination": "a***@e***",
        "DeliveryMedium": "EMAIL",
        "AttributeName": "email"
    }
}
```

Para obtener más información, consulte Inscripción y confirmación de cuentas de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información de la API, consulte GetUserAttributeVerificationCode en la Referencia de comandos de la AWS CLI.

`get-user-auth-factors`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-user-auth-factors`.

AWS CLI

Muestra de los factores de autenticación disponibles para el usuario actual

En el siguiente ejemplo de `get-user-auth-factors`, se muestran los factores de autenticación disponibles para el usuario que ha iniciado sesión actualmente.

```
aws cognito-idp get-user-auth-factors \
    --access-token eyJra456defEXAMPLE
```

Salida:

```
{
    "Username": "testuser",
    "ConfiguredUserAuthFactors": [
        "PASSWORD",
        "EMAIL_OTP",
        "SMS_OTP",
        "WEB_AUTHN"
    ]
}
```

Para obtener más información, consulte Autenticación en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte GetUserAuthFactors en la Referencia de comandos de la AWS CLI.

`get-user-pool-mfa-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-user-pool-mfa-config`.

AWS CLI

Muestra de la configuración de autenticación multifactor y WebAuthn de un grupo de usuarios

En el siguiente ejemplo de `get-user-pool-mfa-config`, se muestra la configuración de MFA y WebAuthn del grupo de usuarios solicitado.

```
aws cognito-idp get-user-pool-mfa-config \
    --user-pool-id us-west-2_EXAMPLE
```

Salida:

```
{
    "SmsMfaConfiguration": {
        "SmsAuthenticationMessage": "Your OTP for MFA or sign-in: use {####}.",
        "SmsConfiguration": {
            "SnsCallerArn": "arn:aws:iam::123456789012:role/service-role/my-SMS-
Role",
            "ExternalId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "SnsRegion": "us-west-2"
```

```
        }
    },
    "SoftwareTokenMfaConfiguration": {
        "Enabled": true
    },
    "EmailMfaConfiguration": {
        "Message": "Your OTP for MFA or sign-in: use {####}",
        "Subject": "OTP test"
    },
    "MfaConfiguration": "OPTIONAL",
    "WebAuthnConfiguration": {
        "RelyingPartyId": "auth.example.com",
        "UserVerification": "preferred"
    }
}
```

Para obtener más información, consulte Agregación de MFA en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte GetUserPoolMfaConfig en la Referencia de comandos de AWS CLI.

`get-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-user`.

AWS CLI

Obtención de los detalles del usuario actual

En el siguiente ejemplo de `get-user`, se muestra el perfil del usuario que ha iniciado sesión actualmente.

```
aws cognito-idp get-user \
    --access-token eyJra456defEXAMPLE
```

Salida:

```
{
    "Username": "johndoe",
    "UserAttributes": [
        {
            "Name": "sub",
```

```
            "Value": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
        },
        {
            "Name": "identities",
            "Value": "[{\"userId\":\"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222\",
\"providerName\":\"SignInWithApple\",\"providerType\":\"SignInWithApple\",\"issuer
\":null,\"primary\":false,\"dateCreated\":1701125599632}]"
        },
        {
            "Name": "email_verified",
            "Value": "true"
        },
        {
            "Name": "custom:state",
            "Value": "Maine"
        },
        {
            "Name": "name",
            "Value": "John Doe"
        },
        {
            "Name": "phone_number_verified",
            "Value": "true"
        },
        {
            "Name": "phone_number",
            "Value": "+12065551212"
        },
        {
            "Name": "preferred_username",
            "Value": "jamesdoe"
        },
        {
            "Name": "locale",
            "Value": "EMEA"
        },
        {
            "Name": "email",
            "Value": "jamesdoe@example.com"
        }
    ]
}
```

Para obtener más información, consulte Administración de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte GetUser en la Referencia de comandos de la AWS CLI.

`global-sign-out`

En el siguiente ejemplo de código, se muestra cómo utilizar `global-sign-out`.

AWS CLI

Cierre de la sesión del usuario actual

En el siguiente ejemplo de `global-sign-out`, se cierra la sesión del usuario actual.

```
aws cognito-idp global-sign-out \
    --access-token eyJra456defEXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte GlobalSignOut en la Referencia de comandos de la AWS CLI.

`initiate-auth`

En el siguiente ejemplo de código, se muestra cómo utilizar `initiate-auth`.

AWS CLI

Inicio de sesión de un usuario

En el siguiente ejemplo de `initiate-auth`, se inicia la sesión de un usuario con el flujo básico de nombre de usuario y contraseña, sin desafíos adicionales.

```
aws cognito-idp initiate-auth \
    --auth-flow USER_PASSWORD_AUTH \
    --client-id 1example23456789 \
```

```
    --analytics-metadata AnalyticsEndpointId=d70b2ba36a8c4dc5a04a0451aEXAMPLE \
    --auth-parameters USERNAME=testuser,PASSWORD=[Password] --user-context-
data EncodedData=mycontextdata --client-metadata MyTestKey=MyTestValue
```

Salida:

```
{
    "AuthenticationResult": {
        "AccessToken": "eyJra456defEXAMPLE",
        "ExpiresIn": 3600,
        "TokenType": "Bearer",
        "RefreshToken": "eyJra123abcEXAMPLE",
        "IdToken": "eyJra789ghiEXAMPLE",
        "NewDeviceMetadata": {
            "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "DeviceGroupKey": "-v7w9UcY6"
        }
    }
}
```

Para obtener más información, consulte Autenticación en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte InitiateAuth en la Referencia de comandos de la AWS CLI.

`list-devices`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-devices`.

AWS CLI

Muestra de los dispositivos de un usuario

En el siguiente ejemplo de `list-devices`, se muestran los dispositivos que el usuario actual ha registrado.

```
aws cognito-idp list-devices \
    --access-token eyJra456defEXAMPLE
```

Salida:

```
{
    "Devices": [
        {
            "DeviceAttributes": [
                {
                    "Name": "device_status",
                    "Value": "valid"
                },
                {
                    "Name": "device_name",
                    "Value": "Dart-device"
                },
                {
                    "Name": "last_ip_used",
                    "Value": "192.0.2.1"
                }
            ],
            "DeviceCreateDate": 1715100742.022,
            "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "DeviceLastAuthenticatedDate": 1715100742.0,
            "DeviceLastModifiedDate": 1723233651.167
        },
        {
            "DeviceAttributes": [
                {
                    "Name": "device_status",
                    "Value": "valid"
                },
                {
                    "Name": "last_ip_used",
                    "Value": "192.0.2.2"
                }
            ],
            "DeviceCreateDate": 1726856147.993,
            "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "DeviceLastAuthenticatedDate": 1726856147.0,
            "DeviceLastModifiedDate": 1726856147.993
        }
    ]
}
```

Para obtener más información, consulte Trabajo con dispositivos en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte ListDevices en la Referencia de comandos de la AWS CLI.

`list-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-groups`.

AWS CLI

Muestra de los grupos en un grupo de usuarios

En el siguiente ejemplo de `list-groups`, se muestran los dos primeros grupos del grupo de usuarios solicitado.

```
aws cognito-idp list-groups \
    --user-pool-id us-west-2_EXAMPLE \
    --max-items 2
```

Salida:

```
{
    "Groups": [
        {
            "CreationDate": 1681760899.633,
            "Description": "My test group",
            "GroupName": "testgroup",
            "LastModifiedDate": 1681760899.633,
            "Precedence": 1,
            "UserPoolId": "us-west-2_EXAMPLE"
        },
        {
            "CreationDate": 1642632749.051,
            "Description": "Autogenerated group for users who sign in using
 Facebook",
            "GroupName": "us-west-2_EXAMPLE_Facebook",
            "LastModifiedDate": 1642632749.051,
            "UserPoolId": "us-west-2_EXAMPLE"
        }
    ],
    "NextToken": "[Pagination token]"
}
```

Para obtener más información, consulte Adding groups to a user pool en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte ListGroups en la Referencia de comandos de la AWS CLI.

`list-identity-providers`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-identity-providers`.

AWS CLI

Muestra de proveedores de identidad

En el siguiente ejemplo de `list-identity-providers`, se muestran los dos primeros proveedores de identidad del grupo de usuarios solicitado.

```
aws cognito-idp list-identity-providers \
    --user-pool-id us-west-2_EXAMPLE \
    --max-items 2
```

Salida:

```
{
    "Providers": [
        {
            "CreationDate": 1619477386.504,
            "LastModifiedDate": 1703798328.142,
            "ProviderName": "Azure",
            "ProviderType": "SAML"
        },
        {
            "CreationDate": 1642698776.175,
            "LastModifiedDate": 1642699086.453,
            "ProviderName": "LoginWithAmazon",
            "ProviderType": "LoginWithAmazon"
        }
    ],
    "NextToken": "[Pagination token]"
}
```

Para obtener más información, consulte Inicio de sesión de IdP de terceros en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte ListIdentityProviders en la Referencia de comandos de la AWS CLI.

`list-resource-servers`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-servers`.

AWS CLI

Muestra de los servidores de recursos

En el siguiente ejemplo de `list-resource-servers`, se muestran los dos primeros servidores de recursos del grupo de usuarios solicitado.

```
aws cognito-idp list-resource-servers \
    --user-pool-id us-west-2_EXAMPLE \
    --max-results 2
```

Salida:

```
{
    "ResourceServers": [
        {
            "Identifier": "myapi.example.com",
            "Name": "Example API with custom access control scopes",
            "Scopes": [
                {
                    "ScopeDescription": "International customers",
                    "ScopeName": "international.read"
                },
                {
                    "ScopeDescription": "Domestic customers",
                    "ScopeName": "domestic.read"
                }
            ],
            "UserPoolId": "us-west-2_EXAMPLE"
        },
        {
            "Identifier": "myapi2.example.com",
```

```
            "Name": "Another example API for access control",
            "Scopes": [
                {
                    "ScopeDescription": "B2B customers",
                    "ScopeName": "b2b.read"
                }
            ],
            "UserPoolId": "us-west-2_EXAMPLE"
        }
    ],
    "NextToken": "[Pagination token]"
}
```

Para obtener más información, consulte Control de acceso con servidores de recursos en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte ListResourceServers en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Muestra de las etiquetas del grupo de usuarios

En el siguiente ejemplo de `list-tags-for-resource`, se muestran las etiquetas asignadas al grupo de usuarios con el ARN solicitado.

```
aws cognito-idp list-tags-for-resource \
    --resource-arn arn:aws:cognito-idp:us-west-2:123456789012:userpool/us-
west-2_EXAMPLE
```

Salida:

```
{
    "Tags": {
        "administrator": "Jie",
        "tenant": "ExampleCorp"
    }
}
```

Para obtener más información, consulte Etiquetado de recursos de Amazon Cognito en la Guía para desarrolladores de Amazon Cognito.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-user-import-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-user-import-jobs`.

AWS CLI

Muestra de los trabajos y estados de importación de usuarios

En el siguiente ejemplo de `list-user-import-jobs`, se muestran los tres primeros trabajos de importación de usuarios y sus detalles en el grupo de usuarios solicitado.

```
aws cognito-idp list-user-import-jobs \
    --user-pool-id us-west-2_EXAMPLE \
    --max-results 3
```

Salida:

```
{
    "PaginationToken": "us-west-2_EXAMPLE#import-example3#1667948397084",
    "UserImportJobs": [
        {
            "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/
Cognito-UserImport-Role",
            "CompletionDate": 1735329786.142,
            "CompletionMessage": "The user import job has expired.",
            "CreationDate": 1735241621.022,
            "FailedUsers": 0,
            "ImportedUsers": 0,
            "JobId": "import-example1",
            "JobName": "Test-import-job-1",
            "PreSignedUrl": "https://aws-cognito-idp-user-import-pdx.s3.us-
west-2.amazonaws.com/123456789012/us-west-2_EXAMPLE/import-mAgUtd8PMm?
X-Amz-Security-Token=[token]&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Date=20241226T193341Z&X-Amz-SignedHeaders=host%3Bx-amz-server-side-encryption&X-Amz-
Expires=899&X-Amz-Credential=[credential]&X-Amz-Signature=[signature]",
            "SkippedUsers": 0,
            "Status": "Expired",
```

```
            "UserPoolId": "us-west-2_EXAMPLE"
        },
        {
            "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/
Cognito-UserImport-Role",
            "CompletionDate": 1681509058.408,
            "CompletionMessage": "Too many users have failed or been skipped during
 the import.",
            "CreationDate": 1681509001.477,
            "FailedUsers": 1,
            "ImportedUsers": 0,
            "JobId": "import-example2",
            "JobName": "Test-import-job-2",
            "PreSignedUrl": "https://aws-cognito-idp-user-import-pdx.s3.us-
west-2.amazonaws.com/123456789012/us-west-2_EXAMPLE/import-mAgUtd8PMm?
X-Amz-Security-Token=[token]&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Date=20241226T193341Z&X-Amz-SignedHeaders=host%3Bx-amz-server-side-encryption&X-Amz-
Expires=899&X-Amz-Credential=[credential]&X-Amz-Signature=[signature]",
            "SkippedUsers": 0,
            "StartDate": 1681509057.965,
            "Status": "Failed",
            "UserPoolId": "us-west-2_EXAMPLE"
        },
        {
            "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/
Cognito-UserImport-Role",
            "CompletionDate": 1.667864578676E9,
            "CompletionMessage": "Import Job Completed Successfully.",
            "CreationDate": 1.667864480281E9,
            "FailedUsers": 0,
            "ImportedUsers": 6,
            "JobId": "import-example3",
            "JobName": "Test-import-job-3",
            "PreSignedUrl": "https://aws-cognito-idp-user-import-pdx.s3.us-
west-2.amazonaws.com/123456789012/us-west-2_EXAMPLE/import-mAgUtd8PMm?
X-Amz-Security-Token=[token]&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Date=20241226T193341Z&X-Amz-SignedHeaders=host%3Bx-amz-server-side-encryption&X-Amz-
Expires=899&X-Amz-Credential=[credential]&X-Amz-Signature=[signature]",
            "SkippedUsers": 0,
            "StartDate": 1.667864578167E9,
            "Status": "Succeeded",
            "UserPoolId": "us-west-2_EXAMPLE"
        }
    ]
```

```
}
```

Para obtener más información, consulte Importación de usuarios de un archivo CSV en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte ListUserImportJobs en la Referencia de comandos de la AWS CLI.

`list-user-pool-clients`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-user-pool-clients`.

AWS CLI

Muestra de los clientes de la aplicación

En el siguiente ejemplo de `list-user-pool-clients`, se muestran los tres primeros clientes de la aplicación del grupo de usuarios solicitado.

```
aws cognito-idp list-user-pool-clients \
    --user-pool-id us-west-2_EXAMPLE \
    --max-results 3
```

Salida:

```
{
    "NextToken": "[Pagination token]",
    "UserPoolClients": [
        {
            "ClientId": "1example23456789",
            "ClientName": "app-client-1",
            "UserPoolId": "us-west-2_EXAMPLE"
        },
        {
            "ClientId": "2example34567890",
            "ClientName": "app-client-2",
            "UserPoolId": "us-west-2_EXAMPLE"
        },
        {
            "ClientId": "3example45678901",
            "ClientName": "app-client-3",
            "UserPoolId": "us-west-2_EXAMPLE"
```

```
        }
    ]
}
```

Para obtener más información, consulte Clientes de la aplicación en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte ListUserPoolClients en la Referencia de comandos de la AWS CLI.

`list-user-pools`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-user-pools`.

AWS CLI

Para mostrar los grupos de usuarios

En el siguiente ejemplo de `list-user-pools`, se muestran 3 de los grupos de usuarios disponibles en la cuenta de AWS de las credenciales de la CLI actuales.

```
aws cognito-idp list-user-pools \
    --max-results 3
```

Salida:

```
{
    "NextToken": "[Pagination token]",
    "UserPools": [
        {
            "CreationDate": 1681502497.741,
            "Id": "us-west-2_EXAMPLE1",
            "LambdaConfig": {
                "CustomMessage": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
                "PreSignUp": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
                "PreTokenGeneration": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
                "PreTokenGenerationConfig": {
                    "LambdaArn": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
                    "LambdaVersion": "V1_0"
```

```
                }
            },
            "LastModifiedDate": 1681502497.741,
            "Name": "user pool 1"
        },
        {
            "CreationDate": 1686064178.717,
            "Id": "us-west-2_EXAMPLE2",
            "LambdaConfig": {
            },
            "LastModifiedDate": 1686064178.873,
            "Name": "user pool 2"
        },
        {
            "CreationDate": 1627681712.237,
            "Id": "us-west-2_EXAMPLE3",
            "LambdaConfig": {
                "UserMigration": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction"
            },
            "LastModifiedDate": 1678486942.479,
            "Name": "user pool 3"
        }
    ]
}
```

Para obtener más información, consulte Grupos de usuarios de Amazon Cognito en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles de la API, consulte ListUserPools en la Referencia de comandos de la AWS CLI.

`list-users-in-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-users-in-group`.

AWS CLI

Para enumerar los usuarios de un grupo

En este ejemplo, se enumeran los usuarios del grupo MyGroup.

Comando:

```
aws cognito-idp list-users-in-group --user-pool-id us-west-2_aaaaaaaaa --group-
name MyGroup
```

Salida:

```
{
  "Users": [
      {
          "Username": "acf10624-80bb-401a-ac61-607bee2110ec",
          "Attributes": [
              {
                  "Name": "sub",
                  "Value": "acf10624-80bb-401a-ac61-607bee2110ec"
              },
              {
                  "Name": "custom:CustomAttr1",
                  "Value": "New Value!"
              },
              {
                  "Name": "email",
                  "Value": "jane@example.com"
              }
          ],
          "UserCreateDate": 1548102770.284,
          "UserLastModifiedDate": 1548103204.893,
          "Enabled": true,
          "UserStatus": "CONFIRMED"
      },
      {
          "Username": "22704aa3-fc10-479a-97eb-2af5806bd327",
          "Attributes": [
              {
                  "Name": "sub",
                  "Value": "22704aa3-fc10-479a-97eb-2af5806bd327"
              },
              {
                  "Name": "email_verified",
                  "Value": "true"
              },
              {
                  "Name": "email",
                  "Value": "diego@example.com"
              }
```

```
            ],
            "UserCreateDate": 1548089817.683,
            "UserLastModifiedDate": 1548089817.683,
            "Enabled": true,
            "UserStatus": "FORCE_CHANGE_PASSWORD"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte ListUsersInGroup en la Referencia de comandos de la AWS CLI.

`list-users`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-users`.

AWS CLI

Ejemplo 1: muestra de usuarios con un filtro del servidor

En el siguiente ejemplo de `list-users`, se muestran 3 usuarios del grupo de usuarios solicitado cuyas direcciones de correo electrónico comienzan por `testuser`.

```
aws cognito-idp list-users \
    --user-pool-id us-west-2_EXAMPLE \
    --filter email^=\"testuser\" \
    --max-items 3
```

Salida:

```
{
    "PaginationToken": "efgh5678EXAMPLE",
    "Users": [
        {
            "Attributes": [
                {
                    "Name": "sub",
                    "Value": "eaad0219-2117-439f-8d46-4db20e59268f"
                },
                {
                    "Name": "email",
                    "Value": "testuser@example.com"
```

```
            }
        ],
        "Enabled": true,
        "UserCreateDate": 1682955829.578,
        "UserLastModifiedDate": 1689030181.63,
        "UserStatus": "CONFIRMED",
        "Username": "testuser"
    },
    {
        "Attributes": [
            {
                "Name": "sub",
                "Value": "3b994cfd-0b07-4581-be46-3c82f9a70c90"
            },
            {
                "Name": "email",
                "Value": "testuser2@example.com"
            }
        ],
        "Enabled": true,
        "UserCreateDate": 1684427979.201,
        "UserLastModifiedDate": 1684427979.201,
        "UserStatus": "UNCONFIRMED",
        "Username": "testuser2"
    },
    {
        "Attributes": [
            {
                "Name": "sub",
                "Value": "5929e0d1-4c34-42d1-9b79-a5ecacfe66f7"
            },
            {
                "Name": "email",
                "Value": "testuser3@example.com"
            }
        ],
        "Enabled": true,
        "UserCreateDate": 1684427823.641,
        "UserLastModifiedDate": 1684427823.641,
        "UserStatus": "UNCONFIRMED",
        "Username": "testuser3@example.com"
    }
]
```

```
}
```

Para obtener más información, consulte Administración y búsqueda de usuarios en la Guía para desarrolladores de Amazon Cognito.

Ejemplo 2: muestra de usuarios con un filtro del cliente

En el siguiente ejemplo de `list-users`, se muestran los atributos de tres usuarios que tienen un atributo, en este caso su dirección de correo electrónico, que contiene el dominio de correo electrónico "@example.com". Si otros atributos contuvieran esta cadena, también se mostrarían. El segundo usuario no tiene atributos que coincidan con la consulta y se excluye del resultado mostrado, pero no de la respuesta del servidor.

```
aws cognito-idp list-users \
    --user-pool-id us-west-2_EXAMPLE \
    --max-items 3
    --query Users\[\*\].Attributes\[\?Value\.contains\(\@\,\'@example.com\'\)\]
```

Salida:

```
[
    [
        {
            "Name": "email",
            "Value": "admin@example.com"
        }
    ],
    [],
    [
        {
            "Name": "email",
            "Value": "operator@example.com"
        }
    ]
]
```

Para obtener más información, consulte Administración y búsqueda de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte ListUsers en la Referencia de comandos de la AWS CLI.

`list-web-authn-credentials`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-web-authn-credentials`.

AWS CLI

Muestra de las credenciales de clave de acceso

En el siguiente ejemplo de `list-web-authn-credentials`, se muestran las credenciales de la clave de acceso o WebAuthn del usuario actual. Tienen un dispositivo registrado.

```
aws cognito-idp list-web-authn-credentials \
    --access-token eyJra456defEXAMPLE
```

Salida:

```
{
    "Credentials": [
        {
            "AuthenticatorAttachment": "cross-platform",
            "CreatedAt": 1736293876.115,
            "CredentialId": "8LApgk4-lNUFHbhm2w6Und7-
uxcc8coJGsPxiogvHoItc64xWQc3r4CEXAMPLE",
            "FriendlyCredentialName": "Roaming passkey",
            "RelyingPartyId": "auth.example.com"
        }
    ]
}
```

Para obtener más información, consulte Inicio de sesión de clave de acceso en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte ListWebAuthnCredentials en la Referencia de comandos de la AWS CLI.

`resend-confirmation-code`

En el siguiente ejemplo de código, se muestra cómo utilizar `resend-confirmation-code`.

AWS CLI

Para reenviar un código de confirmación

En el siguiente ejemplo `resend-confirmation-code`, se envía un código de confirmación al usuario `jane`.

```
aws cognito-idp resend-confirmation-code \
    --client-id 12a3b456c7de890f11g123hijk \
    --username jane
```

Salida:

```
{
    "CodeDeliveryDetails": {
        "Destination": "j***@e***.com",
        "DeliveryMedium": "EMAIL",
        "AttributeName": "email"
    }
}
```

Para obtener más información, consulte Inscripción y confirmación de cuentas de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles de la API, consulte ResendConfirmationCode en la Referencia de comandos de la AWS CLI.

`respond-to-auth-challenge`

En el siguiente ejemplo de código, se muestra cómo utilizar `respond-to-auth-challenge`.

AWS CLI

Ejemplo 1: respuesta a un desafío NEW_PASSWORD_REQUIRED

En el siguiente ejemplo de `respond-to-auth-challenge`, se responde a un desafío NEW_PASSWORD_REQUIRED devuelto por initiate-auth. Establece una contraseña para el usuario `jane@example.com`.

```
aws cognito-idp respond-to-auth-challenge \
    --client-id 1example23456789 \
    --challenge-name NEW_PASSWORD_REQUIRED \
    --challenge-responses USERNAME=jane@example.com,NEW_PASSWORD=[Password] \
    --session AYABeEv5HklEXAMPLE
```

Salida:

```
{
    "ChallengeParameters": {},
    "AuthenticationResult": {
        "AccessToken": "ACCESS_TOKEN",
        "ExpiresIn": 3600,
        "TokenType": "Bearer",
        "RefreshToken": "REFRESH_TOKEN",
        "IdToken": "ID_TOKEN",
        "NewDeviceMetadata": {
            "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "DeviceGroupKey": "-wt2ha1Zd"
        }
    }
}
```

Para obtener más información, consulte Autenticación en la Guía para desarrolladores de Amazon Cognito.

Ejemplo 2: respuesta a un desafío SELECT_MFA_TYPE

En el siguiente ejemplo de `respond-to-auth-challenge`, se elige TOTP MFA como opción de MFA para el usuario actual. Se solicitó al usuario que seleccionara un tipo de MFA y, a continuación, se le pedirá que ingrese su código de MFA.

```
aws cognito-idp respond-to-auth-challenge \
    --client-id 1example23456789
    --session AYABeEv5HklEXAMPLE
    --challenge-name SELECT_MFA_TYPE
    --challenge-responses USERNAME=testuser,ANSWER=SOFTWARE_TOKEN_MFA
```

Salida:

```
{
    "ChallengeName": "SOFTWARE_TOKEN_MFA",
    "Session": "AYABeEv5HklEXAMPLE",
    "ChallengeParameters": {
        "FRIENDLY_DEVICE_NAME": "transparent"
    }
}
```

Para obtener más información, consulte Agregación de MFA en la Guía para desarrolladores de Amazon Cognito.

Ejemplo 3: respuesta a un desafío SOFTWARE_TOKEN_MFA

En el siguiente ejemplo de `respond-to-auth-challenge`, se proporciona un código MFA con TOTP y se completa el inicio de sesión.

```
aws cognito-idp respond-to-auth-challenge \
    --client-id 1example23456789 \
    --session AYABeEv5HklEXAMPLE \
    --challenge-name SOFTWARE_TOKEN_MFA \
    --challenge-responses USERNAME=testuser,SOFTWARE_TOKEN_MFA_CODE=123456
```

Salida:

```
{
    "AuthenticationResult": {
        "AccessToken": "eyJra456defEXAMPLE",
        "ExpiresIn": 3600,
        "TokenType": "Bearer",
        "RefreshToken": "eyJra123abcEXAMPLE",
        "IdToken": "eyJra789ghiEXAMPLE",
        "NewDeviceMetadata": {
            "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "DeviceGroupKey": "-v7w9UcY6"
        }
    }
}
```

Para obtener más información, consulte Agregación de MFA en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles de la API, consulte RespondToAuthChallenge en la Referencia de comandos de la AWS CLI.

`revoke-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `revoke-token`.

AWS CLI

Revocación de un token de actualización

El siguiente `revoke-token` revoca el token de actualización solicitado y los tokens de acceso asociados.

```
aws cognito-idp revoke-token \
    --token eyJjd123abcEXAMPLE \
    --client-id 1example23456789
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Revocación de tokens en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte RevokeToken en la Referencia de comandos de la AWS CLI.

`set-log-delivery-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-log-delivery-configuration`.

AWS CLI

Configuración de la exportación de registros desde un grupo de usuarios

En el siguiente ejemplo de `set-log-delivery-configuration`, se configura el grupo de usuarios solicitado con el registro de errores de las notificaciones de usuario en un grupo de registros y el registro de la información de autenticación del usuario en un bucket de S3.

```
aws cognito-idp set-log-delivery-configuration \
    --user-pool-id us-west-2_EXAMPLE \
    --log-
configurations LogLevel=ERROR,EventSource=userNotification,CloudWatchLogsConfiguration={LogG
west-2:123456789012:log-group:cognito-
exported} LogLevel=INFO,EventSource=userAuthEvents,S3Configuration={BucketArn=arn:aws:s3:::a
s3-demo-bucket1}
```

Salida:

```
{
```

```
   "LogDeliveryConfiguration": {
        "LogConfigurations": [
            {
                "CloudWatchLogsConfiguration": {
                    "LogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:cognito-exported"
                },
                "EventSource": "userNotification",
                "LogLevel": "ERROR"
            },
            {
                "EventSource": "userAuthEvents",
                "LogLevel": "INFO",
                "S3Configuration": {
                    "BucketArn": "arn:aws:s3:::amzn-s3-demo-bucket1"
                }
            }
        ],
        "UserPoolId": "us-west-2_EXAMPLE"
   }
}
```

Para obtener más información, consulte Exportación de registros del grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte SetLogDeliveryConfiguration en la Referencia de comandos de la AWS CLI.

`set-risk-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-risk-configuration`.

AWS CLI

Establecimiento de la configuración de riesgos de protección contra amenazas

En el siguiente ejemplo de `set-risk-configuration`, se configuran los mensajes y las acciones de protección contra amenazas, las credenciales comprometidas y las excepciones de direcciones IP en el cliente de aplicación solicitado. Debido a la complejidad del objeto NotifyConfiguration, se recomienda utilizar JSON como entrada para este comando.

```
aws cognito-idp set-risk-configuration \
```

```
    --cli-input-json file://set-risk-configuration.json
```

Contenido de `set-risk-configuration.json`:

```
{
    "AccountTakeoverRiskConfiguration": {
        "Actions": {
            "HighAction": {
                "EventAction": "MFA_REQUIRED",
                "Notify": true
            },
            "LowAction": {
                "EventAction": "NO_ACTION",
                "Notify": true
            },
            "MediumAction": {
                "EventAction": "MFA_IF_CONFIGURED",
                "Notify": true
            }
        },
        "NotifyConfiguration": {
            "BlockEmail": {
                "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML
 email context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We
 blocked an unrecognized sign-in to your account with this information:\n<ul>
\n<li>Time: {login-time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city},
 {country}</li>\n</ul>\nIf this sign-in was not by you, you should change your
 password and notify us by clicking on <a href={one-click-link-invalid}>this link</
a>\nIf this sign-in was by you, you can follow <a href={one-click-link-valid}>this
 link</a> to let us know</pre>\n</body>\n</html>",
                "Subject": "Blocked sign-in attempt",
                "TextBody": "We blocked an unrecognized sign-in to your account with
 this information:\nTime: {login-time}\nDevice: {device-name}\nLocation: {city},
 {country}\nIf this sign-in was not by you, you should change your password and
 notify us by clicking on {one-click-link-invalid}\nIf this sign-in was by you, you
 can follow {one-click-link-valid} to let us know"
            },
            "From": "admin@example.com",
            "MfaEmail": {
                "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML email
 context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We required
 you to use multi-factor authentication for the following sign-in attempt:\n<ul>
\n<li>Time: {login-time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city},
```

```
 {country}</li>\n</ul>\nIf this sign-in was not by you, you should change your
 password and notify us by clicking on <a href={one-click-link-invalid}>this link</
a>\nIf this sign-in was by you, you can follow <a href={one-click-link-valid}>this
 link</a> to let us know</pre>\n</body>\n</html>",
                "Subject": "New sign-in attempt",
                "TextBody": "We required you to use multi-factor authentication
 for the following sign-in attempt:\nTime: {login-time}\nDevice: {device-
name}\nLocation: {city}, {country}\nIf this sign-in was not by you, you should
 change your password and notify us by clicking on {one-click-link-invalid}\nIf this
 sign-in was by you, you can follow {one-click-link-valid} to let us know"
            },
            "NoActionEmail": {
                "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML
 email context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We
 observed an unrecognized sign-in to your account with this information:\n<ul>
\n<li>Time: {login-time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city},
 {country}</li>\n</ul>\nIf this sign-in was not by you, you should change your
 password and notify us by clicking on <a href={one-click-link-invalid}>this link</
a>\nIf this sign-in was by you, you can follow <a href={one-click-link-valid}>this
 link</a> to let us know</pre>\n</body>\n</html>",
                "Subject": "New sign-in attempt",
                "TextBody": "We observed an unrecognized sign-in to your account
 with this information:\nTime: {login-time}\nDevice: {device-name}\nLocation:
 {city}, {country}\nIf this sign-in was not by you, you should change your password
 and notify us by clicking on {one-click-link-invalid}\nIf this sign-in was by you,
 you can follow {one-click-link-valid} to let us know"
            },
            "ReplyTo": "admin@example.com",
            "SourceArn": "arn:aws:ses:us-west-2:123456789012:identity/
admin@example.com"
        }
    },
    "ClientId": "1example23456789",
    "CompromisedCredentialsRiskConfiguration": {
        "Actions": {
            "EventAction": "BLOCK"
        },
        "EventFilter": [
            "PASSWORD_CHANGE",
            "SIGN_UP",
            "SIGN_IN"
        ]
    },
    "RiskExceptionConfiguration": {
```

```
        "BlockedIPRangeList": [
            "192.0.2.1/32",
            "192.0.2.2/32"
        ],
        "SkippedIPRangeList": [
            "203.0.113.1/32",
            "203.0.113.2/32"
        ]
    },
    "UserPoolId": "us-west-2_EXAMPLE"
}
```

Salida:

```
{
    "RiskConfiguration": {
        "AccountTakeoverRiskConfiguration": {
            "Actions": {
                "HighAction": {
                    "EventAction": "MFA_REQUIRED",
                    "Notify": true
                },
                "LowAction": {
                    "EventAction": "NO_ACTION",
                    "Notify": true
                },
                "MediumAction": {
                    "EventAction": "MFA_IF_CONFIGURED",
                    "Notify": true
                }
            },
            "NotifyConfiguration": {
                "BlockEmail": {
                    "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML
 email context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We
 blocked an unrecognized sign-in to your account with this information:\n<ul>
\n<li>Time: {login-time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city},
 {country}</li>\n</ul>\nIf this sign-in was not by you, you should change your
 password and notify us by clicking on <a href={one-click-link-invalid}>this link</
a>\nIf this sign-in was by you, you can follow <a href={one-click-link-valid}>this
 link</a> to let us know</pre>\n</body>\n</html>",
                    "Subject": "Blocked sign-in attempt",
```

```
                    "TextBody": "We blocked an unrecognized sign-in to your account
 with this information:\nTime: {login-time}\nDevice: {device-name}\nLocation:
 {city}, {country}\nIf this sign-in was not by you, you should change your password
 and notify us by clicking on {one-click-link-invalid}\nIf this sign-in was by you,
 you can follow {one-click-link-valid} to let us know"
                },
                "From": "admin@example.com",
                "MfaEmail": {
                    "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML
 email context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We
 required you to use multi-factor authentication for the following sign-in attempt:
\n<ul>\n<li>Time: {login-time}</li>\n<li>Device: {device-name}</li>\n<li>Location:
 {city}, {country}</li>\n</ul>\nIf this sign-in was not by you, you should change
 your password and notify us by clicking on <a href={one-click-link-invalid}>this
 link</a>\nIf this sign-in was by you, you can follow <a href={one-click-link-
valid}>this link</a> to let us know</pre>\n</body>\n</html>",
                    "Subject": "New sign-in attempt",
                    "TextBody": "We required you to use multi-factor authentication
 for the following sign-in attempt:\nTime: {login-time}\nDevice: {device-
name}\nLocation: {city}, {country}\nIf this sign-in was not by you, you should
 change your password and notify us by clicking on {one-click-link-invalid}\nIf this
 sign-in was by you, you can follow {one-click-link-valid} to let us know"
                },
                "NoActionEmail": {
                    "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML
 email context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We
 observed an unrecognized sign-in to your account with this information:\n<ul>
\n<li>Time: {login-time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city},
 {country}</li>\n</ul>\nIf this sign-in was not by you, you should change your
 password and notify us by clicking on <a href={one-click-link-invalid}>this link</
a>\nIf this sign-in was by you, you can follow <a href={one-click-link-valid}>this
 link</a> to let us know</pre>\n</body>\n</html>",
                    "Subject": "New sign-in attempt",
                    "TextBody": "We observed an unrecognized sign-in to your account
 with this information:\nTime: {login-time}\nDevice: {device-name}\nLocation:
 {city}, {country}\nIf this sign-in was not by you, you should change your password
 and notify us by clicking on {one-click-link-invalid}\nIf this sign-in was by you,
 you can follow {one-click-link-valid} to let us know"
                },
                "ReplyTo": "admin@example.com",
                "SourceArn": "arn:aws:ses:us-west-2:123456789012:identity/
admin@example.com"
            }
        },
```

```
        "ClientId": "1example23456789",
        "CompromisedCredentialsRiskConfiguration": {
            "Actions": {
                "EventAction": "BLOCK"
            },
            "EventFilter": [
                "PASSWORD_CHANGE",
                "SIGN_UP",
                "SIGN_IN"
            ]
        },
        "RiskExceptionConfiguration": {
            "BlockedIPRangeList": [
                "192.0.2.1/32",
                "192.0.2.2/32"
            ],
            "SkippedIPRangeList": [
                "203.0.113.1/32",
                "203.0.113.2/32"
            ]
        },
        "UserPoolId": "us-west-2_EXAMPLE"
    }
}
```

Para obtener más información, consulte Protección contra amenazas en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte SetRiskConfiguration en la Referencia de comandos de la AWS CLI.

`set-ui-customization`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-ui-customization`.

AWS CLI

Ejemplo 1: personalización de la interfaz de usuario alojada clásica para un cliente de aplicación

En el siguiente ejemplo de `set-ui-customization`, se configura el cliente de aplicación solicitado con un CSS personalizado y con el logotipo de Amazon Cognito como logotipo de la aplicación.

```
aws cognito-idp set-ui-customization \
    --user-pool-id us-west-2_ywDJHlIfU \
    --client-id 14pq32c5q2uq2q7keorloqvb23 \
    --css ".logo-customizable {\n\tmax-width: 60%;\n\tmax-height: 30%;\n}\n.banner-
customizable {\n\tpadding: 25px 0px 25px 0px;\n\tbackground-color: lightgray;
\n}\n.label-customizable {\n\tfont-weight: 400;\n}\n.textDescription-customizable
 {\n\tpadding-top: 10px;\n\tpadding-bottom: 10px;\n\tdisplay: block;\n\tfont-
size: 16px;\n}\n.idpDescription-customizable {\n\tpadding-top: 10px;\n\tpadding-
bottom: 10px;\n\tdisplay: block;\n\tfont-size: 16px;\n}\n.legalText-customizable
 {\n\tcolor: #747474;\n\tfont-size: 11px;\n}\n.submitButton-customizable {\n\tfont-
size: 11px;\n\tfont-weight: normal;\n\tmargin: 20px -15px 10px -13px;\n\theight:
 40px;\n\twidth: 108%;\n\tcolor: #fff;\n\tbackground-color: #337ab7;\n\ttext-align:
 center;\n}\n.submitButton-customizable:hover {\n\tcolor: #fff;\n\tbackground-color:
 #286090;\n}\n.errorMessage-customizable {\n\tpadding: 5px;\n\tfont-size: 14px;
\n\twidth: 100%;\n\tbackground: #F5F5F5;\n\tborder: 2px solid #D64958;\n\tcolor:
 #D64958;\n}\n.inputField-customizable {\n\twidth: 100%;\n\theight: 34px;\n\tcolor:
 #555;\n\tbackground-color: #fff;\n\tborder: 1px solid #ccc;\n\tborder-radius:
 0px;\n}\n.inputField-customizable:focus {\n\tborder-color: #66afe9;\n\toutline:
 0;\n}\n.idpButton-customizable {\n\theight: 40px;\n\twidth: 100%;\n\twidth: 100%;
\n\ttext-align: center;\n\tmargin-bottom: 15px;\n\tcolor: #fff;\n\tbackground-
color: #5bc0de;\n\tborder-color: #46b8da;\n}\n.idpButton-customizable:hover {\n
\tcolor: #fff;\n\tbackground-color: #31b0d5;\n}\n.socialButton-customizable {\n
\tborder-radius: 2px;\n\theight: 40px;\n\tmargin-bottom: 15px;\n\tpadding: 1px;
\n\ttext-align: left;\n\twidth: 100%;\n}\n.redirect-customizable {\n\ttext-
align: center;\n}\n.passwordCheck-notValid-customizable {\n\tcolor: #DF3312;
\n}\n.passwordCheck-valid-customizable {\n\tcolor: #19BF00;\n}\n.background-
customizable {\n\tbackground-color: #fff;\n}\n" \
    --image-
file iVBORw0KGgoAAAANSUhEUgAAAFAAAABQCAMAAAC5zwKfAAAAAXNSR0IArs4c6QAAAARnQU1BAACxjwv8YQUAAAA
Cmsfvm6f3y9P////fM0uqAj
+yNmu6ZpvnZ3eNabuFNYuZneehzhPKzvPTAxwAAAOiMMlkAAAASdFJOU/////////////////////
AOK/vxIAAAAJcEhZcwAADsMAAA7DAcdvqGQAAAKDSURBVFhH7ZfpkoMgEISDHKuEw/
d/2u2BQWMiBrG29o+fVsKatdPMAeZxc3Nz8w+ISekzmB++sYIw/I/
tjHzrPpO2Tx62EbR2PNxFac+jVuKxRaV50IzXkUe76NOCoUuwlvnQKei02gNF0ykotOLRBq/
nboeWRxAISx2EbsHFoRhK6Igk2JJlwScfQjgt06dOaWWiTbEDAe/
iq8N9kqCw2uCbHkHlYkaXEF8EYeL9RDqT4FhC6XMIIEifdcUwCc4leNyhabadWU6OlKYJE1Oac3NSPhB5rlaXlSgmr/1
F0L6Q5pZiSG0SfZTSTCOUhxOCH1AdIoCpTTIjtd
+VpEjUDDytQH/0Fpc661Aisas/4qmyUItD557pSCOSQQzlx27J
+meyDGc5zZgfhWuXE1lGgmVOMwmWdeGdzhjqZV14x5vSj7vsC5JDz/Cl0Vhp56n2NQt1wQIpury1EPbwyaYm
+IhmAQKoajkH51wg4cMZ1wQ3QG9efKWWOaDhYWnU6jXjCMdRmm21PArI
+Pb5DYoH93hq0ZCPlxeGJho/DI15C6sQc/L2sTC47UFBKZGHT6k+zlXg7WebA0Nr0HTcLMfk/
Y4Rc65D3iG6WDd7YLSlVqk87bVhUwhnClrx11RsVQwlAA818Mn
+QEs71BhSFU6orsUfKhHp72XMGYXi4q9c64RXRvzkWurRfG2vI2be/VaNcNgpX0Evb/
```

```
vio7nPMmj5qujkpQgSaPd1UcVqciHFDNZpOcGlcOPyi+AamCbIL9fitxAGeFN2Dl
+3vZubm5u/4fH4Bd14HhIPdwZPAAAAAElFTkSuQmCC
```

Salida:

```
{
    "UICustomization": {
        "UserPoolId": "us-west-2_ywDJHlIfU",
        "ClientId": "14pq32c5q2uq2q7keorloqvb23",
        "ImageUrl": "https://
cf.thewrong.club/14pq32c5q2uq2q7keorloqvb23/20250117005911/assets/images/image.jpg",
        "CSS": ".logo-customizable {\n\tmax-width: 60%;\n\tmax-height: 30%;
\n}\n.banner-customizable {\n\tpadding: 25px 0px 25px 0px;\n\tbackground-color:
 lightgray;\n}\n.label-customizable {\n\tfont-weight: 400;\n}\n.textDescription-
customizable {\n\tpadding-top: 10px;\n\tpadding-bottom: 10px;\n\tdisplay: block;
\n\tfont-size: 16px;\n}\n.idpDescription-customizable {\n\tpadding-top: 10px;\n
\tpadding-bottom: 10px;\n\tdisplay: block;\n\tfont-size: 16px;\n}\n.legalText-
customizable {\n\tcolor: #747474;\n\tfont-size: 11px;\n}\n.submitButton-customizable
 {\n\tfont-size: 11px;\n\tfont-weight: normal;\n\tmargin: 20px -15px 10px -13px;
\n\theight: 40px;\n\twidth: 108%;\n\tcolor: #fff;\n\tbackground-color: #337ab7;
\n\ttext-align: center;\n}\n.submitButton-customizable:hover {\n\tcolor: #fff;
\n\tbackground-color: #286090;\n}\n.errorMessage-customizable {\n\tpadding:
 5px;\n\tfont-size: 14px;\n\twidth: 100%;\n\tbackground: #F5F5F5;\n\tborder:
 2px solid #D64958;\n\tcolor: #D64958;\n}\n.inputField-customizable {\n\twidth:
 100%;\n\theight: 34px;\n\tcolor: #555;\n\tbackground-color: #fff;\n\tborder:
 1px solid #ccc;\n\tborder-radius: 0px;\n}\n.inputField-customizable:focus {\n
\tborder-color: #66afe9;\n\toutline: 0;\n}\n.idpButton-customizable {\n\theight:
 40px;\n\twidth: 100%;\n\twidth: 100%;\n\ttext-align: center;\n\tmargin-bottom:
 15px;\n\tcolor: #fff;\n\tbackground-color: #5bc0de;\n\tborder-color: #46b8da;
\n}\n.idpButton-customizable:hover {\n\tcolor: #fff;\n\tbackground-color: #31b0d5;
\n}\n.socialButton-customizable {\n\tborder-radius: 2px;\n\theight: 40px;\n\tmargin-
bottom: 15px;\n\tpadding: 1px;\n\ttext-align: left;\n\twidth: 100%;\n}\n.redirect-
customizable {\n\ttext-align: center;\n}\n.passwordCheck-notValid-customizable
 {\n\tcolor: #DF3312;\n}\n.passwordCheck-valid-customizable {\n\tcolor: #19BF00;
\n}\n.background-customizable {\n\tbackground-color: #fff;\n}\n",
        "CSSVersion": "20250117005911"
    }
}
```

Ejemplo 2: establecimiento de la personalización de la interfaz de usuario predeterminada para todos los clientes de la aplicación

En el siguiente ejemplo de `set-ui-customization`, se configura el grupo de usuarios solicitado para todos los clientes de la aplicación que no tienen una configuración específica para cada cliente. El comando aplica algunos CSS personalizados y con el logotipo de Amazon Cognito como logotipo de la aplicación.

```
aws cognito-idp set-ui-customization \
--user-pool-id us-west-2_ywDJHlIfU \
--client-id ALL \
--css ".logo-customizable {\n\tmax-width: 60%;\n\tmax-height: 30%;\n}\n.banner-
customizable {\n\tpadding: 25px 0px 25px 0px;\n\tbackground-color: lightgray;
\n}\n.label-customizable {\n\tfont-weight: 400;\n}\n.textDescription-customizable
 {\n\tpadding-top: 10px;\n\tpadding-bottom: 10px;\n\tdisplay: block;\n\tfont-
size: 16px;\n}\n.idpDescription-customizable {\n\tpadding-top: 10px;\n\tpadding-
bottom: 10px;\n\tdisplay: block;\n\tfont-size: 16px;\n}\n.legalText-customizable
 {\n\tcolor: #747474;\n\tfont-size: 11px;\n}\n.submitButton-customizable {\n\tfont-
size: 11px;\n\tfont-weight: normal;\n\tmargin: 20px -15px 10px -13px;\n\theight:
 40px;\n\twidth: 108%;\n\tcolor: #fff;\n\tbackground-color: #337ab7;\n\ttext-align:
 center;\n}\n.submitButton-customizable:hover {\n\tcolor: #fff;\n\tbackground-color:
 #286090;\n}\n.errorMessage-customizable {\n\tpadding: 5px;\n\tfont-size: 14px;
\n\twidth: 100%;\n\tbackground: #F5F5F5;\n\tborder: 2px solid #D64958;\n\tcolor:
 #D64958;\n}\n.inputField-customizable {\n\twidth: 100%;\n\theight: 34px;\n\tcolor:
 #555;\n\tbackground-color: #fff;\n\tborder: 1px solid #ccc;\n\tborder-radius:
 0px;\n}\n.inputField-customizable:focus {\n\tborder-color: #66afe9;\n\toutline:
 0;\n}\n.idpButton-customizable {\n\theight: 40px;\n\twidth: 100%;\n\twidth: 100%;
\n\ttext-align: center;\n\tmargin-bottom: 15px;\n\tcolor: #fff;\n\tbackground-
color: #5bc0de;\n\tborder-color: #46b8da;\n}\n.idpButton-customizable:hover {\n
\tcolor: #fff;\n\tbackground-color: #31b0d5;\n}\n.socialButton-customizable {\n
\tborder-radius: 2px;\n\theight: 40px;\n\tmargin-bottom: 15px;\n\tpadding: 1px;
\n\ttext-align: left;\n\twidth: 100%;\n}\n.redirect-customizable {\n\ttext-
align: center;\n}\n.passwordCheck-notValid-customizable {\n\tcolor: #DF3312;
\n}\n.passwordCheck-valid-customizable {\n\tcolor: #19BF00;\n}\n.background-
customizable {\n\tbackground-color: #fff;\n}\n" \
--image-
file iVBORw0KGgoAAAANSUhEUgAAAFAAAABQCAMAAAC5zwKfAAAAAXNSR0IArs4c6QAAAARnQU1BAACxjwv8YQUAAAA
Cmsfvm6f3y9P////fM0uqAj
+yNmu6ZpvnZ3eNabuFNYuZneehzhPKzvPTAxwAAAOiMMlkAAAASdFJOU/////////////////////
AOK/vxIAAAAJcEhZcwAADsMAAA7DAcdvqGQAAAKDSURBVFhH7ZfpkoMgEISDHKuEw/
d/2u2BQWMiBrG29o+fVsKatdPMAeZxc3Nz8w+ISekzmB++sYIw/I/
tjHzrPpO2Tx62EbR2PNxFac+jVuKxRaV50IzXkUe76NOCoUuwlvnQKei02gNF0ykotOLRBq/
nboeWRxAISx2EbsHFoRhK6Igk2JJlwScfQjgt06dOaWWiTbEDAe/
iq8N9kqCw2uCbHkHlYkaXEF8EYeL9RDqT4FhC6XMIIEifdcUwCc4leNyhabadWU6OlKYJE1Oac3NSPhB5rlaXlSgmr/1
F0L6Q5pZiSG0SfZTSTCOUhxOCH1AdIoCpTTIjtd
+VpEjUDDytQH/0Fpc661Aisas/4qmyUItD557pSCOSQQzlx27J
```

```
+meyDGc5zZgfhWuXE1lGgmVOMwmWdeGdzhjqZV14x5vSj7vsC5JDz/Cl0Vhp56n2NQt1wQIpury1EPbwyaYm
+IhmAQKoajkH51wg4cMZ1wQ3QG9efKWWOaDhYWnU6jXjCMdRmm21PArI
+Pb5DYoH93hq0ZCPlxeGJho/DI15C6sQc/L2sTC47UFBKZGHT6k+zlXg7WebA0Nr0HTcLMfk/
Y4Rc65D3iG6WDd7YLSlVqk87bVhUwhnClrx11RsVQwlAA818Mn
+QEs71BhSFU6orsUfKhHp72XMGYXi4q9c64RXRvzkWurRfG2vI2be/VaNcNgpX0Evb/
vio7nPMmj5qujkpQgSaPd1UcVqciHFDNZpOcGlcOPyi+AamCbIL9fitxAGeFN2Dl
+3vZubm5u/4fH4Bd14HhIPdwZPAAAAAElFTkSuQmCC
```

Salida:

```
{
    "UICustomization": {
        "UserPoolId": "us-west-2_ywDJHlIfU",
        "ClientId": "14pq32c5q2uq2q7keorloqvb23",
        "ImageUrl": "https://
cf.thewrong.club/14pq32c5q2uq2q7keorloqvb23/20250117005911/assets/images/image.jpg",
        "CSS": ".logo-customizable {\n\tmax-width: 60%;\n\tmax-height: 30%;
\n}\n.banner-customizable {\n\tpadding: 25px 0px 25px 0px;\n\tbackground-color:
 lightgray;\n}\n.label-customizable {\n\tfont-weight: 400;\n}\n.textDescription-
customizable {\n\tpadding-top: 10px;\n\tpadding-bottom: 10px;\n\tdisplay: block;
\n\tfont-size: 16px;\n}\n.idpDescription-customizable {\n\tpadding-top: 10px;\n
\tpadding-bottom: 10px;\n\tdisplay: block;\n\tfont-size: 16px;\n}\n.legalText-
customizable {\n\tcolor: #747474;\n\tfont-size: 11px;\n}\n.submitButton-customizable
 {\n\tfont-size: 11px;\n\tfont-weight: normal;\n\tmargin: 20px -15px 10px -13px;
\n\theight: 40px;\n\twidth: 108%;\n\tcolor: #fff;\n\tbackground-color: #337ab7;
\n\ttext-align: center;\n}\n.submitButton-customizable:hover {\n\tcolor: #fff;
\n\tbackground-color: #286090;\n}\n.errorMessage-customizable {\n\tpadding:
 5px;\n\tfont-size: 14px;\n\twidth: 100%;\n\tbackground: #F5F5F5;\n\tborder:
 2px solid #D64958;\n\tcolor: #D64958;\n}\n.inputField-customizable {\n\twidth:
 100%;\n\theight: 34px;\n\tcolor: #555;\n\tbackground-color: #fff;\n\tborder:
 1px solid #ccc;\n\tborder-radius: 0px;\n}\n.inputField-customizable:focus {\n
\tborder-color: #66afe9;\n\toutline: 0;\n}\n.idpButton-customizable {\n\theight:
 40px;\n\twidth: 100%;\n\twidth: 100%;\n\ttext-align: center;\n\tmargin-bottom:
 15px;\n\tcolor: #fff;\n\tbackground-color: #5bc0de;\n\tborder-color: #46b8da;
\n}\n.idpButton-customizable:hover {\n\tcolor: #fff;\n\tbackground-color: #31b0d5;
\n}\n.socialButton-customizable {\n\tborder-radius: 2px;\n\theight: 40px;\n\tmargin-
bottom: 15px;\n\tpadding: 1px;\n\ttext-align: left;\n\twidth: 100%;\n}\n.redirect-
customizable {\n\ttext-align: center;\n}\n.passwordCheck-notValid-customizable
 {\n\tcolor: #DF3312;\n}\n.passwordCheck-valid-customizable {\n\tcolor: #19BF00;
\n}\n.background-customizable {\n\tbackground-color: #fff;\n}\n",
        "CSSVersion": "20250117005911"
    }
}
```

Para obtener más información, consulte Marca de la interfaz de usuario alojada (clásica) en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte SetUiCustomization en la Referencia de comandos de la AWS CLI.

`set-user-mfa-preference`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-user-mfa-preference`.

AWS CLI

Configuración de una preferencia de MFA del usuario

En el siguiente ejemplo de `set-user-mfa-preference`, se configura al usuario actual para que utilice TOTP MFA y desactiva todos los demás factores de MFA.

```
aws cognito-idp set-user-mfa-preference \
    --access-token eyJra456defEXAMPLE \
    --software-token-mfa-settings Enabled=true,PreferredMfa=true \
    --sms-mfa-settings Enabled=false,PreferredMfa=false \
    --email-mfa-settings Enabled=false,PreferredMfa=false
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Agregación de MFA en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte SetUserMfaPreference en la Referencia de comandos de la AWS CLI.

`set-user-pool-mfa-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-user-pool-mfa-config`.

AWS CLI

Configuración de MFA y WebAuthn del grupo de usuarios

En el siguiente ejemplo de `set-user-pool-mfa-config`, se configura el grupo de usuarios solicitado con MFA opcional con todos los métodos de MFA disponibles y establece la configuración de WebAuthn.

```
aws cognito-idp set-user-pool-mfa-config \
    --user-pool-id us-west-2_EXAMPLE \
    --sms-mfa-configuration "SmsAuthenticationMessage=\"Your OTP for MFA or sign-
in: use {####}.\",SmsConfiguration={SnsCallerArn=arn:aws:iam::123456789012:role/
service-role/test-SMS-Role,ExternalId=a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111,SnsRegion=us-west-2}" \
    --software-token-mfa-configuration Enabled=true \
    --email-mfa-configuration "Message=\"Your OTP for MFA or sign-in: use
 {####}\",Subject=\"OTP test\"" \
    --mfa-configuration OPTIONAL \
    --web-authn-
configuration RelyingPartyId=auth.example.com,UserVerification=preferred
```

Salida:

```
{
    "EmailMfaConfiguration": {
        "Message": "Your OTP for MFA or sign-in: use {####}",
        "Subject": "OTP test"
    },
    "MfaConfiguration": "OPTIONAL",
    "SmsMfaConfiguration": {
        "SmsAuthenticationMessage": "Your OTP for MFA or sign-in: use {####}.",
        "SmsConfiguration": {
            "ExternalId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "SnsCallerArn": "arn:aws:iam::123456789012:role/service-role/test-SMS-
Role",
            "SnsRegion": "us-west-2"
        }
    },
    "SoftwareTokenMfaConfiguration": {
        "Enabled": true
    },
    "WebAuthnConfiguration": {
        "RelyingPartyId": "auth.example.com",
        "UserVerification": "preferred"
    }
}
```

Para obtener más información, consulte Agregación de MFA e Inicio de sesión de clave de acceso en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte SetUserPoolMfaConfig en la Referencia de comandos de la AWS CLI.

`set-user-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-user-settings`.

AWS CLI

Establecimiento de la configuración de usuario

En este ejemplo, se establece la preferencia de entrega de MFA en CORREO ELECTRÓNICO.

Comando:

```
aws cognito-idp set-user-settings --access-token ACCESS_TOKEN --mfa-
options DeliveryMedium=EMAIL
```

- Para obtener detalles sobre la API, consulte SetUserSettings en la Referencia de comandos de la AWS CLI.

`sign-up`

En el siguiente ejemplo de código, se muestra cómo utilizar `sign-up`.

AWS CLI

Para inscribir a un usuario

En este ejemplo, se registra jane@example.com.

Comando:

```
aws cognito-idp sign-up --client-id 3n4b5urk1ft4fl3mg5e62d9ado --
username jane@example.com --password PASSWORD --user-attributes
 Name="email",Value="jane@example.com" Name="name",Value="Jane"
```

Salida:

```
{
  "UserConfirmed": false,
  "UserSub": "e04d60a6-45dc-441c-a40b-e25a787d4862"
```

```
}
```

- Para obtener detalles de la API, consulte SignUp en la Referencia de comandos de la AWS CLI.

`start-user-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-user-import-job`.

AWS CLI

Inicio de un trabajo de importación

En el siguiente ejemplo de `start-user-import-job`, se inicia el trabajo de importación solicitado en el grupo de usuarios solicitado.

```
aws cognito-idp start-user-import-job \
    --user-pool-id us-west-2_EXAMPLE \
    --job-id import-mAgUtd8PMm
```

Salida:

```
{
    "UserImportJob": {
        "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/example-cloudwatch-
logs-role",
        "CreationDate": 1736442975.904,
        "FailedUsers": 0,
        "ImportedUsers": 0,
        "JobId": "import-mAgUtd8PMm",
        "JobName": "Customer import",
        "PreSignedUrl": "https://aws-cognito-idp-user-import-pdx.s3.us-
west-2.amazonaws.com/123456789012/us-west-2_EXAMPLE/import-mAgUtd8PMm?
X-Amz-Security-Token=[token]&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Date=20241226T193341Z&X-Amz-SignedHeaders=host%3Bx-amz-server-side-encryption&X-Amz-
Expires=899&X-Amz-Credential=[credential]&X-Amz-Signature=[signature]",
        "SkippedUsers": 0,
        "StartDate": 1736443020.081,
        "Status": "Pending",
        "UserPoolId": "us-west-2_EXAMPLE"
    }
}
```

Para obtener más información, consulte Importación de usuarios en un grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte StartUserImportJob en la Referencia de comandos de la AWS CLI.

`start-web-authn-registration`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-web-authn-registration`.

AWS CLI

Obtención de la información de registro de clave de acceso de un usuario que ha iniciado sesión

En el siguiente ejemplo de `start-web-authn-registration`, se generan las opciones de registro de WebAuthn para el usuario actual.

```
aws cognito-idp start-web-authn-registration \
    --access-token eyJra456defEXAMPLE
```

Salida:

```
{
    "CredentialCreationOptions": {
        "authenticatorSelection": {
            "requireResidentKey": true,
            "residentKey": "required",
            "userVerification": "preferred"
        },
        "challenge": "wxvbDicyqQqvF2EXAMPLE",
        "excludeCredentials": [
            {
                "id": "8LApgk4-lNUFHbhm2w6Und7-
uxcc8coJGsPxiogvHoItc64xWQc3r4CEXAMPLE",
                "type": "public-key"
            }
        ],
        "pubKeyCredParams": [
            {
                "alg": -7,
                "type": "public-key"
            },
```

```
            {
                "alg": -257,
                "type": "public-key"
            }
        ],
        "rp": {
            "id": "auth.example.com",
            "name": "auth.example.com"
        },
        "timeout": 60000,
        "user": {
            "displayName": "testuser",
            "id": "ZWFhZDAyMTktMjExNy00MzlmLThkNDYtNGRiMjBlNEXAMPLE",
            "name": "testuser"
        }
    }
}
```

Para obtener más información, consulte Inicio de sesión de clave de acceso en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte StartWebAuthnRegistration en la Referencia de comandos de la AWS CLI.

`stop-user-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-user-import-job`.

AWS CLI

Detención de un trabajo de importación

En el siguiente ejemplo de `stop-user-import-job`, se detiene la ejecución solicitada del trabajo de importación del usuario en el grupo de usuarios solicitado.

```
aws cognito-idp stop-user-import-job \
    --user-pool-id us-west-2_EXAMPLE \
    --job-id import-mAgUtd8PMm
```

Salida:

```
{
```

```
    "UserImportJob": {
        "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/example-cloudwatch-
logs-role",
        "CompletionDate": 1736443496.379,
        "CompletionMessage": "The Import Job was stopped by the developer.",
        "CreationDate": 1736443471.781,
        "FailedUsers": 0,
        "ImportedUsers": 0,
        "JobId": "import-mAgUtd8PMm",
        "JobName": "Customer import",
        "PreSignedUrl": "https://aws-cognito-idp-user-import-pdx.s3.us-
west-2.amazonaws.com/123456789012/us-west-2_EXAMPLE/import-mAgUtd8PMm?
X-Amz-Security-Token=[token]&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Date=20241226T193341Z&X-Amz-SignedHeaders=host%3Bx-amz-server-side-encryption&X-Amz-
Expires=899&X-Amz-Credential=[credential]&X-Amz-Signature=[signature]",
        "SkippedUsers": 0,
        "StartDate": 1736443494.154,
        "Status": "Stopped",
        "UserPoolId": "us-west-2_EXAMPLE"
    }
}
```

Para obtener más información, consulte Importación de usuarios en un grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte StopUserImportJob en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Etiquetado de un grupo de usuarios

En el siguiente ejemplo de `tag-resource`, se aplican las etiquetas `administrator` y `department` al grupo de usuarios solicitado.

```
aws cognito-idp tag-resource \
    --resource-arn arn:aws:cognito-idp:us-west-2:123456789012:userpool/us-
west-2_EXAMPLE \
```

```
    --tags administrator=Jie,tenant=ExampleCorp
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de Amazon Cognito en la Guía para desarrolladores de Amazon Cognito.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de etiquetas de un grupo de usuarios

En el siguiente ejemplo de `untag-resource`, se eliminan las etiquetas `administrator` y `department` del grupo de usuarios solicitado.

```
aws cognito-idp untag-resource \
    --resource-arn arn:aws:cognito-idp:us-west-2:767671399759:userpool/us-
west-2_l5cxwdm2K \
    --tag-keys administrator tenant
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de Amazon Cognito en la Guía para desarrolladores de Amazon Cognito.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-auth-event-feedback`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-auth-event-feedback`.

AWS CLI

Actualización de los comentarios sobre un evento de autenticación

En este ejemplo, se actualizan los comentarios sobre los eventos de autorización. Marca el evento como Válido.

Comando:

```
aws cognito-idp update-auth-event-feedback --user-pool-id us-west-2_aaaaaaaaa --
username diego@example.com --event-id EVENT_ID --feedback-token FEEDBACK_TOKEN --
feedback-value "Valid"
```

- Para obtener detalles sobre la API, consulte UpdateAuthEventFeedback en la Referencia de comandos de la AWS CLI.

`update-device-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-device-status`.

AWS CLI

Actualización del estado del dispositivo

En este ejemplo, se actualiza el estado de un dispositivo a not_remembered.

Comando:

```
aws cognito-idp update-device-status --access-token ACCESS_TOKEN --device-
key DEVICE_KEY --device-remembered-status "not_remembered"
```

- Para obtener detalles sobre la API, consulte UpdateDeviceStatus en la Referencia de comandos de la AWS CLI.

`update-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-group`.

AWS CLI

Actualización de un grupo

En este ejemplo, se actualizan la descripción y la prioridad de MyGroup.

Comando:

```
aws cognito-idp update-group --user-pool-id us-west-2_aaaaaaaaa --group-name MyGroup
 --description "New description" --precedence 2
```

Salida:

```
{
  "Group": {
      "GroupName": "MyGroup",
      "UserPoolId": "us-west-2_aaaaaaaaa",
      "Description": "New description",
      "RoleArn": "arn:aws:iam::111111111111:role/MyRole",
      "Precedence": 2,
      "LastModifiedDate": 1548800862.812,
      "CreationDate": 1548097827.125
  }
}
```

- Para obtener información sobre la API, consulte UpdateGroup en la Referencia de comandos de la AWS CLI.

`update-identity-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-identity-provider`.

AWS CLI

Actualización del proveedor de identidades de un grupo de usuarios

En el siguiente ejemplo de `update-identity-provider`, se actualiza el proveedor de OIDC "MyOIDCIdP" en el grupo de usuarios solicitado.

```
aws cognito-idp update-identity-provider \
    --cli-input-json file://update-identity-provider.json
```

Contenido de `update-identity-provider.json`:

```
{
   "AttributeMapping": {
            "email": "idp_email",
            "email_verified": "idp_email_verified",
```

```
            "username": "sub"
    },
    "CreationDate": 1.701129701653E9,
    "IdpIdentifiers": [
        "corp",
        "dev"
    ],
    "LastModifiedDate": 1.701129701653E9,
    "ProviderDetails": {
        "attributes_request_method": "GET",
        "attributes_url": "https://example.com/userInfo",
        "attributes_url_add_attributes": "false",
        "authorize_scopes": "openid profile",
        "authorize_url": "https://example.com/authorize",
        "client_id": "idpexampleclient123",
        "client_secret": "idpexamplesecret456",
        "jwks_uri": "https://example.com/.well-known/jwks.json",
        "oidc_issuer": "https://example.com",
        "token_url": "https://example.com/token"
    },
    "ProviderName": "MyOIDCIdP",
    "UserPoolId": "us-west-2_EXAMPLE"
}
```

Salida:

```
{
    "IdentityProvider": {
        "AttributeMapping": {
            "email": "idp_email",
            "email_verified": "idp_email_verified",
            "username": "sub"
        },
        "CreationDate": 1701129701.653,
        "IdpIdentifiers": [
            "corp",
            "dev"
        ],
        "LastModifiedDate": 1736444278.211,
        "ProviderDetails": {
            "attributes_request_method": "GET",
            "attributes_url": "https://example.com/userInfo",
            "attributes_url_add_attributes": "false",
```

```
            "authorize_scopes": "openid profile",
            "authorize_url": "https://example.com/authorize",
            "client_id": "idpexampleclient123",
            "client_secret": "idpexamplesecret456",
            "jwks_uri": "https://example.com/.well-known/jwks.json",
            "oidc_issuer": "https://example.com",
            "token_url": "https://example.com/token"
        },
        "ProviderName": "MyOIDCIdP",
        "ProviderType": "OIDC",
        "UserPoolId": "us-west-2_EXAMPLE"
    }
}
```

Para obtener más información, consulte Configuración de un dominio en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte UpdateIdentityProvider en la Referencia de comandos de la AWS CLI.

`update-managed-login-branding`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-managed-login-branding`.

AWS CLI

Actualización de un estilo de marca de inicio de sesión administrado

En el siguiente ejemplo de `update-managed-login-branding`, se actualiza el estilo de marca del cliente de aplicación solicitado.

```
aws cognito-idp update-managed-login-branding \
    --cli-input-json file://update-managed-login-branding.json
```

Contenido de `update-managed-login-branding.json`:

```
{
    "Assets": [
        {
            "Bytes":
 "PHN2ZyB3aWR0aD0iMjAwMDAiIGhlaWdodD0iNDAwIiB2aWV3Qm94PSIwIDAgMjAwMDAgNDAwIiBmaWxsPSJub25lIi
+CjxyZWN0IHdpZHRoPSIyMDAwMCIgaGVpZ2h0PSI0MDAiIGZpbGw9InVybCgjcGFpbnQwX2xpbmVhcl8xNzI1OV8yMzY
```

```
+CjxsaW5lYXJHcmFkaWVudCBpZD0icGFpbnQwX2xpbmVhcl8xNzI1OV8yMzY2NzQiIHgxPSItODk0LjI0OSIgeTE9IjE
+Cjwvc3ZnPgo=",
            "Category": "PAGE_FOOTER_BACKGROUND",
            "ColorMode": "DARK",
            "Extension": "SVG"
        }
    ],
    "ManagedLoginBrandingId": "63f30090-6b1f-4278-b885-2bbb81f8e545",
    "Settings": {
        "categories": {
            "auth": {
                "authMethodOrder": [
                    [
                        {
                            "display": "BUTTON",
                            "type": "FEDERATED"
                        },
                        {
                            "display": "INPUT",
                            "type": "USERNAME_PASSWORD"
                        }
                    ]
                ],
                "federation": {
                    "interfaceStyle": "BUTTON_LIST",
                    "order": [
                    ]
                }
            },
            "form": {
                "displayGraphics": true,
                "instructions": {
                    "enabled": false
                },
                "languageSelector": {
                    "enabled": false
                },
                "location": {
                    "horizontal": "CENTER",
                    "vertical": "CENTER"
                },
                "sessionTimerDisplay": "NONE"
            },
            "global": {
```

```
                "colorSchemeMode": "LIGHT",
                "pageFooter": {
                    "enabled": false
                },
                "pageHeader": {
                    "enabled": false
                },
                "spacingDensity": "REGULAR"
            },
            "signUp": {
                "acceptanceElements": [
                    {
                        "enforcement": "NONE",
                        "textKey": "en"
                    }
                ]
            }
        },
        "componentClasses": {
            "buttons": {
                "borderRadius": 8.0
            },
            "divider": {
                "darkMode": {
                    "borderColor": "232b37ff"
                },
                "lightMode": {
                    "borderColor": "ebebf0ff"
                }
            },
            "dropDown": {
                "borderRadius": 8.0,
                "darkMode": {
                    "defaults": {
                        "itemBackgroundColor": "192534ff"
                    },
                    "hover": {
                        "itemBackgroundColor": "081120ff",
                        "itemBorderColor": "5f6b7aff",
                        "itemTextColor": "e9ebedff"
                    },
                    "match": {
                        "itemBackgroundColor": "d1d5dbff",
                        "itemTextColor": "89bdeeff"
```

```
                    }
                },
                "lightMode": {
                    "defaults": {
                        "itemBackgroundColor": "ffffffff"
                    },
                    "hover": {
                        "itemBackgroundColor": "f4f4f4ff",
                        "itemBorderColor": "7d8998ff",
                        "itemTextColor": "000716ff"
                    },
                    "match": {
                        "itemBackgroundColor": "414d5cff",
                        "itemTextColor": "0972d3ff"
                    }
                }
            },
            "focusState": {
                "darkMode": {
                    "borderColor": "539fe5ff"
                },
                "lightMode": {
                    "borderColor": "0972d3ff"
                }
            },
            "idpButtons": {
                "icons": {
                    "enabled": true
                }
            },
            "input": {
                "borderRadius": 8.0,
                "darkMode": {
                    "defaults": {
                        "backgroundColor": "0f1b2aff",
                        "borderColor": "5f6b7aff"
                    },
                    "placeholderColor": "8d99a8ff"
                },
                "lightMode": {
                    "defaults": {
                        "backgroundColor": "ffffffff",
                        "borderColor": "7d8998ff"
                    },
```

```
                "placeholderColor": "5f6b7aff"
            }
        },
        "inputDescription": {
            "darkMode": {
                "textColor": "8d99a8ff"
            },
            "lightMode": {
                "textColor": "5f6b7aff"
            }
        },
        "inputLabel": {
            "darkMode": {
                "textColor": "d1d5dbff"
            },
            "lightMode": {
                "textColor": "000716ff"
            }
        },
        "link": {
            "darkMode": {
                "defaults": {
                    "textColor": "539fe5ff"
                },
                "hover": {
                    "textColor": "89bdeeff"
                }
            },
            "lightMode": {
                "defaults": {
                    "textColor": "0972d3ff"
                },
                "hover": {
                    "textColor": "033160ff"
                }
            }
        },
        "optionControls": {
            "darkMode": {
                "defaults": {
                    "backgroundColor": "0f1b2aff",
                    "borderColor": "7d8998ff"
                },
                "selected": {
```

```
                    "backgroundColor": "539fe5ff",
                    "foregroundColor": "000716ff"
                }
            },
            "lightMode": {
                "defaults": {
                    "backgroundColor": "ffffffff",
                    "borderColor": "7d8998ff"
                },
                "selected": {
                    "backgroundColor": "0972d3ff",
                    "foregroundColor": "ffffffff"
                }
            }
        },
        "statusIndicator": {
            "darkMode": {
                "error": {
                    "backgroundColor": "1a0000ff",
                    "borderColor": "eb6f6fff",
                    "indicatorColor": "eb6f6fff"
                },
                "pending": {
                    "indicatorColor": "AAAAAAAA"
                },
                "success": {
                    "backgroundColor": "001a02ff",
                    "borderColor": "29ad32ff",
                    "indicatorColor": "29ad32ff"
                },
                "warning": {
                    "backgroundColor": "1d1906ff",
                    "borderColor": "e0ca57ff",
                    "indicatorColor": "e0ca57ff"
                }
            },
            "lightMode": {
                "error": {
                    "backgroundColor": "fff7f7ff",
                    "borderColor": "d91515ff",
                    "indicatorColor": "d91515ff"
                },
                "pending": {
                    "indicatorColor": "AAAAAAAA"
```

```
                },
                "success": {
                    "backgroundColor": "f2fcf3ff",
                    "borderColor": "037f0cff",
                    "indicatorColor": "037f0cff"
                },
                "warning": {
                    "backgroundColor": "fffce9ff",
                    "borderColor": "8d6605ff",
                    "indicatorColor": "8d6605ff"
                }
            }
        }
    },
    "components": {
        "alert": {
            "borderRadius": 12.0,
            "darkMode": {
                "error": {
                    "backgroundColor": "1a0000ff",
                    "borderColor": "eb6f6fff"
                }
            },
            "lightMode": {
                "error": {
                    "backgroundColor": "fff7f7ff",
                    "borderColor": "d91515ff"
                }
            }
        },
        "favicon": {
            "enabledTypes": [
                "ICO",
                "SVG"
            ]
        },
        "form": {
            "backgroundImage": {
                "enabled": false
            },
            "borderRadius": 8.0,
            "darkMode": {
                "backgroundColor": "0f1b2aff",
                "borderColor": "424650ff"
```

```
            },
            "lightMode": {
                "backgroundColor": "ffffffff",
                "borderColor": "c6c6cdff"
            },
            "logo": {
                "enabled": false,
                "formInclusion": "IN",
                "location": "CENTER",
                "position": "TOP"
            }
        },
        "idpButton": {
            "custom": {
            },
            "standard": {
                "darkMode": {
                    "active": {
                        "backgroundColor": "354150ff",
                        "borderColor": "89bdeeff",
                        "textColor": "89bdeeff"
                    },
                    "defaults": {
                        "backgroundColor": "0f1b2aff",
                        "borderColor": "c6c6cdff",
                        "textColor": "c6c6cdff"
                    },
                    "hover": {
                        "backgroundColor": "192534ff",
                        "borderColor": "89bdeeff",
                        "textColor": "89bdeeff"
                    }
                },
                "lightMode": {
                    "active": {
                        "backgroundColor": "d3e7f9ff",
                        "borderColor": "033160ff",
                        "textColor": "033160ff"
                    },
                    "defaults": {
                        "backgroundColor": "ffffffff",
                        "borderColor": "424650ff",
                        "textColor": "424650ff"
                    },
```

```
                    "hover": {
                        "backgroundColor": "f2f8fdff",
                        "borderColor": "033160ff",
                        "textColor": "033160ff"
                    }
                }
            }
        },
        "pageBackground": {
            "darkMode": {
                "color": "0f1b2aff"
            },
            "image": {
                "enabled": true
            },
            "lightMode": {
                "color": "ffffffff"
            }
        },
        "pageFooter": {
            "backgroundImage": {
                "enabled": false
            },
            "darkMode": {
                "background": {
                    "color": "0f141aff"
                },
                "borderColor": "424650ff"
            },
            "lightMode": {
                "background": {
                    "color": "fafafaff"
                },
                "borderColor": "d5dbdbff"
            },
            "logo": {
                "enabled": false,
                "location": "START"
            }
        },
        "pageHeader": {
            "backgroundImage": {
                "enabled": false
            },
```

```
                "darkMode": {
                    "background": {
                        "color": "0f141aff"
                    },
                    "borderColor": "424650ff"
                },
                "lightMode": {
                    "background": {
                        "color": "fafafaff"
                    },
                    "borderColor": "d5dbdbff"
                },
                "logo": {
                    "enabled": false,
                    "location": "START"
                }
            },
            "pageText": {
                "darkMode": {
                    "bodyColor": "b6bec9ff",
                    "descriptionColor": "b6bec9ff",
                    "headingColor": "d1d5dbff"
                },
                "lightMode": {
                    "bodyColor": "414d5cff",
                    "descriptionColor": "414d5cff",
                    "headingColor": "000716ff"
                }
            },
            "phoneNumberSelector": {
                "displayType": "TEXT"
            },
            "primaryButton": {
                "darkMode": {
                    "active": {
                        "backgroundColor": "539fe5ff",
                        "textColor": "000716ff"
                    },
                    "defaults": {
                        "backgroundColor": "539fe5ff",
                        "textColor": "000716ff"
                    },
                    "disabled": {
                        "backgroundColor": "ffffffff",
```

```
                    "borderColor": "ffffffff"
                },
                "hover": {
                    "backgroundColor": "89bdeeff",
                    "textColor": "000716ff"
                }
            },
            "lightMode": {
                "active": {
                    "backgroundColor": "033160ff",
                    "textColor": "ffffffff"
                },
                "defaults": {
                    "backgroundColor": "0972d3ff",
                    "textColor": "ffffffff"
                },
                "disabled": {
                    "backgroundColor": "ffffffff",
                    "borderColor": "ffffffff"
                },
                "hover": {
                    "backgroundColor": "033160ff",
                    "textColor": "ffffffff"
                }
            }
        },
        "secondaryButton": {
            "darkMode": {
                "active": {
                    "backgroundColor": "354150ff",
                    "borderColor": "89bdeeff",
                    "textColor": "89bdeeff"
                },
                "defaults": {
                    "backgroundColor": "0f1b2aff",
                    "borderColor": "539fe5ff",
                    "textColor": "539fe5ff"
                },
                "hover": {
                    "backgroundColor": "192534ff",
                    "borderColor": "89bdeeff",
                    "textColor": "89bdeeff"
                }
            },
```

```
                "lightMode": {
                    "active": {
                        "backgroundColor": "d3e7f9ff",
                        "borderColor": "033160ff",
                        "textColor": "033160ff"
                    },
                    "defaults": {
                        "backgroundColor": "ffffffff",
                        "borderColor": "0972d3ff",
                        "textColor": "0972d3ff"
                    },
                    "hover": {
                        "backgroundColor": "f2f8fdff",
                        "borderColor": "033160ff",
                        "textColor": "033160ff"
                    }
                }
            }
        },
        "UseCognitoProvidedValues": false,
        "UserPoolId": "ca-central-1_EXAMPLE"
}
```

Salida:

```
{
    "ManagedLoginBranding": {
        "Assets": [
            {
                "Bytes":
 "PHN2ZyB3aWR0aD0iMjAwMDAiIGhlaWdodD0iNDAwIiB2aWV3Qm94PSIwIDAgMjAwMDAgNDAwIiBmaWxsPSJub25lIi
+CjxyZWN0IHdpZHRoPSIyMDAwMCIgaGVpZ2h0PSI0MDAiIGZpbGw9InVybCgjcGFpbnQwX2xpbmVhcl8xNzI1OV8yMzY
+CjxsaW5lYXJHcmFkaWVudCBpZD0icGFpbnQwX2xpbmVhcl8xNzI1OV8yMzY2NzQiIHgxPSItODk0LjI0OSIgeTE9IjE
+Cjwvc3ZnPgo=",
                "Category": "PAGE_FOOTER_BACKGROUND",
                "ColorMode": "DARK",
                "Extension": "SVG"
            }
        ],
        "CreationDate": 1732138490.642,
        "LastModifiedDate": 1732140420.301,
        "ManagedLoginBrandingId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
        "Settings": {
            "categories": {
                "auth": {
                    "authMethodOrder": [
                        [
                            {
                                "display": "BUTTON",
                                "type": "FEDERATED"
                            },
                            {
                                "display": "INPUT",
                                "type": "USERNAME_PASSWORD"
                            }
                        ]
                    ],
                    "federation": {
                        "interfaceStyle": "BUTTON_LIST",
                        "order": [
                        ]
                    }
                },
                "form": {
                    "displayGraphics": true,
                    "instructions": {
                        "enabled": false
                    },
                    "languageSelector": {
                        "enabled": false
                    },
                    "location": {
                        "horizontal": "CENTER",
                        "vertical": "CENTER"
                    },
                    "sessionTimerDisplay": "NONE"
                },
                "global": {
                    "colorSchemeMode": "LIGHT",
                    "pageFooter": {
                        "enabled": false
                    },
                    "pageHeader": {
                        "enabled": false
                    },
                    "spacingDensity": "REGULAR"
```

```
            },
            "signUp": {
                "acceptanceElements": [
                    {
                        "enforcement": "NONE",
                        "textKey": "en"
                    }
                ]
            }
        },
        "componentClasses": {
            "buttons": {
                "borderRadius": 8.0
            },
            "divider": {
                "darkMode": {
                    "borderColor": "232b37ff"
                },
                "lightMode": {
                    "borderColor": "ebebf0ff"
                }
            },
            "dropDown": {
                "borderRadius": 8.0,
                "darkMode": {
                    "defaults": {
                        "itemBackgroundColor": "192534ff"
                    },
                    "hover": {
                        "itemBackgroundColor": "081120ff",
                        "itemBorderColor": "5f6b7aff",
                        "itemTextColor": "e9ebedff"
                    },
                    "match": {
                        "itemBackgroundColor": "d1d5dbff",
                        "itemTextColor": "89bdeeff"
                    }
                },
                "lightMode": {
                    "defaults": {
                        "itemBackgroundColor": "ffffffff"
                    },
                    "hover": {
                        "itemBackgroundColor": "f4f4f4ff",
```

```
                        "itemBorderColor": "7d8998ff",
                        "itemTextColor": "000716ff"
                    },
                    "match": {
                        "itemBackgroundColor": "414d5cff",
                        "itemTextColor": "0972d3ff"
                    }
                }
            },
            "focusState": {
                "darkMode": {
                    "borderColor": "539fe5ff"
                },
                "lightMode": {
                    "borderColor": "0972d3ff"
                }
            },
            "idpButtons": {
                "icons": {
                    "enabled": true
                }
            },
            "input": {
                "borderRadius": 8.0,
                "darkMode": {
                    "defaults": {
                        "backgroundColor": "0f1b2aff",
                        "borderColor": "5f6b7aff"
                    },
                    "placeholderColor": "8d99a8ff"
                },
                "lightMode": {
                    "defaults": {
                        "backgroundColor": "ffffffff",
                        "borderColor": "7d8998ff"
                    },
                    "placeholderColor": "5f6b7aff"
                }
            },
            "inputDescription": {
                "darkMode": {
                    "textColor": "8d99a8ff"
                },
                "lightMode": {
```

```
                        "textColor": "5f6b7aff"
                    }
                },
                "inputLabel": {
                    "darkMode": {
                        "textColor": "d1d5dbff"
                    },
                    "lightMode": {
                        "textColor": "000716ff"
                    }
                },
                "link": {
                    "darkMode": {
                        "defaults": {
                            "textColor": "539fe5ff"
                        },
                        "hover": {
                            "textColor": "89bdeeff"
                        }
                    },
                    "lightMode": {
                        "defaults": {
                            "textColor": "0972d3ff"
                        },
                        "hover": {
                            "textColor": "033160ff"
                        }
                    }
                },
                "optionControls": {
                    "darkMode": {
                        "defaults": {
                            "backgroundColor": "0f1b2aff",
                            "borderColor": "7d8998ff"
                        },
                        "selected": {
                            "backgroundColor": "539fe5ff",
                            "foregroundColor": "000716ff"
                        }
                    },
                    "lightMode": {
                        "defaults": {
                            "backgroundColor": "ffffffff",
                            "borderColor": "7d8998ff"
```

```
                    },
                    "selected": {
                        "backgroundColor": "0972d3ff",
                        "foregroundColor": "ffffffff"
                    }
                }
            },
            "statusIndicator": {
                "darkMode": {
                    "error": {
                        "backgroundColor": "1a0000ff",
                        "borderColor": "eb6f6fff",
                        "indicatorColor": "eb6f6fff"
                    },
                    "pending": {
                        "indicatorColor": "AAAAAAAA"
                    },
                    "success": {
                        "backgroundColor": "001a02ff",
                        "borderColor": "29ad32ff",
                        "indicatorColor": "29ad32ff"
                    },
                    "warning": {
                        "backgroundColor": "1d1906ff",
                        "borderColor": "e0ca57ff",
                        "indicatorColor": "e0ca57ff"
                    }
                },
                "lightMode": {
                    "error": {
                        "backgroundColor": "fff7f7ff",
                        "borderColor": "d91515ff",
                        "indicatorColor": "d91515ff"
                    },
                    "pending": {
                        "indicatorColor": "AAAAAAAA"
                    },
                    "success": {
                        "backgroundColor": "f2fcf3ff",
                        "borderColor": "037f0cff",
                        "indicatorColor": "037f0cff"
                    },
                    "warning": {
                        "backgroundColor": "fffce9ff",
```

```
                    "borderColor": "8d6605ff",
                    "indicatorColor": "8d6605ff"
                }
            }
        }
    },
    "components": {
        "alert": {
            "borderRadius": 12.0,
            "darkMode": {
                "error": {
                    "backgroundColor": "1a0000ff",
                    "borderColor": "eb6f6fff"
                }
            },
            "lightMode": {
                "error": {
                    "backgroundColor": "fff7f7ff",
                    "borderColor": "d91515ff"
                }
            }
        },
        "favicon": {
            "enabledTypes": [
                "ICO",
                "SVG"
            ]
        },
        "form": {
            "backgroundImage": {
                "enabled": false
            },
            "borderRadius": 8.0,
            "darkMode": {
                "backgroundColor": "0f1b2aff",
                "borderColor": "424650ff"
            },
            "lightMode": {
                "backgroundColor": "ffffffff",
                "borderColor": "c6c6cdff"
            },
            "logo": {
                "enabled": false,
                "formInclusion": "IN",
```

```
                        "location": "CENTER",
                        "position": "TOP"
                    }
                },
                "idpButton": {
                    "custom": {
                    },
                    "standard": {
                        "darkMode": {
                            "active": {
                                "backgroundColor": "354150ff",
                                "borderColor": "89bdeeff",
                                "textColor": "89bdeeff"
                            },
                            "defaults": {
                                "backgroundColor": "0f1b2aff",
                                "borderColor": "c6c6cdff",
                                "textColor": "c6c6cdff"
                            },
                            "hover": {
                                "backgroundColor": "192534ff",
                                "borderColor": "89bdeeff",
                                "textColor": "89bdeeff"
                            }
                        },
                        "lightMode": {
                            "active": {
                                "backgroundColor": "d3e7f9ff",
                                "borderColor": "033160ff",
                                "textColor": "033160ff"
                            },
                            "defaults": {
                                "backgroundColor": "ffffffff",
                                "borderColor": "424650ff",
                                "textColor": "424650ff"
                            },
                            "hover": {
                                "backgroundColor": "f2f8fdff",
                                "borderColor": "033160ff",
                                "textColor": "033160ff"
                            }
                        }
                    }
                },
```

```
                "pageBackground": {
                    "darkMode": {
                        "color": "0f1b2aff"
                    },
                    "image": {
                        "enabled": true
                    },
                    "lightMode": {
                        "color": "ffffffff"
                    }
                },
                "pageFooter": {
                    "backgroundImage": {
                        "enabled": false
                    },
                    "darkMode": {
                        "background": {
                            "color": "0f141aff"
                        },
                        "borderColor": "424650ff"
                    },
                    "lightMode": {
                        "background": {
                            "color": "fafafaff"
                        },
                        "borderColor": "d5dbdbff"
                    },
                    "logo": {
                        "enabled": false,
                        "location": "START"
                    }
                },
                "pageHeader": {
                    "backgroundImage": {
                        "enabled": false
                    },
                    "darkMode": {
                        "background": {
                            "color": "0f141aff"
                        },
                        "borderColor": "424650ff"
                    },
                    "lightMode": {
                        "background": {
```

```
                        "color": "fafafaff"
                    },
                    "borderColor": "d5dbdbff"
                },
                "logo": {
                    "enabled": false,
                    "location": "START"
                }
            },
            "pageText": {
                "darkMode": {
                    "bodyColor": "b6bec9ff",
                    "descriptionColor": "b6bec9ff",
                    "headingColor": "d1d5dbff"
                },
                "lightMode": {
                    "bodyColor": "414d5cff",
                    "descriptionColor": "414d5cff",
                    "headingColor": "000716ff"
                }
            },
            "phoneNumberSelector": {
                "displayType": "TEXT"
            },
            "primaryButton": {
                "darkMode": {
                    "active": {
                        "backgroundColor": "539fe5ff",
                        "textColor": "000716ff"
                    },
                    "defaults": {
                        "backgroundColor": "539fe5ff",
                        "textColor": "000716ff"
                    },
                    "disabled": {
                        "backgroundColor": "ffffffff",
                        "borderColor": "ffffffff"
                    },
                    "hover": {
                        "backgroundColor": "89bdeeff",
                        "textColor": "000716ff"
                    }
                },
                "lightMode": {
```

```
                    "active": {
                        "backgroundColor": "033160ff",
                        "textColor": "ffffffff"
                    },
                    "defaults": {
                        "backgroundColor": "0972d3ff",
                        "textColor": "ffffffff"
                    },
                    "disabled": {
                        "backgroundColor": "ffffffff",
                        "borderColor": "ffffffff"
                    },
                    "hover": {
                        "backgroundColor": "033160ff",
                        "textColor": "ffffffff"
                    }
                }
            },
            "secondaryButton": {
                "darkMode": {
                    "active": {
                        "backgroundColor": "354150ff",
                        "borderColor": "89bdeeff",
                        "textColor": "89bdeeff"
                    },
                    "defaults": {
                        "backgroundColor": "0f1b2aff",
                        "borderColor": "539fe5ff",
                        "textColor": "539fe5ff"
                    },
                    "hover": {
                        "backgroundColor": "192534ff",
                        "borderColor": "89bdeeff",
                        "textColor": "89bdeeff"
                    }
                },
                "lightMode": {
                    "active": {
                        "backgroundColor": "d3e7f9ff",
                        "borderColor": "033160ff",
                        "textColor": "033160ff"
                    },
                    "defaults": {
                        "backgroundColor": "ffffffff",
```

```
                            "borderColor": "0972d3ff",
                            "textColor": "0972d3ff"
                        },
                        "hover": {
                            "backgroundColor": "f2f8fdff",
                            "borderColor": "033160ff",
                            "textColor": "033160ff"
                        }
                    }
                }
            }
        },
        "UseCognitoProvidedValues": false,
        "UserPoolId": "ca-central-1_EXAMPLE"
    }
}
```

Para obtener más información, consulte Aplicar marca a las páginas de inicio de sesión administradas en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información acerca de la API, consulte UpdateManagedLoginBranding en la Referencia de comandos de la AWS CLI.

`update-resource-server`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-resource-server`.

AWS CLI

Creación de un servidor de recursos

En este ejemplo, se actualiza el servidor de recursos Weather. Agrega un nuevo ámbito.

Comando:

```
aws cognito-idp update-resource-server --user-pool-id us-west-2_aaaaaaaaa
 --identifier weather.example.com --name Weather --scopes
 ScopeName=NewScope,ScopeDescription="New scope description"
```

Salida:

```
{
```

```
  "ResourceServer": {
      "UserPoolId": "us-west-2_aaaaaaaaa",
      "Identifier": "weather.example.com",
      "Name": "Happy",
      "Scopes": [
          {
              "ScopeName": "NewScope",
              "ScopeDescription": "New scope description"
          }
      ]
  }
}
```

- Para obtener detalles sobre la API, consulte UpdateResourceServer en la Referencia de comandos de la AWS CLI.

`update-user-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-user-attributes`.

AWS CLI

Actualización de los atributos de usuario

En este ejemplo, se actualiza el atributo de usuario nickname.

Comando:

```
aws cognito-idp update-user-attributes --access-token ACCESS_TOKEN --user-attributes
 Name="nickname",Value="Dan"
```

- Para obtener detalles sobre la API, consulte UpdateUserAttributes en la Referencia de comandos de la AWS CLI.

`update-user-pool-client`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-user-pool-client`.

AWS CLI

Actualización de un cliente de aplicación

En el siguiente ejemplo de `update-user-pool-client`, se actualiza la configuración del cliente de la aplicación solicitado.

```
aws cognito-idp update-user-pool-client \
    --user-pool-id us-west-2_EXAMPLE \
    --client-id 1example23456789 \
    --client-name my-test-app \
    --refresh-token-validity 30 \
    --access-token-validity 60 \
    --id-token-validity 60 \
    --token-validity-units AccessToken=minutes,IdToken=minutes,RefreshToken=days \
    --read-
attributes "address" "birthdate" "email" "email_verified" "family_name" "gender" "locale" "m
 \
    --write-
attributes "address" "birthdate" "email" "family_name" "gender" "locale" "middle_name" "name
 \
    --explicit-auth-
flows "ALLOW_ADMIN_USER_PASSWORD_AUTH" "ALLOW_CUSTOM_AUTH" "ALLOW_REFRESH_TOKEN_AUTH" "ALLOW
 \
    --supported-identity-providers "MySAML" "COGNITO" "Google" \
    --callback-urls "https://www.example.com" "https://app2.example.com" \
    --logout-urls "https://auth.example.com/login?
client_id=1example23456789&response_type=code&redirect_uri=https%3A%2F
%2Fwww.example.com" "https://example.com/logout" \
    --default-redirect-uri "https://www.example.com" \
    --allowed-o-auth-flows "code" "implicit" \
    --allowed-o-auth-scopes "openid" "profile" "aws.cognito.signin.user.admin" \
    --allowed-o-auth-flows-user-pool-client \
    --prevent-user-existence-errors ENABLED \
    --enable-token-revocation \
    --no-enable-propagate-additional-user-context-data \
    --auth-session-validity 3
```

Salida:

```
{
    "UserPoolClient": {
        "UserPoolId": "us-west-2_EXAMPLE",
        "ClientName": "my-test-app",
        "ClientId": "1example23456789",
        "LastModifiedDate": "2025-01-31T14:40:12.498000-08:00",
        "CreationDate": "2023-09-13T16:26:34.408000-07:00",
```

```
        "RefreshTokenValidity": 30,
        "AccessTokenValidity": 60,
        "IdTokenValidity": 60,
        "TokenValidityUnits": {
            "AccessToken": "minutes",
            "IdToken": "minutes",
            "RefreshToken": "days"
        },
        "ReadAttributes": [
            "website",
            "zoneinfo",
            "address",
            "birthdate",
            "email_verified",
            "gender",
            "profile",
            "phone_number_verified",
            "preferred_username",
            "locale",
            "middle_name",
            "picture",
            "updated_at",
            "name",
            "nickname",
            "phone_number",
            "family_name",
            "email"
        ],
        "WriteAttributes": [
            "website",
            "zoneinfo",
            "address",
            "birthdate",
            "gender",
            "profile",
            "preferred_username",
            "locale",
            "middle_name",
            "picture",
            "updated_at",
            "name",
            "nickname",
            "phone_number",
            "family_name",
```

```
            "email"
        ],
        "ExplicitAuthFlows": [
            "ALLOW_CUSTOM_AUTH",
            "ALLOW_USER_PASSWORD_AUTH",
            "ALLOW_ADMIN_USER_PASSWORD_AUTH",
            "ALLOW_USER_SRP_AUTH",
            "ALLOW_REFRESH_TOKEN_AUTH"
        ],
        "SupportedIdentityProviders": [
            "Google",
            "COGNITO",
            "MySAML"
        ],
        "CallbackURLs": [
            "https://www.example.com",
            "https://app2.example.com"
        ],
        "LogoutURLs": [
            "https://example.com/logout",
            "https://auth.example.com/login?
client_id=1example23456789&response_type=code&redirect_uri=https%3A%2F
%2Fwww.example.com"
        ],
        "DefaultRedirectURI": "https://www.example.com",
        "AllowedOAuthFlows": [
            "implicit",
            "code"
        ],
        "AllowedOAuthScopes": [
            "aws.cognito.signin.user.admin",
            "openid",
            "profile"
        ],
        "AllowedOAuthFlowsUserPoolClient": true,
        "PreventUserExistenceErrors": "ENABLED",
        "EnableTokenRevocation": true,
        "EnablePropagateAdditionalUserContextData": false,
        "AuthSessionValidity": 3
    }
}
```

Para obtener más información, consulte Application-specific settings with app clients en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte UpdateUserPoolClient en la Referencia de comandos de la AWS CLI.

`update-user-pool-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-user-pool-domain`.

AWS CLI

Actualización de un dominio personalizado

En el siguiente ejemplo de `update-user-pool-domain`, se configura la versión de marca y el certificado para el dominio personalizado del grupo de usuarios solicitado.

```
aws cognito-idp update-user-pool-domain \
    --user-pool-id ca-central-1_EXAMPLE \
    --domain auth.example.com \
    --managed-login-version 2 \
    --custom-domain-config CertificateArn=arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "CloudFrontDomain": "example.cloudfront.net",
    "ManagedLoginVersion": 2
}
```

Para obtener más información, consulte Inicio de sesión administrado y Configuración de un dominio en la Guía para desarrolladores de Amazon Cognito.

- Para obtener información sobre la API, consulte UpdateUserPoolDomain en la Referencia de comandos de AWS CLI.

`update-user-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-user-pool`.

AWS CLI

Actualización de un grupo de usuarios

En el siguiente ejemplo de `update-user-pool`, se modifica un grupo de usuarios con un ejemplo de sintaxis para cada una de las opciones de configuración disponibles. Para actualizar un grupo de usuarios, debe especificar todas las opciones configuradas previamente o estas se restablecerán a su valor predeterminado.

```
aws cognito-idp update-user-pool --user-pool-id us-west-2_EXAMPLE \
    --policies PasswordPolicy=
\{MinimumLength=6,RequireUppercase=true,RequireLowercase=true,RequireNumbers=true,RequireSym
 \
    --deletion-protection ACTIVE \
    --lambda-config PreSignUp="arn:aws:lambda:us-
west-2:123456789012:function:cognito-test-presignup-
function",PreTokenGeneration="arn:aws:lambda:us-
west-2:123456789012:function:cognito-test-pretoken-function" \
    --auto-verified-attributes "phone_number" "email" \
    --verification-message-template \{\"SmsMessage\":\""Your code is
 {####}"\",\"EmailMessage\":\""Your code is {####}"\",\"EmailSubject\":\""Your
 verification code"\",\"EmailMessageByLink\":\""Click {##here##} to verify
 your email address."\",\"EmailSubjectByLink\":\""Your verification link"\",
\"DefaultEmailOption\":\"CONFIRM_WITH_LINK\"\} \
    --sms-authentication-message "Your code is {####}" \
    --user-attribute-update-settings
 AttributesRequireVerificationBeforeUpdate="email","phone_number" \
    --mfa-configuration "OPTIONAL" \
    --device-
configuration ChallengeRequiredOnNewDevice=true,DeviceOnlyRememberedOnUserPrompt=true
 \
    --email-configuration SourceArn="arn:aws:ses:us-
west-2:123456789012:identity/admin@example.com",ReplyToEmailAddress="amdin
+noreply@example.com",EmailSendingAccount=DEVELOPER,From="admin@amazon.com",ConfigurationSet
configuration-set" \
    --sms-configuration SnsCallerArn="arn:aws:iam::123456789012:role/service-role/
SNS-SMS-Role",ExternalId="12345",SnsRegion="us-west-2" \
    --admin-create-user-config AllowAdminCreateUserOnly=false,InviteMessageTemplate=
\{SMSMessage=\""Welcome {username}. Your confirmation code is
 {####}"\",EmailMessage=\""Welcome {username}. Your confirmation code is
 {####}"\",EmailSubject=\""Welcome to MyMobileGame"\"\} \
    --user-pool-tags "Function"="MyMobileGame","Developers"="Berlin" \
```

```
    --admin-create-user-config AllowAdminCreateUserOnly=false,InviteMessageTemplate=
\{SMSMessage=\""Welcome {username}. Your confirmation code is
 {####}"\",EmailMessage=\""Welcome {username}. Your confirmation code is
 {####}"\",EmailSubject=\""Welcome to MyMobileGame"\"\} \
    --user-pool-add-ons AdvancedSecurityMode="AUDIT" \
    --account-recovery-setting RecoveryMechanisms=
\[\{Priority=1,Name="verified_email"\},\{Priority=2,Name="verified_phone_number"\}\]
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Updating user pool configuration en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte UpdateUserPool en la Referencia de comandos de la AWS CLI.

`verify-software-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `verify-software-token`.

AWS CLI

Confirmación del registro de una autenticación TOTP

En el siguiente ejemplo de `verify-software-token`, se completa el registro TOTP para el usuario actual.

```
aws cognito-idp verify-software-token \
    --access-token eyJra456defEXAMPLE \
    --user-code 123456
```

Salida:

```
{
    "Status": "SUCCESS"
}
```

Para obtener más información, consulte Adding MFA to a user pool en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte VerifySoftwareToken en la Referencia de comandos de la AWS CLI.

`verify-user-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `verify-user-attribute`.

AWS CLI

Verificación de un cambio de atributo

En el siguiente ejemplo de `verify-user-attribute`, se verifica un cambio en el atributo de correo electrónico del usuario actual.

```
aws cognito-idp verify-user-attribute \
    --access-token eyJra456defEXAMPLE \
    --attribute-name email \
    --code 123456
```

Para obtener más información, consulte Configuración de verificación de correo electrónico o teléfono en la Guía para desarrolladores de Amazon Cognito.

- Para obtener detalles sobre la API, consulte VerifyUserAttribute en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon Comprehend que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon Comprehend.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`batch-detect-dominant-language`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-detect-dominant-language`.

AWS CLI

Detección del idioma dominante de varios textos de entrada

El siguiente ejemplo de `batch-detect-dominant-language` analiza varios textos de entrada y devuelve el idioma dominante de cada uno. La puntuación de confianza de los modelos previamente entrenados también se muestra para cada predicción.

```
aws comprehend batch-detect-dominant-language \
    --text-list "Physics is the natural science that involves the study of matter
 and its motion and behavior through space and time, along with related concepts
 such as energy and force."
```

Salida:

```
{
    "ResultList": [
        {
            "Index": 0,
            "Languages": [
                {
                    "LanguageCode": "en",
                    "Score": 0.9986501932144165
                }
            ]
        }
    ],
    "ErrorList": []
}
```

Para obtener más información, consulte Idioma dominante en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte BatchDetectDominantLanguage en la Referencia de comandos de la AWS CLI.

batch-detect-entities

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-detect-entities`.

AWS CLI

Detección de entidades a partir de varios textos de entrada

El siguiente ejemplo de `batch-detect-entities` analiza varios textos de entrada y devuelve las entidades nombradas de cada uno. La puntuación de confianza del modelo previamente entrenado también se muestra para cada predicción.

```
aws comprehend batch-detect-entities \
    --language-code en \
    --text-list "Dear Jane, Your AnyCompany Financial Services LLC credit card account 1111-XXXX-1111-XXXX has a minimum payment of $24.53 that is due by July 31st." "Please send customer feedback to Sunshine Spa, 123 Main St, Anywhere or to Alice at AnySpa@example.com."
```

Salida:

```
{
    "ResultList": [
        {
            "Index": 0,
            "Entities": [
                {
                    "Score": 0.9985517859458923,
                    "Type": "PERSON",
                    "Text": "Jane",
                    "BeginOffset": 5,
                    "EndOffset": 9
                },
                {
                    "Score": 0.9767839312553406,
                    "Type": "ORGANIZATION",
                    "Text": "AnyCompany Financial Services, LLC",
                    "BeginOffset": 16,
                    "EndOffset": 50
                },
                {
                    "Score": 0.9856694936752319,
                    "Type": "OTHER",
```

```
                    "Text": "1111-XXXX-1111-XXXX",
                    "BeginOffset": 71,
                    "EndOffset": 90
                },
                {
                    "Score": 0.9652159810066223,
                    "Type": "QUANTITY",
                    "Text": ".53",
                    "BeginOffset": 116,
                    "EndOffset": 119
                },
                {
                    "Score": 0.9986667037010193,
                    "Type": "DATE",
                    "Text": "July 31st",
                    "BeginOffset": 135,
                    "EndOffset": 144
                }
            ]
        },
        {
            "Index": 1,
            "Entities": [
                {
                    "Score": 0.720084547996521,
                    "Type": "ORGANIZATION",
                    "Text": "Sunshine Spa",
                    "BeginOffset": 33,
                    "EndOffset": 45
                },
                {
                    "Score": 0.9865870475769043,
                    "Type": "LOCATION",
                    "Text": "123 Main St",
                    "BeginOffset": 47,
                    "EndOffset": 58
                },
                {
                    "Score": 0.5895616412162781,
                    "Type": "LOCATION",
                    "Text": "Anywhere",
                    "BeginOffset": 60,
                    "EndOffset": 68
                },
```

```
                {
                    "Score": 0.6809214353561401,
                    "Type": "PERSON",
                    "Text": "Alice",
                    "BeginOffset": 75,
                    "EndOffset": 80
                },
                {
                    "Score": 0.9979087114334106,
                    "Type": "OTHER",
                    "Text": "AnySpa@example.com",
                    "BeginOffset": 84,
                    "EndOffset": 99
                }
            ]
        }
    ],
    "ErrorList": []
}
```

Para obtener más información, consulte Entidades en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte BatchDetectEntities en la Referencia de comandos de la AWS CLI.

`batch-detect-key-phrases`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-detect-key-phrases`.

AWS CLI

Detección de frases clave de varias entradas de texto

El siguiente ejemplo de `batch-detect-key-phrases` analiza varios textos introducidos y devuelve los sintagmas nominales clave de cada uno de ellos. La puntuación de confianza del modelo previamente entrenado también se muestra para cada predicción.

```
aws comprehend batch-detect-key-phrases \
    --language-code en \
    --text-list "Hello Zhang Wei, I am John, writing to you about the trip for
 next Saturday." "Dear Jane, Your AnyCompany Financial Services LLC credit card
```

```
account 1111-XXXX-1111-XXXX has a minimum payment of $24.53 that is due by July
31st." "Please send customer feedback to Sunshine Spa, 123 Main St, Anywhere or to
Alice at AnySpa@example.com."
```

Salida:

```
{
    "ResultList": [
        {
            "Index": 0,
            "KeyPhrases": [
                {
                    "Score": 0.99700927734375,
                    "Text": "Zhang Wei",
                    "BeginOffset": 6,
                    "EndOffset": 15
                },
                {
                    "Score": 0.9929308891296387,
                    "Text": "John",
                    "BeginOffset": 22,
                    "EndOffset": 26
                },
                {
                    "Score": 0.9997230172157288,
                    "Text": "the trip",
                    "BeginOffset": 49,
                    "EndOffset": 57
                },
                {
                    "Score": 0.9999470114707947,
                    "Text": "next Saturday",
                    "BeginOffset": 62,
                    "EndOffset": 75
                }
            ]
        },
        {
            "Index": 1,
            "KeyPhrases": [
                {
                    "Score": 0.8358274102210999,
                    "Text": "Dear Jane",
```

```
                    "BeginOffset": 0,
                    "EndOffset": 9
                },
                {
                    "Score": 0.989359974861145,
                    "Text": "Your AnyCompany Financial Services",
                    "BeginOffset": 11,
                    "EndOffset": 45
                },
                {
                    "Score": 0.8812323808670044,
                    "Text": "LLC credit card account 1111-XXXX-1111-XXXX",
                    "BeginOffset": 47,
                    "EndOffset": 90
                },
                {
                    "Score": 0.9999381899833679,
                    "Text": "a minimum payment",
                    "BeginOffset": 95,
                    "EndOffset": 112
                },
                {
                    "Score": 0.9997439980506897,
                    "Text": ".53",
                    "BeginOffset": 116,
                    "EndOffset": 119
                },
                {
                    "Score": 0.996875524520874,
                    "Text": "July 31st",
                    "BeginOffset": 135,
                    "EndOffset": 144
                }
            ]
        },
        {
            "Index": 2,
            "KeyPhrases": [
                {
                    "Score": 0.9990295767784119,
                    "Text": "customer feedback",
                    "BeginOffset": 12,
                    "EndOffset": 29
                },
```

```
                {
                    "Score": 0.9994127750396729,
                    "Text": "Sunshine Spa",
                    "BeginOffset": 33,
                    "EndOffset": 45
                },
                {
                    "Score": 0.9892991185188293,
                    "Text": "123 Main St",
                    "BeginOffset": 47,
                    "EndOffset": 58
                },
                {
                    "Score": 0.9969810843467712,
                    "Text": "Alice",
                    "BeginOffset": 75,
                    "EndOffset": 80
                },
                {
                    "Score": 0.9703696370124817,
                    "Text": "AnySpa@example.com",
                    "BeginOffset": 84,
                    "EndOffset": 99
                }
            ]
        }
    ],
    "ErrorList": []
}
```

Para obtener más información, consulte Frases clave en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte BatchDetectKeyPhrases en la Referencia de comandos de AWS CLI.

`batch-detect-sentiment`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-detect-sentiment`.

AWS CLI

Para detectar la opinión predominante de varios textos de entrada

El siguiente ejemplo de `batch-detect-sentiment` analiza varios textos de entrada y devuelve la opinión predominante (`POSITIVE`, `NEUTRAL`, `MIXED` o `NEGATIVE`, en cada caso).

```
aws comprehend batch-detect-sentiment \
    --text-list "That movie was very boring, I can't believe it was over four hours long." "It is a beautiful day for hiking today." "My meal was okay, I'm excited to try other restaurants." \
    --language-code en
```

Salida:

```
{
    "ResultList": [
        {
            "Index": 0,
            "Sentiment": "NEGATIVE",
            "SentimentScore": {
                "Positive": 0.00011316669406369328,
                "Negative": 0.9995445609092712,
                "Neutral": 0.00014722718333359808,
                "Mixed": 0.00019498742767609656
            }
        },
        {
            "Index": 1,
            "Sentiment": "POSITIVE",
            "SentimentScore": {
                "Positive": 0.9981263279914856,
                "Negative": 0.00015240783977787942,
                "Neutral": 0.0013876151060685515,
                "Mixed": 0.00033366199932061136
            }
        },
        {
            "Index": 2,
            "Sentiment": "MIXED",
            "SentimentScore": {
                "Positive": 0.15930435061454773,
                "Negative": 0.11471917480230331,
                "Neutral": 0.26897063851356506,
                "Mixed": 0.45700588822364807
            }
        }
```

```
    ],
    "ErrorList": []
}
```

Para obtener más información, consulte Sentiment en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte BatchDetectSentiment en la Referencia de comandos de la AWS CLI.

`batch-detect-syntax`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-detect-syntax`.

AWS CLI

Inspección de la sintaxis y las partes de la oración de las palabras en textos de varias entradas

El siguiente ejemplo de `batch-detect-syntax` analiza la sintaxis de varios textos de entrada y devuelve las distintas partes de la oración. La puntuación de confianza del modelo previamente entrenado también se muestra para cada predicción.

```
aws comprehend batch-detect-syntax \
    --text-list "It is a beautiful day." "Can you please pass the salt?" "Please pay
 the bill before the 31st." \
    --language-code en
```

Salida:

```
{
    "ResultList": [
        {
            "Index": 0,
            "SyntaxTokens": [
                {
                    "TokenId": 1,
                    "Text": "It",
                    "BeginOffset": 0,
                    "EndOffset": 2,
                    "PartOfSpeech": {
                        "Tag": "PRON",
                        "Score": 0.9999740719795227
```

```
            }
        },
        {
            "TokenId": 2,
            "Text": "is",
            "BeginOffset": 3,
            "EndOffset": 5,
            "PartOfSpeech": {
                "Tag": "VERB",
                "Score": 0.999937117099762
            }
        },
        {
            "TokenId": 3,
            "Text": "a",
            "BeginOffset": 6,
            "EndOffset": 7,
            "PartOfSpeech": {
                "Tag": "DET",
                "Score": 0.9999926686286926
            }
        },
        {
            "TokenId": 4,
            "Text": "beautiful",
            "BeginOffset": 8,
            "EndOffset": 17,
            "PartOfSpeech": {
                "Tag": "ADJ",
                "Score": 0.9987891912460327
            }
        },
        {
            "TokenId": 5,
            "Text": "day",
            "BeginOffset": 18,
            "EndOffset": 21,
            "PartOfSpeech": {
                "Tag": "NOUN",
                "Score": 0.9999778866767883
            }
        },
        {
            "TokenId": 6,
```

```
                    "Text": ".",
                    "BeginOffset": 21,
                    "EndOffset": 22,
                    "PartOfSpeech": {
                        "Tag": "PUNCT",
                        "Score": 0.9999974966049194
                    }
                }
            ]
        },
        {
            "Index": 1,
            "SyntaxTokens": [
                {
                    "TokenId": 1,
                    "Text": "Can",
                    "BeginOffset": 0,
                    "EndOffset": 3,
                    "PartOfSpeech": {
                        "Tag": "AUX",
                        "Score": 0.9999770522117615
                    }
                },
                {
                    "TokenId": 2,
                    "Text": "you",
                    "BeginOffset": 4,
                    "EndOffset": 7,
                    "PartOfSpeech": {
                        "Tag": "PRON",
                        "Score": 0.9999986886978149
                    }
                },
                {
                    "TokenId": 3,
                    "Text": "please",
                    "BeginOffset": 8,
                    "EndOffset": 14,
                    "PartOfSpeech": {
                        "Tag": "INTJ",
                        "Score": 0.9681622385978699
                    }
                },
                {
```

```
                    "TokenId": 4,
                    "Text": "pass",
                    "BeginOffset": 15,
                    "EndOffset": 19,
                    "PartOfSpeech": {
                        "Tag": "VERB",
                        "Score": 0.9999874830245972
                    }
                },
                {
                    "TokenId": 5,
                    "Text": "the",
                    "BeginOffset": 20,
                    "EndOffset": 23,
                    "PartOfSpeech": {
                        "Tag": "DET",
                        "Score": 0.9999827146530151
                    }
                },
                {
                    "TokenId": 6,
                    "Text": "salt",
                    "BeginOffset": 24,
                    "EndOffset": 28,
                    "PartOfSpeech": {
                        "Tag": "NOUN",
                        "Score": 0.9995040893554688
                    }
                },
                {
                    "TokenId": 7,
                    "Text": "?",
                    "BeginOffset": 28,
                    "EndOffset": 29,
                    "PartOfSpeech": {
                        "Tag": "PUNCT",
                        "Score": 0.999998152256012
                    }
                }
            ]
        },
        {
            "Index": 2,
            "SyntaxTokens": [
```

```
                {
                    "TokenId": 1,
                    "Text": "Please",
                    "BeginOffset": 0,
                    "EndOffset": 6,
                    "PartOfSpeech": {
                        "Tag": "INTJ",
                        "Score": 0.9997857809066772
                    }
                },
                {
                    "TokenId": 2,
                    "Text": "pay",
                    "BeginOffset": 7,
                    "EndOffset": 10,
                    "PartOfSpeech": {
                        "Tag": "VERB",
                        "Score": 0.9999252557754517
                    }
                },
                {
                    "TokenId": 3,
                    "Text": "the",
                    "BeginOffset": 11,
                    "EndOffset": 14,
                    "PartOfSpeech": {
                        "Tag": "DET",
                        "Score": 0.9999842643737793
                    }
                },
                {
                    "TokenId": 4,
                    "Text": "bill",
                    "BeginOffset": 15,
                    "EndOffset": 19,
                    "PartOfSpeech": {
                        "Tag": "NOUN",
                        "Score": 0.9999588131904602
                    }
                },
                {
                    "TokenId": 5,
                    "Text": "before",
                    "BeginOffset": 20,
```

```
                    "EndOffset": 26,
                    "PartOfSpeech": {
                        "Tag": "ADP",
                        "Score": 0.9958304762840271
                    }
                },
                {
                    "TokenId": 6,
                    "Text": "the",
                    "BeginOffset": 27,
                    "EndOffset": 30,
                    "PartOfSpeech": {
                        "Tag": "DET",
                        "Score": 0.9999947547912598
                    }
                },
                {
                    "TokenId": 7,
                    "Text": "31st",
                    "BeginOffset": 31,
                    "EndOffset": 35,
                    "PartOfSpeech": {
                        "Tag": "NOUN",
                        "Score": 0.9924124479293823
                    }
                },
                {
                    "TokenId": 8,
                    "Text": ".",
                    "BeginOffset": 35,
                    "EndOffset": 36,
                    "PartOfSpeech": {
                        "Tag": "PUNCT",
                        "Score": 0.9999955892562866
                    }
                }
            ]
        }
    ],
    "ErrorList": []
}
```

Para obtener más información, consulte los Análisis de sintaxis en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte BatchDetectSyntax en la Referencia de comandos de la AWS CLI.

`batch-detect-targeted-sentiment`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-detect-targeted-sentiment`.

AWS CLI

Para detectar la opinión y cada entidad nombrada para varios textos de entrada

El siguiente ejemplo de `batch-detect-targeted-sentiment` analiza varios textos de entrada y devuelve las entidades nombradas junto con la opinión predominante asociada a cada entidad. La puntuación de confianza del modelo previamente entrenado también se muestra para cada predicción.

```
aws comprehend batch-detect-targeted-sentiment \
    --language-code en \
    --text-list "That movie was really boring, the original was way more
 entertaining" "The trail is extra beautiful today." "My meal was just okay."
```

Salida:

```
{
    "ResultList": [
        {
            "Index": 0,
            "Entities": [
                {
                    "DescriptiveMentionIndex": [
                        0
                    ],
                    "Mentions": [
                        {
                            "Score": 0.9999009966850281,
                            "GroupScore": 1.0,
                            "Text": "movie",
                            "Type": "MOVIE",
```

```
                        "MentionSentiment": {
                            "Sentiment": "NEGATIVE",
                            "SentimentScore": {
                                "Positive": 0.13887299597263336,
                                "Negative": 0.8057460188865662,
                                "Neutral": 0.05525200068950653,
                                "Mixed": 0.00012799999967683107
                            }
                        },
                        "BeginOffset": 5,
                        "EndOffset": 10
                    }
                ]
            },
            {
                "DescriptiveMentionIndex": [
                    0
                ],
                "Mentions": [
                    {
                        "Score": 0.9921110272407532,
                        "GroupScore": 1.0,
                        "Text": "original",
                        "Type": "MOVIE",
                        "MentionSentiment": {
                            "Sentiment": "POSITIVE",
                            "SentimentScore": {
                                "Positive": 0.9999989867210388,
                                "Negative": 9.999999974752427e-07,
                                "Neutral": 0.0,
                                "Mixed": 0.0
                            }
                        },
                        "BeginOffset": 34,
                        "EndOffset": 42
                    }
                ]
            }
        ]
    },
    {
        "Index": 1,
        "Entities": [
            {
```

```
                    "DescriptiveMentionIndex": [
                        0
                    ],
                    "Mentions": [
                        {
                            "Score": 0.7545599937438965,
                            "GroupScore": 1.0,
                            "Text": "trail",
                            "Type": "OTHER",
                            "MentionSentiment": {
                                "Sentiment": "POSITIVE",
                                "SentimentScore": {
                                    "Positive": 1.0,
                                    "Negative": 0.0,
                                    "Neutral": 0.0,
                                    "Mixed": 0.0
                                }
                            },
                            "BeginOffset": 4,
                            "EndOffset": 9
                        }
                    ]
                },
                {
                    "DescriptiveMentionIndex": [
                        0
                    ],
                    "Mentions": [
                        {
                            "Score": 0.9999960064888,
                            "GroupScore": 1.0,
                            "Text": "today",
                            "Type": "DATE",
                            "MentionSentiment": {
                                "Sentiment": "NEUTRAL",
                                "SentimentScore": {
                                    "Positive": 9.000000318337698e-06,
                                    "Negative": 1.9999999949504854e-06,
                                    "Neutral": 0.9999859929084778,
                                    "Mixed": 3.999999989900971e-06
                                }
                            },
                            "BeginOffset": 29,
                            "EndOffset": 34
```

```
                    }
                ]
            }
        ]
    },
    {
        "Index": 2,
        "Entities": [
            {
                "DescriptiveMentionIndex": [
                    0
                ],
                "Mentions": [
                    {
                        "Score": 0.9999880194664001,
                        "GroupScore": 1.0,
                        "Text": "My",
                        "Type": "PERSON",
                        "MentionSentiment": {
                            "Sentiment": "NEUTRAL",
                            "SentimentScore": {
                                "Positive": 0.0,
                                "Negative": 0.0,
                                "Neutral": 1.0,
                                "Mixed": 0.0
                            }
                        },
                        "BeginOffset": 0,
                        "EndOffset": 2
                    }
                ]
            },
            {
                "DescriptiveMentionIndex": [
                    0
                ],
                "Mentions": [
                    {
                        "Score": 0.9995260238647461,
                        "GroupScore": 1.0,
                        "Text": "meal",
                        "Type": "OTHER",
                        "MentionSentiment": {
                            "Sentiment": "NEUTRAL",
```

```
                            "SentimentScore": {
                                "Positive": 0.04695599898695946,
                                "Negative": 0.003226999891921878,
                                "Neutral": 0.6091709733009338,
                                "Mixed": 0.34064599871635437
                            }
                        },
                        "BeginOffset": 3,
                        "EndOffset": 7
                    }
                ]
            }
        ]
    }
    ],
    "ErrorList": []
}
```

Para obtener más información, consulte Targeted Sentiment en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte BatchDetectTargetedSentiment en la Referencia de comandos de la AWS CLI.

`classify-document`

En el siguiente ejemplo de código, se muestra cómo utilizar `classify-document`.

AWS CLI

Clasificación del documento con un punto de conexión específico del modelo

En el siguiente ejemplo de `classify-document`, se clasifica un documento con un punto de conexión de un modelo personalizado. El modelo de este ejemplo se ha entrenado para un conjunto de datos que contiene mensajes SMS etiquetados como spam o no spam (denominados falsos).

```
aws comprehend classify-document \
    --endpoint-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier-endpoint/example-classifier-endpoint \
    --text "CONGRATULATIONS! TXT 1235550100 to win $5000"
```

Salida:

```
{
    "Classes": [
        {
            "Name": "spam",
            "Score": 0.9998599290847778
        },
        {
            "Name": "ham",
            "Score": 0.00014001205272506922
        }
    ]
}
```

Para obtener más información, consulte Clasificación personalizada en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ClassifyDocument en la Referencia de comandos de la AWS CLI.

`contains-pii-entities`

En el siguiente ejemplo de código, se muestra cómo utilizar `contains-pii-entities`.

AWS CLI

Análisis del texto introducido con el fin de detectar la presencia de información de identificación personal

En el siguiente ejemplo de `contains-pii-entities`, se analiza el texto introducido para detectar la presencia de información de identificación personal (PII) y se devuelven las etiquetas de los tipos de entidades de PII identificados, como el nombre, la dirección, el número de cuenta bancaria o el número de teléfono.

```
aws comprehend contains-pii-entities \
    --language-code en \
    --text "Hello Zhang Wei, I am John. Your AnyCompany Financial Services, LLC
 credit card
        account 1111-XXXX-1111-XXXX has a minimum payment of $24.53 that is due by
 July 31st. Based on your autopay settings,
```

```
        we will withdraw your payment on the due date from your bank account number
XXXXXX1111 with the routing number XXXXX0000.
        Customer feedback for Sunshine Spa, 100 Main St, Anywhere. Send comments to
Alice at AnySpa@example.com."
```

Salida:

```
{
    "Labels": [
        {
            "Name": "NAME",
            "Score": 1.0
        },
        {
            "Name": "EMAIL",
            "Score": 1.0
        },
        {
            "Name": "BANK_ACCOUNT_NUMBER",
            "Score": 0.9995794296264648
        },
        {
            "Name": "BANK_ROUTING",
            "Score": 0.9173126816749573
        },
        {
            "Name": "CREDIT_DEBIT_NUMBER",
            "Score": 1.0
        }
}
```

Para obtener más información acerca de la lista de tipos de entidad de PII admitidos, consulte Información de identificación personal (PII) en la Guía para desarrolladores de Amazon Comprehend.

- Para ver los detalles de la API, consulte ContainsPiiEntities en la Referencia de comandos de la AWS CLI.

`create-dataset`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-dataset`.

AWS CLI

Creación de un conjunto de datos de volante de inercia

En el siguiente ejemplo de `create-dataset`, se crea un conjunto de datos para un volante de inercia. Este conjunto de datos se utilizará como datos de entrenamiento adicionales, conforme a las especificaciones de la etiqueta `--dataset-type`.

```
aws comprehend create-dataset \
    --flywheel-arn arn:aws:comprehend:us-west-2:111122223333:flywheel/flywheel-entity \
    --dataset-name example-dataset \
    --dataset-type "TRAIN" \
    --input-data-config file://inputConfig.json
```

Contenido de `file://inputConfig.json`:

```
{
    "DataFormat": "COMPREHEND_CSV",
    "DocumentClassifierInputDataConfig": {
        "S3Uri": "s3://amzn-s3-demo-bucket/training-data.csv"
    }
}
```

Salida:

```
{
    "DatasetArn": "arn:aws:comprehend:us-west-2:111122223333:flywheel/flywheel-entity/dataset/example-dataset"
}
```

Para obtener más información, consulte Flywheel Overview en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte CreateDataset en la Referencia de comandos de la AWS CLI.

`create-document-classifier`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-document-classifier`.

AWS CLI

Para crear un clasificador de documentos para clasificar los documentos

El siguiente ejemplo de `create-document-classifier` inicia el proceso de entrenamiento de un modelo de clasificador de documentos. El archivo de datos de entrenamiento, `training.csv`, se encuentra en la etiqueta `--input-data-config`. `training.csv` es un documento de dos columnas donde las etiquetas o clasificaciones se proporcionan en la primera columna y los documentos en la segunda columna.

```
aws comprehend create-document-classifier \
    --document-classifier-name example-classifier \
    --data-access-arn arn:aws:comprehend:us-west-2:111122223333:pii-entities-
detection-job/123456abcdeb0e11022f22a11EXAMPLE \
    --input-data-config "S3Uri=s3://amzn-s3-demo-bucket/" \
    --language-code en
```

Salida:

```
{
    "DocumentClassifierArn": "arn:aws:comprehend:us-west-2:111122223333:document-
classifier/example-classifier"
}
```

Para obtener más información, consulte Clasificación personalizada en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte CreateDocumentClassifier en la Referencia de comandos de la AWS CLI.

`create-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-endpoint`.

AWS CLI

Creación de un punto de conexión para un modelo personalizado

En el siguiente ejemplo de `create-endpoint`, se crea un punto de conexión de inferencia sincrónica para un modelo personalizado entrenado previamente.

```
aws comprehend create-endpoint \
    --endpoint-name example-classifier-endpoint-1 \
    --model-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier/
example-classifier \
    --desired-inference-units 1
```

Salida:

```
{
    "EndpointArn": "arn:aws:comprehend:us-west-2:111122223333:document-classifier-
endpoint/example-classifier-endpoint-1"
}
```

Para obtener más información, consulte Administración de puntos de conexión de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte CreateEndpoint en la Referencia de comandos de la AWS CLI.

`create-entity-recognizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-entity-recognizer`.

AWS CLI

Creación de un reconocedor de entidades personalizado

El siguiente ejemplo de `create-entity-recognizer`, inicia el proceso de entrenamiento de un modelo de reconocedor de entidades personalizado. En este ejemplo, se utiliza un archivo CSV que contiene documentos de entrenamiento, `raw_text.csv`, y una lista de entidades CSV, `entity_list.csv`, para entrenar el modelo. `entity-list.csv` contiene las columnas siguientes: texto y tipo.

```
aws comprehend create-entity-recognizer \
    --recognizer-name example-entity-recognizer
    --data-access-role-arn arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role \
    --input-data-config "EntityTypes=[{Type=DEVICE}],Documents={S3Uri=s3://amzn-s3-
demo-bucket/trainingdata/raw_text.csv},EntityList={S3Uri=s3://amzn-s3-demo-bucket/
trainingdata/entity_list.csv}"
    --language-code en
```

Salida:

```
{
    "EntityRecognizerArn": "arn:aws:comprehend:us-west-2:111122223333:example-
entity-recognizer/entityrecognizer1"
}
```

Para obtener más información, consulte Custom entity recognition en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte CreateEntityRecognizer en la Referencia de comandos de la AWS CLI.

`create-flywheel`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-flywheel`.

AWS CLI

Creación de un volante de inercia

El siguiente ejemplo de `create-flywheel` crea un volante de inercia para orquestar el entrenamiento continuo de un modelo de clasificación de documentos o de reconocimiento de entidades. El volante de inercia de este ejemplo se ha creado para administrar un modelo entrenado existente especificado por la etiqueta `--active-model-arn`. Cuando se crea el volante de inercia, se crea asimismo un lago de datos en la etiqueta `--input-data-lake`.

```
aws comprehend create-flywheel \
    --flywheel-name example-flywheel \
    --active-model-arn arn:aws:comprehend:us-west-2:111122223333:document-
classifier/example-model/version/1 \
    --data-access-role-arn arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role \
    --data-lake-s3-uri "s3://amzn-s3-demo-bucket"
```

Salida:

```
{
    "FlywheelArn": "arn:aws:comprehend:us-west-2:111122223333:flywheel/example-
flywheel"
}
```

Para obtener más información, consulte Flywheel Overview en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte CreateFlywheel en la Referencia de comandos de la AWS CLI.

`delete-document-classifier`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-document-classifier`.

AWS CLI

Para eliminar un clasificador de documentos personalizado

En el siguiente ejemplo de `delete-document-classifier`, se elimina un modelo de clasificador de documentos personalizado.

```
aws comprehend delete-document-classifier \
    --document-classifier-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier/example-classifier-1
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración de puntos de conexión de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte DeleteDocumentClassifier en la Referencia de comandos de la AWS CLI.

`delete-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-endpoint`.

AWS CLI

Para eliminar un punto de enlace de un modelo personalizado

En el siguiente ejemplo de `delete-endpoint`, se elimina un punto de enlace específico del modelo. Para poder eliminar el modelo, se deben borrar todos los puntos de enlace.

```
aws comprehend delete-endpoint \
```

```
    --endpoint-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier-endpoint/example-classifier-endpoint-1
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración de puntos de conexión de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DeleteEndpoint en la Referencia de comandos de la AWS CLI.

`delete-entity-recognizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-entity-recognizer`.

AWS CLI

Eliminación de un modelo de reconocedor de entidades personalizado

En el siguiente ejemplo de `delete-entity-recognizer`, se elimina un modelo de reconocedor de entidades personalizado.

```
aws comprehend delete-entity-recognizer \
    --entity-recognizer-arn arn:aws:comprehend:us-west-2:111122223333:entity-recognizer/example-entity-recognizer-1
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración de puntos de conexión de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DeleteEntityRecognizer en la Referencia de comandos de la AWS CLI.

`delete-flywheel`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-flywheel`.

AWS CLI

Cómo eliminar un volante de inercia

En el siguiente ejemplo de `delete-flywheel` se elimina un volante de inercia. No se elimina ni el lago de datos ni el modelo asociado al volante de inercia.

```
aws comprehend delete-flywheel \
    --flywheel-arn arn:aws:comprehend:us-west-2:111122223333:flywheel/example-flywheel-1
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Flywheel overview en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DeleteFlywheel en la Referencia de comandos de la AWS CLI.

`delete-resource-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-resource-policy`.

AWS CLI

Cómo eliminar una política basada en recursos

El siguiente ejemplo de `delete-resource-policy` elimina una política basada en recursos de un recurso de Amazon Comprehend.

```
aws comprehend delete-resource-policy \
    --resource-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier/example-classifier-1/version/1
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Copying custom models between AWS accounts en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DeleteResourcePolicy en la Referencia de comandos de la AWS CLI.

`describe-dataset`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-dataset`.

AWS CLI

Descripción de un conjunto de datos de volante de inercia

En el siguiente ejemplo de `describe-dataset`, se obtienen las propiedades de un conjunto de datos de volante de inercia.

```
aws comprehend describe-dataset \
    --dataset-arn arn:aws:comprehend:us-west-2:111122223333:flywheel/flywheel-entity/dataset/example-dataset
```

Salida:

```
{
    "DatasetProperties": {
        "DatasetArn": "arn:aws:comprehend:us-west-2:111122223333:flywheel/flywheel-entity/dataset/example-dataset",
        "DatasetName": "example-dataset",
        "DatasetType": "TRAIN",
        "DatasetS3Uri": "s3://amzn-s3-demo-bucket/flywheel-entity/schemaVersion=1/12345678A123456Z/datasets/example-dataset/20230616T203710Z/",
        "Status": "CREATING",
        "CreationTime": "2023-06-16T20:37:10.400000+00:00"
    }
}
```

Para obtener más información, consulte Flywheel Overview en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DescribeDataset en la Referencia de comandos de la AWS CLI.

`describe-document-classification-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-document-classification-job`.

AWS CLI

Para describir un trabajo de clasificación de documentos

En el siguiente ejemplo de `describe-document-classification-job`, se obtienen las propiedades de un trabajo de clasificación de documentos asíncrono.

```
aws comprehend describe-document-classification-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "DocumentClassificationJobProperties": {
        "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
        "JobArn": "arn:aws:comprehend:us-west-2:111122223333:document-
classification-job/123456abcdeb0e11022f22a11EXAMPLE",
        "JobName": "exampleclassificationjob",
        "JobStatus": "COMPLETED",
        "SubmitTime": "2023-06-14T17:09:51.788000+00:00",
        "EndTime": "2023-06-14T17:15:58.582000+00:00",
        "DocumentClassifierArn": "arn:aws:comprehend:us-
west-2:111122223333:document-classifier/mymodel/version/1",
        "InputDataConfig": {
            "S3Uri": "s3://amzn-s3-demo-bucket/jobdata/",
            "InputFormat": "ONE_DOC_PER_LINE"
        },
        "OutputDataConfig": {
            "S3Uri": "s3://amzn-s3-demo-destination-bucket/testfolder/111122223333-
CLN-123456abcdeb0e11022f22a11EXAMPLE/output/output.tar.gz"
        },
        "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-servicerole"
    }
}
```

Para obtener más información, consulte Clasificación personalizada en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte DescribeDocumentClassificationJob en la Referencia de comandos de la AWS CLI.

`describe-document-classifier`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-document-classifier`.

AWS CLI

Para describir un clasificador de documentos

En el siguiente ejemplo de `describe-document-classifier`, se obtienen las propiedades de un modelo de clasificador de documentos personalizado.

```
aws comprehend describe-document-classifier \
    --document-classifier-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier/example-classifier-1
```

Salida:

```
{
    "DocumentClassifierProperties": {
        "DocumentClassifierArn": "arn:aws:comprehend:us-
west-2:111122223333:document-classifier/example-classifier-1",
        "LanguageCode": "en",
        "Status": "TRAINED",
        "SubmitTime": "2023-06-13T19:04:15.735000+00:00",
        "EndTime": "2023-06-13T19:42:31.752000+00:00",
        "TrainingStartTime": "2023-06-13T19:08:20.114000+00:00",
        "TrainingEndTime": "2023-06-13T19:41:35.080000+00:00",
        "InputDataConfig": {
            "DataFormat": "COMPREHEND_CSV",
            "S3Uri": "s3://amzn-s3-demo-bucket/trainingdata"
        },
        "OutputDataConfig": {},
        "ClassifierMetadata": {
            "NumberOfLabels": 3,
            "NumberOfTrainedDocuments": 5016,
            "NumberOfTestDocuments": 557,
            "EvaluationMetrics": {
                "Accuracy": 0.9856,
                "Precision": 0.9919,
                "Recall": 0.9459,
                "F1Score": 0.9673,
                "MicroPrecision": 0.9856,
                "MicroRecall": 0.9856,
                "MicroF1Score": 0.9856,
                "HammingLoss": 0.0144
            }
        },
```

```
        "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role",
        "Mode": "MULTI_CLASS"
    }
}
```

Para obtener más información, consulte Creación y administración de modelos personalizados en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte DescribeDocumentClassifier en la Referencia de comandos de la AWS CLI.

`describe-dominant-language-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-dominant-language-detection-job`.

AWS CLI

Descripción de un trabajo de detección del idioma dominante.

En el siguiente ejemplo de `describe-dominant-language-detection-job`, se obtienen las propiedades de un trabajo de detección de idioma dominante.

```
aws comprehend describe-dominant-language-detection-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "DominantLanguageDetectionJobProperties": {
        "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
        "JobArn": "arn:aws:comprehend:us-west-2:111122223333:dominant-language-
detection-job/123456abcdeb0e11022f22a11EXAMPLE",
        "JobName": "languageanalysis1",
        "JobStatus": "IN_PROGRESS",
        "SubmitTime": "2023-06-09T18:10:38.037000+00:00",
        "InputDataConfig": {
            "S3Uri": "s3://amzn-s3-demo-bucket",
            "InputFormat": "ONE_DOC_PER_LINE"
        },
        "OutputDataConfig": {
```

```
            "S3Uri": "s3://amzn-s3-demo-destination-bucket/testfolder/111122223333-
LANGUAGE-123456abcdeb0e11022f22a11EXAMPLE/output/output.tar.gz"
        },
        "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role"
    }
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DescribeDominantLanguageDetectionJob en la Referencia de comandos de la AWS CLI.

`describe-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-endpoint`.

AWS CLI

Descripción de un punto de conexión específico

En el siguiente ejemplo de `describe-endpoint`, se obtienen las propiedades de un punto de conexión específico del modelo.

```
aws comprehend describe-endpoint \
    --endpoint-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier-
endpoint/example-classifier-endpoint
```

Salida:

```
{
    "EndpointProperties": {
        "EndpointArn": "arn:aws:comprehend:us-west-2:111122223333:document-
classifier-endpoint/example-classifier-endpoint",
        "Status": "IN_SERVICE",
        "ModelArn": "arn:aws:comprehend:us-west-2:111122223333:document-classifier/
exampleclassifier1",
        "DesiredModelArn": "arn:aws:comprehend:us-west-2:111122223333:document-
classifier/exampleclassifier1",
        "DesiredInferenceUnits": 1,
        "CurrentInferenceUnits": 1,
```

```
        "CreationTime": "2023-06-13T20:32:54.526000+00:00",
        "LastModifiedTime": "2023-06-13T20:32:54.526000+00:00"
    }
}
```

Para obtener más información, consulte Administración de puntos de conexión de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte DescribeEndpoint en la Referencia de comandos de la AWS CLI.

`describe-entities-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-entities-detection-job`.

AWS CLI

Descripción de un trabajo de detección de entidades

En el siguiente ejemplo de `describe-entities-detection-job`, se obtienen las propiedades de un trabajo de detección de entidades asíncrono.

```
aws comprehend describe-entities-detection-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "EntitiesDetectionJobProperties": {
        "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
        "JobArn": "arn:aws:comprehend:us-west-2:111122223333:entities-detection-
job/123456abcdeb0e11022f22a11EXAMPLE",
        "JobName": "example-entity-detector",
        "JobStatus": "COMPLETED",
        "SubmitTime": "2023-06-08T21:30:15.323000+00:00",
        "EndTime": "2023-06-08T21:40:23.509000+00:00",
        "InputDataConfig": {
            "S3Uri": "s3://amzn-s3-demo-bucket/AsyncBatchJobs/",
            "InputFormat": "ONE_DOC_PER_LINE"
        },
        "OutputDataConfig": {
```

```
            "S3Uri": "s3://amzn-s3-demo-bucket/thefolder/111122223333-
NER-123456abcdeb0e11022f22a11EXAMPLE/output/output.tar.gz"
        },
        "LanguageCode": "en",
        "DataAccessRoleArn": "arn:aws:iam::12345678012:role/service-role/
AmazonComprehendServiceRole-example-role"
    }
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DescribeEntitiesDetectionJob en la Referencia de comandos de la AWS CLI.

`describe-entity-recognizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-entity-recognizer`.

AWS CLI

Descripción de un reconocedor de entidades

En el siguiente ejemplo de `describe-entity-recognizer`, se obtienen las propiedades de un modelo de reconocedor de entidades personalizado.

```
aws comprehend describe-entity-recognizer \
    entity-recognizer-arn arn:aws:comprehend:us-west-2:111122223333:entity-
recognizer/business-recongizer-1/version/1
```

Salida:

```
{
    "EntityRecognizerProperties": {
        "EntityRecognizerArn": "arn:aws:comprehend:us-west-2:111122223333:entity-
recognizer/business-recongizer-1/version/1",
        "LanguageCode": "en",
        "Status": "TRAINED",
        "SubmitTime": "2023-06-14T20:44:59.631000+00:00",
        "EndTime": "2023-06-14T20:59:19.532000+00:00",
        "TrainingStartTime": "2023-06-14T20:48:52.811000+00:00",
        "TrainingEndTime": "2023-06-14T20:58:11.473000+00:00",
```

```
        "InputDataConfig": {
            "DataFormat": "COMPREHEND_CSV",
            "EntityTypes": [
                {
                    "Type": "BUSINESS"
                }
            ],
            "Documents": {
                "S3Uri": "s3://amzn-s3-demo-bucket/trainingdata/dataset/",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "EntityList": {
                "S3Uri": "s3://amzn-s3-demo-bucket/trainingdata/entity.csv"
            }
        },
        "RecognizerMetadata": {
            "NumberOfTrainedDocuments": 1814,
            "NumberOfTestDocuments": 486,
            "EvaluationMetrics": {
                "Precision": 100.0,
                "Recall": 100.0,
                "F1Score": 100.0
            },
            "EntityTypes": [
                {
                    "Type": "BUSINESS",
                    "EvaluationMetrics": {
                        "Precision": 100.0,
                        "Recall": 100.0,
                        "F1Score": 100.0
                    },
                    "NumberOfTrainMentions": 1520
                }
            ]
        },
        "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role",
        "VersionName": "1"
    }
}
```

Para obtener más información, consulte Custom entity recognition en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DescribeEntityRecognizer en la Referencia de comandos de la AWS CLI.

`describe-events-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-events-detection-job`.

AWS CLI

Descripción de un trabajo de detección de eventos.

En el siguiente ejemplo de `describe-events-detection-job`, se obtienen las propiedades de un trabajo de detección de eventos asíncrono.

```
aws comprehend describe-events-detection-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "EventsDetectionJobProperties": {
        "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
        "JobArn": "arn:aws:comprehend:us-west-2:111122223333:events-detection-
job/123456abcdeb0e11022f22a11EXAMPLE",
        "JobName": "events_job_1",
        "JobStatus": "IN_PROGRESS",
        "SubmitTime": "2023-06-12T18:45:56.054000+00:00",
        "InputDataConfig": {
            "S3Uri": "s3://amzn-s3-demo-bucket/EventsData",
            "InputFormat": "ONE_DOC_PER_LINE"
        },
        "OutputDataConfig": {
            "S3Uri": "s3://amzn-s3-demo-destination-bucket/testfolder/111122223333-
EVENTS-123456abcdeb0e11022f22a11EXAMPLE/output/"
        },
        "LanguageCode": "en",
        "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role",
        "TargetEventTypes": [
            "BANKRUPTCY",
            "EMPLOYMENT",
            "CORPORATE_ACQUISITION",
```

```
            "CORPORATE_MERGER",
            "INVESTMENT_GENERAL"
        ]
    }
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DescribeEventsDetectionJob en la Referencia de comandos de la AWS CLI.

`describe-flywheel-iteration`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-flywheel-iteration`.

AWS CLI

Descripción de una iteración del volante de inercia

En el siguiente ejemplo de `describe-flywheel-iteration`, se obtienen las propiedades de una iteración de volante de inercia.

```
aws comprehend describe-flywheel-iteration \
    --flywheel-arn arn:aws:comprehend:us-west-2:111122223333:flywheel/example-flywheel \
    --flywheel-iteration-id 20232222AEXAMPLE
```

Salida:

```
{
    "FlywheelIterationProperties": {
        "FlywheelArn": "arn:aws:comprehend:us-west-2:111122223333:flywheel/flywheel-entity",
        "FlywheelIterationId": "20232222AEXAMPLE",
        "CreationTime": "2023-06-16T21:10:26.385000+00:00",
        "EndTime": "2023-06-16T23:33:16.827000+00:00",
        "Status": "COMPLETED",
        "Message": "FULL_ITERATION: Flywheel iteration performed all functions successfully.",
        "EvaluatedModelArn": "arn:aws:comprehend:us-west-2:111122223333:document-classifier/example-classifier/version/1",
        "EvaluatedModelMetrics": {
```

```
            "AverageF1Score": 0.7742663922375772,
            "AveragePrecision": 0.8287636394041166,
            "AverageRecall": 0.7427084833645399,
            "AverageAccuracy": 0.8795394154118689
        },
        "TrainedModelArn": "arn:aws:comprehend:us-west-2:111122223333:document-
classifier/example-classifier/version/Comprehend-Generated-v1-bb52d585",
        "TrainedModelMetrics": {
            "AverageF1Score": 0.9767700253081214,
            "AveragePrecision": 0.9767700253081214,
            "AverageRecall": 0.9767700253081214,
            "AverageAccuracy": 0.9858281665190434
        },
        "EvaluationManifestS3Prefix": "s3://amzn-s3-demo-destination-bucket/
flywheel-entity/schemaVersion=1/20230616T200543Z/evaluation/20230616T211026Z/"
    }
}
```

Para obtener más información, consulte Flywheel overview en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DescribeFlywheelIteration en la Referencia de comandos de la AWS CLI.

`describe-flywheel`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-flywheel`.

AWS CLI

Descripción de un volante de inercia

En el siguiente ejemplo de `describe-flywheel`, se obtienen las propiedades de un volante de inercia. En este ejemplo, el modelo asociado al volante de inercia es un modelo de clasificador personalizado que está entrenado para clasificar los documentos como spam o no spam, o bien como falsos.

```
aws comprehend describe-flywheel \
    --flywheel-arn arn:aws:comprehend:us-west-2:111122223333:flywheel/example-
flywheel
```

Salida:

```
{
    "FlywheelProperties": {
        "FlywheelArn": "arn:aws:comprehend:us-west-2:111122223333:flywheel/example-
flywheel",
        "ActiveModelArn": "arn:aws:comprehend:us-west-2:111122223333:document-
classifier/example-model/version/1",
        "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role",
        "TaskConfig": {
            "LanguageCode": "en",
            "DocumentClassificationConfig": {
                "Mode": "MULTI_CLASS",
                "Labels": [
                    "ham",
                    "spam"
                ]
            }
        },
        "DataLakeS3Uri": "s3://amzn-s3-demo-bucket/example-flywheel/
schemaVersion=1/20230616T200543Z/",
        "DataSecurityConfig": {},
        "Status": "ACTIVE",
        "ModelType": "DOCUMENT_CLASSIFIER",
        "CreationTime": "2023-06-16T20:05:43.242000+00:00",
        "LastModifiedTime": "2023-06-16T20:21:43.567000+00:00"
    }
}
```

Para obtener más información, consulte Flywheel Overview en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DescribeFlywheel en la Referencia de comandos de la AWS CLI.

`describe-key-phrases-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-key-phrases-detection-job`.

AWS CLI

Descripción de un trabajo de detección de frases clave

En el siguiente ejemplo de `describe-key-phrases-detection-job`, se obtienen las propiedades de un trabajo de detección de frases clave asíncronas.

```
aws comprehend describe-key-phrases-detection-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "KeyPhrasesDetectionJobProperties": {
        "JobId": "69aa080c00fc68934a6a98f10EXAMPLE",
        "JobArn": "arn:aws:comprehend:us-west-2:111122223333:key-phrases-detection-
job/69aa080c00fc68934a6a98f10EXAMPLE",
        "JobName": "example-key-phrases-detection-job",
        "JobStatus": "COMPLETED",
        "SubmitTime": 1686606439.177,
        "EndTime": 1686606806.157,
        "InputDataConfig": {
            "S3Uri": "s3://dereksbucket1001/EventsData/",
            "InputFormat": "ONE_DOC_PER_LINE"
        },
        "OutputDataConfig": {
            "S3Uri": "s3://dereksbucket1002/testfolder/111122223333-
KP-69aa080c00fc68934a6a98f10EXAMPLE/output/output.tar.gz"
        },
        "LanguageCode": "en",
        "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-testrole"
    }
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DescribeKeyPhrasesDetectionJob en la Referencia de comandos de la AWS CLI.

`describe-pii-entities-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-pii-entities-detection-job`.

AWS CLI

Descripción de un trabajo de detección de entidades de PII

En el siguiente ejemplo de `describe-pii-entities-detection-job`, se obtienen las propiedades de un trabajo de detección de entidades de PII asíncrono.

```
aws comprehend describe-pii-entities-detection-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "PiiEntitiesDetectionJobProperties": {
        "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
        "JobArn": "arn:aws:comprehend:us-west-2:111122223333:pii-entities-detection-
job/123456abcdeb0e11022f22a11EXAMPLE",
        "JobName": "example-pii-entities-job",
        "JobStatus": "IN_PROGRESS",
        "SubmitTime": "2023-06-08T21:30:15.323000+00:00",
        "EndTime": "2023-06-08T21:40:23.509000+00:00",
        "InputDataConfig": {
            "S3Uri": "s3://amzn-s3-demo-bucket/AsyncBatchJobs/",
            "InputFormat": "ONE_DOC_PER_LINE"
        },
        "OutputDataConfig": {
            "S3Uri": "s3://amzn-s3-demo-bucket/thefolder/111122223333-
NER-123456abcdeb0e11022f22a11EXAMPLE/output/output.tar.gz"
        },
        "LanguageCode": "en",
        "DataAccessRoleArn": "arn:aws:iam::12345678012:role/service-role/
AmazonComprehendServiceRole-example-role"
    }
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DescribePiiEntitiesDetectionJob en la Referencia de comandos de la AWS CLI.

`describe-resource-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-resource-policy`.

AWS CLI

Descripción de una política de recursos adjunta a un modelo

En el siguiente ejemplo de `describe-resource-policy`, se obtienen las propiedades de una política basada en recursos asociada a un modelo.

```
aws comprehend describe-resource-policy \
    --resource-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier/
example-classifier/version/1
```

Salida:

```
{
    "ResourcePolicy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":
\"Allow\",\"Principal\":{\"AWS\":\"arn:aws:iam::444455556666:root\"},\"Action\":
\"comprehend:ImportModel\",\"Resource\":\"*\"}]}",
    "CreationTime": "2023-06-19T18:44:26.028000+00:00",
    "LastModifiedTime": "2023-06-19T18:53:02.002000+00:00",
    "PolicyRevisionId": "baa675d069d07afaa2aa3106ae280f61"
}
```

Para obtener más información, consulte Copying custom models between AWS accounts en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DescribeResourcePolicy en la Referencia de comandos de la AWS CLI.

`describe-sentiment-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-sentiment-detection-job`.

AWS CLI

Descripción de un trabajo de detección de opiniones

En el siguiente ejemplo de `describe-sentiment-detection-job`, se obtienen las propiedades de un trabajo de detección de opiniones asíncrono.

```
aws comprehend describe-sentiment-detection-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "SentimentDetectionJobProperties": {
        "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
        "JobArn": "arn:aws:comprehend:us-west-2:111122223333:sentiment-detection-
job/123456abcdeb0e11022f22a11EXAMPLE",
        "JobName": "movie_review_analysis",
        "JobStatus": "IN_PROGRESS",
        "SubmitTime": "2023-06-09T23:16:15.956000+00:00",
        "InputDataConfig": {
            "S3Uri": "s3://amzn-s3-demo-bucket/MovieData",
            "InputFormat": "ONE_DOC_PER_LINE"
        },
        "OutputDataConfig": {
            "S3Uri": "s3://amzn-s3-demo-destination-bucket/testfolder/111122223333-
TS-123456abcdeb0e11022f22a11EXAMPLE/output/output.tar.gz"
        },
        "LanguageCode": "en",
        "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-servicerole"
    }
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DescribeSentimentDetectionJob en la Referencia de comandos de la AWS CLI.

`describe-targeted-sentiment-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-targeted-sentiment-detection-job`.

AWS CLI

Descripción de un trabajo de detección de opiniones dirigido

En el siguiente ejemplo de `describe-targeted-sentiment-detection-job`, se obtienen las propiedades de un trabajo de detección de opiniones específicas asíncrono.

```
aws comprehend describe-targeted-sentiment-detection-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "TargetedSentimentDetectionJobProperties": {
        "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
        "JobArn": "arn:aws:comprehend:us-west-2:111122223333:targeted-sentiment-
detection-job/123456abcdeb0e11022f22a11EXAMPLE",
        "JobName": "movie_review_analysis",
        "JobStatus": "IN_PROGRESS",
        "SubmitTime": "2023-06-09T23:16:15.956000+00:00",
        "InputDataConfig": {
            "S3Uri": "s3://amzn-s3-demo-bucket/MovieData",
            "InputFormat": "ONE_DOC_PER_LINE"
        },
        "OutputDataConfig": {
            "S3Uri": "s3://amzn-s3-demo-destination-bucket/testfolder/111122223333-
TS-123456abcdeb0e11022f22a11EXAMPLE/output/output.tar.gz"
        },
        "LanguageCode": "en",
        "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-servicerole"
    }
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DescribeTargetedSentimentDetectionJob en la Referencia de comandos de la AWS CLI.

describe-topics-detection-job

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-topics-detection-job`.

AWS CLI

Para describir un trabajo de detección de temas

En el siguiente ejemplo de `describe-topics-detection-job`, se obtienen las propiedades de un trabajo de detección de temas asíncrono.

```
aws comprehend describe-topics-detection-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "TopicsDetectionJobProperties": {
        "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
        "JobArn": "arn:aws:comprehend:us-west-2:111122223333:topics-detection-
job/123456abcdeb0e11022f22a11EXAMPLE",
        "JobName": "example_topics_detection",
        "JobStatus": "IN_PROGRESS",
        "SubmitTime": "2023-06-09T18:44:43.414000+00:00",
        "InputDataConfig": {
            "S3Uri": "s3://amzn-s3-demo-bucket",
            "InputFormat": "ONE_DOC_PER_LINE"
        },
        "OutputDataConfig": {
            "S3Uri": "s3://amzn-s3-demo-destination-bucket/testfolder/111122223333-
TOPICS-123456abcdeb0e11022f22a11EXAMPLE/output/output.tar.gz"
        },
        "NumberOfTopics": 10,
        "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-examplerole"
    }
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte DescribeTopicsDetectionJob en la Referencia de comandos de la AWS CLI.

`detect-dominant-language`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-dominant-language`.

AWS CLI

Para detectar el idioma dominante del texto de entrada

El siguiente `detect-dominant-language` analiza el texto de entrada e identifica el idioma dominante. También se muestra la puntuación de confianza del modelo previamente entrenado.

```
aws comprehend detect-dominant-language \
    --text "It is a beautiful day in Seattle."
```

Salida:

```
{
    "Languages": [
        {
            "LanguageCode": "en",
            "Score": 0.9877256155014038
        }
    ]
}
```

Para obtener más información, consulte Idioma dominante en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte DetectDominantLanguage en la Referencia de comandos de AWS CLI.

`detect-entities`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-entities`.

AWS CLI

Detección de entidades con nombre en el texto de entrada

El siguiente ejemplo de `detect-entities` analiza el texto de entrada y devuelve las entidades nombradas. La puntuación de confianza del modelo previamente entrenado también se muestra para cada predicción.

```
aws comprehend detect-entities \
    --language-code en \
    --text "Hello Zhang Wei, I am John. Your AnyCompany Financial Services, LLC
 credit card \
    account 1111-XXXX-1111-XXXX has a minimum payment of $24.53 that is due by July
 31st. Based on your autopay settings, \
    we will withdraw your payment on the due date from your bank account number
 XXXXXX1111 with the routing number XXXXX0000. \
    Customer feedback for Sunshine Spa, 123 Main St, Anywhere. Send comments to
 Alice at AnySpa@example.com."
```

Salida:

```
{
    "Entities": [
        {
            "Score": 0.9994556307792664,
            "Type": "PERSON",
            "Text": "Zhang Wei",
            "BeginOffset": 6,
            "EndOffset": 15
        },
        {
            "Score": 0.9981022477149963,
            "Type": "PERSON",
            "Text": "John",
            "BeginOffset": 22,
            "EndOffset": 26
        },
        {
            "Score": 0.9986887574195862,
            "Type": "ORGANIZATION",
            "Text": "AnyCompany Financial Services, LLC",
            "BeginOffset": 33,
            "EndOffset": 67
        },
        {
            "Score": 0.9959119558334351,
            "Type": "OTHER",
            "Text": "1111-XXXX-1111-XXXX",
            "BeginOffset": 88,
            "EndOffset": 107
        },
```

```
        {
            "Score": 0.9708039164543152,
            "Type": "QUANTITY",
            "Text": ".53",
            "BeginOffset": 133,
            "EndOffset": 136
        },
        {
            "Score": 0.9987268447875977,
            "Type": "DATE",
            "Text": "July 31st",
            "BeginOffset": 152,
            "EndOffset": 161
        },
        {
            "Score": 0.9858865737915039,
            "Type": "OTHER",
            "Text": "XXXXXX1111",
            "BeginOffset": 271,
            "EndOffset": 281
        },
        {
            "Score": 0.9700471758842468,
            "Type": "OTHER",
            "Text": "XXXXX0000",
            "BeginOffset": 306,
            "EndOffset": 315
        },
        {
            "Score": 0.9591118693351746,
            "Type": "ORGANIZATION",
            "Text": "Sunshine Spa",
            "BeginOffset": 340,
            "EndOffset": 352
        },
        {
            "Score": 0.9797496795654297,
            "Type": "LOCATION",
            "Text": "123 Main St",
            "BeginOffset": 354,
            "EndOffset": 365
        },
        {
            "Score": 0.994929313659668,
```

```
            "Type": "PERSON",
            "Text": "Alice",
            "BeginOffset": 394,
            "EndOffset": 399
        },
        {
            "Score": 0.9949769377708435,
            "Type": "OTHER",
            "Text": "AnySpa@example.com",
            "BeginOffset": 403,
            "EndOffset": 418
        }
    ]
}
```

Para obtener más información, consulte Entidades en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte DetectEntities en la Referencia de comandos de la AWS CLI.

`detect-key-phrases`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-key-phrases`.

AWS CLI

Para detectar frases clave en el texto de entrada

El siguiente ejemplo de `detect-key-phrases` analiza el texto de entrada e identifica las frases nominales clave. La puntuación de confianza del modelo previamente entrenado también se muestra para cada predicción.

```
aws comprehend detect-key-phrases \
    --language-code en \
    --text "Hello Zhang Wei, I am John. Your AnyCompany Financial Services, LLC
 credit card \
        account 1111-XXXX-1111-XXXX has a minimum payment of $24.53 that is due by
 July 31st. Based on your autopay settings, \
        we will withdraw your payment on the due date from your bank account number
 XXXXXX1111 with the routing number XXXXX0000. \
```

```
        Customer feedback for Sunshine Spa, 123 Main St, Anywhere. Send comments to
 Alice at AnySpa@example.com."
```

Salida:

```
{
    "KeyPhrases": [
        {
            "Score": 0.8996376395225525,
            "Text": "Zhang Wei",
            "BeginOffset": 6,
            "EndOffset": 15
        },
        {
            "Score": 0.9992469549179077,
            "Text": "John",
            "BeginOffset": 22,
            "EndOffset": 26
        },
        {
            "Score": 0.988385021686554,
            "Text": "Your AnyCompany Financial Services",
            "BeginOffset": 28,
            "EndOffset": 62
        },
        {
            "Score": 0.8740853071212769,
            "Text": "LLC credit card account 1111-XXXX-1111-XXXX",
            "BeginOffset": 64,
            "EndOffset": 107
        },
        {
            "Score": 0.9999437928199768,
            "Text": "a minimum payment",
            "BeginOffset": 112,
            "EndOffset": 129
        },
        {
            "Score": 0.9998900890350342,
            "Text": ".53",
            "BeginOffset": 133,
            "EndOffset": 136
        },
```

```
        {
            "Score": 0.9979453086853027,
            "Text": "July 31st",
            "BeginOffset": 152,
            "EndOffset": 161
        },
        {
            "Score": 0.9983011484146118,
            "Text": "your autopay settings",
            "BeginOffset": 172,
            "EndOffset": 193
        },
        {
            "Score": 0.9996572136878967,
            "Text": "your payment",
            "BeginOffset": 211,
            "EndOffset": 223
        },
        {
            "Score": 0.9995037317276001,
            "Text": "the due date",
            "BeginOffset": 227,
            "EndOffset": 239
        },
        {
            "Score": 0.9702621698379517,
            "Text": "your bank account number XXXXXX1111",
            "BeginOffset": 245,
            "EndOffset": 280
        },
        {
            "Score": 0.9179925918579102,
            "Text": "the routing number XXXXX0000.Customer feedback",
            "BeginOffset": 286,
            "EndOffset": 332
        },
        {
            "Score": 0.9978160858154297,
            "Text": "Sunshine Spa",
            "BeginOffset": 337,
            "EndOffset": 349
        },
        {
            "Score": 0.9706913232803345,
```

```
            "Text": "123 Main St",
            "BeginOffset": 351,
            "EndOffset": 362
        },
        {
            "Score": 0.9941995143890381,
            "Text": "comments",
            "BeginOffset": 379,
            "EndOffset": 387
        },
        {
            "Score": 0.9759287238121033,
            "Text": "Alice",
            "BeginOffset": 391,
            "EndOffset": 396
        },
        {
            "Score": 0.8376792669296265,
            "Text": "AnySpa@example.com",
            "BeginOffset": 400,
            "EndOffset": 415
        }
    ]
}
```

Para obtener más información, consulte Frases clave en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte DetectKeyPhrases en la Referencia de comandos de la AWS CLI.

`detect-pii-entities`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-pii-entities`.

AWS CLI

Para detectar entidades pii con nombre en el texto de entrada

En el siguiente ejemplo de `detect-pii-entities` se analiza el texto de entrada e identifica las entidades que contienen información de identificación personal (PII, por sus siglas en inglés). La puntuación de confianza del modelo previamente entrenado también se muestra para cada predicción.

```
aws comprehend detect-pii-entities \
    --language-code en \
    --text "Hello Zhang Wei, I am John. Your AnyCompany Financial Services, LLC
 credit card \
       account 1111-XXXX-1111-XXXX has a minimum payment of $24.53 that is due by
 July 31st. Based on your autopay settings, \
       we will withdraw your payment on the due date from your bank account number
 XXXXXX1111 with the routing number XXXXX0000. \
       Customer feedback for Sunshine Spa, 123 Main St, Anywhere. Send comments to
 Alice at AnySpa@example.com."
```

Salida:


```
{
    "Entities": [
        {
            "Score": 0.9998322129249573,
            "Type": "NAME",
            "BeginOffset": 6,
            "EndOffset": 15
        },
        {
            "Score": 0.9998878240585327,
            "Type": "NAME",
            "BeginOffset": 22,
            "EndOffset": 26
        },
        {
            "Score": 0.9994089603424072,
            "Type": "CREDIT_DEBIT_NUMBER",
            "BeginOffset": 88,
            "EndOffset": 107
        },
        {
            "Score": 0.9999760985374451,
            "Type": "DATE_TIME",
            "BeginOffset": 152,
            "EndOffset": 161
        },
        {
            "Score": 0.9999449253082275,
            "Type": "BANK_ACCOUNT_NUMBER",
            "BeginOffset": 271,
```

```
            "EndOffset": 281
        },
        {
            "Score": 0.9999847412109375,
            "Type": "BANK_ROUTING",
            "BeginOffset": 306,
            "EndOffset": 315
        },
        {
            "Score": 0.999925434589386,
            "Type": "ADDRESS",
            "BeginOffset": 354,
            "EndOffset": 365
        },
        {
            "Score": 0.9989161491394043,
            "Type": "NAME",
            "BeginOffset": 394,
            "EndOffset": 399
        },
        {
            "Score": 0.9994171857833862,
            "Type": "EMAIL",
            "BeginOffset": 403,
            "EndOffset": 418
        }
    ]
}
```

Para obtener más información acerca de la lista de tipos de entidad de PII admitidos, consulte Información de identificación personal (PII) en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte DetectPiiEntities en la Referencia de comandos de la AWS CLI.

`detect-sentiment`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-sentiment`.

AWS CLI

Para detectar la opinión de un texto de entrada

El siguiente ejemplo de `detect-sentiment` analiza el texto de entrada y devuelve una inferencia de la opinión predominante (`POSITIVE`, `NEUTRAL`, `MIXED` o `NEGATIVE`).

```
aws comprehend detect-sentiment \
    --language-code en \
    --text "It is a beautiful day in Seattle"
```

Salida:

```
{
    "Sentiment": "POSITIVE",
    "SentimentScore": {
        "Positive": 0.9976957440376282,
        "Negative": 9.653854067437351e-05,
        "Neutral": 0.002169104292988777,
        "Mixed": 3.857641786453314e-05
    }
}
```

Para obtener más información, consulte Opinión en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte DetectSentiment en la Referencia de comandos de la AWS CLI.

`detect-syntax`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-syntax`.

AWS CLI

Para detectar las partes del discurso en un texto de entrada

El siguiente ejemplo de `detect-syntax` analiza la sintaxis del texto de entrada y devuelve las distintas partes de la oración. La puntuación de confianza del modelo previamente entrenado también se muestra para cada predicción.

```
aws comprehend detect-syntax \
    --language-code en \
    --text "It is a beautiful day in Seattle."
```

Salida:


```
{
    "SyntaxTokens": [
        {
            "TokenId": 1,
            "Text": "It",
            "BeginOffset": 0,
            "EndOffset": 2,
            "PartOfSpeech": {
                "Tag": "PRON",
                "Score": 0.9999740719795227
            }
        },
        {
            "TokenId": 2,
            "Text": "is",
            "BeginOffset": 3,
            "EndOffset": 5,
            "PartOfSpeech": {
                "Tag": "VERB",
                "Score": 0.999901294708252
            }
        },
        {
            "TokenId": 3,
            "Text": "a",
            "BeginOffset": 6,
            "EndOffset": 7,
            "PartOfSpeech": {
                "Tag": "DET",
                "Score": 0.9999938607215881
            }
        },
        {
            "TokenId": 4,
            "Text": "beautiful",
            "BeginOffset": 8,
            "EndOffset": 17,
            "PartOfSpeech": {
                "Tag": "ADJ",
                "Score": 0.9987351894378662
            }
        },
```

```
        {
            "TokenId": 5,
            "Text": "day",
            "BeginOffset": 18,
            "EndOffset": 21,
            "PartOfSpeech": {
                "Tag": "NOUN",
                "Score": 0.9999796748161316
            }
        },
        {
            "TokenId": 6,
            "Text": "in",
            "BeginOffset": 22,
            "EndOffset": 24,
            "PartOfSpeech": {
                "Tag": "ADP",
                "Score": 0.9998047947883606
            }
        },
        {
            "TokenId": 7,
            "Text": "Seattle",
            "BeginOffset": 25,
            "EndOffset": 32,
            "PartOfSpeech": {
                "Tag": "PROPN",
                "Score": 0.9940530061721802
            }
        }
    ]
}
```

Para obtener más información, consulte los Análisis de sintaxis en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte DetectSyntax en la Referencia de comandos de la AWS CLI.

`detect-targeted-sentiment`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-targeted-sentiment`.

AWS CLI

Para detectar la opinión específica de las entidades con nombre en un texto de entrada

En el siguiente ejemplo de `detect-targeted-sentiment`, se analiza el texto de entrada y se devuelven las entidades con nombre, además del sentimiento específico asociado a cada entidad. La puntuación de confianza de los modelos previamente entrenados también se muestra para cada predicción.

```
aws comprehend detect-targeted-sentiment \
    --language-code en \
    --text "I do not enjoy January because it is too cold but August is the perfect
 temperature"
```

Salida:

```
{
    "Entities": [
        {
            "DescriptiveMentionIndex": [
                0
            ],
            "Mentions": [
                {
                    "Score": 0.9999979734420776,
                    "GroupScore": 1.0,
                    "Text": "I",
                    "Type": "PERSON",
                    "MentionSentiment": {
                        "Sentiment": "NEUTRAL",
                        "SentimentScore": {
                            "Positive": 0.0,
                            "Negative": 0.0,
                            "Neutral": 1.0,
                            "Mixed": 0.0
                        }
                    },
                    "BeginOffset": 0,
                    "EndOffset": 1
                }
            ]
        },
        {
```

```
            "DescriptiveMentionIndex": [
                0
            ],
            "Mentions": [
                {
                    "Score": 0.9638869762420654,
                    "GroupScore": 1.0,
                    "Text": "January",
                    "Type": "DATE",
                    "MentionSentiment": {
                        "Sentiment": "NEGATIVE",
                        "SentimentScore": {
                            "Positive": 0.0031610000878572464,
                            "Negative": 0.9967250227928162,
                            "Neutral": 0.00011100000119768083,
                            "Mixed": 1.9999999949504854e-06
                        }
                    },
                    "BeginOffset": 15,
                    "EndOffset": 22
                }
            ]
        },
        {
            "DescriptiveMentionIndex": [
                0
            ],
            "Mentions": [
                {
                {
                    "Score": 0.9664419889450073,
                    "GroupScore": 1.0,
                    "Text": "August",
                    "Type": "DATE",
                    "MentionSentiment": {
                        "Sentiment": "POSITIVE",
                        "SentimentScore": {
                            "Positive": 0.9999549984931946,
                            "Negative": 3.999999989900971e-06,
                            "Neutral": 4.099999932805076e-05,
                            "Mixed": 0.0
                        }
                    },
                    "BeginOffset": 50,
```

```
                    "EndOffset": 56
                }
            ]
        },
        {
            "DescriptiveMentionIndex": [
                0
            ],
            "Mentions": [
                {
                    "Score": 0.9803199768066406,
                    "GroupScore": 1.0,
                    "Text": "temperature",
                    "Type": "ATTRIBUTE",
                    "MentionSentiment": {
                        "Sentiment": "POSITIVE",
                        "SentimentScore": {
                            "Positive": 1.0,
                            "Negative": 0.0,
                            "Neutral": 0.0,
                            "Mixed": 0.0
                        }
                    },
                    "BeginOffset": 77,
                    "EndOffset": 88
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Targeted Sentiment en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte DetectTargetedSentiment en la Referencia de comandos de la AWS CLI.

`import-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-model`.

AWS CLI

Importación de un modelo

En el siguiente ejemplo de `import-model`, se importa un modelo de una cuenta de AWS diferente. El modelo de clasificador de documentos de la cuenta de 444455556666 tiene una política basada en recursos que permite a la cuenta 111122223333 importar el modelo.

```
aws comprehend import-model \
    --source-model-arn arn:aws:comprehend:us-west-2:444455556666:document-classifier/example-classifier
```

Salida:

```
{
    "ModelArn": "arn:aws:comprehend:us-west-2:111122223333:document-classifier/example-classifier"
}
```

Para obtener más información, consulte Copying custom models between AWS accounts en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ImportModel en la Referencia de comandos de la AWS CLI.

`list-datasets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-datasets`.

AWS CLI

Para enumerar todos los conjuntos de datos del volante de inercia

En el siguiente ejemplo de `list-datasets`, se enumeran todos los conjuntos de datos asociados a un volante de inercia.

```
aws comprehend list-datasets \
    --flywheel-arn arn:aws:comprehend:us-west-2:111122223333:flywheel/flywheel-entity
```

Salida:

```
{
    "DatasetPropertiesList": [
        {
            "DatasetArn": "arn:aws:comprehend:us-west-2:111122223333:flywheel/
flywheel-entity/dataset/example-dataset-1",
            "DatasetName": "example-dataset-1",
            "DatasetType": "TRAIN",
            "DatasetS3Uri": "s3://amzn-s3-demo-bucket/flywheel-entity/
schemaVersion=1/20230616T200543Z/datasets/example-dataset-1/20230616T203710Z/",
            "Status": "CREATING",
            "CreationTime": "2023-06-16T20:37:10.400000+00:00"
        },
        {
            "DatasetArn": "arn:aws:comprehend:us-west-2:111122223333:flywheel/
flywheel-entity/dataset/example-dataset-2",
            "DatasetName": "example-dataset-2",
            "DatasetType": "TRAIN",
            "DatasetS3Uri": "s3://amzn-s3-demo-bucket/flywheel-entity/
schemaVersion=1/20230616T200543Z/datasets/example-dataset-2/20230616T200607Z/",
            "Description": "TRAIN Dataset created by Flywheel creation.",
            "Status": "COMPLETED",
            "NumberOfDocuments": 5572,
            "CreationTime": "2023-06-16T20:06:07.722000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Flywheel Overview en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ListDatasets en la Referencia de comandos de la AWS CLI.

`list-document-classification-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-document-classification-jobs`.

AWS CLI

Para enumerar todos los trabajos de clasificación de documentos

El siguiente ejemplo de `list-document-classification-jobs` enumera todos los trabajos de clasificación de documentos.

```
aws comprehend list-document-classification-jobs
```

Salida:

```
{
    "DocumentClassificationJobPropertiesList": [
        {
            "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:1234567890101:document-
classification-job/123456abcdeb0e11022f22a11EXAMPLE",
            "JobName": "exampleclassificationjob",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2023-06-14T17:09:51.788000+00:00",
            "EndTime": "2023-06-14T17:15:58.582000+00:00",
            "DocumentClassifierArn": "arn:aws:comprehend:us-
west-2:1234567890101:document-classifier/mymodel/version/12",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket/jobdata/",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
thefolder/1234567890101-CLN-e758dd56b824aa717ceab551f11749fb/output/output.tar.gz"
            },
            "DataAccessRoleArn": "arn:aws:iam::1234567890101:role/service-role/
AmazonComprehendServiceRole-example-role"
        },
        {
            "JobId": "123456abcdeb0e11022f22a1EXAMPLE2",
            "JobArn": "arn:aws:comprehend:us-west-2:1234567890101:document-
classification-job/123456abcdeb0e11022f22a1EXAMPLE2",
            "JobName": "exampleclassificationjob2",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2023-06-14T17:22:39.829000+00:00",
            "EndTime": "2023-06-14T17:28:46.107000+00:00",
            "DocumentClassifierArn": "arn:aws:comprehend:us-
west-2:1234567890101:document-classifier/mymodel/version/12",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket/jobdata/",
                "InputFormat": "ONE_DOC_PER_LINE"
```

```
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
thefolder/1234567890101-CLN-123456abcdeb0e11022f22a1EXAMPLE2/output/output.tar.gz"
            },
            "DataAccessRoleArn": "arn:aws:iam::1234567890101:role/service-role/
AmazonComprehendServiceRole-example-role"
        }
    ]
}
```

Para obtener más información, consulte Clasificación personalizada en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ListDocumentClassificationJobs en la Referencia del comando de la AWS CLI.

`list-document-classifier-summaries`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-document-classifier-summaries`.

AWS CLI

Para enumerar los resúmenes de todos los clasificadores de documentos creados

En el siguiente ejemplo de `list-document-classifier-summaries`, se enumeran todos los resúmenes de clasificación de documentos creados.

```
aws comprehend list-document-classifier-summaries
```

Salida:

```
{
    "DocumentClassifierSummariesList": [
        {
            "DocumentClassifierName": "example-classifier-1",
            "NumberOfVersions": 1,
            "LatestVersionCreatedAt": "2023-06-13T22:07:59.825000+00:00",
            "LatestVersionName": "1",
            "LatestVersionStatus": "TRAINED"
        },
```

```
        {
            "DocumentClassifierName": "example-classifier-2",
            "NumberOfVersions": 2,
            "LatestVersionCreatedAt": "2023-06-13T21:54:59.589000+00:00",
            "LatestVersionName": "2",
            "LatestVersionStatus": "TRAINED"
        }
    ]
}
```

Para obtener más información, consulte Creación y administración de modelos personalizados en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ListDocumentClassifierSummaries en la Referencia de comandos de la AWS CLI.

`list-document-classifiers`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-document-classifiers`.

AWS CLI

Para enumerar todos los clasificadores de documentos

El siguiente ejemplo de `list-document-classifiers` enumera todos los modelos de clasificadores de documentos entrenados y en proceso de entrenamiento.

```
aws comprehend list-document-classifiers
```

Salida:

```
{
    "DocumentClassifierPropertiesList": [
        {
            "DocumentClassifierArn": "arn:aws:comprehend:us-
west-2:111122223333:document-classifier/exampleclassifier1",
            "LanguageCode": "en",
            "Status": "TRAINED",
            "SubmitTime": "2023-06-13T19:04:15.735000+00:00",
            "EndTime": "2023-06-13T19:42:31.752000+00:00",
            "TrainingStartTime": "2023-06-13T19:08:20.114000+00:00",
            "TrainingEndTime": "2023-06-13T19:41:35.080000+00:00",
            "InputDataConfig": {
```

```
                "DataFormat": "COMPREHEND_CSV",
                "S3Uri": "s3://amzn-s3-demo-bucket/trainingdata"
            },
            "OutputDataConfig": {},
            "ClassifierMetadata": {
                "NumberOfLabels": 3,
                "NumberOfTrainedDocuments": 5016,
                "NumberOfTestDocuments": 557,
                "EvaluationMetrics": {
                    "Accuracy": 0.9856,
                    "Precision": 0.9919,
                    "Recall": 0.9459,
                    "F1Score": 0.9673,
                    "MicroPrecision": 0.9856,
                    "MicroRecall": 0.9856,
                    "MicroF1Score": 0.9856,
                    "HammingLoss": 0.0144
                }
            },
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-testorle",
            "Mode": "MULTI_CLASS"
        },
        {
            "DocumentClassifierArn": "arn:aws:comprehend:us-
west-2:111122223333:document-classifier/exampleclassifier2",
            "LanguageCode": "en",
            "Status": "TRAINING",
            "SubmitTime": "2023-06-13T21:20:28.690000+00:00",
            "InputDataConfig": {
                "DataFormat": "COMPREHEND_CSV",
                "S3Uri": "s3://amzn-s3-demo-bucket/trainingdata"
            },
            "OutputDataConfig": {},
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-testorle",
            "Mode": "MULTI_CLASS"
        }
    ]
}
```

Para obtener más información, consulte Creación y administración de modelos personalizados en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte ListDocumentClassifiers en la Referencia de comandos de la AWS CLI.

`list-dominant-language-detection-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-dominant-language-detection-jobs`.

AWS CLI

Para enumerar todos los trabajos de detección de idioma dominante

En el siguiente ejemplo de `list-dominant-language-detection-jobs`, se enumeran todos los trabajos de detección de idioma dominante asíncronos en curso y finalizados.

```
aws comprehend list-dominant-language-detection-jobs
```

Salida:

```
{
    "DominantLanguageDetectionJobPropertiesList": [
        {
            "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:dominant-language-
detection-job/123456abcdeb0e11022f22a11EXAMPLE",
            "JobName": "languageanalysis1",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2023-06-09T18:10:38.037000+00:00",
            "EndTime": "2023-06-09T18:18:45.498000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
testfolder/111122223333-LANGUAGE-123456abcdeb0e11022f22a11EXAMPLE/output/
output.tar.gz"
            },
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role"
        },
        {
```

```
            "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:dominant-language-
detection-job/123456abcdeb0e11022f22a11EXAMPLE",
            "JobName": "languageanalysis2",
            "JobStatus": "STOPPED",
            "SubmitTime": "2023-06-09T18:16:33.690000+00:00",
            "EndTime": "2023-06-09T18:24:40.608000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
testfolder/111122223333-LANGUAGE-123456abcdeb0e11022f22a11EXAMPLE/output/
output.tar.gz"
            },
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role"
        }
    ]
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ListDominantLanguageDetectionJobs en la Referencia de comandos de la AWS CLI.

`list-endpoints`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-endpoints`.

AWS CLI

Para enumerar todos los puntos de conexión

En el siguiente ejemplo de `list-endpoints`, se enumeran todos los puntos de conexión específicos del modelo activos.

```
aws comprehend list-endpoints
```

Salida:

```
{
    "EndpointPropertiesList": [
        {
            "EndpointArn": "arn:aws:comprehend:us-west-2:111122223333:document-
classifier-endpoint/ExampleClassifierEndpoint",
            "Status": "IN_SERVICE",
            "ModelArn": "arn:aws:comprehend:us-west-2:111122223333:document-
classifier/exampleclassifier1",
            "DesiredModelArn": "arn:aws:comprehend:us-west-2:111122223333:document-
classifier/exampleclassifier1",
            "DesiredInferenceUnits": 1,
            "CurrentInferenceUnits": 1,
            "CreationTime": "2023-06-13T20:32:54.526000+00:00",
            "LastModifiedTime": "2023-06-13T20:32:54.526000+00:00"
        },
        {
            "EndpointArn": "arn:aws:comprehend:us-west-2:111122223333:document-
classifier-endpoint/ExampleClassifierEndpoint2",
            "Status": "IN_SERVICE",
            "ModelArn": "arn:aws:comprehend:us-west-2:111122223333:document-
classifier/exampleclassifier2",
            "DesiredModelArn": "arn:aws:comprehend:us-west-2:111122223333:document-
classifier/exampleclassifier2",
            "DesiredInferenceUnits": 1,
            "CurrentInferenceUnits": 1,
            "CreationTime": "2023-06-13T20:32:54.526000+00:00",
            "LastModifiedTime": "2023-06-13T20:32:54.526000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Administración de puntos de conexión de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ListEndpoints en la Referencia de comandos de la AWS CLI.

`list-entities-detection-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-entities-detection-jobs`.

AWS CLI

Para enumerar todos los trabajos de detección de entidades

En el siguiente ejemplo de `list-entities-detection-jobs`, se enumeran todos los trabajos de detección de entidades asíncronas.

```
aws comprehend list-entities-detection-jobs
```

Salida:

```
{
    "EntitiesDetectionJobPropertiesList": [
        {
            "JobId": "468af39c28ab45b83eb0c4ab9EXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:entities-detection-
job/468af39c28ab45b83eb0c4ab9EXAMPLE",
            "JobName": "example-entities-detection",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2023-06-08T20:57:46.476000+00:00",
            "EndTime": "2023-06-08T21:05:53.718000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket/AsyncBatchJobs/",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
thefolder/111122223333-NER-468af39c28ab45b83eb0c4ab9EXAMPLE/output/output.tar.gz"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role"
        },
        {
            "JobId": "809691caeaab0e71406f80a28EXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:entities-detection-
job/809691caeaab0e71406f80a28EXAMPLE",
            "JobName": "example-entities-detection-2",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2023-06-08T21:30:15.323000+00:00",
            "EndTime": "2023-06-08T21:40:23.509000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket/AsyncBatchJobs/",
```

```
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
thefolder/111122223333-NER-809691caeaab0e71406f80a28EXAMPLE/output/output.tar.gz"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role"
        },
        {
            "JobId": "e00597c36b448b91d70dea165EXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:entities-detection-
job/e00597c36b448b91d70dea165EXAMPLE",
            "JobName": "example-entities-detection-3",
            "JobStatus": "STOPPED",
            "SubmitTime": "2023-06-08T22:19:28.528000+00:00",
            "EndTime": "2023-06-08T22:27:33.991000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket/AsyncBatchJobs/",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
thefolder/111122223333-NER-e00597c36b448b91d70dea165EXAMPLE/output/output.tar.gz"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role"
        }
    ]
}
```

Para obtener más información, consulte Entidades en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ListEntitiesDetectionJobs en la Referencia de comandos de la AWS CLI.

`list-entity-recognizer-summaries`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-entity-recognizer-summaries`.

AWS CLI

Para enumerar resúmenes de todos los reconocedores de entidades creados

En el siguiente ejemplo de `list-entity-recognizer-summaries`, se enumeran todos los resúmenes de los reconocedores de entidades.

```
aws comprehend list-entity-recognizer-summaries
```

Salida:

```
{
    "EntityRecognizerSummariesList": [
        {
            "RecognizerName": "entity-recognizer-3",
            "NumberOfVersions": 2,
            "LatestVersionCreatedAt": "2023-06-15T23:15:07.621000+00:00",
            "LatestVersionName": "2",
            "LatestVersionStatus": "STOP_REQUESTED"
        },
        {
            "RecognizerName": "entity-recognizer-2",
            "NumberOfVersions": 1,
            "LatestVersionCreatedAt": "2023-06-14T22:55:27.805000+00:00",
            "LatestVersionName": "2"
            "LatestVersionStatus": "TRAINED"
        },
        {
            "RecognizerName": "entity-recognizer-1",
            "NumberOfVersions": 1,
            "LatestVersionCreatedAt": "2023-06-14T20:44:59.631000+00:00",
            "LatestVersionName": "1",
            "LatestVersionStatus": "TRAINED"
        }
    ]
}
```

Para obtener más información, consulte Custom entity recognition en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ListEntityRecognizerSummaries en la Referencia de comandos de la AWS CLI.

`list-entity-recognizers`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-entity-recognizers`.

AWS CLI

Para enumerar todos los reconocedores de entidades personalizados

En el siguiente ejemplo de `list-entity-recognizers`, se enumeran todos los reconocedores de entidades personalizados creados.

```
aws comprehend list-entity-recognizers
```

Salida:

```
{
    "EntityRecognizerPropertiesList": [
        {
            "EntityRecognizerArn": "arn:aws:comprehend:us-
west-2:111122223333:entity-recognizer/EntityRecognizer/version/1",
            "LanguageCode": "en",
            "Status": "TRAINED",
            "SubmitTime": "2023-06-14T20:44:59.631000+00:00",
            "EndTime": "2023-06-14T20:59:19.532000+00:00",
            "TrainingStartTime": "2023-06-14T20:48:52.811000+00:00",
            "TrainingEndTime": "2023-06-14T20:58:11.473000+00:00",
            "InputDataConfig": {
                "DataFormat": "COMPREHEND_CSV",
                "EntityTypes": [
                    {
                        "Type": "BUSINESS"
                    }
                ],
                "Documents": {
                    "S3Uri": "s3://amzn-s3-demo-bucket/trainingdata/dataset/",
                    "InputFormat": "ONE_DOC_PER_LINE"
                },
                "EntityList": {
                    "S3Uri": "s3://amzn-s3-demo-bucket/trainingdata/entity.csv"
                }
            },
            "RecognizerMetadata": {
                "NumberOfTrainedDocuments": 1814,
```

```
                "NumberOfTestDocuments": 486,
                "EvaluationMetrics": {
                    "Precision": 100.0,
                    "Recall": 100.0,
                    "F1Score": 100.0
                },
                "EntityTypes": [
                    {
                        "Type": "BUSINESS",
                        "EvaluationMetrics": {
                            "Precision": 100.0,
                            "Recall": 100.0,
                            "F1Score": 100.0
                        },
                        "NumberOfTrainMentions": 1520
                    }
                ]
            },
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-servicerole",
            "VersionName": "1"
        },
        {
            "EntityRecognizerArn": "arn:aws:comprehend:us-
west-2:111122223333:entity-recognizer/entityrecognizer3",
            "LanguageCode": "en",
            "Status": "TRAINED",
            "SubmitTime": "2023-06-14T22:57:51.056000+00:00",
            "EndTime": "2023-06-14T23:14:13.894000+00:00",
            "TrainingStartTime": "2023-06-14T23:01:33.984000+00:00",
            "TrainingEndTime": "2023-06-14T23:13:02.984000+00:00",
            "InputDataConfig": {
                "DataFormat": "COMPREHEND_CSV",
                "EntityTypes": [
                    {
                        "Type": "DEVICE"
                    }
                ],
                "Documents": {
                    "S3Uri": "s3://amzn-s3-demo-bucket/trainingdata/raw_txt.csv",
                    "InputFormat": "ONE_DOC_PER_LINE"
                },
                "EntityList": {
                    "S3Uri": "s3://amzn-s3-demo-bucket/trainingdata/entity_list.csv"
```

```
                }
            },
            "RecognizerMetadata": {
                "NumberOfTrainedDocuments": 4616,
                "NumberOfTestDocuments": 3489,
                "EvaluationMetrics": {
                    "Precision": 98.54227405247813,
                    "Recall": 100.0,
                    "F1Score": 99.26578560939794
                },
                "EntityTypes": [
                    {
                        "Type": "DEVICE",
                        "EvaluationMetrics": {
                            "Precision": 98.54227405247813,
                            "Recall": 100.0,
                            "F1Score": 99.26578560939794
                        },
                        "NumberOfTrainMentions": 2764
                    }
                ]
            },
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-servicerole"
        }
    ]
}
```

Para obtener más información, consulte Custom entity recognition en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ListEntityRecognizers en la Referencia de comandos de la AWS CLI.

`list-events-detection-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-events-detection-jobs`.

AWS CLI

Para enumerar todos los trabajos de detección de eventos

En el siguiente ejemplo de `list-events-detection-jobs`, se enumeran todos los trabajos de detección de eventos asíncronos.

```
aws comprehend list-events-detection-jobs
```

Salida:

```
{
    "EventsDetectionJobPropertiesList": [
        {
            "JobId": "aa9593f9203e84f3ef032ce18EXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:1111222233333:events-detection-
job/aa9593f9203e84f3ef032ce18EXAMPLE",
            "JobName": "events_job_1",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2023-06-12T19:14:57.751000+00:00",
            "EndTime": "2023-06-12T19:21:04.962000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-source-bucket/EventsData/",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
testfolder/1111222233333-EVENTS-aa9593f9203e84f3ef032ce18EXAMPLE/output/"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::1111222233333:role/service-role/
AmazonComprehendServiceRole-example-role",
            "TargetEventTypes": [
                "BANKRUPTCY",
                "EMPLOYMENT",
                "CORPORATE_ACQUISITION",
                "CORPORATE_MERGER",
                "INVESTMENT_GENERAL"
            ]
        },
        {
            "JobId": "4a990a2f7e82adfca6e171135EXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:1111222233333:events-detection-
job/4a990a2f7e82adfca6e171135EXAMPLE",
            "JobName": "events_job_2",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2023-06-12T19:55:43.702000+00:00",
```

```
            "EndTime": "2023-06-12T20:03:49.893000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-source-bucket/EventsData/",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
testfolder/1111222233333-EVENTS-4a990a2f7e82adfca6e171135EXAMPLE/output/"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::1111222233333:role/service-role/
AmazonComprehendServiceRole-example-role",
            "TargetEventTypes": [
                "BANKRUPTCY",
                "EMPLOYMENT",
                "CORPORATE_ACQUISITION",
                "CORPORATE_MERGER",
                "INVESTMENT_GENERAL"
            ]
        }
    ]
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ListEventsDetectionJobs en la Referencia de comandos de la AWS CLI.

`list-flywheel-iteration-history`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-flywheel-iteration-history`.

AWS CLI

Para enumerar todo el historial de iteraciones del volante de inercia

En el siguiente ejemplo de `list-flywheel-iteration-history`, se enumeran todas las iteraciones de un volante de inercia.

```
aws comprehend list-flywheel-iteration-history
```

```
    --flywheel-arn arn:aws:comprehend:us-west-2:111122223333:flywheel/example-
flywheel
```

Salida:

```
{
    "FlywheelIterationPropertiesList": [
        {
            "FlywheelArn": "arn:aws:comprehend:us-west-2:111122223333:flywheel/
example-flywheel",
            "FlywheelIterationId": "20230619TEXAMPLE",
            "CreationTime": "2023-06-19T04:00:32.594000+00:00",
            "EndTime": "2023-06-19T04:00:49.248000+00:00",
            "Status": "COMPLETED",
            "Message": "FULL_ITERATION: Flywheel iteration performed all functions
 successfully.",
            "EvaluatedModelArn": "arn:aws:comprehend:us-
west-2:111122223333:document-classifier/example-classifier/version/1",
            "EvaluatedModelMetrics": {
                "AverageF1Score": 0.7742663922375772,
                "AverageF1Score": 0.9876464664646313,
                "AveragePrecision": 0.9800000253081214,
                "AverageRecall": 0.9445600253081214,
                "AverageAccuracy": 0.9997281665190434
            },
            "EvaluationManifestS3Prefix": "s3://amzn-s3-demo-bucket/example-
flywheel/schemaVersion=1/20230619TEXAMPLE/evaluation/20230619TEXAMPLE/"
        },
        {
            "FlywheelArn": "arn:aws:comprehend:us-west-2:111122223333:flywheel/
example-flywheel-2",
            "FlywheelIterationId": "20230616TEXAMPLE",
            "CreationTime": "2023-06-16T21:10:26.385000+00:00",
            "EndTime": "2023-06-16T23:33:16.827000+00:00",
            "Status": "COMPLETED",
            "Message": "FULL_ITERATION: Flywheel iteration performed all functions
 successfully.",
            "EvaluatedModelArn": "arn:aws:comprehend:us-
west-2:111122223333:document-classifier/spamvshamclassify/version/1",
            "EvaluatedModelMetrics": {
                "AverageF1Score": 0.7742663922375772,
                "AverageF1Score": 0.9767700253081214,
                "AveragePrecision": 0.9767700253081214,
```

```
                "AverageRecall": 0.9767700253081214,
                "AverageAccuracy": 0.9858281665190434
            },
            "EvaluationManifestS3Prefix": "s3://amzn-s3-demo-bucket/example-
flywheel-2/schemaVersion=1/20230616TEXAMPLE/evaluation/20230616TEXAMPLE/"
        }
    ]
}
```

Para obtener más información, consulte Flywheel overview en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ListFlywheelIterationHistory en la Referencia de comandos de la AWS CLI.

`list-flywheels`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-flywheels`.

AWS CLI

Para enumerar todos los volantes de inercia

En el siguiente ejemplo de `list-flywheels`, se enumeran todos los volantes de inercia creados.

```
aws comprehend list-flywheels
```

Salida:

```
{
    "FlywheelSummaryList": [
        {
            "FlywheelArn": "arn:aws:comprehend:us-west-2:111122223333:flywheel/
example-flywheel-1",
            "ActiveModelArn": "arn:aws:comprehend:us-west-2:111122223333:document-
classifier/exampleclassifier/version/1",
            "DataLakeS3Uri": "s3://amzn-s3-demo-bucket/example-flywheel-1/
schemaVersion=1/20230616T200543Z/",
            "Status": "ACTIVE",
            "ModelType": "DOCUMENT_CLASSIFIER",
            "CreationTime": "2023-06-16T20:05:43.242000+00:00",
            "LastModifiedTime": "2023-06-19T04:00:43.027000+00:00",
```

```
            "LatestFlywheelIteration": "20230619T040032Z"
        },
        {
            "FlywheelArn": "arn:aws:comprehend:us-west-2:111122223333:flywheel/
example-flywheel-2",
            "ActiveModelArn": "arn:aws:comprehend:us-west-2:111122223333:document-
classifier/exampleclassifier2/version/1",
            "DataLakeS3Uri": "s3://amzn-s3-demo-bucket/example-flywheel-2/
schemaVersion=1/20220616T200543Z/",
            "Status": "ACTIVE",
            "ModelType": "DOCUMENT_CLASSIFIER",
            "CreationTime": "2022-06-16T20:05:43.242000+00:00",
            "LastModifiedTime": "2022-06-19T04:00:43.027000+00:00",
            "LatestFlywheelIteration": "20220619T040032Z"
        }
    ]
}
```

Para obtener más información, consulte Flywheel overview en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ListFlywheels en la Referencia de comandos de la AWS CLI.

`list-key-phrases-detection-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-key-phrases-detection-jobs`.

AWS CLI

Para enumerar todos los trabajos de detección de frases clave

El siguiente ejemplo de `list-key-phrases-detection-jobs`, se enumeran todos los trabajos de detección de frases clave asíncronos en curso y finalizados.

```
aws comprehend list-key-phrases-detection-jobs
```

Salida:

```
{
    "KeyPhrasesDetectionJobPropertiesList": [
```

```
        {
            "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:key-phrases-
detection-job/123456abcdeb0e11022f22a11EXAMPLE",
            "JobName": "keyphrasesanalysis1",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2023-06-08T22:31:43.767000+00:00",
            "EndTime": "2023-06-08T22:39:52.565000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-source-bucket/AsyncBatchJobs/",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
testfolder/111122223333-KP-123456abcdeb0e11022f22a11EXAMPLE/output/output.tar.gz"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role"
        },
        {
            "JobId": "123456abcdeb0e11022f22a33EXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:key-phrases-
detection-job/123456abcdeb0e11022f22a33EXAMPLE",
            "JobName": "keyphrasesanalysis2",
            "JobStatus": "STOPPED",
            "SubmitTime": "2023-06-08T22:57:52.154000+00:00",
            "EndTime": "2023-06-08T23:05:48.385000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket/AsyncBatchJobs/",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
testfolder/111122223333-KP-123456abcdeb0e11022f22a33EXAMPLE/output/output.tar.gz"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role"
        },
        {
            "JobId": "123456abcdeb0e11022f22a44EXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:key-phrases-
detection-job/123456abcdeb0e11022f22a44EXAMPLE",
```

```
            "JobName": "keyphrasesanalysis3",
            "JobStatus": "FAILED",
            "Message": "NO_READ_ACCESS_TO_INPUT: The provided data access role does
 not have proper access to the input data.",
            "SubmitTime": "2023-06-09T16:47:04.029000+00:00",
            "EndTime": "2023-06-09T16:47:18.413000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
testfolder/111122223333-KP-123456abcdeb0e11022f22a44EXAMPLE/output/output.tar.gz"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role"
        }
    ]
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ListKeyPhrasesDetectionJobs en la Referencia de comandos de la AWS CLI.

`list-pii-entities-detection-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-pii-entities-detection-jobs`.

AWS CLI

Para enumerar todos los trabajos de detección de entidades de PII

En el siguiente ejemplo de `list-pii-entities-detection-jobs`, se enumeran todos los trabajos de detección de PII asíncronos en curso y finalizados.

```
aws comprehend list-pii-entities-detection-jobs
```

Salida:

```
{
    "PiiEntitiesDetectionJobPropertiesList": [
        {
            "JobId": "6f9db0c42d0c810e814670ee4EXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:pii-entities-
detection-job/6f9db0c42d0c810e814670ee4EXAMPLE",
            "JobName": "example-pii-detection-job",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2023-06-09T21:02:46.241000+00:00",
            "EndTime": "2023-06-09T21:12:52.602000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket/AsyncBatchJobs/",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-source-bucket/111122223333-
PII-6f9db0c42d0c810e814670ee4EXAMPLE/output/"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role",
            "Mode": "ONLY_OFFSETS"
        },
        {
            "JobId": "d927562638cfa739331a99b3cEXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:pii-entities-
detection-job/d927562638cfa739331a99b3cEXAMPLE",
            "JobName": "example-pii-detection-job-2",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2023-06-09T21:20:58.211000+00:00",
            "EndTime": "2023-06-09T21:31:06.027000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket/AsyncBatchJobs/",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
thefolder/111122223333-PII-d927562638cfa739331a99b3cEXAMPLE/output/"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role",
            "Mode": "ONLY_OFFSETS"
```

```
        }
    ]
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ListPiiEntitiesDetectionJobs en la Referencia de comandos de la AWS CLI.

`list-sentiment-detection-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-sentiment-detection-jobs`.

AWS CLI

Para enumerar todos los trabajos de detección de opiniones

En el siguiente ejemplo de `list-sentiment-detection-jobs`, se enumeran todos los trabajos de detección de opiniones asíncronos en curso y finalizados.

```
aws comprehend list-sentiment-detection-jobs
```

Salida:

```
{
    "SentimentDetectionJobPropertiesList": [
        {
            "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:sentiment-
detection-job/123456abcdeb0e11022f22a11EXAMPLE",
            "JobName": "example-sentiment-detection-job",
            "JobStatus": "IN_PROGRESS",
            "SubmitTime": "2023-06-09T22:42:20.545000+00:00",
            "EndTime": "2023-06-09T22:52:27.416000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket/MovieData",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
testfolder/111122223333-TS-123456abcdeb0e11022f22a11EXAMPLE/output/output.tar.gz"
            },
```

```
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role"
        },
        {
            "JobId": "123456abcdeb0e11022f22a1EXAMPLE2",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:sentiment-
detection-job/123456abcdeb0e11022f22a1EXAMPLE2",
            "JobName": "example-sentiment-detection-job-2",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2023-06-09T23:16:15.956000+00:00",
            "EndTime": "2023-06-09T23:26:00.168000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket/MovieData2",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
testfolder/111122223333-TS-123456abcdeb0e11022f22a1EXAMPLE2/output/output.tar.gz"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role"
        }
    ]
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ListSentimentDetectionJobs en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran las etiquetas de un recurso de Amazon Comprehend.

```
aws comprehend list-tags-for-resource \
    --resource-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier/
example-classifier/version/1
```

Salida:

```
{
    "ResourceArn": "arn:aws:comprehend:us-west-2:111122223333:document-classifier/
example-classifier/version/1",
    "Tags": [
        {
            "Key": "Department",
            "Value": "Finance"
        },
        {
            "Key": "location",
            "Value": "Seattle"
        }
    ]
}
```

Para obtener más información, consulte Tagging your resources en la Guía para desarrolladores de Amazon Comprehend.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-targeted-sentiment-detection-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-targeted-sentiment-detection-jobs`.

AWS CLI

Para enumerar todos los trabajos de detección de opiniones específicas

En el siguiente ejemplo de `list-targeted-sentiment-detection-jobs`, se enumeran todos los trabajos de detección de opiniones específicas asíncronos en curso y finalizados.

```
aws comprehend list-targeted-sentiment-detection-jobs
```

Salida:

```
{
    "TargetedSentimentDetectionJobPropertiesList": [
        {
            "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:targeted-sentiment-
detection-job/123456abcdeb0e11022f22a11EXAMPLE",
            "JobName": "example-targeted-sentiment-detection-job",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2023-06-09T22:42:20.545000+00:00",
            "EndTime": "2023-06-09T22:52:27.416000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket/MovieData",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
testfolder/111122223333-TS-123456abcdeb0e11022f22a11EXAMPLE/output/output.tar.gz"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-IOrole"
        },
        {
            "JobId": "123456abcdeb0e11022f22a1EXAMPLE2",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:targeted-sentiment-
detection-job/123456abcdeb0e11022f22a1EXAMPLE2",
            "JobName": "example-targeted-sentiment-detection-job-2",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2023-06-09T23:16:15.956000+00:00",
            "EndTime": "2023-06-09T23:26:00.168000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket/MovieData2",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
testfolder/111122223333-TS-123456abcdeb0e11022f22a1EXAMPLE2/output/output.tar.gz"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role"
        }
```

```
    ]
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte ListTargetedSentimentDetectionJobs en la Referencia de comandos de la AWS CLI.

`list-topics-detection-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-topics-detection-jobs`.

AWS CLI

Para enumerar todos los trabajos de detección de temas

El siguiente ejemplo de `list-topics-detection-jobs`, se enumeran todos los trabajos de detección de temas asíncronos en curso y finalizados.

```
aws comprehend list-topics-detection-jobs
```

Salida:

```
{
    "TopicsDetectionJobPropertiesList": [
        {
            "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:topics-detection-
job/123456abcdeb0e11022f22a11EXAMPLE",
            "JobName" "topic-analysis-1"
            "JobStatus": "IN_PROGRESS",
            "SubmitTime": "2023-06-09T18:40:35.384000+00:00",
            "EndTime": "2023-06-09T18:46:41.936000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
thefolder/111122223333-TOPICS-123456abcdeb0e11022f22a11EXAMPLE/output/output.tar.gz"
            },
            "NumberOfTopics": 10,
```

```
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role"
        },
        {
            "JobId": "123456abcdeb0e11022f22a1EXAMPLE2",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:topics-detection-
job/123456abcdeb0e11022f22a1EXAMPLE2",
            "JobName": "topic-analysis-2",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2023-06-09T18:44:43.414000+00:00",
            "EndTime": "2023-06-09T18:50:50.872000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
thefolder/111122223333-TOPICS-123456abcdeb0e11022f22a1EXAMPLE2/output/output.tar.gz"
            },
            "NumberOfTopics": 10,
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role"
        },
        {
            "JobId": "123456abcdeb0e11022f22a1EXAMPLE3",
            "JobArn": "arn:aws:comprehend:us-west-2:111122223333:topics-detection-
job/123456abcdeb0e11022f22a1EXAMPLE3",
            "JobName": "topic-analysis-2",
            "JobStatus": "IN_PROGRESS",
            "SubmitTime": "2023-06-09T18:50:56.737000+00:00",
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket",
                "InputFormat": "ONE_DOC_PER_LINE"
            },
            "OutputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-destination-bucket/
thefolder/111122223333-TOPICS-123456abcdeb0e11022f22a1EXAMPLE3/output/output.tar.gz"
            },
            "NumberOfTopics": 10,
            "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role"
        }
    ]
```

```
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte ListTopicsDetectionJobs en la Referencia de comandos de la AWS CLI.

`put-resource-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-resource-policy`.

AWS CLI

Para asociar una política basada en recursos

En el siguiente ejemplo de `put-resource-policy`, se asocia una política basada en recursos a un modelo para que otra cuenta de AWS pueda importarla. La política está asociada al modelo de la cuenta `111122223333` y permite a la cuenta `444455556666` importar el modelo.

```
aws comprehend put-resource-policy \
    --resource-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier/
example-classifier/version/1 \
    --resource-policy '{"Version":"2012-10-17",       "Statement":
[{"Effect":"Allow","Action":"comprehend:ImportModel","Resource":"*","Principal":
{"AWS":["arn:aws:iam::444455556666:root"]}}]}'
```

Salida:

```
{
    "PolicyRevisionId": "aaa111d069d07afaa2aa3106aEXAMPLE"
}
```

Para obtener más información, consulte Copying custom models between AWS accounts en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte PutResourcePolicy en la Referencia de comandos de la AWS CLI.

`start-document-classification-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-document-classification-job`.

AWS CLI

Para empezar un trabajo de clasificación de documentos

El siguiente ejemplo de `start-document-classification-job` inicia un trabajo de clasificación de documentos con un modelo personalizado en todos los archivos de la dirección especificada en la etiqueta `--input-data-config`. En este ejemplo, el bucket de S3 de entrada contiene `SampleSMStext1.txt`, `SampleSMStext2.txt` y `SampleSMStext3.txt`. El modelo se entrenó previamente para clasificar los mensajes SMS spam y no spam (denominados "falsos"). Cuando se completa el trabajo, `output.tar.gz` se coloca en la ubicación especificada por la etiqueta `--output-data-config`. `output.tar.gz` contiene `predictions.jsonl`, que enumera la clasificación de cada documento. La salida Json se imprime en una sola línea por archivo, pero se formatea aquí para que sea legible.

```
aws comprehend start-document-classification-job \
    --job-name exampleclassificationjob \
    --input-data-config "S3Uri=s3://amzn-s3-demo-bucket-INPUT/jobdata/" \
    --output-data-config "S3Uri=s3://amzn-s3-demo-destination-bucket/testfolder/" \
    --data-access-role-arn arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role \
    --document-classifier-arn arn:aws:comprehend:us-west-2:111122223333:document-
classifier/mymodel/version/12
```

Contenido de `SampleSMStext1.txt`:

```
"CONGRATULATIONS! TXT 2155550100 to win $5000"
```

Contenido de `SampleSMStext2.txt`:

```
"Hi, when do you want me to pick you up from practice?"
```

Contenido de `SampleSMStext3.txt`:

```
"Plz send bank account # to 2155550100 to claim prize!!"
```

Salida:

```
{
    "JobId": "e758dd56b824aa717ceab551fEXAMPLE",
    "JobArn": "arn:aws:comprehend:us-west-2:111122223333:document-classification-
job/e758dd56b824aa717ceab551fEXAMPLE",
    "JobStatus": "SUBMITTED"
}
```

Contenido de `predictions.jsonl`:

```
{"File": "SampleSMSText1.txt", "Line": "0", "Classes": [{"Name": "spam", "Score":
 0.9999}, {"Name": "ham", "Score": 0.0001}]}
{"File": "SampleSMStext2.txt", "Line": "0", "Classes": [{"Name": "ham", "Score":
 0.9994}, {"Name": "spam", "Score": 0.0006}]}
{"File": "SampleSMSText3.txt", "Line": "0", "Classes": [{"Name": "spam", "Score":
 0.9999}, {"Name": "ham", "Score": 0.0001}]}
```

Para obtener más información, consulte Clasificación personalizada en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte StartDocumentClassificationJob en la Referencia de comandos de la AWS CLI.

`start-dominant-language-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-dominant-language-detection-job`.

AWS CLI

Inicio de un trabajo de detección de idioma asíncrono

En el siguiente ejemplo de `start-dominant-language-detection-job`, se inicia un trabajo de detección de idiomas asíncrono para todos los archivos ubicados en la dirección especificada por la etiqueta `--input-data-config`. En este ejemplo, el bucket de S3 contiene `Sampletext1.txt`. Una vez completado el trabajo, la carpeta, `output`, se coloca en la ubicación que especifique la etiqueta `--output-data-config`. La carpeta contiene `output.txt`, que contiene a su vez el idioma dominante de cada uno de los archivos de texto, así como la puntuación de confianza del modelo previamente entrenado para cada predicción.

```
aws comprehend start-dominant-language-detection-job \
    --job-name example_language_analysis_job \
    --language-code en \
    --input-data-config "S3Uri=s3://amzn-s3-demo-bucket/" \
    --output-data-config "S3Uri=s3://amzn-s3-demo-destination-bucket/testfolder/" \
    --data-access-role-arn arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role \
    --language-code en
```

Contenido de Sampletext1.txt:

```
"Physics is the natural science that involves the study of matter and its motion and
 behavior through space and time, along with related concepts such as energy and
 force."
```

Salida:

```
{
    "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
    "JobArn": "arn:aws:comprehend:us-west-2:111122223333:dominant-language-
detection-job/123456abcdeb0e11022f22a11EXAMPLE",
    "JobStatus": "SUBMITTED"
}
```

Contenido de `output.txt`:

```
{"File": "Sampletext1.txt", "Languages": [{"LanguageCode": "en", "Score":
 0.9913753867149353}], "Line": 0}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StartDominantLanguageDetectionJob en la Referencia de comandos de la AWS CLI.

`start-entities-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-entities-detection-job`.

AWS CLI

Ejemplo 1: iniciar un trabajo de detección de entidades estándar utilizando el modelo previamente entrenado

En el siguiente ejemplo de `start-entities-detection-job`, se inicia un trabajo de detección de entidades asíncrono para todos los archivos ubicados en la dirección especificada por la etiqueta `--input-data-config`. En este ejemplo, el bucket de S3 contiene `Sampletext1.txt`, `Sampletext2.txt` y `Sampletext3.txt`. Una vez completado el trabajo, la carpeta, `output`, se coloca en la ubicación que especifique la etiqueta `--output-data-config`. La carpeta contiene `output.txt`, que contiene a su vez una lista de todas las entidades con nombre detectadas en cada archivo de texto, así como la puntuación de confianza del modelo previamente entrenado para cada predicción. La salida Json se imprime en una sola línea por archivo de entrada, pero se formatea aquí para que sea legible.

```
aws comprehend start-entities-detection-job \
    --job-name entitiestest \
    --language-code en \
    --input-data-config "S3Uri=s3://amzn-s3-demo-bucket/" \
    --output-data-config "S3Uri=s3://amzn-s3-demo-destination-bucket/testfolder/" \
    --data-access-role-arn arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role \
    --language-code en
```

Contenido de `Sampletext1.txt`:

```
"Hello Zhang Wei, I am John. Your AnyCompany Financial Services, LLC credit card
 account 1111-XXXX-1111-XXXX has a minimum payment of $24.53 that is due by July
 31st."
```

Contenido de `Sampletext2.txt`:

```
"Dear Max, based on your autopay settings for your account example1.org account, we
 will withdraw your payment on the due date from your bank account number XXXXXX1111
 with the routing number XXXXX0000. "
```

Contenido de `Sampletext3.txt`:

```
"Jane, please submit any customer feedback from this weekend to AnySpa, 123 Main St,
 Anywhere and send comments to Alice at AnySpa@example.com."
```

Salida:

```
{
    "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
    "JobArn": "arn:aws:comprehend:us-west-2:111122223333:entities-detection-
job/123456abcdeb0e11022f22a11EXAMPLE",
    "JobStatus": "SUBMITTED"
}
```

El contenido de `output.txt` muestra las líneas con sangría para facilitar la lectura:

```
{
"Entities": [
    {
    "BeginOffset": 6,
    "EndOffset": 15,
    "Score": 0.9994006636420306,
    "Text": "Zhang Wei",
    "Type": "PERSON"
    },
    {
    "BeginOffset": 22,
    "EndOffset": 26,
    "Score": 0.9976647915128143,
    "Text": "John",
    "Type": "PERSON"
    },
    {
    "BeginOffset": 33,
    "EndOffset": 67,
    "Score": 0.9984608700836206,
    "Text": "AnyCompany Financial Services, LLC",
    "Type": "ORGANIZATION"
    },
    {
    "BeginOffset": 88,
    "EndOffset": 107,
    "Score": 0.9868521019555556,
    "Text": "1111-XXXX-1111-XXXX",
    "Type": "OTHER"
    },
    {
    "BeginOffset": 133,
```

```
    "EndOffset": 139,
    "Score": 0.998242565709204,
    "Text": "$24.53",
    "Type": "QUANTITY"
    },
    {
    "BeginOffset": 155,
    "EndOffset": 164,
    "Score": 0.9993039263159287,
    "Text": "July 31st",
    "Type": "DATE"
    }
],
"File": "SampleText1.txt",
"Line": 0
}
{
"Entities": [
    {
    "BeginOffset": 5,
    "EndOffset": 8,
    "Score": 0.9866232147545232,
    "Text": "Max",
    "Type": "PERSON"
    },
    {
    "BeginOffset": 156,
    "EndOffset": 166,
    "Score": 0.9797723450933329,
    "Text": "XXXXXX1111",
    "Type": "OTHER"
    },
    {
    "BeginOffset": 191,
    "EndOffset": 200,
    "Score": 0.9247838572396843,
    "Text": "XXXXX0000",
    "Type": "OTHER"
    }
],
"File": "SampleText2.txt",
"Line": 0
}
{
```

```
  "Entities": [
     {
     "Score": 0.9990532994270325,
     "Type": "PERSON",
     "Text": "Jane",
     "BeginOffset": 0,
     "EndOffset": 4
     },
     {
     "Score": 0.9519651532173157,
     "Type": "DATE",
     "Text": "this weekend",
     "BeginOffset": 47,
     "EndOffset": 59
     },
     {
     "Score": 0.5566426515579224,
     "Type": "ORGANIZATION",
     "Text": "AnySpa",
     "BeginOffset": 63,
     "EndOffset": 69
     },
     {
     "Score": 0.8059805631637573,
     "Type": "LOCATION",
     "Text": "123 Main St, Anywhere",
     "BeginOffset": 71,
     "EndOffset": 92
     },
     {
     "Score": 0.998830258846283,
     "Type": "PERSON",
     "Text": "Alice",
     "BeginOffset": 114,
     "EndOffset": 119
     },
     {
     "Score": 0.997818112373352,
     "Type": "OTHER",
     "Text": "AnySpa@example.com",
     "BeginOffset": 123,
     "EndOffset": 138
     }
     ],
```

```
    "File": "SampleText3.txt",
    "Line": 0
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

Ejemplo 2: cómo iniciar un trabajo de detección de entidades personalizado

En el siguiente ejemplo de `start-entities-detection-job`, se inicia un trabajo de detección de entidades personalizadas asíncrono para todos los archivos ubicados en la dirección especificada por la etiqueta `--input-data-config`. En este ejemplo, el bucket de S3 de entrada contiene `SampleFeedback1.txt`, `SampleFeedback2.txt` y `SampleFeedback3.txt`. El modelo de reconocimiento de entidades se entrenó a partir de los comentarios del servicio de atención al cliente para que reconociera los nombres de los dispositivos. Una vez completado el trabajo, la carpeta, `output`, se coloca en la ubicación que especifique la etiqueta `--output-data-config`. La carpeta contiene `output.txt`, que contiene a su vez una lista de todas las entidades con nombre detectadas en cada archivo de texto, así como la puntuación de confianza del modelo previamente entrenado para cada predicción. La salida Json se imprime en una sola línea por archivo, pero se formatea aquí para que sea legible.

```
aws comprehend start-entities-detection-job \
    --job-name customentitiestest \
    --entity-recognizer-arn "arn:aws:comprehend:us-west-2:111122223333:entity-
recognizer/entityrecognizer" \
    --language-code en \
    --input-data-config "S3Uri=s3://amzn-s3-demo-bucket/jobdata/" \
    --output-data-config "S3Uri=s3://amzn-s3-demo-destination-bucket/testfolder/" \
    --data-access-role-arn "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-IOrole"
```

Contenido de `SampleFeedback1.txt`:

```
"I've been on the AnyPhone app have had issues for 24 hours when trying to pay bill.
 Cannot make payment. Sigh. | Oh man! Lets get that app up and running. DM me, and
 we can get to work!"
```

Contenido de `SampleFeedback2.txt`:

```
"Hi, I have a discrepancy with my new bill. Could we get it sorted out? A rep added
 stuff I didnt sign up for when I did my AnyPhone 10 upgrade. | We can absolutely
 get this sorted!"
```

Contenido de `SampleFeedback3.txt`:

```
"Is the by 1 get 1 free AnySmartPhone promo still going on? | Hi Christian! It ended
 yesterday, send us a DM if you have any questions and we can take a look at your
 options!"
```

Salida:

```
{
    "JobId": "019ea9edac758806850fa8a79ff83021",
    "JobArn": "arn:aws:comprehend:us-west-2:111122223333:entities-detection-
job/019ea9edac758806850fa8a79ff83021",
    "JobStatus": "SUBMITTED"
}
```

El contenido de `output.txt` muestra las líneas con sangría para facilitar la lectura:

```
{
"Entities": [
    {
    "BeginOffset": 17,
    "EndOffset": 25,
    "Score": 0.9999728210205924,
    "Text": "AnyPhone",
    "Type": "DEVICE"
    }
],
"File": "SampleFeedback1.txt",
"Line": 0
}
{
"Entities": [
    {
    "BeginOffset": 123,
    "EndOffset": 133,
    "Score": 0.9999892116761524,
    "Text": "AnyPhone 10",
    "Type": "DEVICE"
```

```
    }
],
"File": "SampleFeedback2.txt",
"Line": 0
}
{
"Entities": [
    {
    "BeginOffset": 23,
    "EndOffset": 35,
    "Score": 0.9999971389852362,
    "Text": "AnySmartPhone",
    "Type": "DEVICE"
    }
],
"File": "SampleFeedback3.txt",
"Line": 0
}
```

Para obtener más información, consulte Custom entity recognition en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StartEntitiesDetectionJob en la Referencia de comandos de la AWS CLI.

`start-events-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-events-detection-job`.

AWS CLI

Inicio de un trabajo de detección de eventos asíncronos

El siguiente ejemplo de `start-events-detection-job` inicia un trabajo de detección de eventos asíncrono para todos los archivos ubicados en la dirección especificada por la etiqueta `--input-data-config`. Los posibles tipos de eventos de destino incluyen `BANKRUPCTY`, `EMPLOYMENT`, `CORPORATE_ACQUISITION`, `INVESTMENT_GENERAL`, `CORPORATE_MERGER`, `IPO`, `RIGHTS_ISSUE`, `SECONDARY_OFFERING`, `SHELF_OFFERING`, `TENDER_OFFERING` y `STOCK_SPLIT`. En este ejemplo, el bucket de S3 contiene `SampleText1.txt`, `SampleText2.txt` y `SampleText3.txt`. Una vez completado el trabajo, la carpeta, `output`, se coloca en la ubicación que especifique la etiqueta `--output-data-config`. La carpeta contiene `SampleText1.txt.out`, `SampleText2.txt.out` y `SampleText3.txt.out`. La

salida JSON se imprime en una sola línea por archivo, pero se formatea aquí para que sea legible.

```
aws comprehend start-events-detection-job \
    --job-name events-detection-1 \
    --input-data-config "S3Uri=s3://amzn-s3-demo-bucket/EventsData" \
    --output-data-config "S3Uri=s3://amzn-s3-demo-destination-bucket/testfolder/" \
    --data-access-role-arn arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-servicerole \
    --language-code en \
    --target-event-
types "BANKRUPTCY" "EMPLOYMENT" "CORPORATE_ACQUISITION" "CORPORATE_MERGER" "INVESTMENT_GENER
```

Contenido de `SampleText1.txt`:

```
"Company AnyCompany grew by increasing sales and through acquisitions. After
 purchasing competing firms in 2020, AnyBusiness, a part of the AnyBusinessGroup,
 gave Jane Does firm a going rate of one cent a gallon or forty-two cents a barrel."
```

Contenido de `SampleText2.txt`:

```
"In 2021, AnyCompany officially purchased AnyBusiness for 100 billion dollars,
 surprising and exciting the shareholders."
```

Contenido de `SampleText3.txt`:

```
"In 2022, AnyCompany stock crashed 50. Eventually later that year they filed for
 bankruptcy."
```

Salida:

```
{
    "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
    "JobArn": "arn:aws:comprehend:us-west-2:111122223333:events-detection-
job/123456abcdeb0e11022f22a11EXAMPLE",
    "JobStatus": "SUBMITTED"
}
```

El contenido de `SampleText1.txt.out` muestra las líneas con sangría para facilitar la lectura:

```
{
```

```
    "Entities": [
        {
        "Mentions": [
            {
            "BeginOffset": 8,
            "EndOffset": 18,
            "Score": 0.99977,
            "Text": "AnyCompany",
            "Type": "ORGANIZATION",
            "GroupScore": 1
            },
            {
            "BeginOffset": 112,
            "EndOffset": 123,
            "Score": 0.999747,
            "Text": "AnyBusiness",
            "Type": "ORGANIZATION",
            "GroupScore": 0.979826
            },
            {
            "BeginOffset": 171,
            "EndOffset": 175,
            "Score": 0.999615,
            "Text": "firm",
            "Type": "ORGANIZATION",
            "GroupScore": 0.871647
            }
        ]
        },
        {
        "Mentions": [
            {
            "BeginOffset": 97,
            "EndOffset": 102,
            "Score": 0.987687,
            "Text": "firms",
            "Type": "ORGANIZATION",
            "GroupScore": 1
            }
        ]
        },
        {
        "Mentions": [
            {
```

```
            "BeginOffset": 103,
            "EndOffset": 110,
            "Score": 0.999458,
            "Text": "in 2020",
            "Type": "DATE",
            "GroupScore": 1
            }
        ]
        },
        {
        "Mentions": [
            {
            "BeginOffset": 160,
            "EndOffset": 168,
            "Score": 0.999649,
            "Text": "John Doe",
            "Type": "PERSON",
            "GroupScore": 1
            }
        ]
        }
    ],
    "Events": [
        {
        "Type": "CORPORATE_ACQUISITION",
        "Arguments": [
            {
            "EntityIndex": 0,
            "Role": "INVESTOR",
            "Score": 0.99977
            }
        ],
        "Triggers": [
            {
            "BeginOffset": 56,
            "EndOffset": 68,
            "Score": 0.999967,
            "Text": "acquisitions",
            "Type": "CORPORATE_ACQUISITION",
            "GroupScore": 1
            }
        ]
        },
        {
```

```
        "Type": "CORPORATE_ACQUISITION",
        "Arguments": [
            {
            "EntityIndex": 1,
            "Role": "INVESTEE",
            "Score": 0.987687
            },
            {
            "EntityIndex": 2,
            "Role": "DATE",
            "Score": 0.999458
            },
            {
            "EntityIndex": 3,
            "Role": "INVESTOR",
            "Score": 0.999649
            }
        ],
        "Triggers": [
            {
            "BeginOffset": 76,
            "EndOffset": 86,
            "Score": 0.999973,
            "Text": "purchasing",
            "Type": "CORPORATE_ACQUISITION",
            "GroupScore": 1
            }
        ]
        }
    ],
    "File": "SampleText1.txt",
    "Line": 0
}
```

Contenido de `SampleText2.txt.out`:

```
{
    "Entities": [
        {
        "Mentions": [
            {
            "BeginOffset": 0,
            "EndOffset": 7,
```

```
            "Score": 0.999473,
            "Text": "In 2021",
            "Type": "DATE",
            "GroupScore": 1
            }
        ]
        },
        {
        "Mentions": [
            {
            "BeginOffset": 9,
            "EndOffset": 19,
            "Score": 0.999636,
            "Text": "AnyCompany",
            "Type": "ORGANIZATION",
            "GroupScore": 1
            }
        ]
        },
        {
        "Mentions": [
            {
            "BeginOffset": 45,
            "EndOffset": 56,
            "Score": 0.999712,
            "Text": "AnyBusiness",
            "Type": "ORGANIZATION",
            "GroupScore": 1
            }
        ]
        },
        {
        "Mentions": [
            {
            "BeginOffset": 61,
            "EndOffset": 80,
            "Score": 0.998886,
            "Text": "100 billion dollars",
            "Type": "MONETARY_VALUE",
            "GroupScore": 1
            }
        ]
        }
    ],
```

```
    "Events": [
        {
        "Type": "CORPORATE_ACQUISITION",
        "Arguments": [
            {
            "EntityIndex": 3,
            "Role": "AMOUNT",
            "Score": 0.998886
            },
            {
            "EntityIndex": 2,
            "Role": "INVESTEE",
            "Score": 0.999712
            },
            {
            "EntityIndex": 0,
            "Role": "DATE",
            "Score": 0.999473
            },
            {
            "EntityIndex": 1,
            "Role": "INVESTOR",
            "Score": 0.999636
            }
        ],
        "Triggers": [
            {
            "BeginOffset": 31,
            "EndOffset": 40,
            "Score": 0.99995,
            "Text": "purchased",
            "Type": "CORPORATE_ACQUISITION",
            "GroupScore": 1
            }
        ]
        }
    ],
    "File": "SampleText2.txt",
    "Line": 0
}
```


Contenido de `SampleText3.txt.out`:

```
{
    "Entities": [
        {
        "Mentions": [
            {
            "BeginOffset": 9,
            "EndOffset": 19,
            "Score": 0.999774,
            "Text": "AnyCompany",
            "Type": "ORGANIZATION",
            "GroupScore": 1
            },
            {
            "BeginOffset": 66,
            "EndOffset": 70,
            "Score": 0.995717,
            "Text": "they",
            "Type": "ORGANIZATION",
            "GroupScore": 0.997626
            }
        ]
        },
        {
        "Mentions": [
            {
            "BeginOffset": 50,
            "EndOffset": 65,
            "Score": 0.999656,
            "Text": "later that year",
            "Type": "DATE",
            "GroupScore": 1
            }
        ]
        }
    ],
    "Events": [
        {
        "Type": "BANKRUPTCY",
        "Arguments": [
            {
            "EntityIndex": 1,
            "Role": "DATE",
            "Score": 0.999656
```

```
            },
            {
            "EntityIndex": 0,
            "Role": "FILER",
            "Score": 0.995717
            }
        ],
        "Triggers": [
            {
            "BeginOffset": 81,
            "EndOffset": 91,
            "Score": 0.999936,
            "Text": "bankruptcy",
            "Type": "BANKRUPTCY",
            "GroupScore": 1
            }
        ]
        }
    ],
    "File": "SampleText3.txt",
    "Line": 0
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StartEventsDetectionJob en la Referencia de comandos de la AWS CLI.

`start-flywheel-iteration`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-flywheel-iteration`.

AWS CLI

Inicio de una iteración con volante de inercia

En el siguiente ejemplo de `start-flywheel-iteration`, se inicia una iteración de un volante de inercia. Esta operación utiliza cualquier conjunto de datos nuevo del volante de inercia para entrenar una nueva versión del modelo.

```
aws comprehend start-flywheel-iteration \
```

```
    --flywheel-arn arn:aws:comprehend:us-west-2:111122223333:flywheel/example-
flywheel
```

Salida:

```
{
    "FlywheelArn": "arn:aws:comprehend:us-west-2:111122223333:flywheel/example-
flywheel",
    "FlywheelIterationId": "12345123TEXAMPLE"
}
```

Para obtener más información, consulte Flywheel overview en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StartFlywheelIteration en la Referencia de comandos de la AWS CLI.

`start-key-phrases-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-key-phrases-detection-job`.

AWS CLI

Detención de un trabajo de detección de frases clave

En el siguiente ejemplo de `start-key-phrases-detection-job`, se inicia un trabajo de detección de frases clave asíncrono para todos los archivos ubicados en la dirección especificada por la etiqueta `--input-data-config`. En este ejemplo, el bucket de S3 contiene `Sampletext1.txt`, `Sampletext2.txt` y `Sampletext3.txt`. Una vez completado el trabajo, la carpeta, `output`, se coloca en la ubicación que especifique la etiqueta `--output-data-config`. La carpeta contiene el archivo `output.txt`, que contiene a su vez una lista de todas las frases clave detectadas en cada archivo de texto, así como la puntuación de confianza del modelo previamente entrenado para cada predicción. La salida Json se imprime en una sola línea por archivo, pero se formatea aquí para que sea legible.

```
aws comprehend start-key-phrases-detection-job \
    --job-name keyphrasesanalysistest1 \
    --language-code en \
    --input-data-config "S3Uri=s3://amzn-s3-demo-bucket/" \
    --output-data-config "S3Uri=s3://amzn-s3-demo-destination-bucket/testfolder/" \
```

```
    --data-access-role-arn "arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role" \
    --language-code en
```

Contenido de `Sampletext1.txt`:

```
"Hello Zhang Wei, I am John. Your AnyCompany Financial Services, LLC credit card
 account 1111-XXXX-1111-XXXX has a minimum payment of $24.53 that is due by July
 31st."
```

Contenido de `Sampletext2.txt`:

```
"Dear Max, based on your autopay settings for your account Internet.org account, we
 will withdraw your payment on the due date from your bank account number XXXXXX1111
 with the routing number XXXXX0000. "
```

Contenido de `Sampletext3.txt`:

```
"Jane, please submit any customer feedback from this weekend to Sunshine Spa, 123
 Main St, Anywhere and send comments to Alice at AnySpa@example.com."
```

Salida:

```
{
    "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
    "JobArn": "arn:aws:comprehend:us-west-2:111122223333:key-phrases-detection-
job/123456abcdeb0e11022f22a11EXAMPLE",
    "JobStatus": "SUBMITTED"
}
```

El contenido de `output.txt` muestra las líneas con sangría para facilitar la lectura:

```
{
    "File": "SampleText1.txt",
    "KeyPhrases": [
        {
        "BeginOffset": 6,
        "EndOffset": 15,
        "Score": 0.9748965572679326,
        "Text": "Zhang Wei"
        },
```

```
        {
        "BeginOffset": 22,
        "EndOffset": 26,
        "Score": 0.9997344722354619,
        "Text": "John"
        },
        {
        "BeginOffset": 28,
        "EndOffset": 62,
        "Score": 0.9843791074032948,
        "Text": "Your AnyCompany Financial Services"
        },
        {
        "BeginOffset": 64,
        "EndOffset": 107,
        "Score": 0.8976122401721824,
        "Text": "LLC credit card account 1111-XXXX-1111-XXXX"
        },
        {
        "BeginOffset": 112,
        "EndOffset": 129,
        "Score": 0.9999612982629748,
        "Text": "a minimum payment"
        },
        {
        "BeginOffset": 133,
        "EndOffset": 139,
        "Score": 0.99975728947036,
        "Text": "$24.53"
        },
        {
        "BeginOffset": 155,
        "EndOffset": 164,
        "Score": 0.9940866241449973,
        "Text": "July 31st"
        }
    ],
    "Line": 0
    }
    {
    "File": "SampleText2.txt",
    "KeyPhrases": [
        {
        "BeginOffset": 0,
```

```
        "EndOffset": 8,
        "Score": 0.9974021100118472,
        "Text": "Dear Max"
        },
        {
        "BeginOffset": 19,
        "EndOffset": 40,
        "Score": 0.9961120519515884,
        "Text": "your autopay settings"
        },
        {
        "BeginOffset": 45,
        "EndOffset": 78,
        "Score": 0.9980620070116009,
        "Text": "your account Internet.org account"
        },
        {
        "BeginOffset": 97,
        "EndOffset": 109,
        "Score": 0.999919660140754,
        "Text": "your payment"
        },
        {
        "BeginOffset": 113,
        "EndOffset": 125,
        "Score": 0.9998370719754205,
        "Text": "the due date"
        },
        {
        "BeginOffset": 131,
        "EndOffset": 166,
        "Score": 0.9955068678502509,
        "Text": "your bank account number XXXXXX1111"
        },
        {
        "BeginOffset": 172,
        "EndOffset": 200,
        "Score": 0.8653433315829526,
        "Text": "the routing number XXXXX0000"
        }
    ],
    "Line": 0
    }
    {
```

```
    "File": "SampleText3.txt",
    "KeyPhrases": [
        {
        "BeginOffset": 0,
        "EndOffset": 4,
        "Score": 0.9142947833681668,
        "Text": "Jane"
        },
        {
        "BeginOffset": 20,
        "EndOffset": 41,
        "Score": 0.9984325676596763,
        "Text": "any customer feedback"
        },
        {
        "BeginOffset": 47,
        "EndOffset": 59,
        "Score": 0.9998782448150636,
        "Text": "this weekend"
        },
        {
        "BeginOffset": 63,
        "EndOffset": 75,
        "Score": 0.99866741830757,
        "Text": "Sunshine Spa"
        },
        {
        "BeginOffset": 77,
        "EndOffset": 88,
        "Score": 0.9695803485466054,
        "Text": "123 Main St"
        },
        {
        "BeginOffset": 108,
        "EndOffset": 116,
        "Score": 0.9997065928550928,
        "Text": "comments"
        },
        {
        "BeginOffset": 120,
        "EndOffset": 125,
        "Score": 0.9993466833825161,
        "Text": "Alice"
        },
```

```
        {
        "BeginOffset": 129,
        "EndOffset": 144,
        "Score": 0.9654563612885667,
        "Text": "AnySpa@example.com"
        }
    ],
    "Line": 0
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StartKeyPhrasesDetectionJob en la Referencia de comandos de la AWS CLI.

`start-pii-entities-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-pii-entities-detection-job`.

AWS CLI

Inicio de un trabajo de detección de PII asíncrono

En el siguiente ejemplo de `start-pii-entities-detection-job`, se inicia un trabajo de detección de entidades de información de identificación personal (PII) asíncrono para todos los archivos ubicados en la dirección especificada por la etiqueta `--input-data-config`. En este ejemplo, el bucket de S3 contiene `Sampletext1.txt`, `Sampletext2.txt` y `Sampletext3.txt`. Una vez completado el trabajo, la carpeta, `output`, se coloca en la ubicación que especifique la etiqueta `--output-data-config`. La carpeta contiene `SampleText1.txt.out`, `SampleText2.txt.out` y `SampleText3.txt.out`, en donde se enumeran las entidades con nombre dentro de cada archivo de texto. La salida Json se imprime en una sola línea por archivo, pero se formatea aquí para que sea legible.

```
aws comprehend start-pii-entities-detection-job \
    --job-name entities_test \
    --language-code en \
    --input-data-config "S3Uri=s3://amzn-s3-demo-bucket/" \
    --output-data-config "S3Uri=s3://amzn-s3-demo-destination-bucket/testfolder/" \
```

```
    --data-access-role-arn arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role \
    --language-code en \
    --mode ONLY_OFFSETS
```

Contenido de `Sampletext1.txt`:

```
"Hello Zhang Wei, I am John. Your AnyCompany Financial Services, LLC credit card
 account 1111-XXXX-1111-XXXX has a minimum payment of $24.53 that is due by July
 31st."
```

Contenido de `Sampletext2.txt`:

```
"Dear Max, based on your autopay settings for your account Internet.org account, we
 will withdraw your payment on the due date from your bank account number XXXXXX1111
 with the routing number XXXXX0000. "
```

Contenido de `Sampletext3.txt`:

```
"Jane, please submit any customer feedback from this weekend to Sunshine Spa, 123
 Main St, Anywhere and send comments to Alice at AnySpa@example.com."
```

Salida:

```
{
    "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
    "JobArn": "arn:aws:comprehend:us-west-2:111122223333:pii-entities-detection-
job/123456abcdeb0e11022f22a11EXAMPLE",
    "JobStatus": "SUBMITTED"
}
```

El contenido de `SampleText1.txt.out` muestra las líneas con sangría para facilitar la lectura:

```
{
    "Entities": [
        {
        "BeginOffset": 6,
        "EndOffset": 15,
        "Type": "NAME",
        "Score": 0.9998490510222595
```

```
        },
        {
        "BeginOffset": 22,
        "EndOffset": 26,
        "Type": "NAME",
        "Score": 0.9998937958019426
        },
        {
        "BeginOffset": 88,
        "EndOffset": 107,
        "Type": "CREDIT_DEBIT_NUMBER",
        "Score": 0.9554297245278491
        },
        {
        "BeginOffset": 155,
        "EndOffset": 164,
        "Type": "DATE_TIME",
        "Score": 0.9999720462925257
        }
    ],
    "File": "SampleText1.txt",
    "Line": 0
}
```

El contenido de `SampleText2.txt.out` muestra las líneas con sangría para facilitar la lectura:

```
{
    "Entities": [
        {
        "BeginOffset": 5,
        "EndOffset": 8,
        "Type": "NAME",
        "Score": 0.9994390774924007
        },
        {
        "BeginOffset": 58,
        "EndOffset": 70,
        "Type": "URL",
        "Score": 0.9999958276922101
        },
        {
        "BeginOffset": 156,
        "EndOffset": 166,
```

```
        "Type": "BANK_ACCOUNT_NUMBER",
        "Score": 0.9999721058045592
        },
        {
        "BeginOffset": 191,
        "EndOffset": 200,
        "Type": "BANK_ROUTING",
        "Score": 0.9998968945989909
        }
    ],
    "File": "SampleText2.txt",
    "Line": 0
}
```

El contenido de `SampleText3.txt.out` muestra las líneas con sangría para facilitar la lectura:

```
{
    "Entities": [
        {
        "BeginOffset": 0,
        "EndOffset": 4,
        "Type": "NAME",
        "Score": 0.999949934606805
        },
        {
        "BeginOffset": 77,
        "EndOffset": 88,
        "Type": "ADDRESS",
        "Score": 0.9999035300466904
        },
        {
        "BeginOffset": 120,
        "EndOffset": 125,
        "Type": "NAME",
        "Score": 0.9998203838716296
        },
        {
        "BeginOffset": 129,
        "EndOffset": 144,
        "Type": "EMAIL",
        "Score": 0.9998313473105228
        }
    ],
```

```
    "File": "SampleText3.txt",
    "Line": 0
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StartPiiEntitiesDetectionJob en la Referencia de comandos de la AWS CLI.

`start-sentiment-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-sentiment-detection-job`.

AWS CLI

Inicio de un trabajo de análisis de opiniones asíncrono

En el siguiente ejemplo de `start-sentiment-detection-job`, se inicia un trabajo de detección de análisis de opiniones asíncrono para todos los archivos ubicados en la dirección especificada por la etiqueta `--input-data-config`. En este ejemplo, la carpeta del bucket de S3 contiene `SampleMovieReview1.txt`, `SampleMovieReview2.txt` y `SampleMovieReview3.txt`. Una vez completado el trabajo, la carpeta, `output`, se coloca en la ubicación que especifique la etiqueta `--output-data-config`. La carpeta contiene el archivo, `output.txt`, que contiene a su vez las opiniones predominantes para cada archivo de texto, así como la puntuación de confianza del modelo previamente entrenado para cada predicción. La salida Json se imprime en una sola línea por archivo, pero se formatea aquí para que sea legible.

```
aws comprehend start-sentiment-detection-job \
    --job-name example-sentiment-detection-job \
    --language-code en \
    --input-data-config "S3Uri=s3://amzn-s3-demo-bucket/MovieData" \
    --output-data-config "S3Uri=s3://amzn-s3-demo-destination-bucket/testfolder/" \
    --data-access-role-arn arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role
```

Contenido de `SampleMovieReview1.txt`:

```
"The film, AnyMovie2, is fairly predictable and just okay."
```

Contenido de `SampleMovieReview2.txt`:

```
"AnyMovie2 is the essential sci-fi film that I grew up watching when I was a kid. I
 highly recommend this movie."
```

Contenido de `SampleMovieReview3.txt`:

```
"Don't get fooled by the 'awards' for AnyMovie2. All parts of the film were poorly
 stolen from other modern directors."
```

Salida:

```
{
    "JobId": "0b5001e25f62ebb40631a9a1a7fde7b3",
    "JobArn": "arn:aws:comprehend:us-west-2:111122223333:sentiment-detection-
job/0b5001e25f62ebb40631a9a1a7fde7b3",
    "JobStatus": "SUBMITTED"
}
```

El contenido de `output.txt` muestra las líneas con sangría para facilitar la lectura:

```
{
    "File": "SampleMovieReview1.txt",
        "Line": 0,
        "Sentiment": "MIXED",
        "SentimentScore": {
            "Mixed": 0.6591159105300903,
            "Negative": 0.26492202281951904,
            "Neutral": 0.035430654883384705,
            "Positive": 0.04053137078881264
            }
        }
    {
    "File": "SampleMovieReview2.txt",
        "Line": 0,
        "Sentiment": "POSITIVE",
        "SentimentScore": {
            "Mixed": 0.00000871846623340388,
            "Negative": 0.00006134175055194646,
            "Neutral": 0.0002941041602753103,
            "Positive": 0.9996358156204224
            }
```

```
        }
    {
    "File": "SampleMovieReview3.txt",
        "Line": 0,
        "Sentiment": "NEGATIVE",
        "SentimentScore": {
            "Mixed": 0.004146667663007975,
            "Negative": 0.9645107984542847,
            "Neutral": 0.016559595242142677,
            "Positive": 0.014782938174903393
        }
    }
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StartSentimentDetectionJob en la Referencia de comandos de la AWS CLI.

`start-targeted-sentiment-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-targeted-sentiment-detection-job`.

AWS CLI

Inicio de un trabajo de análisis de opiniones específicas asíncrono

En el siguiente ejemplo de `start-targeted-sentiment-detection-job`, se inicia un trabajo de detección de análisis de opiniones específicas asíncrono para todos los archivos ubicados en la dirección especificada por la etiqueta `--input-data-config`. En este ejemplo, la carpeta del bucket de S3 contiene `SampleMovieReview1.txt`, `SampleMovieReview2.txt` y `SampleMovieReview3.txt`. Cuando se completa el trabajo, `output.tar.gz` se coloca en la ubicación que especifique la etiqueta `--output-data-config`. `output.tar.gz`contiene los archivos `SampleMovieReview1.txt.out`, `SampleMovieReview2.txt.out` y `SampleMovieReview3.txt.out`, cada uno de los cuales contiene todas las entidades con nombre y las opiniones asociadas para un único archivo de texto de entrada.

```
aws comprehend start-targeted-sentiment-detection-job \
    --job-name targeted_movie_review_analysis1 \
```

```
    --language-code en \
    --input-data-config "S3Uri=s3://amzn-s3-demo-bucket/MovieData" \
    --output-data-config "S3Uri=s3://amzn-s3-demo-destination-bucket/testfolder/" \
    --data-access-role-arn arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role
```

Contenido de `SampleMovieReview1.txt`:

```
"The film, AnyMovie, is fairly predictable and just okay."
```

Contenido de `SampleMovieReview2.txt`:

```
"AnyMovie is the essential sci-fi film that I grew up watching when I was a kid. I
 highly recommend this movie."
```

Contenido de `SampleMovieReview3.txt`:

```
"Don't get fooled by the 'awards' for AnyMovie. All parts of the film were poorly
 stolen from other modern directors."
```

Salida:

```
{
    "JobId": "0b5001e25f62ebb40631a9a1a7fde7b3",
    "JobArn": "arn:aws:comprehend:us-west-2:111122223333:targeted-sentiment-
detection-job/0b5001e25f62ebb40631a9a1a7fde7b3",
    "JobStatus": "SUBMITTED"
}
```

El contenido de `SampleMovieReview1.txt.out` muestra las líneas con sangría para facilitar la lectura:

```
{
    "Entities": [
        {
        "DescriptiveMentionIndex": [
            0
        ],
        "Mentions": [
            {
            "BeginOffset": 4,
```

```
            "EndOffset": 8,
            "Score": 0.994972,
            "GroupScore": 1,
            "Text": "film",
            "Type": "MOVIE",
            "MentionSentiment": {
                "Sentiment": "NEUTRAL",
                "SentimentScore": {
                "Mixed": 0,
                "Negative": 0,
                "Neutral": 1,
                "Positive": 0
                }
            }
            }
        ]
        },
        {
        "DescriptiveMentionIndex": [
            0
        ],
        "Mentions": [
            {
            "BeginOffset": 10,
            "EndOffset": 18,
            "Score": 0.631368,
            "GroupScore": 1,
            "Text": "AnyMovie",
            "Type": "ORGANIZATION",
            "MentionSentiment": {
                "Sentiment": "POSITIVE",
                "SentimentScore": {
                "Mixed": 0.001729,
                "Negative": 0.000001,
                "Neutral": 0.000318,
                "Positive": 0.997952
                }
            }
            }
        ]
        }
    ],
    "File": "SampleMovieReview1.txt",
    "Line": 0
```

```
}
```

El contenido de `SampleMovieReview2.txt.out` muestra las líneas con sangría para facilitar la lectura:

```
{
    "Entities": [
        {
        "DescriptiveMentionIndex": [
            0
        ],
        "Mentions": [
            {
            "BeginOffset": 0,
            "EndOffset": 8,
            "Score": 0.854024,
            "GroupScore": 1,
            "Text": "AnyMovie",
            "Type": "MOVIE",
            "MentionSentiment": {
                "Sentiment": "POSITIVE",
                "SentimentScore": {
                "Mixed": 0,
                "Negative": 0,
                "Neutral": 0.000007,
                "Positive": 0.999993
                }
            }
            },
            {
            "BeginOffset": 104,
            "EndOffset": 109,
            "Score": 0.999129,
            "GroupScore": 0.502937,
            "Text": "movie",
            "Type": "MOVIE",
            "MentionSentiment": {
                "Sentiment": "POSITIVE",
                "SentimentScore": {
                "Mixed": 0,
                "Negative": 0,
                "Neutral": 0,
                "Positive": 1
```

```
                }
            }
            },
            {
            "BeginOffset": 33,
            "EndOffset": 37,
            "Score": 0.999823,
            "GroupScore": 0.999252,
            "Text": "film",
            "Type": "MOVIE",
            "MentionSentiment": {
                "Sentiment": "POSITIVE",
                "SentimentScore": {
                "Mixed": 0,
                "Negative": 0,
                "Neutral": 0.000001,
                "Positive": 0.999999
                }
            }
            }
        ]
        },
        {
        "DescriptiveMentionIndex": [
            0,
            1,
            2
        ],
        "Mentions": [
            {
            "BeginOffset": 43,
            "EndOffset": 44,
            "Score": 0.999997,
            "GroupScore": 1,
            "Text": "I",
            "Type": "PERSON",
            "MentionSentiment": {
                "Sentiment": "NEUTRAL",
                "SentimentScore": {
                "Mixed": 0,
                "Negative": 0,
                "Neutral": 1,
                "Positive": 0
                }
```

```
            }
            },
            {
            "BeginOffset": 80,
            "EndOffset": 81,
            "Score": 0.999996,
            "GroupScore": 0.52523,
            "Text": "I",
            "Type": "PERSON",
            "MentionSentiment": {
                "Sentiment": "NEUTRAL",
                "SentimentScore": {
                "Mixed": 0,
                "Negative": 0,
                "Neutral": 1,
                "Positive": 0
                }
            }
            },
            {
            "BeginOffset": 67,
            "EndOffset": 68,
            "Score": 0.999994,
            "GroupScore": 0.999499,
            "Text": "I",
            "Type": "PERSON",
            "MentionSentiment": {
                "Sentiment": "NEUTRAL",
                "SentimentScore": {
                "Mixed": 0,
                "Negative": 0,
                "Neutral": 1,
                "Positive": 0
                }
            }
            }
        ]
        },
        {
        "DescriptiveMentionIndex": [
            0
        ],
        "Mentions": [
            {
```

```
            "BeginOffset": 75,
            "EndOffset": 78,
            "Score": 0.999978,
            "GroupScore": 1,
            "Text": "kid",
            "Type": "PERSON",
            "MentionSentiment": {
                "Sentiment": "NEUTRAL",
                "SentimentScore": {
                "Mixed": 0,
                "Negative": 0,
                "Neutral": 1,
                "Positive": 0
                }
            }
            }
        ]
        }
    ],
    "File": "SampleMovieReview2.txt",
    "Line": 0
}
```

El contenido de `SampleMovieReview3.txt.out` muestra las líneas con sangría para facilitar la lectura:

```
{
    "Entities": [
        {
        "DescriptiveMentionIndex": [
            1
        ],
        "Mentions": [
            {
            "BeginOffset": 64,
            "EndOffset": 68,
            "Score": 0.992953,
            "GroupScore": 0.999814,
            "Text": "film",
            "Type": "MOVIE",
            "MentionSentiment": {
                "Sentiment": "NEUTRAL",
                "SentimentScore": {
```

```
                "Mixed": 0.000004,
                "Negative": 0.010425,
                "Neutral": 0.989543,
                "Positive": 0.000027
                }
            }
            },
            {
            "BeginOffset": 37,
            "EndOffset": 45,
            "Score": 0.999782,
            "GroupScore": 1,
            "Text": "AnyMovie",
            "Type": "ORGANIZATION",
            "MentionSentiment": {
                "Sentiment": "POSITIVE",
                "SentimentScore": {
                "Mixed": 0.000095,
                "Negative": 0.039847,
                "Neutral": 0.000673,
                "Positive": 0.959384
                }
            }
            }
        ]
        },
        {
        "DescriptiveMentionIndex": [
            0
        ],
        "Mentions": [
            {
            "BeginOffset": 47,
            "EndOffset": 50,
            "Score": 0.999991,
            "GroupScore": 1,
            "Text": "All",
            "Type": "QUANTITY",
            "MentionSentiment": {
                "Sentiment": "NEUTRAL",
                "SentimentScore": {
                "Mixed": 0.000001,
                "Negative": 0.000001,
                "Neutral": 0.999998,
```

```
                "Positive": 0
                }
            }
            }
        ]
        },
        {
        "DescriptiveMentionIndex": [
            0
        ],
        "Mentions": [
            {
            "BeginOffset": 106,
            "EndOffset": 115,
            "Score": 0.542083,
            "GroupScore": 1,
            "Text": "directors",
            "Type": "PERSON",
            "MentionSentiment": {
                "Sentiment": "NEUTRAL",
                "SentimentScore": {
                "Mixed": 0,
                "Negative": 0,
                "Neutral": 1,
                "Positive": 0
                }
            }
            }
        ]
        }
    ],
    "File": "SampleMovieReview3.txt",
    "Line": 0
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StartTargetedSentimentDetectionJob en la Referencia de comandos de la AWS CLI.

`start-topics-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-topics-detection-job`.

AWS CLI

Para iniciar un trabajo de análisis de detección de temas

El siguiente ejemplo de `start-topics-detection-job` inicia un trabajo de detección de temas asíncrono para todos los archivos ubicados en la dirección especificada por la etiqueta `--input-data-config`. Una vez finalizado el trabajo, la carpeta, `output`, se coloca en la ubicación especificada por la etiqueta `--ouput-data-config`. `output` contiene topic-terms.csv y doc-topics.csv. El primer archivo de salida, topic-terms.csv, es una lista de temas del conjunto. Para cada tema, la lista incluye, de forma predeterminada, los principales términos por tema según su importancia. El segundo archivo, `doc-topics.csv`, enumera los documentos relacionados con un tema y la proporción del documento que trata sobre el tema.

```
aws comprehend start-topics-detection-job \
    --job-name example_topics_detection_job \
    --language-code en \
    --input-data-config "S3Uri=s3://amzn-s3-demo-bucket/" \
    --output-data-config "S3Uri=s3://amzn-s3-demo-destination-bucket/testfolder/" \
    --data-access-role-arn arn:aws:iam::111122223333:role/service-role/
AmazonComprehendServiceRole-example-role \
    --language-code en
```

Salida:

```
{
    "JobId": "123456abcdeb0e11022f22a11EXAMPLE",
    "JobArn": "arn:aws:comprehend:us-west-2:111122223333:key-phrases-detection-
job/123456abcdeb0e11022f22a11EXAMPLE",
    "JobStatus": "SUBMITTED"
}
```

Para obtener más información, consulte Modelado de temas en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener información sobre la API, consulte StartTopicsDetectionJob en la Referencia de comandos de la AWS CLI.

`stop-dominant-language-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-dominant-language-detection-job`.

AWS CLI

Detención de un trabajo de detección de idioma dominante asíncrono

En el siguiente ejemplo de `stop-dominant-language-detection-job`, se detiene un trabajo de detección de idioma dominante asíncrono en curso. Si el estado actual del trabajo es `IN_PROGRESS`, el trabajo se marca para su finalización y se coloca en el estado `STOP_REQUESTED`. Si el trabajo se completa antes de poder detenerlo, se coloca en el estado `COMPLETED`.

```
aws comprehend stop-dominant-language-detection-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "JobId": "123456abcdeb0e11022f22a11EXAMPLE,
    "JobStatus": "STOP_REQUESTED"
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StopDominantLanguageDetectionJob en la Referencia de comandos de la AWS CLI.

`stop-entities-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-entities-detection-job`.

AWS CLI

Detención de un trabajo de detección de eventos asíncrono

En el siguiente ejemplo de `stop-entities-detection-job`, se detiene un trabajo de detección de entidades asíncrono en curso. Si el estado actual del trabajo es `IN_PROGRESS`, el

trabajo se marca para su finalización y se coloca en el estado STOP_REQUESTED. Si el trabajo se completa antes de poder detenerlo, se coloca en el estado COMPLETED.

```
aws comprehend stop-entities-detection-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "JobId": "123456abcdeb0e11022f22a11EXAMPLE,
    "JobStatus": "STOP_REQUESTED"
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StopEntitiesDetectionJob en la Referencia de comandos de la AWS CLI.

stop-events-detection-job

En el siguiente ejemplo de código, se muestra cómo utilizar stop-events-detection-job.

AWS CLI

Detención de un trabajo de detección de eventos asíncrono

En el siguiente ejemplo de stop-events-detection-job, se detiene un trabajo de detección de eventos asíncrono en curso. Si el estado actual del trabajo es IN_PROGRESS, el trabajo se marca para su finalización y se coloca en el estado STOP_REQUESTED. Si el trabajo se completa antes de poder detenerlo, se coloca en el estado COMPLETED.

```
aws comprehend stop-events-detection-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "JobId": "123456abcdeb0e11022f22a11EXAMPLE,
    "JobStatus": "STOP_REQUESTED"
```

```
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StopEventsDetectionJob en la Referencia de comandos de la AWS CLI.

`stop-key-phrases-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-key-phrases-detection-job`.

AWS CLI

Detención de un trabajo de detección de frases clave asíncrono

En el siguiente ejemplo de `stop-key-phrases-detection-job`, se detiene un trabajo de detección de frases clave asíncrono en curso. Si el estado actual del trabajo es `IN_PROGRESS`, el trabajo se marca para su finalización y se coloca en el estado `STOP_REQUESTED`. Si el trabajo se completa antes de poder detenerlo, se coloca en el estado `COMPLETED`.

```
aws comprehend stop-key-phrases-detection-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "JobId": "123456abcdeb0e11022f22a11EXAMPLE,
    "JobStatus": "STOP_REQUESTED"
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StopKeyPhrasesDetectionJob en la Referencia de comandos de la AWS CLI.

`stop-pii-entities-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-pii-entities-detection-job`.

AWS CLI

Detención de un trabajo de detección de entidades de PII asíncrono

En el siguiente ejemplo de `stop-pii-entities-detection-job`, se detiene un trabajo de detección de entidades de PII asíncrono en curso. Si el estado actual del trabajo es `IN_PROGRESS`, el trabajo se marca para su finalización y se coloca en el estado `STOP_REQUESTED`. Si el trabajo se completa antes de poder detenerlo, se coloca en el estado `COMPLETED`.

```
aws comprehend stop-pii-entities-detection-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "JobId": "123456abcdeb0e11022f22a11EXAMPLE,
    "JobStatus": "STOP_REQUESTED"
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StopPiiEntitiesDetectionJob en la Referencia de comandos de la AWS CLI.

`stop-sentiment-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-sentiment-detection-job`.

AWS CLI

Detención de un trabajo de detección de opiniones asíncrono

En el siguiente ejemplo de `stop-sentiment-detection-job`, se detiene un trabajo de detección de opiniones asíncrono en curso. Si el estado actual del trabajo es `IN_PROGRESS`, el trabajo se marca para su finalización y se coloca en el estado `STOP_REQUESTED`. Si el trabajo se completa antes de poder detenerlo, se coloca en el estado `COMPLETED`.

```
aws comprehend stop-sentiment-detection-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "JobId": "123456abcdeb0e11022f22a11EXAMPLE,
    "JobStatus": "STOP_REQUESTED"
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StopSentimentDetectionJob en la Referencia de comandos de la AWS CLI.

`stop-targeted-sentiment-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-targeted-sentiment-detection-job`.

AWS CLI

Detención de un trabajo de detección de opiniones específicas asíncrono

En el siguiente ejemplo de `stop-targeted-sentiment-detection-job`, se detiene un trabajo de detección de opiniones específicas asíncrono en curso. Si el estado actual del trabajo es `IN_PROGRESS`, el trabajo se marca para su finalización y se coloca en el estado `STOP_REQUESTED`. Si el trabajo se completa antes de poder detenerlo, se coloca en el estado `COMPLETED`.

```
aws comprehend stop-targeted-sentiment-detection-job \
    --job-id 123456abcdeb0e11022f22a11EXAMPLE
```

Salida:

```
{
    "JobId": "123456abcdeb0e11022f22a11EXAMPLE,
    "JobStatus": "STOP_REQUESTED"
}
```

Para obtener más información, consulte Análisis asincrónico para información de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StopTargetedSentimentDetectionJob en la Referencia de comandos de la AWS CLI.

`stop-training-document-classifier`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-training-document-classifier`.

AWS CLI

Detención del entrenamiento de un modelo clasificador de documentos

En el siguiente ejemplo de `stop-training-document-classifier`, se detiene el entrenamiento de un modelo clasificador de documentos en curso.

```
aws comprehend stop-training-document-classifier
    --document-classifier-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier/example-classifier
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación y administración de modelos personalizados en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StopTrainingDocumentClassifier en la Referencia de comandos de la AWS CLI.

`stop-training-entity-recognizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-training-entity-recognizer`.

AWS CLI

Detención del entrenamiento de un modelo de reconocimiento de entidades

En el siguiente ejemplo de `stop-training-entity-recognizer`, se detiene el entrenamiento de un modelo de reconocimiento de entidades en curso.

```
aws comprehend stop-training-entity-recognizer
```

```
    --entity-recognizer-arn "arn:aws:comprehend:us-west-2:111122223333:entity-
recognizer/examplerecognizer1"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación y administración de modelos personalizados en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte StopTrainingEntityRecognizer en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Ejemplo 1: etiquetar un recurso

En el siguiente ejemplo de `tag-resource`, se añade una sola etiqueta a un recurso de Amazon Comprehend.

```
aws comprehend tag-resource \
    --resource-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier/
example-classifier/version/1 \
    --tags Key=Location,Value=Seattle
```

El comando no genera ningún resultado.

Para obtener más información, consulte Tagging your resources en la Guía para desarrolladores de Amazon Comprehend.

Ejemplo 2: añadir varias etiquetas a un recurso

En el siguiente ejemplo de `tag-resource`, se añaden varias etiquetas a un recurso de Amazon Comprehend.

```
aws comprehend tag-resource \
    --resource-arn "arn:aws:comprehend:us-west-2:111122223333:document-classifier/
example-classifier/version/1" \
    --tags Key=location,Value=Seattle Key=Department,Value=Finance
```

El comando no genera ningún resultado.

Para obtener más información, consulte Tagging your resources en la Guía para desarrolladores de Amazon Comprehend.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Ejemplo 1: cómo eliminar una sola etiqueta de un recurso

En el siguiente ejemplo de `untag-resource`, se elimina una sola etiqueta de un recurso de Amazon Comprehend.

```
aws comprehend untag-resource \
    --resource-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier/
example-classifier/version/1
    --tag-keys Location
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging your resources en la Guía para desarrolladores de Amazon Comprehend.

Ejemplo 2: eliminar varias etiquetas de un recurso

En el siguiente ejemplo de `untag-resource`, se eliminan varias etiquetas de un recurso de Amazon Comprehend.

```
aws comprehend untag-resource \
    --resource-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier/
example-classifier/version/1
    --tag-keys Location Department
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging your resources en la Guía para desarrolladores de Amazon Comprehend.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-endpoint`.

AWS CLI

Ejemplo 1: cómo actualizar las unidades de inferencia de un punto de conexión

En el siguiente ejemplo de `update-endpoint`, se actualiza la información sobre un punto de conexión. En este ejemplo, se aumenta el número de unidades de inferencia.

```
aws comprehend update-endpoint \
    --endpoint-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier-endpoint/example-classifier-endpoint
    --desired-inference-units 2
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración de puntos de conexión de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

Ejemplo 2: cómo actualizar un modelo activo de un punto de conexión

En el siguiente ejemplo de `update-endpoint`, se actualiza la información sobre un punto de conexión. En este ejemplo, se cambia el modelo activo.

```
aws comprehend update-endpoint \
    --endpoint-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier-endpoint/example-classifier-endpoint
    --active-model-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier/example-classifier-new
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración de puntos de conexión de Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte UpdateEndpoint en la Referencia de comandos de la AWS CLI.

update-flywheel

En el siguiente ejemplo de código, se muestra cómo utilizar `update-flywheel`.

AWS CLI

Actualización de una configuración de volante de inercia

En el siguiente ejemplo de `update-flywheel`, se actualiza una configuración de volante de inercia. En este ejemplo, se actualiza el modelo activo del volante de inercia.

```
aws comprehend update-flywheel \
    --flywheel-arn arn:aws:comprehend:us-west-2:111122223333:flywheel/example-flywheel-1 \
    --active-model-arn arn:aws:comprehend:us-west-2:111122223333:document-classifier/example-classifier/version/new-example-classifier-model
```

Salida:

```
{
    "FlywheelProperties": {
        "FlywheelArn": "arn:aws:comprehend:us-west-2:111122223333:flywheel/flywheel-entity",
        "ActiveModelArn": "arn:aws:comprehend:us-west-2:111122223333:document-classifier/example-classifier/version/new-example-classifier-model",
        "DataAccessRoleArn": "arn:aws:iam::111122223333:role/service-role/AmazonComprehendServiceRole-example-role",
        "TaskConfig": {
            "LanguageCode": "en",
            "DocumentClassificationConfig": {
                "Mode": "MULTI_CLASS"
            }
        },
        "DataLakeS3Uri": "s3://amzn-s3-demo-bucket/flywheel-entity/schemaVersion=1/20230616T200543Z/",
        "DataSecurityConfig": {},
        "Status": "ACTIVE",
        "ModelType": "DOCUMENT_CLASSIFIER",
        "CreationTime": "2023-06-16T20:05:43.242000+00:00",
        "LastModifiedTime": "2023-06-19T04:00:43.027000+00:00",
        "LatestFlywheelIteration": "20230619T040032Z"
    }
}
```

Para obtener más información, consulte Flywheel overview en la Guía para desarrolladores de Amazon Comprehend.

- Para obtener detalles sobre la API, consulte UpdateFlywheel en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon Comprehend Medical que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando la AWS Command Line Interface con Amazon Comprehend Medical.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`describe-entities-detection-v2-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-entities-detection-v2-job`.

AWS CLI

Descripción de un trabajo de detección de entidades

En el siguiente ejemplo de `describe-entities-detection-v2-job`, se muestran las propiedades asociadas a un trabajo de detección de entidades asíncrono.

```
aws comprehendmedical describe-entities-detection-v2-job \
    --job-id "ab9887877365fe70299089371c043b96"
```

Salida:

```
{
```

```
    "ComprehendMedicalAsyncJobProperties": {
        "JobId": "ab9887877365fe70299089371c043b96",
        "JobStatus": "COMPLETED",
        "SubmitTime": "2020-03-18T21:20:15.614000+00:00",
        "EndTime": "2020-03-18T21:27:07.350000+00:00",
        "ExpirationTime": "2020-07-16T21:20:15+00:00",
        "InputDataConfig": {
            "S3Bucket": "comp-med-input",
            "S3Key": ""
        },
        "OutputDataConfig": {
            "S3Bucket": "comp-med-output",
            "S3Key": "867139942017-EntitiesDetection-
ab9887877365fe70299089371c043b96/"
        },
        "LanguageCode": "en",
        "DataAccessRoleArn": "arn:aws:iam::867139942017:role/
ComprehendMedicalBatchProcessingRole",
        "ModelVersion": "DetectEntitiesModelV20190930"
    }
}
```

Para obtener más información, consulte la sección sobre Batch APIs en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte DescribeEntitiesDetectionV2Job en la Referencia de comandos de la AWS CLI.

`describe-icd10-cm-inference-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-icd10-cm-inference-job`.

AWS CLI

Descripción de un trabajo de inferencia ICD-10-CM

En el siguiente ejemplo de `describe-icd10-cm-inference-job`, se describen las propiedades del trabajo de inferencia solicitado con el job-id especificado.

```
aws comprehendmedical describe-icd10-cm-inference-job \
    --job-id "5780034166536cdb52ffa3295a1b00a7"
```

Salida:

```
{
    "ComprehendMedicalAsyncJobProperties": {
        "JobId": "5780034166536cdb52ffa3295a1b00a7",
        "JobStatus": "COMPLETED",
        "SubmitTime": "2020-05-18T21:20:15.614000+00:00",
        "EndTime": "2020-05-18T21:27:07.350000+00:00",
        "ExpirationTime": "2020-09-16T21:20:15+00:00",
        "InputDataConfig": {
            "S3Bucket": "comp-med-input",
            "S3Key": "AKIAIOSFODNN7EXAMPLE"
        },
        "OutputDataConfig": {
            "S3Bucket": "comp-med-output",
            "S3Key": "AKIAIOSFODNN7EXAMPLE"
        },
        "LanguageCode": "en",
        "DataAccessRoleArn": "arn:aws:iam::867139942017:role/
ComprehendMedicalBatchProcessingRole",
        "ModelVersion":  "0.1.0"
    }
}
```

Para obtener más información, consulte la sección Ontology linking batch analysis en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte DescribeIcd10CmInferenceJob en la Referencia de comandos de la AWS CLI.

`describe-phi-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-phi-detection-job`.

AWS CLI

Descripción de un trabajo de detección de PHI

En el siguiente ejemplo de `describe-phi-detection-job`, se muestran las propiedades asociadas a un trabajo de detección de información sanitaria protegida (PHI) asíncrono.

```
aws comprehendmedical describe-phi-detection-job \
```

```
    --job-id "4750034166536cdb52ffa3295a1b00a3"
```

Salida:

```
{
    "ComprehendMedicalAsyncJobProperties": {
        "JobId": "4750034166536cdb52ffa3295a1b00a3",
        "JobStatus": "COMPLETED",
        "SubmitTime": "2020-03-19T20:38:37.594000+00:00",
        "EndTime": "2020-03-19T20:45:07.894000+00:00",
        "ExpirationTime": "2020-07-17T20:38:37+00:00",
        "InputDataConfig": {
            "S3Bucket": "comp-med-input",
            "S3Key": ""
        },
        "OutputDataConfig": {
            "S3Bucket": "comp-med-output",
            "S3Key": "867139942017-PHIDetection-4750034166536cdb52ffa3295a1b00a3/"
        },
        "LanguageCode": "en",
        "DataAccessRoleArn": "arn:aws:iam::867139942017:role/
ComprehendMedicalBatchProcessingRole",
        "ModelVersion": "PHIModelV20190903"
    }
}
```

Para obtener más información, consulte la sección sobre Batch APIs en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte DescribePhiDetectionJob en la Referencia de comandos de la AWS CLI.

`describe-rx-norm-inference-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-rx-norm-inference-job`.

AWS CLI

Descripción de un trabajo de inferencia de RxNorm

En el siguiente ejemplo de `describe-rx-norm-inference-job`, se describen las propiedades del trabajo de inferencia solicitado con el job-id especificado.

```
aws comprehendmedical describe-rx-norm-inference-job \
    --job-id "eg8199877365fc70299089371c043b96"
```

Salida:

```
{
    "ComprehendMedicalAsyncJobProperties": {
        "JobId": "g8199877365fc70299089371c043b96",
        "JobStatus": "COMPLETED",
        "SubmitTime": "2020-05-18T21:20:15.614000+00:00",
        "EndTime": "2020-05-18T21:27:07.350000+00:00",
        "ExpirationTime": "2020-09-16T21:20:15+00:00",
        "InputDataConfig": {
            "S3Bucket": "comp-med-input",
            "S3Key": "AKIAIOSFODNN7EXAMPLE"
        },
        "OutputDataConfig": {
            "S3Bucket": "comp-med-output",
            "S3Key": "AKIAIOSFODNN7EXAMPLE"
        },
        "LanguageCode": "en",
        "DataAccessRoleArn": "arn:aws:iam::867139942017:role/
ComprehendMedicalBatchProcessingRole",
        "ModelVersion": "0.0.0"
    }
}
```

Para obtener más información, consulte la sección Ontology linking batch analysis en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte DescribeRxNormInferenceJob en la Referencia de comandos de la AWS CLI.

`describe-snomedct-inference-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-snomedct-inference-job`.

AWS CLI

Descripción de un trabajo de inferencia de SNOMED CT

En el siguiente ejemplo de `describe-snomedct-inference-job`, se describen las propiedades del trabajo de inferencia solicitado con el job-id especificado.

```
aws comprehendmedical describe-snomedct-inference-job \
    --job-id "2630034166536cdb52ffa3295a1b00a7"
```

Salida:

```
{
    "ComprehendMedicalAsyncJobProperties": {
        "JobId": "2630034166536cdb52ffa3295a1b00a7",
        "JobStatus": "COMPLETED",
        "SubmitTime": "2021-12-18T21:20:15.614000+00:00",
        "EndTime": "2021-12-18T21:27:07.350000+00:00",
        "ExpirationTime": "2022-05-16T21:20:15+00:00",
        "InputDataConfig": {
            "S3Bucket": "comp-med-input",
            "S3Key": "AKIAIOSFODNN7EXAMPLE"
        },
        "OutputDataConfig": {
            "S3Bucket": "comp-med-output",
            "S3Key": "AKIAIOSFODNN7EXAMPLE"
        },
        "LanguageCode": "en",
        "DataAccessRoleArn": "arn:aws:iam::867139942017:role/
ComprehendMedicalBatchProcessingRole",
        "ModelVersion":  "0.1.0"
    }
}
```

Para obtener más información, consulte la sección Ontology linking batch analysis en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte DescribeSnomedctInferenceJob en la Referencia de comandos de la AWS CLI.

`detect-entities-v2`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-entities-v2`.

AWS CLI

Ejemplo 1: detección de entidades directamente desde el texto

En el siguiente ejemplo de `detect-entities-v2`, se muestran las entidades detectadas y se etiquetas según el tipo directamente a partir del texto introducido.

```
aws comprehendmedical detect-entities-v2 \
    --text "Sleeping trouble on present dosage of Clonidine. Severe rash on face and
 leg, slightly itchy."
```

Salida:

```
{
    "Id": 0,
    "BeginOffset": 38,
    "EndOffset": 47,
    "Score": 0.9942955374717712,
    "Text": "Clonidine",
    "Category": "MEDICATION",
    "Type": "GENERIC_NAME",
    "Traits": []
}
```

Para obtener más información, consulte Detect Entities Version 2 en la Guía para desarrolladores de Amazon Comprehend Medical.

Ejemplo 2: detección de entidades en una ruta de archivo

En el siguiente ejemplo de `detect-entities-v2`, se muestran las entidades detectadas y se etiquetan según el tipo directamente a partir de una ruta de archivo.

```
aws comprehendmedical detect-entities-v2 \
    --text file://medical_entities.txt
```

Contenido de `medical_entities.txt`:

```
{
    "Sleeping trouble on present dosage of Clonidine. Severe rash on face and leg,
 slightly itchy."
}
```

Salida:

```
{
    "Id": 0,
    "BeginOffset": 38,
    "EndOffset": 47,
    "Score": 0.9942955374717712,
    "Text": "Clonidine",
    "Category": "MEDICATION",
    "Type": "GENERIC_NAME",
    "Traits": []
}
```

Para obtener más información, consulte Detect Entities Version 2 en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte DetectEntitiesV2 en la Referencia de comandos de la AWS CLI.

`detect-phi`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-phi`.

AWS CLI

Ejemplo 1: detección de información sanitaria protegida (PHI) directamente a partir del texto

En el siguiente ejemplo de `detect-phi`, se muestran las entidades de información sanitaria protegida (PHI) detectadas directamente en el texto introducido.

```
aws comprehendmedical detect-phi \
    --text "Patient Carlos Salazar presented with rash on his upper extremities and
 dry cough. He lives at 100 Main Street, Anytown, USA where he works from his home
 as a carpenter."
```

Salida:

```
{
    "Entities": [
        {
            "Id": 0,
            "BeginOffset": 8,
```

```
            "EndOffset": 21,
            "Score": 0.9914507269859314,
            "Text": "Carlos Salazar",
            "Category": "PROTECTED_HEALTH_INFORMATION",
            "Type": "NAME",
            "Traits": []
        },
        {
            "Id": 1,
            "BeginOffset": 94,
            "EndOffset": 109,
            "Score": 0.871849775314331,
            "Text": "100 Main Street, Anytown, USA",
            "Category": "PROTECTED_HEALTH_INFORMATION",
            "Type": "ADDRESS",
            "Traits": []
        },
        {
            "Id": 2,
            "BeginOffset": 145,
            "EndOffset": 154,
            "Score": 0.8302185535430908,
            "Text": "carpenter",
            "Category": "PROTECTED_HEALTH_INFORMATION",
            "Type": "PROFESSION",
            "Traits": []
        }
    ],
    "ModelVersion": "0.0.0"
}
```

Para obtener más información, consulte Detect PHI en la Guía para desarrolladores de Amazon Comprehend Medical.

Ejemplo 2: detección de información sanitaria protegida (PHI) directamente a partir una ruta de archivo

En el siguiente ejemplo de `detect-phi`, se muestran las entidades de información sanitaria protegida (PHI) detectadas en una ruta de archivo.

```
aws comprehendmedical detect-phi \
    --text file://phi.txt
```

Contenido de `phi.txt`:

```
"Patient Carlos Salazar presented with a rash on his upper extremities and a dry
 cough. He lives at 100 Main Street, Anytown, USA, where he works from his home as a
 carpenter."
```

Salida:

```
{
    "Entities": [
        {
            "Id": 0,
            "BeginOffset": 8,
            "EndOffset": 21,
            "Score": 0.9914507269859314,
            "Text": "Carlos Salazar",
            "Category": "PROTECTED_HEALTH_INFORMATION",
            "Type": "NAME",
            "Traits": []
        },
        {
            "Id": 1,
            "BeginOffset": 94,
            "EndOffset": 109,
            "Score": 0.871849775314331,
            "Text": "100 Main Street, Anytown, USA",
            "Category": "PROTECTED_HEALTH_INFORMATION",
            "Type": "ADDRESS",
            "Traits": []
        },
        {
            "Id": 2,
            "BeginOffset": 145,
            "EndOffset": 154,
            "Score": 0.8302185535430908,
            "Text": "carpenter",
            "Category": "PROTECTED_HEALTH_INFORMATION",
            "Type": "PROFESSION",
            "Traits": []
        }
    ],
    "ModelVersion": "0.0.0"
}
```

Para obtener más información, consulte Detect PHI en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte DetectPhi en la Referencia de comandos de la AWS CLI.

`infer-icd10-cm`

En el siguiente ejemplo de código, se muestra cómo utilizar `infer-icd10-cm`.

AWS CLI

Ejemplo 1: detección de entidades relacionadas con afecciones médicas y establecer un enlace a la ontología ICD-10-CM directamente desde el texto

En el siguiente ejemplo de `infer-icd10-cm`, se etiquetan las entidades de afecciones médicas detectadas y se vinculan con los códigos de la edición de 2019 de la CLASIFICACIÓN INTERNACIONAL DE ENFERMEDADES - MODIFICACIÓN CLÍNICA (ICD-10-CM).

```
aws comprehendmedical infer-icd10-cm \
    --text "The patient complains of abdominal pain, has a long-standing history of
 diabetes treated with Micronase daily."
```

Salida:

```
{
    "Entities": [
        {
            "Id": 0,
            "Text": "abdominal pain",
            "Category": "MEDICAL_CONDITION",
            "Type": "DX_NAME",
            "Score": 0.9475538730621338,
            "BeginOffset": 28,
            "EndOffset": 42,
            "Attributes": [],
            "Traits": [
                {
                    "Name": "SYMPTOM",
                    "Score": 0.6724207401275635
                }
            ],
```

```
            "ICD10CMConcepts": [
                {
                    "Description": "Unspecified abdominal pain",
                    "Code": "R10.9",
                    "Score": 0.6904221177101135
                },
                {
                    "Description": "Epigastric pain",
                    "Code": "R10.13",
                    "Score": 0.1364113688468933
                },
                {
                    "Description": "Generalized abdominal pain",
                    "Code": "R10.84",
                    "Score": 0.12508003413677216
                },
                {
                    "Description": "Left lower quadrant pain",
                    "Code": "R10.32",
                    "Score": 0.10063883662223816
                },
                {
                    "Description": "Lower abdominal pain, unspecified",
                    "Code": "R10.30",
                    "Score": 0.09933677315711975
                }
            ]
        },
        {
            "Id": 1,
            "Text": "diabetes",
            "Category": "MEDICAL_CONDITION",
            "Type": "DX_NAME",
            "Score": 0.9899052977561951,
            "BeginOffset": 75,
            "EndOffset": 83,
            "Attributes": [],
            "Traits": [
                {
                    "Name": "DIAGNOSIS",
                    "Score": 0.9258432388305664
                }
            ],
            "ICD10CMConcepts": [
```

```
                {
                    "Description": "Type 2 diabetes mellitus without complications",
                    "Code": "E11.9",
                    "Score": 0.7158446311950684
                },
                {
                    "Description": "Family history of diabetes mellitus",
                    "Code": "Z83.3",
                    "Score": 0.5704703330993652
                },
                {
                    "Description": "Family history of other endocrine, nutritional
 and metabolic diseases",
                    "Code": "Z83.49",
                    "Score": 0.19856023788452148
                },
                {
                    "Description": "Type 1 diabetes mellitus with ketoacidosis
 without coma",
                    "Code": "E10.10",
                    "Score": 0.13285516202449799
                },
                {
                    "Description": "Type 2 diabetes mellitus with hyperglycemia",
                    "Code": "E11.65",
                    "Score": 0.0993388369679451
                }
            ]
        }
    ],
    "ModelVersion": "0.1.0"
}
```

Para obtener más información, consulte la sección sobre Infer ICD10-CM en la Guía para desarrolladores de Amazon Comprehend Medical.

Ejemplo 2: detección de entidades relacionadas con afecciones médicas y establecer un enlace a la ontología ICD-10-CM desde una ruta de archivo

En el siguiente ejemplo de `infer-icd-10-cm`, se etiquetan las entidades de afecciones médicas detectadas y se vinculan con los códigos de la edición de 2019 de la CLASIFICACIÓN INTERNACIONAL DE ENFERMEDADES - MODIFICACIÓN CLÍNICA (ICD-10-CM).

```
aws comprehendmedical infer-icd10-cm \
    --text file://icd10cm.txt
```

Contenido de `icd10cm.txt`:

```
{
    "The patient complains of abdominal pain, has a long-standing history of
 diabetes treated with Micronase daily."
}
```

Salida:

```
{
    "Entities": [
        {
            "Id": 0,
            "Text": "abdominal pain",
            "Category": "MEDICAL_CONDITION",
            "Type": "DX_NAME",
            "Score": 0.9475538730621338,
            "BeginOffset": 28,
            "EndOffset": 42,
            "Attributes": [],
            "Traits": [
                {
                    "Name": "SYMPTOM",
                    "Score": 0.6724207401275635
                }
            ],
            "ICD10CMConcepts": [
                {
                    "Description": "Unspecified abdominal pain",
                    "Code": "R10.9",
                    "Score": 0.6904221177101135
                },
                {
                    "Description": "Epigastric pain",
                    "Code": "R10.13",
                    "Score": 0.1364113688468933
                },
                {
                    "Description": "Generalized abdominal pain",
```

```
                    "Code": "R10.84",
                    "Score": 0.12508003413677216
                },
                {
                    "Description": "Left lower quadrant pain",
                    "Code": "R10.32",
                    "Score": 0.10063883662223816
                },
                {
                    "Description": "Lower abdominal pain, unspecified",
                    "Code": "R10.30",
                    "Score": 0.09933677315711975
                }
            ]
        },
        {
            "Id": 1,
            "Text": "diabetes",
            "Category": "MEDICAL_CONDITION",
            "Type": "DX_NAME",
            "Score": 0.9899052977561951,
            "BeginOffset": 75,
            "EndOffset": 83,
            "Attributes": [],
            "Traits": [
                {
                    "Name": "DIAGNOSIS",
                    "Score": 0.9258432388305664
                }
            ],
            "ICD10CMConcepts": [
                {
                    "Description": "Type 2 diabetes mellitus without complications",
                    "Code": "E11.9",
                    "Score": 0.7158446311950684
                },
                {
                    "Description": "Family history of diabetes mellitus",
                    "Code": "Z83.3",
                    "Score": 0.5704703330993652
                },
                {
                    "Description": "Family history of other endocrine, nutritional
and metabolic diseases",
```

```
                    "Code": "Z83.49",
                    "Score": 0.19856023788452148
                },
                {
                    "Description": "Type 1 diabetes mellitus with ketoacidosis
 without coma",
                    "Code": "E10.10",
                    "Score": 0.13285516202449799
                },
                {
                    "Description": "Type 2 diabetes mellitus with hyperglycemia",
                    "Code": "E11.65",
                    "Score": 0.0993388369679451
                }
            ]
        }
    ],
    "ModelVersion": "0.1.0"
}
```

Para obtener más información, consulte la sección sobre Infer-ICD10-CM en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte InferIcd10Cm en la Referencia de comandos de la AWS CLI.

`infer-rx-norm`

En el siguiente ejemplo de código, se muestra cómo utilizar `infer-rx-norm`.

AWS CLI

Ejemplo 1: detección de entidades de medicación y vincularlas a RxNorm directamente desde el texto

En el siguiente ejemplo de `infer-rx-norm`, se muestran y etiquetan las entidades de medicación detectadas y las vincula a los identificadores de conceptos (RxCUI) de la base de datos RxNorm de la Biblioteca Nacional de Medicina.

```
aws comprehendmedical infer-rx-norm \
    --text "Patient reports taking Levothyroxine 125 micrograms p.o. once daily, but
 denies taking Synthroid."
```

Salida:


```
{
    "Entities": [
        {
            "Id": 0,
            "Text": "Levothyroxine",
            "Category": "MEDICATION",
            "Type": "GENERIC_NAME",
            "Score": 0.9996285438537598,
            "BeginOffset": 23,
            "EndOffset": 36,
            "Attributes": [
                {
                    "Type": "DOSAGE",
                    "Score": 0.9892290830612183,
                    "RelationshipScore": 0.9997978806495667,
                    "Id": 1,
                    "BeginOffset": 37,
                    "EndOffset": 51,
                    "Text": "125 micrograms",
                    "Traits": []
                },
                {
                    "Type": "ROUTE_OR_MODE",
                    "Score": 0.9988924860954285,
                    "RelationshipScore": 0.998291552066803,
                    "Id": 2,
                    "BeginOffset": 52,
                    "EndOffset": 56,
                    "Text": "p.o.",
                    "Traits": []
                },
                {
                    "Type": "FREQUENCY",
                    "Score": 0.9953463673591614,
                    "RelationshipScore": 0.9999889135360718,
                    "Id": 3,
                    "BeginOffset": 57,
                    "EndOffset": 67,
                    "Text": "once daily",
                    "Traits": []
                }
            ],
```

```
            "Traits": [],
            "RxNormConcepts": [
                {
                    "Description": "Levothyroxine Sodium 0.125 MG Oral Tablet",
                    "Code": "966224",
                    "Score": 0.9912070631980896
                },
                {
                    "Description": "Levothyroxine Sodium 0.125 MG Oral Capsule",
                    "Code": "966405",
                    "Score": 0.8698278665542603
                },
                {
                    "Description": "Levothyroxine Sodium 0.125 MG Oral Tablet
[Synthroid]",
                    "Code": "966191",
                    "Score": 0.7448257803916931
                },
                {
                    "Description": "levothyroxine",
                    "Code": "10582",
                    "Score": 0.7050482630729675
                },
                {
                    "Description": "Levothyroxine Sodium 0.125 MG Oral Tablet
[Levoxyl]",
                    "Code": "966190",
                    "Score": 0.6921631693840027
                }
            ]
        },
        {
            "Id": 4,
            "Text": "Synthroid",
            "Category": "MEDICATION",
            "Type": "BRAND_NAME",
            "Score": 0.9946461319923401,
            "BeginOffset": 86,
            "EndOffset": 95,
            "Attributes": [],
            "Traits": [
                {
                    "Name": "NEGATION",
                    "Score": 0.5167351961135864
```

```
                }
            ],
            "RxNormConcepts": [
                {
                    "Description": "Synthroid",
                    "Code": "224920",
                    "Score": 0.9462039470672607
                },
                {
                    "Description": "Levothyroxine Sodium 0.088 MG Oral Tablet
 [Synthroid]",
                    "Code": "966282",
                    "Score": 0.8309829235076904
                },
                {
                    "Description": "Levothyroxine Sodium 0.125 MG Oral Tablet
 [Synthroid]",
                    "Code": "966191",
                    "Score": 0.4945160448551178
                },
                {
                    "Description": "Levothyroxine Sodium 0.05 MG Oral Tablet
 [Synthroid]",
                    "Code": "966247",
                    "Score": 0.3674522042274475
                },
                {
                    "Description": "Levothyroxine Sodium 0.025 MG Oral Tablet
 [Synthroid]",
                    "Code": "966158",
                    "Score": 0.2588822841644287
                }
            ]
        }
    ],
    "ModelVersion": "0.0.0"
}
```

Para obtener más información, consulte la sección sobre Infer RxNorm en la Guía para desarrolladores de Amazon Comprehend Medical.

Ejemplo 2: detección de entidades de medicación y vincularlas a RxNorm directamente desde una ruta de archivo.

En el siguiente ejemplo de `infer-rx-norm`, se muestran y etiquetan las entidades de medicación detectadas y las vincula a los identificadores de conceptos (RxCUI) de la base de datos RxNorm de la Biblioteca Nacional de Medicina.

```
aws comprehendmedical infer-rx-norm \
    --text file://rxnorm.txt
```

Contenido de `rxnorm.txt`:

```
{
    "Patient reports taking Levothyroxine 125 micrograms p.o. once daily, but denies
 taking Synthroid."
}
```

Salida:

```
{
    "Entities": [
        {
            "Id": 0,
            "Text": "Levothyroxine",
            "Category": "MEDICATION",
            "Type": "GENERIC_NAME",
            "Score": 0.9996285438537598,
            "BeginOffset": 23,
            "EndOffset": 36,
            "Attributes": [
                {
                    "Type": "DOSAGE",
                    "Score": 0.9892290830612183,
                    "RelationshipScore": 0.9997978806495667,
                    "Id": 1,
                    "BeginOffset": 37,
                    "EndOffset": 51,
                    "Text": "125 micrograms",
                    "Traits": []
                },
                {
                    "Type": "ROUTE_OR_MODE",
                    "Score": 0.9988924860954285,
                    "RelationshipScore": 0.998291552066803,
                    "Id": 2,
```

```
                    "BeginOffset": 52,
                    "EndOffset": 56,
                    "Text": "p.o.",
                    "Traits": []
                },
                {
                    "Type": "FREQUENCY",
                    "Score": 0.9953463673591614,
                    "RelationshipScore": 0.9999889135360718,
                    "Id": 3,
                    "BeginOffset": 57,
                    "EndOffset": 67,
                    "Text": "once daily",
                    "Traits": []
                }
            ],
            "Traits": [],
            "RxNormConcepts": [
                {
                    "Description": "Levothyroxine Sodium 0.125 MG Oral Tablet",
                    "Code": "966224",
                    "Score": 0.9912070631980896
                },
                {
                    "Description": "Levothyroxine Sodium 0.125 MG Oral Capsule",
                    "Code": "966405",
                    "Score": 0.8698278665542603
                },
                {
                    "Description": "Levothyroxine Sodium 0.125 MG Oral Tablet
[Synthroid]",
                    "Code": "966191",
                    "Score": 0.7448257803916931
                },
                {
                    "Description": "levothyroxine",
                    "Code": "10582",
                    "Score": 0.7050482630729675
                },
                {
                    "Description": "Levothyroxine Sodium 0.125 MG Oral Tablet
[Levoxyl]",
                    "Code": "966190",
                    "Score": 0.6921631693840027
```

```
                }
            ]
        },
        {
            "Id": 4,
            "Text": "Synthroid",
            "Category": "MEDICATION",
            "Type": "BRAND_NAME",
            "Score": 0.9946461319923401,
            "BeginOffset": 86,
            "EndOffset": 95,
            "Attributes": [],
            "Traits": [
                {
                    "Name": "NEGATION",
                    "Score": 0.5167351961135864
                }
            ],
            "RxNormConcepts": [
                {
                    "Description": "Synthroid",
                    "Code": "224920",
                    "Score": 0.9462039470672607
                },
                {
                    "Description": "Levothyroxine Sodium 0.088 MG Oral Tablet
[Synthroid]",
                    "Code": "966282",
                    "Score": 0.8309829235076904
                },
                {
                    "Description": "Levothyroxine Sodium 0.125 MG Oral Tablet
[Synthroid]",
                    "Code": "966191",
                    "Score": 0.4945160448551178
                },
                {
                    "Description": "Levothyroxine Sodium 0.05 MG Oral Tablet
[Synthroid]",
                    "Code": "966247",
                    "Score": 0.3674522042274475
                },
                {
```

```
                    "Description": "Levothyroxine Sodium 0.025 MG Oral Tablet
 [Synthroid]",
                    "Code": "966158",
                    "Score": 0.2588822841644287
                }
            ]
        }
    ],
    "ModelVersion": "0.0.0"
}
```

Para obtener más información, consulte la sección sobre Infer RxNorm en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte InferRxNorm en la Referencia de comandos de la AWS CLI.

`infer-snomedct`

En el siguiente ejemplo de código, se muestra cómo utilizar `infer-snomedct`.

AWS CLI

Ejemplo: detección de entidades de medicación y vincularlas a la ontología de SNOMED CT directamente desde el texto

En el siguiente ejemplo de `infer-snomedct`, se muestra cómo detectar entidades médicas y vincularlas con conceptos de la versión de marzo de 2021-03 de la Nomenclatura Sistematizada de Medicina, Términos Clínicos (SNOMED CT).

```
aws comprehendmedical infer-snomedct \
    --text "The patient complains of abdominal pain, has a long-standing history of
 diabetes treated with Micronase daily."
```

Salida:

```
{
    "Entities": [
        {
            "Id": 3,
            "BeginOffset": 26,
            "EndOffset": 40,
```

```
            "Score": 0.9598260521888733,
            "Text": "abdominal pain",
            "Category": "MEDICAL_CONDITION",
            "Type": "DX_NAME",
            "Traits": [
                {
                    "Name": "SYMPTOM",
                    "Score": 0.6819021701812744
                }
            ]
        },
        {
            "Id": 4,
            "BeginOffset": 73,
            "EndOffset": 81,
            "Score": 0.9905840158462524,
            "Text": "diabetes",
            "Category": "MEDICAL_CONDITION",
            "Type": "DX_NAME",
            "Traits": [
                {
                    "Name": "DIAGNOSIS",
                    "Score": 0.9255214333534241
                }
            ]
        },
        {
            "Id": 1,
            "BeginOffset": 95,
            "EndOffset": 104,
            "Score": 0.6371926665306091,
            "Text": "Micronase",
            "Category": "MEDICATION",
            "Type": "BRAND_NAME",
            "Traits": [],
            "Attributes": [
                {
                    "Type": "FREQUENCY",
                    "Score": 0.9761165380477905,
                    "RelationshipScore": 0.9984188079833984,
                    "RelationshipType": "FREQUENCY",
                    "Id": 2,
                    "BeginOffset": 105,
                    "EndOffset": 110,
```

```
                    "Text": "daily",
                    "Category": "MEDICATION",
                    "Traits": []
                }
            ]
        }
    ],
    "UnmappedAttributes": [],
    "ModelVersion": "1.0.0"
}
```

Para obtener más información, consulte la sección sobre InferSNOMEDCT en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte InferSnomedct en la Referencia de comandos de la AWS CLI.

`list-entities-detection-v2-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-entities-detection-v2-jobs`.

AWS CLI

Para enumerar los trabajos de detección de entidades

En el siguiente ejemplo de `list-entities-detection-v2-jobs`, se enumeran los trabajos de detección de entidades asíncronas actuales.

```
aws comprehendmedical list-entities-detection-v2-jobs
```

Salida:

```
{
    "ComprehendMedicalAsyncJobPropertiesList": [
        {
            "JobId": "ab9887877365fe70299089371c043b96",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2020-03-19T20:38:37.594000+00:00",
            "EndTime": "2020-03-19T20:45:07.894000+00:00",
            "ExpirationTime": "2020-07-17T20:38:37+00:00",
            "InputDataConfig": {
```

```
                "S3Bucket": "comp-med-input",
                "S3Key": ""
            },
            "OutputDataConfig": {
                "S3Bucket": "comp-med-output",
                "S3Key": "867139942017-EntitiesDetection-
ab9887877365fe70299089371c043b96/"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::867139942017:role/
ComprehendMedicalBatchProcessingRole",
            "ModelVersion": "DetectEntitiesModelV20190930"
        }
    ]
}
```

Para obtener más información, consulte la sección sobre Batch APIs en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte ListEntitiesDetectionV2Jobs en la Referencia de comandos de la AWS CLI.

`list-icd10-cm-inference-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-icd10-cm-inference-jobs`.

AWS CLI

Para enumerar todos los trabajos de inferencia ICD-10-CM actuales

El siguiente ejemplo muestra cómo la `list-icd10-cm-inference-jobs` operación devuelve una lista de los trabajos de inferencia por lotes asíncronos actuales del ICD-10-CM.

```
aws comprehendmedical list-icd10-cm-inference-jobs
```

Salida:

```
{
    "ComprehendMedicalAsyncJobPropertiesList": [
        {
            "JobId": "5780034166536cdb52ffa3295a1b00a7",
            "JobStatus": "COMPLETED",
```

```
            "SubmitTime": "2020-05-19T20:38:37.594000+00:00",
            "EndTime": "2020-05-19T20:45:07.894000+00:00",
            "ExpirationTime": "2020-09-17T20:38:37+00:00",
            "InputDataConfig": {
                "S3Bucket": "comp-med-input",
                "S3Key": "AKIAIOSFODNN7EXAMPLE"
            },
            "OutputDataConfig": {
                "S3Bucket": "comp-med-output",
                "S3Key": "AKIAIOSFODNN7EXAMPLE"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::867139942017:role/
ComprehendMedicalBatchProcessingRole",
            "ModelVersion":  "0.1.0"
        }
    ]
}
```

Para obtener más información, consulte la sección Ontology linking batch analysis en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte ListIcd10CmInferenceJobs en la Referencia de comandos de la AWS CLI.

`list-phi-detection-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-phi-detection-jobs`.

AWS CLI

Para enumerar los trabajos de detección de información sanitaria protegida (PHI)

En el siguiente ejemplo de `list-phi-detection-jobs`, se enumeran los trabajos de detección de información sanitaria protegida (PHI) actuales.

```
aws comprehendmedical list-phi-detection-jobs
```

Salida:

```
{
    "ComprehendMedicalAsyncJobPropertiesList": [
```

```
        {
            "JobId": "4750034166536cdb52ffa3295a1b00a3",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2020-03-19T20:38:37.594000+00:00",
            "EndTime": "2020-03-19T20:45:07.894000+00:00",
            "ExpirationTime": "2020-07-17T20:38:37+00:00",
            "InputDataConfig": {
                "S3Bucket": "comp-med-input",
                "S3Key": ""
            },
            "OutputDataConfig": {
                "S3Bucket": "comp-med-output",
                "S3Key": "867139942017-
PHIDetection-4750034166536cdb52ffa3295a1b00a3/"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::867139942017:role/
ComprehendMedicalBatchProcessingRole",
            "ModelVersion": "PHIModelV20190903"
        }
    ]
}
```

Para obtener más información, consulte la sección sobre Batch APIs en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte ListPhiDetectionJobs en la Referencia de comandos de la AWS CLI.

`list-rx-norm-inference-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-rx-norm-inference-jobs`.

AWS CLI

Para enumerar todos los trabajos de inferencia RxNorm actuales

En el siguiente ejemplo, se muestra cómo la operación `list-rx-norm-inference-jobs` devuelve una lista de los trabajos de inferencia por lotes asíncronos actuales de RxNorm.

```
aws comprehendmedical list-rx-norm-inference-jobs
```

Salida:

```
{
    "ComprehendMedicalAsyncJobPropertiesList": [
        {
            "JobId": "4980034166536cfb52gga3295a1b00a3",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2020-05-19T20:38:37.594000+00:00",
            "EndTime": "2020-05-19T20:45:07.894000+00:00",
            "ExpirationTime": "2020-09-17T20:38:37+00:00",
            "InputDataConfig": {
                "S3Bucket": "comp-med-input",
                "S3Key": "AKIAIOSFODNN7EXAMPLE"
            },
            "OutputDataConfig": {
                "S3Bucket": "comp-med-output",
                "S3Key": "AKIAIOSFODNN7EXAMPLE"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::867139942017:role/
ComprehendMedicalBatchProcessingRole",
            "ModelVersion": "0.0.0"
        }
    ]
}
```

Para obtener más información, consulte la sección Ontology linking batch analysis en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte ListRxNormInferenceJobs en la Referencia de comandos de la AWS CLI.

`list-snomedct-inference-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-snomedct-inference-jobs`.

AWS CLI

Para enumerar todos los trabajos de inferencia de SNOMED CT

En el siguiente ejemplo, se muestra cómo la operación `list-snomedct-inference-jobs` devuelve una lista de los trabajos de inferencia por lotes asíncronos actuales de SNOMED CT.

```
aws comprehendmedical list-snomedct-inference-jobs
```

Salida:

```
{
    "ComprehendMedicalAsyncJobPropertiesList": [
        {
            "JobId": "5780034166536cdb52ffa3295a1b00a7",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2020-05-19T20:38:37.594000+00:00",
            "EndTime": "2020-05-19T20:45:07.894000+00:00",
            "ExpirationTime": "2020-09-17T20:38:37+00:00",
            "InputDataConfig": {
                "S3Bucket": "comp-med-input",
                "S3Key": "AKIAIOSFODNN7EXAMPLE"
            },
            "OutputDataConfig": {
                "S3Bucket": "comp-med-output",
                "S3Key": "AKIAIOSFODNN7EXAMPLE"
            },
            "LanguageCode": "en",
            "DataAccessRoleArn": "arn:aws:iam::867139942017:role/
ComprehendMedicalBatchProcessingRole",
            "ModelVersion":  "0.1.0"
        }
    ]
}
```

Para obtener más información, consulte la sección Ontology linking batch analysis en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte ListSnomedctInferenceJobs en la Referencia de comandos de la AWS CLI.

`start-entities-detection-v2-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-entities-detection-v2-job`.

AWS CLI

Inicio de un trabajo de detección de entidades

En el siguiente ejemplo de `start-entities-detection-v2-job`, se inicia un trabajo de detección de entidades asíncrono.

```
aws comprehendmedical start-entities-detection-v2-job \
    --input-data-config "S3Bucket=comp-med-input" \
    --output-data-config "S3Bucket=comp-med-output" \
    --data-access-role-arn arn:aws:iam::867139942017:role/
ComprehendMedicalBatchProcessingRole \
    --language-code en
```

Salida:

```
{
    "JobId": "ab9887877365fe70299089371c043b96"
}
```

Para obtener más información, consulte la sección sobre Batch APIs en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte StartEntitiesDetectionV2Job en la Referencia de comandos de la AWS CLI.

`start-icd10-cm-inference-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-icd10-cm-inference-job`.

AWS CLI

Para iniciar un trabajo de inferencia de ICD-10-CM

En el siguiente ejemplo de `start-icd10-cm-inference-job`, se inicia un trabajo de análisis por lotes de inferencia de ICD-10-CM.

```
aws comprehendmedical start-icd10-cm-inference-job \
    --input-data-config "S3Bucket=comp-med-input" \
    --output-data-config "S3Bucket=comp-med-output" \
    --data-access-role-arn arn:aws:iam::867139942017:role/
ComprehendMedicalBatchProcessingRole \
    --language-code en
```

Salida:

```
{
    "JobId": "ef7289877365fc70299089371c043b96"
```

```
}
```

Para obtener más información, consulte la sección Ontology linking batch analysis en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte StartIcd10CmInferenceJob en la Referencia de comandos de la AWS CLI.

`start-phi-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-phi-detection-job`.

AWS CLI

Inicio de un trabajo de detección de PHI

En el siguiente ejemplo de `start-phi-detection-job`, se inicia un trabajo de detección de entidades de PHI asíncrono.

```
aws comprehendmedical start-phi-detection-job \
    --input-data-config "S3Bucket=comp-med-input" \
    --output-data-config "S3Bucket=comp-med-output" \
    --data-access-role-arn arn:aws:iam::867139942017:role/
ComprehendMedicalBatchProcessingRole \
    --language-code en
```

Salida:

```
{
    "JobId": "ab9887877365fe70299089371c043b96"
}
```

Para obtener más información, consulte la sección sobre Batch APIs en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte StartPhiDetectionJob en la Referencia de comandos de la AWS CLI.

`start-rx-norm-inference-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-rx-norm-inference-job`.

AWS CLI

Inicio de un trabajo de inferencia de RxNorm

En el siguiente ejemplo de `start-rx-norm-inference-job`, se inicia un trabajo de análisis por lotes de inferencia de RxNorm.

```
aws comprehendmedical start-rx-norm-inference-job \
    --input-data-config "S3Bucket=comp-med-input" \
    --output-data-config "S3Bucket=comp-med-output" \
    --data-access-role-arn arn:aws:iam::867139942017:role/
ComprehendMedicalBatchProcessingRole \
    --language-code en
```

Salida:

```
{
    "JobId": "eg8199877365fc70299089371c043b96"
}
```

Para obtener más información, consulte la sección Ontology linking batch analysis en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte StartRxNormInferenceJob en la Referencia de comandos de la AWS CLI.

`start-snomedct-inference-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-snomedct-inference-job`.

AWS CLI

Inicio de un trabajo de inferencia de SNOMED CT

En el siguiente ejemplo de `start-snomedct-inference-job`, se inicia un trabajo de análisis por lotes de inferencia de SNOMED CT.

```
aws comprehendmedical start-snomedct-inference-job \
    --input-data-config "S3Bucket=comp-med-input" \
    --output-data-config "S3Bucket=comp-med-output" \
```

```
    --data-access-role-arn arn:aws:iam::867139942017:role/
ComprehendMedicalBatchProcessingRole \
    --language-code en
```

Salida:

```
{
    "JobId": "dg7289877365fc70299089371c043b96"
}
```

Para obtener más información, consulte la sección Ontology linking batch analysis en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte StartSnomedctInferenceJob en la Referencia de comandos de la AWS CLI.

`stop-entities-detection-v2-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-entities-detection-v2-job`.

AWS CLI

Detención de un trabajo de detección de entidades

En el siguiente ejemplo de `stop-entities-detection-v2-job`, se detiene un trabajo de detección de entidades asíncrono.

```
aws comprehendmedical stop-entities-detection-v2-job \
    --job-id "ab9887877365fe70299089371c043b96"
```

Salida:

```
{
    "JobId": "ab9887877365fe70299089371c043b96"
}
```

Para obtener más información, consulte la sección sobre Batch APIs en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte StopEntitiesDetectionV2Job en la Referencia de comandos de la AWS CLI.

`stop-icd10-cm-inference-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-icd10-cm-inference-job`.

AWS CLI

Para detectar un trabajo de inferencia de ICD-10-CM

En el siguiente ejemplo de `stop-icd10-cm-inference-job`, se detiene un trabajo de análisis por lotes de inferencia de ICD-10-CM.

```
aws comprehendmedical stop-icd10-cm-inference-job \
    --job-id "4750034166536cdb52ffa3295a1b00a3"
```

Salida:

```
{
    "JobId": "ef7289877365fc70299089371c043b96",
}
```

Para obtener más información, consulte la sección Ontology linking batch analysis en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte StopIcd10CmInferenceJob en la Referencia de comandos de la AWS CLI.

`stop-phi-detection-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-phi-detection-job`.

AWS CLI

Detención de un trabajo de detección de información sanitaria protegida (PHI)

En el siguiente ejemplo de `stop-phi-detection-job`, se detiene un trabajo de detección de información sanitaria protegida (PHI) asíncrono.

```
aws comprehendmedical stop-phi-detection-job \
    --job-id "4750034166536cdb52ffa3295a1b00a3"
```

Salida:

```
{
    "JobId": "ab9887877365fe70299089371c043b96"
}
```

Para obtener más información, consulte la sección sobre Batch APIs en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte StopPhiDetectionJob en la Referencia de comandos de la AWS CLI.

`stop-rx-norm-inference-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-rx-norm-inference-job`.

AWS CLI

Detención de un trabajo de inferencia de RxNorm

En el siguiente ejemplo de `stop-rx-norm-inference-job`, se detiene un trabajo de análisis por lotes de inferencia de ICD-10-CM.

```
aws comprehendmedical stop-rx-norm-inference-job \
    --job-id "eg8199877365fc70299089371c043b96"
```

Salida:

```
{
    "JobId": "eg8199877365fc70299089371c043b96",
}
```

Para obtener más información, consulte la sección Ontology linking batch analysis en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte StopRxNormInferenceJob en la Referencia de comandos de la AWS CLI.

`stop-snomedct-inference-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-snomedct-inference-job`.

AWS CLI

Detención de un trabajo de inferencia de SNOMED CT

En el siguiente ejemplo de `stop-snomedct-inference-job`, se detiene un trabajo de análisis por lotes de inferencia de SNOMED CT.

```
aws comprehendmedical stop-snomedct-inference-job \
    --job-id "8750034166436cdb52ffa3295a1b00a1"
```

Salida:

```
{
    "JobId": "8750034166436cdb52ffa3295a1b00a1",
}
```

Para obtener más información, consulte la sección Ontology linking batch analysis en la Guía para desarrolladores de Amazon Comprehend Medical.

- Para obtener detalles sobre la API, consulte StopSnomedctInferenceJob en la Referencia de comandos de la AWS CLI.

AWS Config Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS Config.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`delete-config-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-config-rule`.

AWS CLI

Eliminación de una regla de configuración de AWS

El siguiente comando elimina una regla de configuración de AWS denominada `MyConfigRule`:

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- Para obtener información sobre la API, consulte DeleteConfigRule en la Referencia de comandos de la AWS CLI.

`delete-delivery-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-delivery-channel`.

AWS CLI

Eliminación de un canal de entrega

El siguiente comando elimina el canal de entrega predeterminado:

```
aws configservice delete-delivery-channel --delivery-channel-name default
```

- Para obtener detalles sobre la API, consulte DeleteDeliveryChannel en la Referencia de comandos de la AWS CLI.

`delete-evaluation-results`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-evaluation-results`.

AWS CLI

Eliminación manual de los resultados de la evaluación

El comando siguiente elimina los resultados de evaluación actuales de la regla de AWS administrada s3-bucket-versioning-enabled:

```
aws configservice delete-evaluation-results --config-rule-name s3-bucket-versioning-enabled
```

- Para obtener detalles sobre la API, consulte DeleteEvaluationResults en la Referencia de comandos de la AWS CLI.

`deliver-config-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `deliver-config-snapshot`.

AWS CLI

Entrega de una instantánea de configuración

El comando siguiente entrega una instantánea de configuración al bucket de Amazon S3 que pertenece al canal de entrega predeterminado:

```
aws configservice deliver-config-snapshot --delivery-channel-name default
```

Salida:

```
{
    "configSnapshotId": "d0333b00-a683-44af-921e-examplefb794"
}
```

- Para obtener detalles sobre la API, consulte DeliverConfigSnapshot en la Referencia de comandos de la AWS CLI.

`describe-compliance-by-config-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-compliance-by-config-rule`.

AWS CLI

Para obtener información sobre el cumplimiento de sus reglas de AWS Config

El siguiente comando devuelve la información de conformidad de cada regla de AWS Config infringida por uno o más recursos de AWS:

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

En el resultado, el valor de cada atributo de `CappedCount` indica cuántos recursos no cumplen con la regla relacionada. Por ejemplo, el siguiente resultado indica que tres recursos no cumplen con la regla denominada `InstanceTypesAreT2micro`.

Salida:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeComplianceByConfigRule en la Referencia de comandos de la AWS CLI.

`describe-compliance-by-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-compliance-by-resource`.

AWS CLI

Para obtener información sobre el cumplimiento de sus recursos de AWS

El siguiente comando devuelve la información de conformidad de cada instancia de EC2 registrada por AWS Config que infrinja una o más reglas:

```
aws configservice describe-compliance-by-resource --resource-type AWS::EC2::Instance
 --compliance-types NON_COMPLIANT
```

En el resultado, el valor de cada atributo de `CappedCount` indica cuántas reglas infringe el recurso. Por ejemplo, el siguiente resultado indica que la instancia `i-1a2b3c4d` infringe dos reglas.

Salida:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeComplianceByResource en la Referencia de comandos de la AWS CLI.

`describe-config-rule-evaluation-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-config-rule-evaluation-status`.

AWS CLI

Para obtener información de estado de una regla de AWS Config

El siguiente comando devuelve la información de estado de una regla de AWS Config denominada `MyConfigRule`:

```
aws configservice describe-config-rule-evaluation-status --config-rule-
names MyConfigRule
```

Salida:

```
{
    "ConfigRulesEvaluationStatus": [
        {
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "FirstActivatedTime": 1450311703.844,
            "ConfigRuleId": "config-rule-abcdef",
            "LastSuccessfulInvocationTime": 1450314643.156,
            "ConfigRuleName": "MyConfigRule"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeConfigRuleEvaluationStatus en la Referencia de comandos de la AWS CLI.

`describe-config-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-config-rules`.

AWS CLI

Obtención de detalles de una regla de configuración de AWS

El siguiente comando devuelve los detalles de una regla de configuración de AWS denominada `InstanceTypesAreT2micro`:

```
aws configservice describe-config-rules --config-rule-names InstanceTypesAreT2micro
```

Salida:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeConfigRules en la Referencia de comandos de la AWS CLI.

describe-configuration-recorder-status

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-configuration-recorder-status`.

AWS CLI

Para obtener información de estado del registro de configuración

El siguiente comando devuelve el estado del registro de configuración predeterminado:

```
aws configservice describe-configuration-recorder-status
```

Salida:

```
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "recording": true,
            "lastStatusChangeTime": 1452193834.344,
            "lastStartTime": 1441039997.819,
            "lastStopTime": 1441039992.835
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeConfigurationRecorderStatus en la Referencia de comandos de la AWS CLI.

describe-configuration-recorders

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-configuration-recorders`.

AWS CLI

Para obtener detalles sobre el registro de configuración

El comando siguiente devuelve información sobre el registro de configuración predeterminado:

```
aws configservice describe-configuration-recorders
```

Salida:

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": true,
                "resourceTypes": [],
                "includeGlobalResourceTypes": true
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-ConfigRole-
A1B2C3D4E5F6",
            "name": "default"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeConfigurationRecorders en la Referencia de comandos de la AWS CLI.

`describe-delivery-channel-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-delivery-channel-status`.

AWS CLI

Obtención de información del estado del canal de entrega

El comando siguiente devuelve el estado del canal de entrega:

```
aws configservice describe-delivery-channel-status
```

Salida:

```
{
    "DeliveryChannelsStatus": [
        {
            "configStreamDeliveryInfo": {
```

```
                "lastStatusChangeTime": 1452193834.381,
                "lastStatus": "SUCCESS"
            },
            "configHistoryDeliveryInfo": {
                "lastSuccessfulTime": 1450317838.412,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1450317838.412
            },
            "configSnapshotDeliveryInfo": {
                "lastSuccessfulTime": 1452185597.094,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1452185597.094
            },
            "name": "default"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeDeliveryChannelStatus en la Referencia de comandos de la AWS CLI.

`describe-delivery-channels`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-delivery-channels`.

AWS CLI

Para obtener información sobre el canal de entrega

El comando siguiente devuelve información detallada sobre el canal de entrega:

```
aws configservice describe-delivery-channels
```

Salida:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
```

```
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeDeliveryChannels en la Referencia de comandos de la AWS CLI.

`get-compliance-details-by-config-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-compliance-details-by-config-rule`.

AWS CLI

Obtención de los resultados de la evaluación de una regla de AWS Config

El siguiente comando devuelve los resultados de la evaluación de todos los recursos que no cumplan con una regla de AWS Config denominada `InstanceTypesAreT2micro`:

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Salida:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
```

```
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte GetComplianceDetailsByConfigRule en la Referencia de comandos de la AWS CLI.

`get-compliance-details-by-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-compliance-details-by-resource`.

AWS CLI

Obtención de los resultados de la evaluación de un recurso de AWS

El siguiente comando devuelve los resultados de la evaluación para cada regla infringida por la instancia de EC2 `i-1a2b3c4d`:

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Salida:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte GetComplianceDetailsByResource en la Referencia de comandos de la AWS CLI.

`get-compliance-summary-by-config-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-compliance-summary-by-config-rule`.

AWS CLI

Obtención de un resumen de la conformidad de sus reglas de AWS Config

El comando siguiente devuelve el número de reglas conformes y el de las reglas no conformes:

```
aws configservice get-compliance-summary-by-config-rule
```

En el resultado, el valor de cada atributo `CappedCount` indica el número de reglas conformes o no conformes.

Salida:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- Para obtener detalles sobre la API, consulte GetComplianceSummaryByConfigRule en la Referencia de comandos de la AWS CLI.

`get-compliance-summary-by-resource-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-compliance-summary-by-resource-type`.

AWS CLI

Para obtener el resumen de conformidad para todos los tipos de recursos

El comando siguiente devuelve el número de recursos de AWS no conformes y el número de los conformes:

```
aws configservice get-compliance-summary-by-resource-type
```

En el resultado, el valor de cada atributo `CappedCount` indica el número de recursos conformes y el de no conformes.

Salida:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

Obtención del resumen de conformidad de un tipo de recurso específico

El comando siguiente devuelve el número de instancias de EC2 no conformes y el número de las conformes:

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

En el resultado, el valor de cada atributo `CappedCount` indica el número de recursos conformes y el de no conformes.

Salida:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
```

```
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte GetComplianceSummaryByResourceType en la Referencia de comandos de la AWS CLI.

`get-resource-config-history`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource-config-history`.

AWS CLI

Obtención del historial de configuración de un recurso de AWS

El comando siguiente devuelve una lista de los elementos de configuración de una instancia de EC2 con un ID de `i-1a2b3c4d`:

```
aws configservice get-resource-config-history --resource-type AWS::EC2::Instance --
resource-id i-1a2b3c4d
```

- Para obtener detalles sobre la API, consulte GetResourceConfigHistory en la Referencia de comandos de la AWS CLI.

`get-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-status`.

AWS CLI

Obtención del estado de AWS Config

El comando siguiente devuelve el estado del canal de entrega y el registro de configuración:

```
aws configservice get-status
```

Salida:

```
Configuration Recorders:

name: default
recorder: ON
last status: SUCCESS

Delivery Channels:

name: default
last stream delivery status: SUCCESS
last history delivery status: SUCCESS
last snapshot delivery status: SUCCESS
```

- Para obtener detalles sobre la API, consulte GetStatus en la Referencia de comandos de la AWS CLI.

`list-discovered-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-discovered-resources`.

AWS CLI

Para enumerar los recursos que AWS Config ha detectado

El siguiente comando muestra las instancias de EC2 que AWS Config ha detectado:

```
aws configservice list-discovered-resources --resource-type AWS::EC2::Instance
```

Salida:

```
{
    "resourceIdentifiers": [
        {
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-1a2b3c4d"
        },
```

```
        {
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-2a2b3c4d"
        },
        {
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-3a2b3c4d"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte ListDiscoveredResources en la Referencia de comandos de la AWS CLI.

`put-config-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-config-rule`.

AWS CLI

Adición de una regla de configuración administrada por AWS

En el siguiente comando se proporciona un código JSON para añadir una regla de configuración administrada por AWS:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` es un archivo JSON que contiene la configuración de la regla:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
```

```
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Para el atributo `ComplianceResourceTypes`, este código JSON limita el alcance a los recursos del tipo `AWS::EC2::Instance`, por lo que AWS Config evaluará solo las instancias EC2 con respecto a la regla. Puesto que la regla es una regla administrada, el atributo `Owner` se establece en `AWS` y el atributo `SourceIdentifier` en el identificador de la regla, `REQUIRED_TAGS`. Para el atributo `InputParameters`, se especifican las claves de etiqueta que requiere la regla, `CostCenter` y `Owner`.

Si el comando se ejecuta correctamente, la configuración de AWS no devuelve salida. Para verificar la configuración de la regla, ejecute el comando describe-config-rules y especifique el nombre de la regla.

Adición de una regla de configuración administrada por el cliente

En el siguiente comando se proporciona un código JSON para añadir una regla de configuración administrada por el cliente:

```
aws configservice put-config-rule --config-rule file://InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json` es un archivo JSON que contiene la configuración de la regla:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
```

```
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

Para el atributo `ComplianceResourceTypes`, este código JSON limita el alcance a los recursos del tipo `AWS::EC2::Instance`, por lo que AWS Config evaluará solo las instancias EC2 con respecto a la regla. Puesto que esta regla es una regla administrada por el cliente, el atributo `Owner` se establece en `CUSTOM_LAMBDA` y el atributo `SourceIdentifier` se establece en el ARN de la función de Lambda AWS. El objeto `SourceDetails` es obligatorio. Los parámetros que se especifican para el atributo `InputParameters` se pasan a la función de Lambda AWS cuando AWS Config la invoca para evaluar los recursos conforme a la regla.

Si el comando se ejecuta correctamente, la configuración de AWS no devuelve salida. Para verificar la configuración de la regla, ejecute el comando describe-config-rules y especifique el nombre de la regla.

- Para obtener información acerca de la API, consulte PutConfigRule en la Referencia de comandos de la AWS CLI.

`put-configuration-recorder`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-configuration-recorder`.

AWS CLI

Ejemplo 1: registro de todos los recursos compatibles

El siguiente comando crea un registro de configuración que rastrea los cambios en todos los tipos de recursos compatibles, incluidos los tipos de recursos globales:

```
aws configservice put-configuration-recorder \
    --configuration-recorder name=default,roleARN=arn:aws:iam::123456789012:role/
config-role \
    --recording-group allSupported=true,includeGlobalResourceTypes=true
```

Si el comando se ejecuta correctamente, la configuración de AWS no devuelve salida. Para comprobar los ajustes del registro de configuración, ejecute el comando describe-configuration-recorders.

Ejemplo 2: Registro de tipos específicos de recursos

El siguiente comando crea un registro de configuración que rastrea los cambios realizados únicamente en los tipos de recursos que se especifican en el archivo JSON para la opción --recording-group:

```
aws configservice put-configuration-recorder \
    --configuration-recorder name=default,roleARN=arn:aws:iam::123456789012:role/config-role \
    --recording-group file://recordingGroup.json
```

RecordingGroup.json es un archivo JSON que especifica los tipos de recursos que AWS Config registrará:

```
{
    "allSupported": false,
    "includeGlobalResourceTypes": false,
    "resourceTypes": [
        "AWS::EC2::EIP",
        "AWS::EC2::Instance",
        "AWS::EC2::NetworkAcl",
        "AWS::EC2::SecurityGroup",
        "AWS::CloudTrail::Trail",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC",
        "AWS::IAM::User",
        "AWS::IAM::Policy"
    ]
}
```

Antes de poder especificar tipos de recursos para la clave resourceTypes, tendrá que ajustar las opciones allSupported e includeGlobalResourceTypes en falso u omitirlas.

Si el comando se ejecuta correctamente, la configuración de AWS no devuelve salida. Para comprobar los ajustes del registro de configuración, ejecute el comando describe-configuration-recorders.

Ejemplo 3: selección de todos los recursos compatibles, excepto los tipos específicos de recursos

El siguiente comando crea un registro de configuración que rastrea los cambios realizados en todos los tipos de recursos compatibles actuales y futuros, excepto aquellos tipos de recursos que se especifican en el archivo JSON para la opción --recording-group:

```
aws configservice put-configuration-recorder \
    --configuration-recorder name=default,roleARN=arn:aws:iam::123456789012:role/config-role \
    --recording-group file://recordingGroup.json
```

RecordingGroup.json es un archivo JSON que especifica los tipos de recursos que AWS Config registrará:

```
{
    "allSupported": false,
    "exclusionByResourceTypes": {
        "resourceTypes": [
        "AWS::Redshift::ClusterSnapshot",
        "AWS::RDS::DBClusterSnapshot",
        "AWS::CloudFront::StreamingDistribution"
    ]
    },
        "includeGlobalResourceTypes": false,
        "recordingStrategy": {
        "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
    },
}
```

Para poder especificar los tipos de recursos para excluirlos de la grabación: 1) Debe configurar las opciones allSupported e includeGlobalResourceTypes en false u omitirlas, y 2) Debe establecer el campo useOnly de RecordingStrategy en EXCLUSION_BY_RESOURCE_TYPES.

Si el comando se ejecuta correctamente, la configuración de AWS no devuelve salida. Para comprobar los ajustes del registro de configuración, ejecute el comando describe-configuration-recorders.

- Para obtener detalles sobre la API, consulte PutConfigurationRecorder en la Referencia de comandos de la AWS CLI.

`put-delivery-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-delivery-channel`.

AWS CLI

Creación de un canal de entrega

El siguiente comando proporciona la configuración del canal de entrega en forma de código JSON:

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

El archivo `deliveryChannel.json` especifica los atributos del canal de entrega:

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

Este ejemplo establece los siguientes atributos:

`name`: El nombre del canal de entrega. De forma predeterminada, AWS Config asigna el nombre `default` a un nuevo canal de entrega. No puede actualizar el nombre del canal de entrega con el comando `put-delivery-channel`. Si desea saber cuáles son los pasos para cambiar el nombre, consulte Renaming the Delivery Channel. `s3BucketName`: - El nombre del bucket de Amazon S3 al que AWS Config entrega instantáneas de configuración y los archivos de historial de configuración. Si especifica un bucket que pertenece a otra cuenta de AWS, dicho bucket debe tener políticas que concedan permisos de acceso a AWS Config. Para obtener más información, consulte Permisos para el bucket de Amazon S3.

`snsTopicARN` - El nombre de recurso de Amazon (ARN) del tema de Amazon SNS al que AWS Config envía notificaciones sobre los cambios de configuración. Si elige un tema de otra cuenta, el tema debe tener políticas que concedan permisos de acceso a AWS Config. Para obtener más información, consulte Permissions for the Amazon SNS Topic.

`configSnapshotDeliveryProperties` - Contiene el atributo `deliveryFrequency`, que establece la frecuencia con la que AWS Config entrega instantáneas de la configuración y con la que invoca las evaluaciones de las reglas de Config periódicas.

Si el comando se ejecuta correctamente, la configuración de AWS no devuelve salida. Para verificar la configuración de su canal de entrega, ejecute el comando describe-delivery-channels.

- Para obtener detalles sobre la API, consulte PutDeliveryChannel en la Referencia de comandos de la AWS CLI.

`start-config-rules-evaluation`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-config-rules-evaluation`.

AWS CLI

Ejecución de una evaluación bajo demanda de las reglas de AWS Config

El siguiente comando inicia una evaluación de dos reglas AWS administradas:

```
aws configservice start-config-rules-evaluation --config-rule-names s3-bucket-versioning-enabled cloudtrail-enabled
```

- Para obtener detalles sobre la API, consulte StartConfigRulesEvaluation en la Referencia de comandos de la AWS CLI.

`start-configuration-recorder`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-configuration-recorder`.

AWS CLI

Inicio del registro de configuración

El comando siguiente inicia el registro de configuración predeterminado:

```
aws configservice start-configuration-recorder --configuration-recorder-name default
```

Si el comando se ejecuta correctamente, la configuración de AWS no devuelve salida. Para comprobar que AWS Config está registrando sus recursos, ejecute el comando get-status.

- Para obtener detalles sobre la API, consulte StartConfigurationRecorder en la Referencia de comandos de la AWS CLI.

`stop-configuration-recorder`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-configuration-recorder`.

AWS CLI

Detención del registro de configuración

El comando siguiente detiene el registro de configuración predeterminado:

```
aws configservice stop-configuration-recorder --configuration-recorder-name default
```

Si el comando se ejecuta correctamente, la configuración de AWS no devuelve salida. Para comprobar que AWS Config no está registrando sus recursos, ejecute el comando get-status.

- Para obtener detalles sobre la API, consulte StopConfigurationRecorder en la Referencia de comandos de la AWS CLI.

`subscribe`

En el siguiente ejemplo de código, se muestra cómo utilizar `subscribe`.

AWS CLI

Suscripción a AWS Config

El comando siguiente crea el canal de entrega y el registro de configuración predeterminados: El comando también especifica el bucket de Amazon S3 y el tema de Amazon SNS a los que AWS Config entregará la información de configuración:

```
aws configservice subscribe --s3-bucket config-bucket-123456789012
 --sns-topic arn:aws:sns:us-east-1:123456789012:config-topic --iam-
role arn:aws:iam::123456789012:role/ConfigRole-A1B2C3D4E5F6
```

Salida:

```
Using existing S3 bucket: config-bucket-123456789012
Using existing SNS topic: arn:aws:sns:us-east-1:123456789012:config-topic
Subscribe succeeded:

Configuration Recorders: [
    {
        "recordingGroup": {
            "allSupported": true,
            "resourceTypes": [],
            "includeGlobalResourceTypes": false
```

```
        },
        "roleARN": "arn:aws:iam::123456789012:role/ConfigRole-A1B2C3D4E5F6",
        "name": "default"
    }
]

Delivery Channels: [
    {
        "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
        "name": "default",
        "s3BucketName": "config-bucket-123456789012"
    }
]
```

- Para obtener detalles sobre la API, consulte Subscribe en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon Connect que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando la AWS Command Line Interface con Amazon Connect.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-user`.

AWS CLI

Para crear un usuario

En el siguiente ejemplo de `create-user`, se añade un usuario con los atributos especificados a la instancia de Amazon Connect especificada.

```
aws connect create-user \
    --username Mary \
    --password Pass@Word1 \
    --identity-info FirstName=Mary,LastName=Major \
    --phone-
config PhoneType=DESK_PHONE,AutoAccept=true,AfterContactWorkTimeLimit=60,DeskPhoneNumber=
+15555551212 \
    --security-profile-id 12345678-1111-2222-aaaa-a1b2c3d4f5g7 \
    --routing-profile-id 87654321-9999-3434-abcd-x1y2z3a1b2c3 \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "UserId": "87654321-2222-1234-1234-111234567891",
    "UserArn": "arn:aws:connect:us-west-2:123456789012:instance/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111/agent/87654321-2222-1234-1234-111234567891"
}
```

Para obtener más información, consulte Add Users en la Guía del administrador de Amazon Connect.

- Para obtener información sobre la API, consulte CreateUser en la Referencia de comandos de la AWS CLI.

`delete-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-user`.

AWS CLI

Cómo eliminar un usuario

En el siguiente ejemplo de `delete-user`, se elimina un usuario con los atributos especificados a la instancia de Amazon Connect especificada.

```
aws connect delete-user \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
```

```
    --user-id 87654321-2222-1234-1234-111234567891
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Manage Users en la Guía del administrador de Amazon Connect.

- Para obtener información sobre la API, consulte DeleteUser en la Referencia de comandos de la AWS CLI.

`describe-user-hierarchy-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-user-hierarchy-group`.

AWS CLI

Visualización de los detalles de un grupo jerárquico

En el siguiente ejemplo de `describe-user-hierarchy-group`, se muestran los detalles del grupo jerárquico de Amazon Connect especificado.

```
aws connect describe-user-hierarchy-group \
    --hierarchy-group-id 12345678-1111-2222-800e-aaabbb555gg \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
     "HierarchyGroup": {
         "Id": "12345678-1111-2222-800e-a2b3c4d5f6g7",
         "Arn": "arn:aws:connect:us-west-2:123456789012:instance/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111/agent-group/12345678-1111-2222-800e-a2b3c4d5f6g7",
         "Name": "Example Corporation",
         "LevelId": "1",
         "HierarchyPath": {
             "LevelOne": {
                 "Id": "abcdefgh-3333-4444-8af3-201123456789",
                 "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/agent-group/
abcdefgh-3333-4444-8af3-201123456789",
                 "Name": "Example Corporation"
             }
         }
```

```
    }
}
```

Para obtener más información, consulte Set Up Agent Hierarchies en la Guía del administrador de Amazon Connect.

- Para obtener detalles sobre la API, consulte DescribeUserHierarchyGroup en la Referencia de comandos de la AWS CLI.

`describe-user-hierarchy-structure`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-user-hierarchy-structure`.

AWS CLI

Visualización de los detalles de una estructura jerárquica

En el siguiente ejemplo de `describe-user-hierarchy-structure`, se muestra la estructura del grupo jerárquico de la instancia de Amazon Connect especificada.

```
aws connect describe-user-hierarchy-group \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "HierarchyStructure": {
        "LevelOne": {
            "Id": "12345678-1111-2222-800e-aaabbb555gg",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/agent-group-level/1",
            "Name": "Corporation"
        },
        "LevelTwo": {
            "Id": "87654321-2222-3333-ac99-123456789102",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/agent-group-level/2",
            "Name": "Services Division"
        },
        "LevelThree": {
            "Id": "abcdefgh-3333-4444-8af3-201123456789",
```

```
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/agent-group-level/3",
            "Name": "EU Site"
        }
    }
}
```

Para obtener más información, consulte Set Up Agent Hierarchies en la Guía del administrador de Amazon Connect.

- Para obtener detalles sobre la API, consulte DescribeUserHierarchyStructure en la Referencia de comandos de la AWS CLI.

`describe-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-user`.

AWS CLI

Visualización de los detalles de un usuario

En el siguiente ejemplo de `describe-user`, se muestran los detalles del usuario de Amazon Connect especificado.

```
aws connect describe-user \
    --user-id 0c245dc0-0cf5-4e37-800e-2a7481cc8a60
    --instance-id 40c83b68-ea62-414c-97bb-d018e39e158e
```

Salida:

```
{
    "User": {
        "Id": "0c245dc0-0cf5-4e37-800e-2a7481cc8a60",
        "Arn": "arn:aws:connect:us-west-2:123456789012:instance/40c83b68-
ea62-414c-97bb-d018e39e158e/agent/0c245dc0-0cf5-4e37-800e-2a7481cc8a60",
        "Username": "Jane",
        "IdentityInfo": {
            "FirstName": "Jane",
            "LastName": "Doe",
            "Email": "example.com"
        },
        "PhoneConfig": {
```

```
            "PhoneType": "SOFT_PHONE",
            "AutoAccept": false,
            "AfterContactWorkTimeLimit": 0,
            "DeskPhoneNumber": ""
        },
        "DirectoryUserId": "8b444cf6-b368-4f29-ba18-07af27405658",
        "SecurityProfileIds": [
            "b6f85a42-1dc5-443b-b621-de0abf70c9cf"
        ],
        "RoutingProfileId": "0be36ee9-2b5f-4ef4-bcf7-87738e5be0e5",
        "Tags": {}
    }
}
```

Para obtener más información, consulte Manage Users en la Guía del administrador de Amazon Connect.

- Para obtener detalles sobre la API, consulte DescribeUser en la Referencia de comandos de la AWS CLI.

`get-contact-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-contact-attributes`.

AWS CLI

Recuperación de los atributos de un contacto

En el siguiente ejemplo de `get-contact-attributes`, se recuperan los atributos que se establecieron para el contacto de Amazon Connect especificado.

```
aws connect get-contact-attributes \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --initial-contact-id 12345678-1111-2222-800e-a2b3c4d5f6g7
```

Salida:

```
{
    "Attributes": {
        "greetingPlayed": "true"
    }
}
```

Para obtener más información, consulte Amazon Connect Contact Attributes en la Guía del administrador de Amazon Connect.

- Para obtener detalles sobre la API, consulte GetContactAttributes en la Referencia de comandos de la AWS CLI.

`list-contact-flows`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-contact-flows`.

AWS CLI

Para enumerar los flujos de contactos de una instancia

En el siguiente ejemplo de `list-contact-flows`, se enumeran los flujos de contactos de la instancia de Amazon Connect especificada.

```
aws connect list-contact-flows \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
     "ContactFlowSummaryList": [
         {
             "Id": "12345678-1111-2222-800e-a2b3c4d5f6g7",
             "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/contact-flow/12345678-1111-2222-800e-
a2b3c4d5f6g7",
             "Name": "Default queue transfer",
             "ContactFlowType": "QUEUE_TRANSFER"
         },
         {
             "Id": "87654321-2222-3333-ac99-123456789102",
             "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/contact-flow/87654321-2222-3333-
ac99-123456789102",
             "Name": "Default agent hold",
             "ContactFlowType": "AGENT_HOLD"
         },
         {
             "Id": "abcdefgh-3333-4444-8af3-201123456789",
```

```
                "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/contact-flow/
abcdefgh-3333-4444-8af3-201123456789",
            "Name": "Default customer hold",
            "ContactFlowType": "CUSTOMER_HOLD"
        },
    ]
}
```

Para obtener más información, consulte Create Amazon Connect Contact Flows en la Guía del administrador de Amazon Connect.

- Para obtener detalles sobre la API, consulte ListContactFlows en la Referencia de comandos de la AWS CLI.

`list-hours-of-operations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-hours-of-operations`.

AWS CLI

Para enumerar las horas de funcionamiento de una instancia

En el siguiente ejemplo de `list-hours-of-operations`, se enumeran las horas de funcionamiento para una instancia de Amazon Connect especificada.

```
aws connect list-hours-of-operations \
    --instance-id 40c83b68-ea62-414c-97bb-d018e39e158e
```

Salida:

```
{
    "HoursOfOperationSummaryList": [
        {
            "Id": "d69f1f84-7457-4924-8fbe-e64875546259",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/40c83b68-
ea62-414c-97bb-d018e39e158e/operating-hours/d69f1f84-7457-4924-8fbe-e64875546259",
            "Name": "Basic Hours"
        }
    ]
}
```

Para obtener más información, consulte Set the Hours of Operation for a Queue en la Guía del administrador de Amazon Connect.

- Para obtener detalles sobre la API, consulte ListHoursOfOperations en la Referencia de comandos de la AWS CLI.

`list-phone-numbers`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-phone-numbers`.

AWS CLI

Para enumerar los números de teléfono de una instancia

En el siguiente ejemplo de `list-phone-numbers`, se enumeran los números de teléfono de la instancia de Amazon Connect especificada.

```
aws connect list-phone-numbers \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "PhoneNumberSummaryList": [
        {
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/phone-number/xyz80zxy-xyz1-80zx-
zx80-11111EXAMPLE",
            "PhoneNumber": "+17065551212",
            "PhoneNumberType": "DID",
            "PhoneNumberCountryCode": "US"
        },
        {
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/phone-number/ccc0ccc-xyz1-80zx-
zx80-22222EXAMPLE",
            "PhoneNumber": "+18555551212",
            "PhoneNumberType": "TOLL_FREE",
            "PhoneNumberCountryCode": "US"
        }
```

```
    ]
}
```

Para obtener más información, consulte Set Up Phone Numbers for Your Contact Center en la Guía del administrador de Amazon Connect.

- Para obtener información sobre la API, consulte ListPhoneNumbers en la Referencia de comandos de la AWS CLI.

`list-queues`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-queues`.

AWS CLI

Para enumerar las colas de una instancia

En el siguiente ejemplo de `list-queues`, se enumeran las colas de la instancia de Amazon Connect especificada.

```
aws connect list-queues \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "QueueSummaryList": [
        {
            "Id": "12345678-1111-2222-800e-a2b3c4d5f6g7",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/queue/agent/12345678-1111-2222-800e-
a2b3c4d5f6g7",
            "QueueType": "AGENT"
        },
        {
            "Id": "87654321-2222-3333-ac99-123456789102",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/queue/agent/87654321-2222-3333-
ac99-123456789102",
            "QueueType": "AGENT"
        },
```

```
        {
            "Id": "abcdefgh-3333-4444-8af3-201123456789",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/queue/agent/
abcdefgh-3333-4444-8af3-201123456789",
            "QueueType": "AGENT"
        },
        {
            "Id": "hgfedcba-4444-5555-a31f-123456789102",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/queue/hgfedcba-4444-5555-a31f-123456789102",
            "Name": "BasicQueue",
            "QueueType": "STANDARD"
        },
    ]
}
```

Para obtener más información, consulte Create a Queue en la Guía del administrador de Amazon Connect.

- Para obtener información sobre la API, consulte ListQueues en la Referencia de comandos de la AWS CLI.

`list-routing-profiles`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-routing-profiles`.

AWS CLI

Para enumerar los perfiles de enrutamiento de una instancia

En el siguiente ejemplo de `list-routing-profiles`, se enumeran los perfiles de enrutamiento de la instancia de Amazon Connect especificada.

```
aws connect list-routing-profiles \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "RoutingProfileSummaryList": [
        {
```

```
            "Id": "12345678-1111-2222-800e-a2b3c4d5f6g7",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/routing-profile/12345678-1111-2222-800e-
a2b3c4d5f6g7",
            "Name": "Basic Routing Profile"
        },
    ]
}
```

Para obtener más información, consulte Create a Routing Profile en la Guía del administrador de Amazon Connect.

- Para obtener detalles sobre la API, consulte ListRoutingProfiles en la Referencia de comandos de la AWS CLI.

`list-security-profiles`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-security-profiles`.

AWS CLI

Para enumerar los perfiles de seguridad de la instancia

En el siguiente ejemplo de `list-security-profiles`, se enumeran los perfiles de seguridad de la instancia de Amazon Connect especificada.

```
aws connect list-security-profiles \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "SecurityProfileSummaryList": [
        {
            "Id": "12345678-1111-2222-800e-a2b3c4d5f6g7",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/security-profile/12345678-1111-2222-800e-
a2b3c4d5f6g7",
            "Name": "CallCenterManager"
        },
        {
            "Id": "87654321-2222-3333-ac99-123456789102",
```

```
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/security-profile/87654321-2222-3333-
ac99-123456789102",
            "Name": "QualityAnalyst"
        },
        {
            "Id": "abcdefgh-3333-4444-8af3-201123456789",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/security-profile/
abcdefgh-3333-4444-8af3-201123456789",
            "Name": "Agent"
        },
        {
            "Id": "12345678-1111-2222-800e-x2y3c4d5fzzzz",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/security-profile/12345678-1111-2222-800e-
x2y3c4d5fzzzz",
            "Name": "Admin"
        }
    ]
}
```

Para obtener más información, consulte Assign Permissions: Security Profiles en la Guía del administrador de Amazon Connect.

- Para obtener detalles sobre la API, consulte ListSecurityProfiles en la Referencia de comandos de la AWS CLI.

`list-user-hierarchy-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-user-hierarchy-groups`.

AWS CLI

Para enumerar los grupos jerárquicos de usuarios de una instancia

En el siguiente ejemplo de `list-user-hierarchy-groups`, se enumeran los grupos jerárquicos de la instancia de Amazon Connect especificada.

```
aws connect list-user-hierarchy-groups \
    --instance-id 40c83b68-ea62-414c-97bb-d018e39e158e
```

Salida:

```
{
    "UserHierarchyGroupSummaryList": [
        {
            "Id": "0e2f6d1d-b3ca-494b-8dbc-ba81d9f8182a",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/40c83b68-
ea62-414c-97bb-d018e39e158e/agent-group/0e2f6d1d-b3ca-494b-8dbc-ba81d9f8182a",
            "Name": "Example Corporation"
        },
    ]
}
```

Para obtener más información, consulte Set Up Agent Hierarchies en la Guía del administrador de Amazon Connect.

- Para obtener detalles sobre la API, consulte ListUserHierarchyGroups en la Referencia de comandos de la AWS CLI.

`list-users`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-users`.

AWS CLI

Para enumerar los grupos jerárquicos de usuarios de una instancia

En el siguiente ejemplo de `list-users`, se enumeran los usuarios de la instancia de Amazon Connect especificada.

```
aws connect list-users \
    --instance-id 40c83b68-ea62-414c-97bb-d018e39e158e
```

Salida:

```
{
    "UserSummaryList": [
        {
            "Id": "0c245dc0-0cf5-4e37-800e-2a7481cc8a60",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/40c83b68-
ea62-414c-97bb-d018e39e158e/agent/0c245dc0-0cf5-4e37-800e-2a7481cc8a60",
            "Username": "Jane"
        },
```

```
        {
            "Id": "46f0c67c-3fc7-4806-ac99-403798788c14",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/40c83b68-
ea62-414c-97bb-d018e39e158e/agent/46f0c67c-3fc7-4806-ac99-403798788c14",
            "Username": "Paulo"
        },
        {
            "Id": "55a83578-95e1-4710-8af3-2b7afe310e48",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/40c83b68-
ea62-414c-97bb-d018e39e158e/agent/55a83578-95e1-4710-8af3-2b7afe310e48",
            "Username": "JohnD"
        },
        {
            "Id": "703e27b5-c9f0-4f1f-a239-64ccbb160125",
            "Arn": "arn:aws:connect:us-west-2:123456789012:instance/40c83b68-
ea62-414c-97bb-d018e39e158e/agent/703e27b5-c9f0-4f1f-a239-64ccbb160125",
            "Username": "JohnS"
        }
    ]
}
```

Para obtener más información, consulte Add Users en la Guía del administrador de Amazon Connect.

- Para obtener información sobre la API, consulte ListUsers en la Referencia de comandos de la AWS CLI.

`update-contact-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-contact-attributes`.

AWS CLI

Actualización del atributo de un contacto

En el siguiente ejemplo de `update-contact-attributes`, se actualiza el atributo `greetingPlayed` del usuario de Amazon Connect especificado.

```
aws connect update-contact-attributes \
    --initial-contact-id 11111111-2222-3333-4444-12345678910 \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --attributes greetingPlayed=false
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Amazon Connect Contact Attributes en la Guía del administrador de Amazon Connect.

- Para obtener detalles sobre la API, consulte UpdateContactAttributes en la Referencia de comandos de la AWS CLI.

`update-user-hierarchy`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-user-hierarchy`.

AWS CLI

Actualización de la jerarquía del usuario

En el siguiente ejemplo de `update-user-hierarchy`, se actualiza la jerarquía del agente para el usuario de Amazon Connect especificado.

```
aws connect update-user-hierarchy \
    --hierarchy-group-id 12345678-a1b2-c3d4-e5f6-123456789abc \
    --user-id 87654321-2222-1234-1234-111234567891 \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configure Agent Settings en la Guía del administrador de Amazon Connect.

- Para obtener detalles sobre la API, consulte UpdateUserHierarchy en la Referencia de comandos de la AWS CLI.

`update-user-identity-info`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-user-identity-info`.

AWS CLI

Actualización de la información de identidad de un usuario

En el siguiente ejemplo de `update-user-identity-info`, se actualiza la información de identidad del usuario de Amazon Connect especificado.

```
aws connect update-user-identity-info \
    --identity-info FirstName=Mary,LastName=Major,Email=marym@example.com \
    --user-id 87654321-2222-1234-1234-111234567891 \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configure Agent Settings en la Guía del administrador de Amazon Connect.

- Para obtener detalles sobre la API, consulte UpdateUserIdentityInfo en la Referencia de comandos de la AWS CLI.

`update-user-phone-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-user-phone-config`.

AWS CLI

Actualización de la configuración del teléfono de un usuario

En el siguiente de ejemplo de `update-user-phone-config`, se actualiza la configuración del teléfono para el usuario especificado.

```
aws connect update-user-phone-config \
    --phone-
config PhoneType=SOFT_PHONE,AutoAccept=false,AfterContactWorkTimeLimit=60,DeskPhoneNumber=
+18005551212 \
    --user-id 12345678-4444-3333-2222-111122223333 \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configure Agent Settings en la Guía del administrador de Amazon Connect.

- Para obtener detalles sobre la API, consulte UpdateUserPhoneConfig en la Referencia de comandos de la AWS CLI.

`update-user-routing-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-user-routing-profile`.

AWS CLI

Actualización del perfil de enrutamiento de un usuario

En el siguiente ejemplo de `update-user-routing-profile`, se actualiza el perfil de enrutamiento del usuario de Amazon Connect especificado.

```
aws connect update-user-routing-profile \
    --routing-profile-id 12345678-1111-3333-2222-4444EXAMPLE \
    --user-id 87654321-2222-1234-1234-111234567891 \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configure Agent Settings en la Guía del administrador de Amazon Connect.

- Para obtener detalles sobre la API, consulte UpdateUserRoutingProfile en la Referencia de comandos de la AWS CLI.

`update-user-security-profiles`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-user-security-profiles`.

AWS CLI

Actualización de los perfiles de seguridad de un usuario

En el siguiente ejemplo de `update-user-security-profiles`, se actualiza el perfil de seguridad del usuario de Amazon Connect especificado.

```
aws connect update-user-security-profiles \
    --security-profile-ids 12345678-1234-1234-1234-1234567892111 \
    --user-id 87654321-2222-1234-1234-111234567891 \
    --instance-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Assign Permissions: Security Profiles en la Guía del administrador de Amazon Connect.

- Para obtener detalles sobre la API, consulte UpdateUserSecurityProfiles en la Referencia de comandos de la AWS CLI.

AWS Cost and Usage Report Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS Cost and Usage Report.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`delete-report-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-report-definition`.

AWS CLI

Eliminación de un informe de Costo y uso de AWS

En este ejemplo, se elimina un informe de Costo y uso de AWS.

Comando:

```
aws cur --region us-east-1 delete-report-definition --report-name "ExampleReport"
```

- Para obtener detalles sobre la API, consulte DeleteReportDefinition en la Referencia de comandos de la AWS CLI.

`describe-report-definitions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-report-definitions`.

AWS CLI

Recuperación de una lista de informes de Costo y uso de AWS

En este ejemplo, se describe una lista de informes de Costo y uso de AWS que sean propiedad de una cuenta.

Comando:

```
aws cur --region us-east-1 describe-report-definitions --max-items 5
```

Salida:

```
  {
"ReportDefinitions": [
  {
      "ReportName": "ExampleReport",
      "Compression": "ZIP",
      "S3Region": "us-east-1",
      "Format": "textORcsv",
      "S3Prefix": "exampleprefix",
      "S3Bucket": "example-s3-bucket",
      "TimeUnit": "DAILY",
      "AdditionalArtifacts": [
          "REDSHIFT",
          "QUICKSIGHT"
      ],
      "AdditionalSchemaElements": [
          "RESOURCES"
      ]
  }
]
  }
```

- Para obtener detalles sobre la API, consulte DescribeReportDefinitions en la Referencia de comandos de la AWS CLI.

`put-report-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-report-definition`.

AWS CLI

Creación de informes de Costo y uso de AWS

En el siguiente ejemplo de `put-report-definition`, se crea un informe diario de Costo y uso de AWS que puede cargar en Amazon Redshift o Amazon QuickSight.

```
aws cur put-report-definition --report-definition file://report-definition.json
```

Contenido de `report-definition.json`:

```
{
    "ReportName": "ExampleReport",
    "TimeUnit": "DAILY",
    "Format": "textORcsv",
    "Compression": "ZIP",
    "AdditionalSchemaElements": [
        "RESOURCES"
    ],
    "S3Bucket": "example-s3-bucket",
    "S3Prefix": "exampleprefix",
    "S3Region": "us-east-1",
    "AdditionalArtifacts": [
        "REDSHIFT",
        "QUICKSIGHT"
    ]
}
```

- Para obtener detalles sobre la API, consulte PutReportDefinition en la Referencia de comandos de la AWS CLI.

Ejemplos del Cost Explorer Service que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando la AWS Command Line Interface con Cost Explorer Service.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`get-cost-and-usage`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-cost-and-usage`.

AWS CLI

Recuperación del uso de una cuenta en S3 durante el mes de septiembre de 2017

En el siguiente ejemplo de `get-cost-and-usage`, se recupera el uso de una cuenta en S3 durante el mes de septiembre de 2017.

```
aws ce get-cost-and-usage \
    --time-period Start=2017-09-01,End=2017-10-01 \
    --granularity MONTHLY \
    --metrics "BlendedCost" "UnblendedCost" "UsageQuantity" \
    --group-by Type=DIMENSION,Key=SERVICE Type=TAG,Key=Environment \
    --filter file://filters.json
```

Contenido de `filters.json`:

```
{
    "Dimensions": {
        "Key": "SERVICE",
        "Values": [
            "Amazon Simple Storage Service"
        ]
    }
}
```

Salida:

```
{
    "GroupDefinitions": [
```

```
        {
            "Type": "DIMENSION",
            "Key": "SERVICE"
        },
        {
            "Type": "TAG",
            "Key": "Environment"
        }
    ],
    "ResultsByTime": [
        {
            "Estimated": false,
            "TimePeriod": {
                "Start": "2017-09-01",
                "End": "2017-10-01"
            },
            "Total": {},
            "Groups": [
                {
                    "Keys": [
                        "Amazon Simple Storage Service",
                        "Environment$"
                    ],
                    "Metrics": {
                        "BlendedCost": {
                            "Amount": "40.3527508453",
                            "Unit": "USD"
                        },
                        "UnblendedCost": {
                            "Amount": "40.3543773134",
                            "Unit": "USD"
                        },
                        "UsageQuantity": {
                            "Amount": "9312771.098461578",
                            "Unit": "N/A"
                        }
                    }
                },
                {
                    "Keys": [
                        "Amazon Simple Storage Service",
                        "Environment$Dev"
                    ],
                    "Metrics": {
```

```
                        "BlendedCost": {
                            "Amount": "0.2682364644",
                            "Unit": "USD"
                        },
                        "UnblendedCost": {
                            "Amount": "0.2682364644",
                            "Unit": "USD"
                        },
                        "UsageQuantity": {
                            "Amount": "22403.4395271182",
                            "Unit": "N/A"
                        }
                    }
                }
            ]
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte GetCostAndUsage en la Referencia de comandos de la AWS CLI.

`get-dimension-values`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-dimension-values`.

AWS CLI

Recuperación de las etiquetas de la dimensión SERVICE con el valor Elastic

En este ejemplo, se recuperan las etiquetas de la dimensión SERVICE, con un valor Elastic del 1 de enero al 18 de mayo de 2017.

Comando:

```
aws ce get-dimension-values --search-string Elastic --time-
period Start=2017-01-01,End=2017-05-18 --dimension SERVICE
```

Salida:

```
{
   "TotalSize": 6,
```

```
    "DimensionValues": [
        {
            "Attributes": {},
            "Value": "Amazon ElastiCache"
        },
        {
            "Attributes": {},
            "Value": "EC2 - Other"
        },
        {
            "Attributes": {},
            "Value": "Amazon Elastic Compute Cloud - Compute"
        },
        {
            "Attributes": {},
            "Value": "Amazon Elastic Load Balancing"
        },
        {
            "Attributes": {},
            "Value": "Amazon Elastic MapReduce"
        },
        {
            "Attributes": {},
            "Value": "Amazon Elasticsearch Service"
        }
    ],
    "ReturnSize": 6
}
```

- Para obtener detalles sobre la API, consulte GetDimensionValues en la Referencia de comandos de la AWS CLI.

`get-reservation-coverage`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-reservation-coverage`.

AWS CLI

Recuperación de la cobertura de reservas para las instancias t2.nano de EC2 en la región us-east-1

En este ejemplo, se recupera la cobertura de reservas para las instancias t2.nano de EC2 en la región us-east-1 de julio a septiembre de 2017.

Comando:

```
aws ce get-reservation-coverage --time-period Start=2017-07-01,End=2017-10-01 --
group-by Type=Dimension,Key=REGION --filter file://filters.json
```

filters.json:

```
{
   "And": [
     {
       "Dimensions": {
         "Key": "INSTANCE_TYPE",
         "Values": [
           "t2.nano"
         ]
       },
       "Dimensions": {
         "Key": "REGION",
         "Values": [
           "us-east-1"
         ]
       }
     }
   ]
 }
```

Salida:

```
{
   "TotalSize": 6,
   "DimensionValues": [
       {
           "Attributes": {},
           "Value": "Amazon ElastiCache"
       },
       {
           "Attributes": {},
           "Value": "EC2 - Other"
       },
       {
           "Attributes": {},
           "Value": "Amazon Elastic Compute Cloud - Compute"
```

```
        },
        {
            "Attributes": {},
            "Value": "Amazon Elastic Load Balancing"
        },
        {
            "Attributes": {},
            "Value": "Amazon Elastic MapReduce"
        },
        {
            "Attributes": {},
            "Value": "Amazon Elasticsearch Service"
        }
    ],
    "ReturnSize": 6
}
```

- Para obtener detalles sobre la API, consulte GetReservationCoverage en la Referencia de comandos de la AWS CLI.

`get-reservation-purchase-recommendation`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-reservation-purchase-recommendation`.

AWS CLI

Obtención de recomendaciones de reserva para las RI de EC2 con pago inicial parcial con un plazo de tres años

En el siguiente ejemplo de `get-reservation-purchase-recommendation`, se recuperan las recomendaciones para las instancias de EC2 con pago inicial parcial con un plazo de tres años, en función de los últimos 60 días de uso de EC2.

```
aws ce get-reservation-purchase-recommendation \
    --service "Amazon Redshift" \
    --lookback-period-in-days SIXTY_DAYS \
    --term-in-years THREE_YEARS \
    --payment-option PARTIAL_UPFRONT
```

Salida:

```
{
    "Recommendations": [],
    "Metadata": {
        "GenerationTimestamp": "2018-08-08T15:20:57Z",
        "RecommendationId": "00d59dde-a1ad-473f-8ff2-iexample3330b"
    }
}
```

- Para obtener detalles sobre la API, consulte GetReservationPurchaseRecommendation en la Referencia de comandos de la AWS CLI.

`get-reservation-utilization`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-reservation-utilization`.

AWS CLI

Recuperación de la utilización de la reserva para su cuenta

En el siguiente ejemplo de `get-reservation-utilization`, se recupera el uso de la RI en todos los tipos de instancias t2.nano entre el 1 de marzo de 2018 y el 1 de agosto de 2018 para la cuenta.

```
aws ce get-reservation-utilization \
    --time-period Start=2018-03-01,End=2018-08-01 \
    --filter file://filters.json
```

Contenido de `filters.json`:

```
{
    "Dimensions": {
        "Key": "INSTANCE_TYPE",
        "Values": [
            "t2.nano"
        ]
    }
}
```

Salida:

```
{
```

```
    "Total": {
        "TotalAmortizedFee": "0",
        "UtilizationPercentage": "0",
        "PurchasedHours": "0",
        "NetRISavings": "0",
        "TotalActualHours": "0",
        "AmortizedRecurringFee": "0",
        "UnusedHours": "0",
        "TotalPotentialRISavings": "0",
        "OnDemandCostOfRIHoursUsed": "0",
        "AmortizedUpfrontFee": "0"
    },
    "UtilizationsByTime": []
}
```

- Para obtener detalles sobre la API, consulte GetReservationUtilization en la Referencia de comandos de la AWS CLI.

`get-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-tags`.

AWS CLI

Recuperación de las claves y los valores de una etiqueta de asignación de costes

En este ejemplo, se recuperan todas las etiquetas de asignación de costes con la clave Project y un valor que contiene secretProject.

Comando:

```
aws ce get-tags --search-string secretProject --time-
period Start=2017-01-01,End=2017-05-18 --tag-key Project
```

Salida:

```
{
  "ReturnSize": 2,
  "Tags": [
    "secretProject1",
    "secretProject2"
  ],
```

```
  "TotalSize": 2
}
```

- Para obtener detalles sobre la API, consulte GetTags en la Referencia de comandos de la AWS CLI.

Ejemplos de Firehose que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Firehose.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`list-delivery-streams`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-delivery-streams`.

AWS CLI

Para enumerar los flujos de entrega disponibles

En el siguiente ejemplo de `list-delivery-streams`, se enumeran los flujos de entrega disponibles en su cuenta de AWS.

```
aws firehose list-delivery-streams
```

Salida:

```
{
    "DeliveryStreamNames": [
```

```
        "my-stream"
    ],
    "HasMoreDeliveryStreams": false
}
```

Para obtener más información, consulte la sección sobre creación de una secuencia de entrega de Amazon Kinesis Data Firehose en la guía para desarrolladores de Amazon Kinesis Data Firehose.

- Para obtener información sobre la API, consulte ListDeliveryStreams en la Referencia de comandos de la AWS CLI.

`put-record-batch`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-record-batch`.

AWS CLI

Para escribir varios registros en un flujo

En el siguiente ejemplo `put-record-batch`, se escriben tres registros en una secuencia. Los datos se codifican en formato Base64.

```
aws firehose put-record-batch \
    --delivery-stream-name my-stream \
    --records file://records.json
```

Contenidos de `myfile.json`:

```
[
    {"Data": "Rmlyc3QgdGhpbmc="},
    {"Data": "U2Vjb25kIHRoaW5n"},
    {"Data": "VGhpcmQgdGhpbmc="}
]
```

Salida:

```
{
    "FailedPutCount": 0,
    "Encrypted": false,
    "RequestResponses": [
        {
```

```
            "RecordId": "9D2OJ6t2EqCTZTXwGzeSv/EVHxRoRCw89xd+o3+sXg8DhYOaWKPSmZy/
CGlRVEys1u1xbeKh6VofEYKkoeiDrcjrxhQp9iF7sUW7pujiMEQ5LzlrzCkGosxQn
+3boDnURDEaD42V7GiixpOyLJkYZcae1i7HzlCEoy9LJhMr8EjDSi4Om/9Vc2uhwwuAtGE0XKpxJ2WD7ZRWtAnYlKAnv
        },
        {
            "RecordId": "jFirejqxCLlK5xjH/UNmlMVcjktEN76I7916X9PaZ
+PVaOSXDfU1WGOqEZhxq2js7xcZ552eoeDxsuTU1MSq9nZTbVfb6cQTIXnm/GsuF37Uhg67GKmR5z90l6XKJ
+/+pDloFv7Hh9a3oUS6wYm3DcNRLTHHAimANp1PhkQvWpvLRfzbuCUkBphR2QVzhP9OiHLbzGwy8/
DfH8sqWEUYASNJKS8GXP5s"
        },
        {
            "RecordId":
 "oy0amQ40o5Y2YV4vxzufdcMOOw6n3EPr3tpPJGoYVNKH4APPVqNcbUgefo1stEFRg4hTLrf2k6eliHu/9+YJ5R3iie
DTBt3qBlmTj7Xq8SKVbO1S7YvMTpWkMKA86f8JfmT8BMKoMb4XZS/sOkQLe+qh0sYKXWl"
        }
    ]
}
```

Para obtener más información, consulte Envío de una secuencia de entrega de Amazon Kinesis Data Firehose en la Guía para desarrolladores de Amazon Kinesis Data Firehose.

- Para obtener información sobre la API, consulte PutRecordBatch en la Referencia de comandos de la AWS CLI.

`put-record`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-record`.

AWS CLI

Para escribir un registro en un flujo

En el siguiente ejemplo de `put-record`, se escriben datos en un flujo. Los datos se codifican en formato Base64.

```
aws firehose put-record \
    --delivery-stream-name my-stream \
    --record '{"Data":"SGVsbG8gd29ybGQ="}'
```

Salida:

```
{
```

```
    "RecordId": "RjB5K/nnoGFHqwTsZlNd/
TTqvjE8V5dsyXZTQn2JXrdpMTOwssyEb6nfC8fwf1whhwnItt4mvrn+gsqeK5jB7QjuLg283+Ps4Sz/
j1Xujv31iDhnPdaLw4BOyM9Amv7PcCuB2079RuM0NhoakbyUymlwY8yt20G8X2420wu1jlFafhci4erAt7QhDEvpwuK8
    "Encrypted": false
}
```

Para obtener más información, consulte Envío de una secuencia de entrega de Amazon Kinesis Data Firehose en la Guía para desarrolladores de Amazon Kinesis Data Firehose.

- Para obtener información sobre la API, consulte PutRecord en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon Data Lifecycle Manager que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios comunes utilizando la AWS Command Line Interface con Amazon Data Lifecycle Manager.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-default-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-default-role`.

AWS CLI

Creación del rol de IAM requerido para Amazon DLM

El siguiente ejemplo de `dlm create-default-role` crea el rol predeterminado de AWSDataLifecycleManagerDefaultRole para la administración de instantáneas.

```
aws dlm create-default-role \
```

```
    --resource-type snapshot
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Default service roles for Amazon Data Lifecycle Manager en la Guía del usuario de Amazon Elastic Compute Cloud.

- Para obtener detalles sobre la API, consulte CreateDefaultRole en la Referencia de comandos de la AWS CLI.

`create-lifecycle-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-lifecycle-policy`.

AWS CLI

Creación de una política de ciclo de vida

En el siguiente ejemplo de `create-lifecycle-policy`, se crea una política de ciclo de vida que crea una instantánea diaria de los volúmenes a la hora especificado. Las etiquetas especificadas se añaden a las instantáneas y las etiquetas también se copian del volumen y se añaden a las instantáneas. Si la creación de una instantánea nueva supera el recuento máximo especificado, se elimina la instantánea más antigua.

```
aws dlm create-lifecycle-policy \
    --description "My first policy" \
    --state ENABLED \
    --execution-role-arn arn:aws:iam::12345678910:role/
AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Contenido de `policyDetails.json`:

```
{
    "ResourceTypes": [
        "VOLUME"
    ],
    "TargetTags": [
        {
            "Key": "costCenter",
            "Value": "115"
        }
```

```
    ],
    "Schedules":[
        {
            "Name": "DailySnapshots",
            "CopyTags": true,
            "TagsToAdd": [
                {
                    "Key": "type",
                     "Value": "myDailySnapshot"
                }
            ],
            "CreateRule": {
                "Interval": 24,
                "IntervalUnit": "HOURS",
                "Times": [
                    "03:00"
                ]
            },
            "RetainRule": {
                "Count":5
            }
        }
    ]
}
```

Salida:

```
{
    "PolicyId": "policy-0123456789abcdef0"
}
```

- Para obtener detalles sobre la API, consulte CreateLifecyclePolicy en la Referencia de comandos de la AWS CLI.

`delete-lifecycle-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-lifecycle-policy`.

AWS CLI

Eliminación de una política de ciclo de vida

En el siguiente ejemplo, se elimina la política de ciclo de vida especificada:

```
aws dlm delete-lifecycle-policy --policy-id policy-0123456789abcdef0
```

- Para obtener información sobre la API, consulte DeleteLifecyclePolicy en la Referencia de comandos de la AWS CLI.

`get-lifecycle-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-lifecycle-policies`.

AWS CLI

Obtención de un resumen de sus políticas de ciclo de vida

En el siguiente ejemplo de `get-lifecycle-policies`, se enumeran todas sus políticas de ciclo de vida.

```
aws dlm get-lifecycle-policies
```

Salida:

```
{
    "Policies": [
        {
            "PolicyId": "policy-0123456789abcdef0",
            "Description": "My first policy",
            "State": "ENABLED"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte GetLifecyclePolicies en la Referencia de comandos de la AWS CLI.

`get-lifecycle-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-lifecycle-policy`.

AWS CLI

Descripción de una política de ciclo de vida

En el siguiente ejemplo de `get-lifecycle-policy`, se muestran los detalles de la política de ciclo de vida especificada.

```
aws dlm get-lifecycle-policy \
    --policy-id policy-0123456789abcdef0
```

Salida:

```
{
    "Policy": {
        "PolicyId": "policy-0123456789abcdef0",
        "Description": "My policy",
        "State": "ENABLED",
        "ExecutionRoleArn": "arn:aws:iam::123456789012:role/
AWSDataLifecycleManagerDefaultRole",
        "DateCreated": "2019-08-08T17:45:42Z",
        "DateModified": "2019-08-08T17:45:42Z",
        "PolicyDetails": {
            "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
            "ResourceTypes": [
                "VOLUME"
            ],
            "TargetTags": [
              {
                  "Key": "costCenter",
                  "Value": "115"
              }
            ],
            "Schedules": [
              {
                  "Name": "DailySnapshots",
                  "CopyTags": true,
                  "TagsToAdd": [
                    {
                        "Key": "type",
                        "Value": "myDailySnapshot"
                    }
                  ],
                  "CreateRule": {
                    "Interval": 24,
                    "IntervalUnit": "HOURS",
                    "Times": [
                        "03:00"
```

```
                    ]
                },
                "RetainRule": {
                    "Count": 5
                }
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte GetLifecyclePolicy en la Referencia de comandos de la AWS CLI.

`update-lifecycle-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-lifecycle-policy`.

AWS CLI

Ejemplo 1: habilitar una política de ciclo de vida

En el siguiente ejemplo de `update-lifecycle-policy`, se habilita la política de ciclo de vida especificada.

```
aws dlm update-lifecycle-policy \
    --policy-id policy-0123456789abcdef0 \
    --state ENABLED
```

Ejemplo 2: deshabilitar una política de ciclo de vida

En el siguiente ejemplo de `update-lifecycle-policy`, se deshabilita la política de ciclo de vida especificada.

```
aws dlm update-lifecycle-policy \
    --policy-id policy-0123456789abcdef0 \
    --state DISABLED
```

Ejemplo 3: actualizar los detalles de la política de ciclo de vida

En el siguiente ejemplo de `update-lifecycle-policy`, se actualizan las etiquetas de destino de la política de ciclo de vida especificada.

```
aws dlm update-lifecycle-policy \
    --policy-id policy-0123456789abcdef0
    --policy-details file://policyDetails.json
```

Contenido de `policyDetails.json`. El comando no modifica otros detalles a los que no se hace referencia en este archivo.

```
{
    "TargetTags": [
        {
            "Key": "costCenter",
            "Value": "120"
        },
        {
            "Key": "project",
            "Value": "lima"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte UpdateLifecyclePolicy en la Referencia de comandos de la AWS CLI.

AWS Data Pipeline Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS Data Pipeline.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`activate-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `activate-pipeline`.

AWS CLI

Activación de una canalización

En este ejemplo, se activa la canalización especificada:

```
aws datapipeline activate-pipeline --pipeline-id df-00627471SOVYZEXAMPLE
```

Para activar la canalización en una fecha y hora específicas, usa el siguiente comando:

```
aws datapipeline activate-pipeline --pipeline-id df-00627471SOVYZEXAMPLE --start-
timestamp 2015-04-07T00:00:00Z
```

- Para obtener detalles sobre la API, consulte ActivatePipeline en la Referencia de comandos de la AWS CLI.

`add-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-tags`.

AWS CLI

Adición de una etiqueta a una canalización

En este ejemplo, se añade la etiqueta especificada a la canalización especificada:

```
aws datapipeline add-tags --pipeline-id df-00627471SOVYZEXAMPLE --
tags key=environment,value=production key=owner,value=sales
```

Para ver las etiquetas, utilice el comando describe-pipelines. Por ejemplo, las etiquetas añadidas en el comando del ejemplo aparecen de la siguiente manera en el resultado de describe-pipelines:

```
{
```

```
    ...
        "tags": [
            {
                "value": "production",
                "key": "environment"
            },
            {
                "value": "sales",
                "key": "owner"
            }
        ]
    ...
}
```

- Para obtener detalles sobre la API, consulte AddTags en la Referencia de comandos de la AWS CLI.

`create-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-pipeline`.

AWS CLI

Creación de una canalización

En este ejemplo, se crea una canalización:

```
aws datapipeline create-pipeline --name my-pipeline --unique-id my-pipeline-token
```

A continuación, se muestra un ejemplo de la salida:

```
{
    "pipelineId": "df-00627471SOVYZEXAMPLE"
}
```

- Para obtener detalles sobre la API, consulte CreatePipeline en la Referencia de comandos de la AWS CLI.

`deactivate-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `deactivate-pipeline`.

AWS CLI

Desactivación de una canalización

En este ejemplo, se desactiva la canalización especificada:

```
aws datapipeline deactivate-pipeline --pipeline-id df-00627471SOVYZEXAMPLE
```

Para desactivar la canalización solo una vez que hayan finalizado todas las actividades en ejecución, use el comando siguiente:

```
aws datapipeline deactivate-pipeline --pipeline-id df-00627471SOVYZEXAMPLE --no-cancel-active
```

- Para obtener detalles sobre la API, consulte DeactivatePipeline en la Referencia de comandos de la AWS CLI.

`delete-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-pipeline`.

AWS CLI

Para eliminar una canalización

En este ejemplo, se elimina la canalización especificada.

```
aws datapipeline delete-pipeline --pipeline-id df-00627471SOVYZEXAMPLE
```

- Para obtener detalles sobre la API, consulte DeletePipeline en la Referencia de comandos de la AWS CLI.

`describe-pipelines`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-pipelines`.

AWS CLI

Descripción de sus canalizaciones

En este ejemplo, se describe la canalización especificada.

```
aws datapipeline describe-pipelines --pipeline-ids df-00627471SOVYZEXAMPLE
```

A continuación, se muestra un ejemplo de la salida:

```
{
  "pipelineDescriptionList": [
      {
          "fields": [
              {
                  "stringValue": "PENDING",
                  "key": "@pipelineState"
              },
              {
                  "stringValue": "my-pipeline",
                  "key": "name"
              },
              {
                  "stringValue": "2015-04-07T16:05:58",
                  "key": "@creationTime"
              },
              {
                  "stringValue": "df-00627471SOVYZEXAMPLE",
                  "key": "@id"
              },
              {
                  "stringValue": "123456789012",
                  "key": "pipelineCreator"
              },
              {
                  "stringValue": "PIPELINE",
                  "key": "@sphere"
              },
              {
                  "stringValue": "123456789012",
                  "key": "@userId"
              },
              {
                  "stringValue": "123456789012",
                  "key": "@accountId"
              },
              {
                  "stringValue": "my-pipeline-token",
                  "key": "uniqueId"
```

```
                }
            ],
            "pipelineId": "df-00627471SOVYZEXAMPLE",
            "name": "my-pipeline",
            "tags": []
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribePipelines en la Referencia de comandos de la AWS CLI.

`get-pipeline-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-pipeline-definition`.

AWS CLI

Obtención de una definición de canalización

En el ejemplo siguiente, se obtiene la definición de canalización para la canalización especificada.

```
aws datapipeline get-pipeline-definition --pipeline-id df-00627471SOVYZEXAMPLE
```

A continuación, se muestra un ejemplo de la salida:

```
{
  "parameters": [
      {
          "type": "AWS::S3::ObjectKey",
          "id": "myS3OutputLoc",
          "description": "S3 output folder"
      },
      {
          "default": "s3://us-east-1.elasticmapreduce.samples/pig-apache-logs/data",
          "type": "AWS::S3::ObjectKey",
          "id": "myS3InputLoc",
          "description": "S3 input folder"
      },
      {
          "default": "grep -rc \"GET\" ${INPUT1_STAGING_DIR}/* >
 ${OUTPUT1_STAGING_DIR}/output.txt",
```

```
          "type": "String",
          "id": "myShellCmd",
          "description": "Shell command to run"
      }
  ],
  "objects": [
      {
          "type": "Ec2Resource",
          "terminateAfter": "20 Minutes",
          "instanceType": "t1.micro",
          "id": "EC2ResourceObj",
          "name": "EC2ResourceObj"
      },
      {
          "name": "Default",
          "failureAndRerunMode": "CASCADE",
          "resourceRole": "DataPipelineDefaultResourceRole",
          "schedule": {
              "ref": "DefaultSchedule"
          },
          "role": "DataPipelineDefaultRole",
          "scheduleType": "cron",
          "id": "Default"
      },
      {
          "directoryPath": "#{myS3OutputLoc}/#{format(@scheduledStartTime, 'YYYY-MM-
dd-HH-mm-ss')}",
          "type": "S3DataNode",
          "id": "S3OutputLocation",
          "name": "S3OutputLocation"
      },
      {
          "directoryPath": "#{myS3InputLoc}",
          "type": "S3DataNode",
          "id": "S3InputLocation",
          "name": "S3InputLocation"
      },
      {
          "startAt": "FIRST_ACTIVATION_DATE_TIME",
          "name": "Every 15 minutes",
          "period": "15 minutes",
          "occurrences": "4",
          "type": "Schedule",
          "id": "DefaultSchedule"
```

```
      },
      {
          "name": "ShellCommandActivityObj",
          "command": "#{myShellCmd}",
          "output": {
              "ref": "S3OutputLocation"
          },
          "input": {
              "ref": "S3InputLocation"
          },
          "stage": "true",
          "type": "ShellCommandActivity",
          "id": "ShellCommandActivityObj",
          "runsOn": {
              "ref": "EC2ResourceObj"
          }
      }
  ],
  "values": {
      "myS3OutputLoc": "s3://amzn-s3-demo-bucket/",
      "myS3InputLoc": "s3://us-east-1.elasticmapreduce.samples/pig-apache-logs/
data",
      "myShellCmd": "grep -rc \"GET\" ${INPUT1_STAGING_DIR}/* >
 ${OUTPUT1_STAGING_DIR}/output.txt"
  }
}
```

- Para obtener detalles sobre la API, consulte GetPipelineDefinition en la Referencia de comandos de la AWS CLI.

`list-pipelines`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-pipelines`.

AWS CLI

Para enumerar sus canalizaciones

En este ejemplo, se enumeran sus canalizaciones:

```
aws datapipeline list-pipelines
```

A continuación, se muestra un ejemplo de la salida:

```
{
  "pipelineIdList": [
      {
          "id": "df-00627471SOVYZEXAMPLE",
          "name": "my-pipeline"
      },
      {
          "id": "df-09028963KNVMREXAMPLE",
          "name": "ImportDDB"
      },
      {
          "id": "df-0870198233ZYVEXAMPLE",
          "name": "CrossRegionDDB"
      },
      {
          "id": "df-00189603TB4MZEXAMPLE",
          "name": "CopyRedshift"
      }
  ]
}
```

- Para obtener detalles sobre la API, consulte ListPipelines en la Referencia de comandos de la AWS CLI.

`list-runs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-runs`.

AWS CLI

Ejemplo 1: cómo enumerar las ejecuciones de su canalización

En el siguiente ejemplo de `list-runs`, se enumeran las ejecuciones de la canalización especificada.

```
aws datapipeline list-runs --pipeline-id df-00627471SOVYZEXAMPLE
```

Salida:

```
    Name                          Scheduled Start        Status                    ID
                                                Started                Ended
```

```
 --------------------------------------------------------------------------------
1.  EC2ResourceObj             2015-04-12T17:33:02    CREATING
 @EC2ResourceObj_2015-04-12T17:33:02             2015-04-12T17:33:10
2.  S3InputLocation            2015-04-12T17:33:02    FINISHED
      @S3InputLocation_2015-04-12T17:33:02            2015-04-12T17:33:09
 2015-04-12T17:33:09
3.  S3OutputLocation           2015-04-12T17:33:02    WAITING_ON_DEPENDENCIES
 @S3OutputLocation_2015-04-12T17:33:02           2015-04-12T17:33:09
4.  ShellCommandActivityObj    2015-04-12T17:33:02    WAITING_FOR_RUNNER
 @ShellCommandActivityObj_2015-04-12T17:33:02    2015-04-12T17:33:09
```

Ejemplo 2: cómo enumerar las ejecuciones de la canalización entre las fechas especificadas

En el siguiente ejemplo de `list-runs`, se utiliza `--start-interval` para especificar las fechas que se van a incluir en la salida.

```
aws datapipeline list-runs --pipeline-id df-01434553B58A2SHZUKO5 --start-
interval 2017-10-07T00:00:00,2017-10-08T00:00:00
```

- Para obtener detalles sobre la API, consulte ListRuns en la Referencia de comandos de la AWS CLI.

`put-pipeline-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-pipeline-definition`.

AWS CLI

Carga de una definición de canalización

En este ejemplo, se carga la definición de canalización especificada en la canalización especificada:

```
aws datapipeline put-pipeline-definition --pipeline-id df-00627471SOVYZEXAMPLE --
pipeline-definition file://my-pipeline-definition.json
```

A continuación, se muestra un ejemplo de la salida:

```
{
```

```
  "validationErrors": [],
  "errored": false,
  "validationWarnings": []
}
```

- Para obtener detalles sobre la API, consulte PutPipelineDefinition en la Referencia de comandos de la AWS CLI.

`remove-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-tags`.

AWS CLI

Eliminación de una etiqueta de una canalización

En este ejemplo, se elimina la etiqueta especificada de la canalización especificada:

```
aws datapipeline remove-tags --pipeline-id df-00627471SOVYZEXAMPLE --tag-
keys environment
```

- Para obtener detalles sobre la API, consulte RemoveTags en la Referencia de comandos de la AWS CLI.

Ejemplos de DataSync que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con DataSync.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`update-location-azure-blob`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-location-azure-blob`.

AWS CLI

Actualización de su ubicación de transferencia con un agente nuevo

En el siguiente ejemplo de `update-location-object-storage`, se actualiza la ubicación de DataSync para Microsoft Azure Blob Storage con un agente nuevo.

```
aws datasync update-location-azure-blob \
    --location-arn arn:aws:datasync:us-west-2:123456789012:location/loc-
abcdef01234567890 \
    --agent-arns arn:aws:datasync:us-west-2:123456789012:agent/
agent-1234567890abcdef0 \
    --sas-configuration '{ \
        "Token": "sas-token-for-azure-blob-storage-access" \
    }'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Replacing your agent en la Guía del usuario de AWS DataSync.

- Para obtener detalles sobre la API, consulte UpdateLocationAzureBlob en la Referencia de comandos de la AWS CLI.

`update-location-hdfs`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-location-hdfs`.

AWS CLI

Actualización de su ubicación de transferencia con un agente nuevo

En el siguiente ejemplo de `update-location-hdfs`, se actualiza la ubicación de HDFS de DataSync con un agente nuevo. Solo necesitará las opciones `--kerberos-keytab` y `--kerberos-krb5-conf` si su clúster de HDFS utiliza la autenticación Kerberos.

```
aws datasync update-location-hdfs \
    --location-arn arn:aws:datasync:us-west-2:123456789012:location/loc-
abcdef01234567890 \
    --agent-arns arn:aws:datasync:us-west-2:123456789012:agent/
agent-1234567890abcdef0 \
    --kerberos-keytab file://hdfs.keytab
    --kerberos-krb5-conf file://krb5.conf
```

Contenido de `hdfs.keytab`:

```
N/A. The content of this file is encrypted and not human readable.
```

Contenido de `krb5.conf`:

```
[libdefaults]
    default_realm = EXAMPLE.COM
    dns_lookup_realm = false
    dns_lookup_kdc = false
    rdns = true
    ticket_lifetime = 24h
    forwardable = true
    udp_preference_limit = 1000000
    default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 des3-cbc-
sha1
    default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 des3-cbc-
sha1
    permitted_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 des3-cbc-
sha1

[realms]
    EXAMPLE.COM = {
      kdc = kdc1.example.com
      admin_server = krbadmin.example.com
      default_domain = example.com
    }

[domain_realm]
    .example.com = EXAMPLE.COM
    example.com = EXAMPLE.COM

[logging]
    kdc = FILE:/var/log/krb5kdc.log
```

```
    admin_server = FILE:/var/log/kerberos/kadmin.log
    default = FILE:/var/log/krb5libs.log
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Replacing your agent en la Guía del usuario de AWS DataSync.

- Para obtener detalles sobre la API, consulte UpdateLocationHdfs en la Referencia de comandos de la AWS CLI.

`update-location-nfs`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-location-nfs`.

AWS CLI

Actualización de su ubicación de transferencia con un agente nuevo

En el siguiente ejemplo de `update-location-nfs`, se actualiza la ubicación NFS de DataSync con un agente nuevo.

```
aws datasync update-location-nfs \
    --location-arn arn:aws:datasync:us-west-2:123456789012:location/loc-abcdef01234567890 \
    --on-prem-config AgentArns=arn:aws:datasync:us-west-2:123456789012:agent/agent-1234567890abcdef0
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Replacing your agent en la Guía del usuario de AWS DataSync.

- Para obtener detalles sobre la API, consulte UpdateLocationNfs en la Referencia de comandos de la AWS CLI.

`update-location-object-storage`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-location-object-storage`.

AWS CLI

Actualización de su ubicación de transferencia con un agente nuevo

En el siguiente ejemplo de `update-location-object-storage`, se actualiza la ubicación de almacenamiento de objetos de DataSync con un agente nuevo.

```
aws datasync update-location-object-storage \
    --location-arn arn:aws:datasync:us-west-2:123456789012:location/loc-abcdef01234567890 \
    --agent-arns arn:aws:datasync:us-west-2:123456789012:agent/agent-1234567890abcdef0 \
    --secret-key secret-key-for-object-storage
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Replacing your agent en la Guía del usuario de AWS DataSync.

- Para obtener detalles sobre la API, consulte UpdateLocationObjectStorage en la Referencia de comandos de la AWS CLI.

`update-location-smb`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-location-smb`.

AWS CLI

Actualización de su ubicación de transferencia con un agente nuevo

En el siguiente ejemplo de `update-location-smb`, se actualiza la ubicación de SMB de DataSync con un agente nuevo.

```
aws datasync update-location-smb \
    --location-arn arn:aws:datasync:us-west-2:123456789012:location/loc-abcdef01234567890 \
    --agent-arns arn:aws:datasync:us-west-2:123456789012:agent/agent-1234567890abcdef0 \
    --password smb-file-server-password
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Replacing your agent en la Guía del usuario de AWS DataSync.

- Para obtener detalles sobre la API, consulte UpdateLocationSmb en la Referencia de comandos de la AWS CLI.

Ejemplos de DAX que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando la con AWS Command Line Interface.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-cluster`.

AWS CLI

Creación de un clúster de DAX

En el siguiente ejemplo de `create-cluster`, se crea un clúster de DAX con la configuración especificada.

```
aws dax create-cluster \
    --cluster-name daxcluster \
    --node-type dax.r4.large \
    --replication-factor 3 \
    --iam-role-arn roleARN  \
    --sse-specification Enabled=true
```

Salida:

```
{
    "Cluster": {
```

```
        "ClusterName": "daxcluster",
        "ClusterArn": "arn:aws:dax:us-west-2:123456789012:cache/daxcluster",
        "TotalNodes": 3,
        "ActiveNodes": 0,
        "NodeType": "dax.r4.large",
        "Status": "creating",
        "ClusterDiscoveryEndpoint": {
            "Port": 8111
        },
        "PreferredMaintenanceWindow": "thu:13:00-thu:14:00",
        "SubnetGroup": "default",
        "SecurityGroups": [
            {
                "SecurityGroupIdentifier": "sg-1af6e36e",
                "Status": "active"
            }
        ],
        "IamRoleArn": "arn:aws:iam::123456789012:role/
DAXServiceRoleForDynamoDBAccess",
        "ParameterGroup": {
            "ParameterGroupName": "default.dax1.0",
            "ParameterApplyStatus": "in-sync",
            "NodeIdsToReboot": []
        },
        "SSEDescription": {
            "Status": "ENABLED"
        }
    }
}
```

Para obtener más información, consulte Paso 3: crear un clúster de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte CreateCluster en la Referencia de comandos de la AWS CLI.

`create-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-parameter-group`.

AWS CLI

Para crear un grupo de parámetros

En el siguiente ejemplo de create-parameter-group, se crea un grupo de parámetros con la configuración especificada.

```
aws dax create-parameter-group \
    --parameter-group-name daxparametergroup \
    --description "A new parameter group"
```

Salida:

```
{
    "ParameterGroup": {
        "ParameterGroupName": "daxparametergroup",
        "Description": "A new parameter group"
    }
}
```

Para obtener más información, consulte Administración de los clústeres de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte CreateParameterGroup en la Referencia de comandos de la AWS CLI.

`create-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-subnet-group`.

AWS CLI

Creación de un grupo de subredes de DAX

En el siguiente ejemplo de `create-subnet-group`, se crea un grupo de subredes con la configuración especificada.

```
aws dax create-subnet-group \
    --subnet-group-name daxSubnetGroup \
    --subnet-ids subnet-11111111 subnet-22222222
```

Salida:

```
{
    "SubnetGroup": {
        "SubnetGroupName": "daxSubnetGroup",
```

```
        "VpcId": "vpc-05a1fa8e00c325226",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-11111111",
                "SubnetAvailabilityZone": "us-west-2b"
            },
            {
                "SubnetIdentifier": "subnet-22222222",
                "SubnetAvailabilityZone": "us-west-2c"
            }
        ]
    }
}
```

Para obtener más información, consulte Paso 2: crear un grupo de subredes en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte CreateSubnetGroup en la Referencia de comandos de la AWS CLI.

`decrease-replication-factor`

En el siguiente ejemplo de código, se muestra cómo utilizar `decrease-replication-factor`.

AWS CLI

Eliminación de uno o varios nodos del clúster

En el siguiente ejemplo de `decrease-replication-factor`, se reduce a uno el número de nodos en el clúster de DAX especificado.

```
aws dax decrease-replication-factor \
    --cluster-name daxcluster \
    --new-replication-factor 1
```

Salida:

```
{
    "Cluster": {
        "ClusterName": "daxcluster",
        "ClusterArn": "arn:aws:dax:us-west-2:123456789012:cache/daxcluster",
        "TotalNodes": 3,
        "ActiveNodes": 3,
```

```
        "NodeType": "dax.r4.large",
        "Status": "modifying",
        "ClusterDiscoveryEndpoint": {
            "Address": "daxcluster.ey3o9d.clustercfg.dax.usw2.cache.amazonaws.com",
            "Port": 8111
        },
        "Nodes": [
            {
                "NodeId": "daxcluster-a",
                "Endpoint": {
                    "Address": "daxcluster-
a.ey3o9d.0001.dax.usw2.cache.amazonaws.com",
                    "Port": 8111
                },
                "NodeCreateTime": 1576625059.509,
                "AvailabilityZone": "us-west-2c",
                "NodeStatus": "available",
                "ParameterGroupStatus": "in-sync"
            },
            {
                "NodeId": "daxcluster-b",
                "Endpoint": {
                    "Address": "daxcluster-
b.ey3o9d.0001.dax.usw2.cache.amazonaws.com",
                    "Port": 8111
                },
                "NodeCreateTime": 1576625059.509,
                "AvailabilityZone": "us-west-2a",
                "NodeStatus": "available",
                "ParameterGroupStatus": "in-sync"
            },
            {
                "NodeId": "daxcluster-c",
                "Endpoint": {
                    "Address": "daxcluster-
c.ey3o9d.0001.dax.usw2.cache.amazonaws.com",
                    "Port": 8111
                },
                "NodeCreateTime": 1576625059.509,
                "AvailabilityZone": "us-west-2b",
                "NodeStatus": "available",
                "ParameterGroupStatus": "in-sync"
            }
        ],
```

```
        "PreferredMaintenanceWindow": "thu:13:00-thu:14:00",
        "SubnetGroup": "default",
        "SecurityGroups": [
            {
                "SecurityGroupIdentifier": "sg-1af6e36e",
                "Status": "active"
            }
        ],
        "IamRoleArn": "arn:aws:iam::123456789012:role/
DAXServiceRoleForDynamoDBAccess",
        "ParameterGroup": {
            "ParameterGroupName": "default.dax1.0",
            "ParameterApplyStatus": "in-sync",
            "NodeIdsToReboot": []
        },
        "SSEDescription": {
            "Status": "ENABLED"
        }
    }
}
```

Para obtener más información, consulte Administración de los clústeres de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte DecreaseReplicationFactor en la Referencia de comandos de la AWS CLI.

`delete-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-cluster`.

AWS CLI

Eliminación de un clúster de DAX

En el siguiente ejemplo de `delete-cluster`, se elimina el clúster de DAX especificado.

```
aws dax delete-cluster \
    --cluster-name daxcluster
```

Salida:

```
{
```

```
    "Cluster": {
        "ClusterName": "daxcluster",
        "ClusterArn": "arn:aws:dax:us-west-2:123456789012:cache/daxcluster",
        "TotalNodes": 3,
        "ActiveNodes": 0,
        "NodeType": "dax.r4.large",
        "Status": "deleting",
        "ClusterDiscoveryEndpoint": {
            "Address": "dd.ey3o9d.clustercfg.dax.usw2.cache.amazonaws.com",
            "Port": 8111
        },
        "PreferredMaintenanceWindow": "fri:06:00-fri:07:00",
        "SubnetGroup": "default",
        "SecurityGroups": [
            {
                "SecurityGroupIdentifier": "sg-1af6e36e",
                "Status": "active"
            }
        ],
        "IamRoleArn": "arn:aws:iam::123456789012:role/
DAXServiceRoleForDynamoDBAccess",
        "ParameterGroup": {
            "ParameterGroupName": "default.dax1.0",
            "ParameterApplyStatus": "in-sync",
            "NodeIdsToReboot": []
        },
        "SSEDescription": {
            "Status": "ENABLED"
        }
    }
}
```

Para obtener más información, consulte Administración de los clústeres de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte DeleteCluster en la Referencia de comandos de la AWS CLI.

`delete-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-parameter-group`.

AWS CLI

Para eliminar un grupo de parámetros

En el siguiente ejemplo de `delete-parameter-group`, se elimina el grupo de parámetros de DAX especificado.

```
aws dax  delete-parameter-group \
    --parameter-group-name daxparametergroup
```

Salida:

```
{
    "DeletionMessage": "Parameter group daxparametergroup has been deleted."
}
```

Para obtener más información, consulte Administración de los clústeres de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte DeleteParameterGroup en la Referencia de comandos de la AWS CLI.

`delete-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-subnet-group`.

AWS CLI

Para eliminar un grupo de subredes

En el siguiente ejemplo de `delete-subnet-group`, se elimina el grupo de subredes de DAX especificado.

```
aws dax delete-subnet-group \
    --subnet-group-name daxSubnetGroup
```

Salida:

```
{
    "DeletionMessage": "Subnet group daxSubnetGroup has been deleted."
```

```
}
```

Para obtener más información, consulte Administración de los clústeres de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte DeleteSubnetGroup en la Referencia de comandos de la AWS CLI.

`describe-clusters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-clusters`.

AWS CLI

Devolución de información acerca de todos los clústeres de DAX aprovisionados

En el siguiente ejemplo de `describe-clusters`, se muestran detalles acerca de los clústeres de DAX aprovisionados.

```
aws dax describe-clusters
```

Salida:

```
{
    "Clusters": [
        {
            "ClusterName": "daxcluster",
            "ClusterArn": "arn:aws:dax:us-west-2:123456789012:cache/daxcluster",
            "TotalNodes": 1,
            "ActiveNodes": 1,
            "NodeType": "dax.r4.large",
            "Status": "available",
            "ClusterDiscoveryEndpoint": {
                "Address":
 "daxcluster.ey3o9d.clustercfg.dax.usw2.cache.amazonaws.com",
                "Port": 8111
            },
            "Nodes": [
                {
                    "NodeId": "daxcluster-a",
                    "Endpoint": {
                        "Address": "daxcluster-
a.ey3o9d.0001.dax.usw2.cache.amazonaws.com",
```

```
                        "Port": 8111
                    },
                    "NodeCreateTime": 1576625059.509,
                    "AvailabilityZone": "us-west-2c",
                    "NodeStatus": "available",
                    "ParameterGroupStatus": "in-sync"
                }
            ],
            "PreferredMaintenanceWindow": "thu:13:00-thu:14:00",
            "SubnetGroup": "default",
            "SecurityGroups": [
                {
                    "SecurityGroupIdentifier": "sg-1af6e36e",
                    "Status": "active"
                }
            ],
            "IamRoleArn": "arn:aws:iam::123456789012:role/
DAXServiceRoleForDynamoDBAccess",
            "ParameterGroup": {
                "ParameterGroupName": "default.dax1.0",
                "ParameterApplyStatus": "in-sync",
                "NodeIdsToReboot": []
            },
            "SSEDescription": {
                "Status": "ENABLED"
            }
        }
    ]
}
```

Para obtener más información, consulte Administración de los clústeres de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte DescribeClusters en la Referencia de comandos de la AWS CLI.

`describe-default-parameters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-default-parameters`.

AWS CLI

Devolución de información de parámetros del sistema predeterminado para DAX

En el siguiente ejemplo de `describe-default-parameters`, se muestra información de parámetros del sistema predeterminado para DAX.

```
aws dax describe-default-parameters
```

Salida:

```
{
    "Parameters": [
        {
            "ParameterName": "query-ttl-millis",
            "ParameterType": "DEFAULT",
            "ParameterValue": "300000",
            "NodeTypeSpecificValues": [],
            "Description": "Duration in milliseconds for queries to remain cached",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": "TRUE",
            "ChangeType": "IMMEDIATE"
        },
        {
            "ParameterName": "record-ttl-millis",
            "ParameterType": "DEFAULT",
            "ParameterValue": "300000",
            "NodeTypeSpecificValues": [],
            "Description": "Duration in milliseconds for records to remain valid in
 cache (Default: 0 = infinite)",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": "TRUE",
            "ChangeType": "IMMEDIATE"
        }
    ]
}
```

Para obtener más información, consulte Administración de los clústeres de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte DescribeDefaultParameters en la Referencia de comandos de la AWS CLI.

describe-events

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-events`.

AWS CLI

Devolución de todos los eventos relacionados con clústeres y grupos de parámetros de DAX

En el siguiente ejemplo de `describe-events`, se muestran detalles de los eventos relacionados con los grupos de parámetros y clústeres de DAX.

```
aws dax describe-events
```

Salida:

```
{
    "Events": [
        {
            "SourceName": "daxcluster",
            "SourceType": "CLUSTER",
            "Message": "Cluster deleted.",
            "Date": 1576702736.706
        },
        {
            "SourceName": "daxcluster",
            "SourceType": "CLUSTER",
            "Message": "Removed node daxcluster-b.",
            "Date": 1576702691.738
        },
        {
            "SourceName": "daxcluster",
            "SourceType": "CLUSTER",
            "Message": "Removed node daxcluster-a.",
            "Date": 1576702633.498
        },
        {
            "SourceName": "daxcluster",
            "SourceType": "CLUSTER",
            "Message": "Removed node daxcluster-c.",
            "Date": 1576702631.329
        },
        {
            "SourceName": "daxcluster",
```

```
            "SourceType": "CLUSTER",
            "Message": "Cluster created.",
            "Date": 1576626560.057
        }
    ]
}
```

Para obtener más información, consulte Administración de los clústeres de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte DescribeEvents en la Referencia de comandos de la AWS CLI.

`describe-parameter-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-parameter-groups`.

AWS CLI

Descripción de los grupos de parámetros definidos en DAX

En el siguiente ejemplo de `describe-parameter-groups`, se recuperan los detalles sobre los grupos de parámetros definidos en DAX.

```
aws dax describe-parameter-groups
```

Salida:

```
{
    "ParameterGroups": [
        {
            "ParameterGroupName": "default.dax1.0",
            "Description": "Default parameter group for dax1.0"
        }
    ]
}
```

Para obtener más información, consulte Administración de los clústeres de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte DescribeParameterGroups en la Referencia de comandos de la AWS CLI.

describe-parameters

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-parameters`.

AWS CLI

Descripción de los parámetros definidos en un grupo de parámetros de DAX

En el siguiente ejemplo de `describe-parameters`, se recupera información sobre los parámetros definidos en el grupo de parámetros de DAX especificado.

```
aws dax describe-parameters \
    --parameter-group-name default.dax1.0
```

Salida:

```
{
    "Parameters": [
        {
            "ParameterName": "query-ttl-millis",
            "ParameterType": "DEFAULT",
            "ParameterValue": "300000",
            "NodeTypeSpecificValues": [],
            "Description": "Duration in milliseconds for queries to remain cached",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": "TRUE",
            "ChangeType": "IMMEDIATE"
        },
        {
            "ParameterName": "record-ttl-millis",
            "ParameterType": "DEFAULT",
            "ParameterValue": "300000",
            "NodeTypeSpecificValues": [],
            "Description": "Duration in milliseconds for records to remain valid in
 cache (Default: 0 = infinite)",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": "TRUE",
            "ChangeType": "IMMEDIATE"
        }
```

```
    ]
}
```

Para obtener más información, consulte Administración de los clústeres de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte DescribeParameters en la Referencia de comandos de la AWS CLI.

`describe-subnet-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-subnet-groups`.

AWS CLI

Descripción de los grupos de subredes definidos en DAX

En el siguiente ejemplo de `describe-subnet-groups`, se recupera la información de los grupos de subredes definidos en DAX.

```
aws dax describe-subnet-groups
```

Salida:

```
{
    "SubnetGroups": [
        {
            "SubnetGroupName": "default",
            "Description": "Default CacheSubnetGroup",
            "VpcId": "vpc-ee70a196",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-874953af",
                    "SubnetAvailabilityZone": "us-west-2d"
                },
                {
                    "SubnetIdentifier": "subnet-bd3d1fc4",
                    "SubnetAvailabilityZone": "us-west-2a"
                },
                {
                    "SubnetIdentifier": "subnet-72c2ff28",
                    "SubnetAvailabilityZone": "us-west-2c"
                },
```

```
                {
                    "SubnetIdentifier": "subnet-09e6aa42",
                    "SubnetAvailabilityZone": "us-west-2b"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Administración de los clústeres de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte DescribeSubnetGroups en la Referencia de comandos de la AWS CLI.

`increase-replication-factor`

En el siguiente ejemplo de código, se muestra cómo utilizar `increase-replication-factor`.

AWS CLI

Aumento del factor de replicación de un clúster de DAX

En el siguiente ejemplo de `increase-replication-factor`, se aumenta a 3 el factor de replicación del clúster DAX especificado.

```
aws dax increase-replication-factor \
    --cluster-name daxcluster \
    --new-replication-factor 3
```

Salida:

```
{
    "Cluster": {
        "ClusterName": "daxcluster",
        "ClusterArn": "arn:aws:dax:us-west-2:123456789012:cache/daxcluster",
        "TotalNodes": 3,
        "ActiveNodes": 1,
        "NodeType": "dax.r4.large",
        "Status": "modifying",
        "ClusterDiscoveryEndpoint": {
            "Address": "daxcluster.ey3o9d.clustercfg.dax.usw2.cache.amazonaws.com",
            "Port": 8111
```

```
        },
        "Nodes": [
            {
                "NodeId": "daxcluster-a",
                "Endpoint": {
                    "Address": "daxcluster-
a.ey3o9d.0001.dax.usw2.cache.amazonaws.com",
                    "Port": 8111
                },
                "NodeCreateTime": 1576625059.509,
                "AvailabilityZone": "us-west-2c",
                "NodeStatus": "available",
                "ParameterGroupStatus": "in-sync"
            },
            {
                "NodeId": "daxcluster-b",
                "NodeStatus": "creating"
            },
            {
                "NodeId": "daxcluster-c",
                "NodeStatus": "creating"
            }
        ],
        "PreferredMaintenanceWindow": "thu:13:00-thu:14:00",
        "SubnetGroup": "default",
        "SecurityGroups": [
            {
                "SecurityGroupIdentifier": "sg-1af6e36e",
                "Status": "active"
            }
        ],
        "IamRoleArn": "arn:aws:iam::123456789012:role/
DAXServiceRoleForDynamoDBAccess",
        "ParameterGroup": {
            "ParameterGroupName": "default.dax1.0",
            "ParameterApplyStatus": "in-sync",
            "NodeIdsToReboot": []
        },
        "SSEDescription": {
            "Status": "ENABLED"
        }
    }
}
```

Para obtener más información, consulte Administración de los clústeres de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte IncreaseReplicationFactor en la Referencia de comandos de la AWS CLI.

`list-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags`.

AWS CLI

Para enumerar etiquetas de un recurso de DAX

En el siguiente ejemplo de `list-tags`, se enumeran las claves y los valores de las etiquetas adjuntos al clúster de DAX especificado.

```
aws dax list-tags \
    --resource-name arn:aws:dax:us-west-2:123456789012:cache/daxcluster
```

Salida:

```
{
    "Tags": [
        {
            "Key": "ClusterUsage",
            "Value": "prod"
        }
    ]
}
```

Para obtener más información, consulte Administración de los clústeres de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener más información sobre la API, consulte ListTags en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Etiquetado de un recurso de DAX

En el siguiente ejemplo de `tag-resource`, se asocia el nombre de la clave de etiqueta especificada y el valor asociado al clúster de DAX especificado para describir el uso del clúster.

```
aws dax tag-resource \
    --resource-name arn:aws:dax:us-west-2:123456789012:cache/daxcluster \
    --tags="Key=ClusterUsage,Value=prod"
```

Salida:

```
{
    "Tags": [
        {
            "Key": "ClusterUsage",
            "Value": "prod"
        }
    ]
}
```

Para obtener más información, consulte Administración de los clústeres de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de etiquetas de un recurso de DAX

En el siguiente ejemplo de `untag-resource`, se elimina la etiqueta con un nombre de clave especificado de un clúster de DAX.

```
aws dax untag-resource  \
```

```
    --resource-name arn:aws:dax:us-west-2:123456789012:cache/daxcluster \
    --tag-keys="ClusterUsage"
```

Salida:

```
{
    "Tags": []
}
```

Para obtener más información, consulte Administración de los clústeres de DAX en la Guía para desarrolladores de Amazon DynamoDB.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

Ejemplos de Detective que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Detective.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`accept-invitation`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-invitation`.

AWS CLI

Aceptación de una invitación para ser una cuenta miembro de un gráfico de comportamiento

En el siguiente ejemplo de `accept-invitation`, se acepta una invitación para convertirse en una cuenta miembro de un gráfico de comportamiento arn:aws:detective:us-east-1:111122223333:graph:123412341234.

```
aws detective accept-invitation \
    --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Responding to a behavior graph invitation en la Guía de administración de Amazon Detective.

- Para obtener detalles sobre la API, consulte AcceptInvitation en la Referencia de comandos de la AWS CLI.

`create-graph`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-graph`.

AWS CLI

Activación de Amazon Detective y creación de un nuevo gráfico de comportamiento

En el siguiente ejemplo de `create-graph`, se habilita Detective para la cuenta de AWS que ejecuta el comando en la región en la que se ejecuta el comando. Se crea un nuevo gráfico de comportamiento que tiene esa cuenta como cuenta de administrador. El comando también asigna el valor Finance a la etiqueta Department.

```
aws detective create-graph \
    --tags '{"Department": "Finance"}'
```

Salida:

```
{
    "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
}
```

Para obtener más información, consulte Enabling Amazon Detective en la Guía de administración de Amazon Detective.

- Para obtener detalles sobre la API, consulte CreateGraph en la Referencia de comandos de la AWS CLI.

`create-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-members`.

AWS CLI

Invitación de cuentas de miembros a un gráfico de comportamiento

En el siguiente ejemplo de `create-members`, se invita a dos cuentas de AWS para convertirse en una cuenta miembro de un gráfico de comportamiento arn:aws:detective:us-east-1:111122223333:graph:123412341234. Por cada cuenta, la solicitud proporciona el identificador de la cuenta de AWS y la dirección de correo electrónico del usuario raíz. La solicitud incluye un mensaje personalizado para insertarlo en el correo electrónico de invitación.

```
aws detective create-members \
    --
accounts AccountId=444455556666,EmailAddress=mmajor@example.com AccountId=123456789012,Email
 \
    --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 \
    --message "This is Paul Santos. I need to add your account to the data we use
 for security investigation in Amazon Detective. If you have any questions, contact
 me at psantos@example.com."
```

Salida:

```
{
    "Members": [
    {
        "AccountId": "444455556666",
        "AdministratorId": "111122223333",
        "EmailAddress": "mmajor@example.com",
        "GraphArn": "arn:aws:detective:us-east-1:111122223333:graph:123412341234",
        "InvitedTime": 1579826107000,
        "MasterId": "111122223333",
        "Status": "INVITED",
        "UpdatedTime": 1579826107000
   },
   {
        "AccountId": "123456789012",
```

```
        "AdministratorId": "111122223333",
        "EmailAddress": "jstiles@example.com",
        "GraphArn": "arn:aws:detective:us-east-1:111122223333:graph:123412341234",
        "InvitedTime": 1579826107000,
        "MasterId": "111122223333",
        "Status": "VERIFICATION_IN_PROGRESS",
        "UpdatedTime": 1579826107000
     }
    ],
    "UnprocessedAccounts": [ ]
}
```

Para obtener más información, consulte Inviting member accounts to a behavior graph<https://docs.aws.amazon.com/detective/latest/adminguide/graph-admin-add-member-accounts.html> en la Guía de administración de Amazon Detective.

Invitación a cuentas de miembros sin enviar correos electrónicos de invitación

En el siguiente ejemplo de `create-members`, se invita a dos cuentas de AWS para convertirse en una cuenta miembro de un gráfico de comportamiento arn:aws:detective:us-east-1:111122223333:graph:123412341234. Por cada cuenta, la solicitud proporciona el identificador de la cuenta de AWS y la dirección de correo electrónico del usuario raíz. Las cuentas de los miembros no reciben correos electrónicos de invitación.

```
aws detective create-members \
    --
accounts AccountId=444455556666,EmailAddress=mmajor@example.com AccountId=123456789012,Email
 \
    --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 \
    --disable-email-notification
```

Salida:

```
{
    "Members": [
    {
        "AccountId": "444455556666",
        "AdministratorId": "111122223333",
        "EmailAddress": "mmajor@example.com",
        "GraphArn": "arn:aws:detective:us-east-1:111122223333:graph:123412341234",
        "InvitedTime": 1579826107000,
        "MasterId": "111122223333",
```

```
        "Status": "INVITED",
        "UpdatedTime": 1579826107000
    },
    {
        "AccountId": "123456789012",
        "AdministratorId": "111122223333",
        "EmailAddress": "jstiles@example.com",
        "GraphArn": "arn:aws:detective:us-east-1:111122223333:graph:123412341234",
        "InvitedTime": 1579826107000,
        "MasterId": "111122223333",
        "Status": "VERIFICATION_IN_PROGRESS",
        "UpdatedTime": 1579826107000
     }
    ],
    "UnprocessedAccounts": [ ]
}
```

Para obtener más información, consulte Inviting member accounts to a behavior graph<https://docs.aws.amazon.com/detective/latest/adminguide/graph-admin-add-member-accounts.html> en la Guía de administración de Amazon Detective.

- Para obtener detalles sobre la API, consulte CreateMembers en la Referencia de comandos de la AWS CLI.

`delete-graph`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-graph`.

AWS CLI

Deshabilitación de Detective y eliminación del gráfico de comportamiento

En el siguiente ejemplo de `delete-graph`, se desactiva Detective y se elimina el gráfico de comportamiento especificado.

```
aws detective delete-graph \
    --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Disabling Amazon Detective en la Guía de administración de Amazon Detective.

- Para obtener detalles sobre la API, consulte DeleteGraph en la Referencia de comandos de la AWS CLI.

`delete-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-members`.

AWS CLI

Eliminación de cuentas de miembro de un gráfico de comportamiento

En el siguiente ejemplo de `delete-members`, se eliminan dos cuentas de miembro del gráfico de comportamiento arn:aws:detective:us-east-1:111122223333:graph:123412341234. Para identificar las cuentas, la solicitud proporciona los identificadores de las cuentas de AWS.

```
aws detective delete-members \
    --account-ids 444455556666 123456789012 \
    --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Salida:

```
 {
    "AccountIds": [ "444455556666", "123456789012" ],
    "UnprocessedAccounts": [ ]
}
```

Para obtener más información, consulte Removing member accounts from a behavior graph<https://docs.aws.amazon.com/detective/latest/adminguide/graph-admin-remove-member-accounts.html> en la Guía de administración de Amazon Detective.

- Para obtener detalles sobre la API, consulte DeleteMembers en la Referencia de comandos de la AWS CLI.

`disassociate-membership`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-membership`.

AWS CLI

Renuncia de pertenencia a un gráfico de comportamiento

En el siguiente ejemplo de disassociate-membership, se elimina la cuenta de AWS que ejecuta el comando en el gráfico de comportamiento arn:aws:detective:us-east-1:111122223333:graph:123412341234.

```
aws detective disassociate-membership \
     --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Para obtener más información, consulte Removing your account from a behavior graph<https://docs.aws.amazon.com/detective/latest/adminguide/member-remove-self-from-graph.html> en la Guía de administración de Amazon Detective.

- Para obtener detalles sobre la API, consulte DisassociateMembership en la Referencia de comandos de la AWS CLI.

`get-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-members`.

AWS CLI

Recuperación de información sobre las cuentas de los miembros seleccionadas

En el siguiente ejemplo de `get-members`, se recupera información sobre dos cuentas de miembro del gráfico de comportamiento arn:aws:detective:us-east-1:111122223333:graph:123412341234. En el caso de ambas cuentas, la solicitud proporciona los identificadores de las cuentas de AWS.

```
aws detective get-members \
    --account-ids 444455556666 123456789012 \
    --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Salida:

```
{
    "MemberDetails": [
    {
        "AccountId": "444455556666",
        "AdministratorId": "111122223333",
        "EmailAddress": "mmajor@example.com",
        "GraphArn": "arn:aws:detective:us-east-1:111122223333:graph:123412341234",
        "InvitedTime": 1579826107000,
```

```
        "MasterId": "111122223333",
        "Status": "INVITED",
        "UpdatedTime": 1579826107000
    }
    {
        "AccountId": "123456789012",
        "AdministratorId": "111122223333",
        "EmailAddress": "jstiles@example.com",
        "GraphArn": "arn:aws:detective:us-east-1:111122223333:graph:123412341234",
        "InvitedTime": 1579826107000,
        "MasterId": "111122223333",
        "Status": "INVITED",
        "UpdatedTime": 1579826107000
    }
],
    "UnprocessedAccounts": [ ]
}
```

Para obtener más información, consulte Viewing the list of accounts in a behavior graph<https://docs.aws.amazon.com/detective/latest/adminguide/graph-admin-view-accounts.html> en la Guía de administración de Amazon Detective.

- Para obtener detalles sobre la API, consulte GetMembers en la Referencia de comandos de la AWS CLI.

`list-graphs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-graphs`.

AWS CLI

Visualización de una lista de los gráficos de comportamiento que administra su cuenta

En el siguiente ejemplo de `list-graphs`, se recuperan los gráficos de comportamiento que administra su cuenta en la región actual.

```
aws detective list-graphs
```

Salida:

```
{
    "GraphList": [
```

```
        {
            "Arn": "arn:aws:detective:us-east-1:111122223333:graph:123412341234",
            "CreatedTime": 1579736111000
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte ListGraphs en la Referencia de comandos de la AWS CLI.

`list-invitations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-invitations`.

AWS CLI

Visualización de una lista de gráficos de comportamiento de los que una cuenta es miembro o a los que está invitada

En el siguiente ejemplo de `list-invitations`, se recuperan los gráficos de comportamiento a los que se ha invitado a la cuenta que realiza la llamada. Los resultados incluyen solo las invitaciones abiertas y aceptadas. No incluyen las invitaciones rechazadas ni las suscripciones eliminadas.

```
aws detective list-invitations
```

Salida:

```
{
    "Invitations": [
    {
        "AccountId": "444455556666",
        "AdministratorId": "111122223333",
        "EmailAddress": "mmajor@example.com",
        "GraphArn": "arn:aws:detective:us-east-1:111122223333:graph:123412341234",
        "InvitedTime": 1579826107000,
        "MasterId": "111122223333",
        "Status": "INVITED",
        "UpdatedTime": 1579826107000
    }
]
```

```
}
```

Para obtener más información, consulte Viewing your list of behavior graph invitations<https://docs.aws.amazon.com/detective/latest/adminguide/member-view-graph-invitations.html> en la Guía de administración de Amazon Detective.

- Para obtener detalles sobre la API, consulte ListInvitations en la Referencia de comandos de la AWS CLI.

`list-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-members`.

AWS CLI

Para enumerar las cuentas de miembros de un gráfico de comportamiento

En el siguiente ejemplo de `list-members`, se recuperan las cuentas de los miembros invitados y habilitados para el gráfico de comportamiento de `arn:aws:detective:us-east-1:111122223333:graph:123412341234`. Los resultados no incluyen las cuentas de miembro eliminadas.

```
aws detective list-members \
    --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Salida:

```
{
    "MemberDetails": [
        {
            "AccountId": "444455556666",
            "AdministratorId": "111122223333",
            "EmailAddress": "mmajor@example.com",
            "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:123412341234",
            "InvitedTime": 1579826107000,
            "MasterId": "111122223333",
            "Status": "INVITED",
            "UpdatedTime": 1579826107000
        },
        {
            "AccountId": "123456789012",
```

```
            "AdministratorId": "111122223333",
            "EmailAddress": "jstiles@example.com",
            "GraphArn": "arn:aws:detective:us-
east-1:111122223333:graph:123412341234",
            "InvitedTime": 1579826107000,
            "MasterId": "111122223333",
            "PercentOfGraphUtilization": 2,
            "PercentOfGraphUtilizationUpdatedTime": 1586287843,
            "Status": "ENABLED",
            "UpdatedTime": 1579973711000,
            "VolumeUsageInBytes": 200,
            "VolumeUsageUpdatedTime": 1586287843
        }
    ]
}
```

Para obtener más información, consulte Viewing the list of accounts in a behavior graph en la Guía de administración de Amazon Detective.

- Para obtener detalles sobre la API, consulte ListMembers en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Recuperación de las etiquetas asignadas a un gráfico de comportamiento

En el ejemplo siguiente de `list-tags-for-resource`, se devuelven las etiquetas asignadas al gráfico de comportamiento especificado.

```
aws detective list-tags-for-resource \
    --resource-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Salida:

```
{
    "Tags": {
        "Department" : "Finance"
    }
```

```
}
```

Para obtener más información, consulte Managing tags for a behavior graph en la Guía de administración de Amazon Detective.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`reject-invitation`

En el siguiente ejemplo de código, se muestra cómo utilizar `reject-invitation`.

AWS CLI

Rechazo de una invitación para ser una cuenta miembro de un gráfico de comportamiento

En el siguiente ejemplo de `reject-invitation`, se rechaza una invitación para convertirse en una cuenta miembro de un gráfico de comportamiento arn:aws:detective:us-east-1:111122223333:graph:123412341234.

```
aws detective reject-invitation \
    --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Responding to a behavior graph invitation<https://docs.aws.amazon.com/detective/latest/adminguide/member-invitation-response.html> en la Guía de administración de Amazon Detective.

- Para obtener detalles sobre la API, consulte RejectInvitation en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Asignación de una etiqueta a un recurso

En el siguiente ejemplo de `tag-resource`, se asigna un valor para la etiqueta Department al gráfico de comportamiento especificado.

```
aws detective tag-resource \
    --resource-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 \
    --tags '{"Department":"Finance"}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing tags for a behavior graph en la Guía de administración de Amazon Detective.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de un valor de etiqueta de un recurso

En el siguiente ejemplo de `untag-resource`, se elimina la etiqueta Department del gráfico de comportamiento especificado.

```
aws detective untag-resource \
    --resource-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 \
    --tag-keys "Department"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing tags for a behavior graph en la Guía de administración de Amazon Detective.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

Ejemplos de Device Farm que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Device Farm.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-device-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-device-pool`.

AWS CLI

Creación de un grupo de dispositivos

El siguiente comando crea un grupo de dispositivos Android para un proyecto:

```
aws devicefarm create-device-pool --name pool1 --rules file://
device-pool-rules.json --project-arn "arn:aws:devicefarm:us-
west-2:123456789012:project:070fc3ca-7ec1-4741-9c1f-d3e044efc506"
```

Puede obtener el ARN del proyecto a partir de la salida de `create-project` o `list-projects`. El archivo `device-pool-rules.json` es un documento JSON en la carpeta actual que especifica la plataforma del dispositivo:

```
[
    {
        "attribute": "PLATFORM",
        "operator": "EQUALS",
        "value": "\"ANDROID\""
    }
]
```

Salida:

```
{
    "devicePool": {
        "rules": [
            {
                "operator": "EQUALS",
                "attribute": "PLATFORM",
                "value": "\"ANDROID\""
            }
        ],
        "type": "PRIVATE",
        "name": "pool1",
        "arn": "arn:aws:devicefarm:us-
west-2:123456789012:devicepool:070fc3ca-7ec1-4741-9c1f-
d3e044efc506/2aa8d2a9-5e73-47ca-b929-659cb34b7dcd"
    }
}
```

- Para obtener detalles sobre la API, consulte CreateDevicePool en la Referencia de comandos de la AWS CLI.

`create-project`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-project`.

AWS CLI

Creación de un proyecto

El comando siguiente crea un nuevo proyecto llamado `my-project`:

```
aws devicefarm create-project --name my-project
```

Salida:

```
{
    "project": {
        "name": "myproject",
        "arn": "arn:aws:devicefarm:us-
west-2:123456789012:project:070fc3ca-7ec1-4741-9c1f-d3e044efc506",
        "created": 1503612890.057
    }
```

```
}
```

- Para obtener información sobre la API, consulte CreateProject en la Referencia de comandos de la AWS CLI.

`create-upload`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-upload`.

AWS CLI

Creación de una carga

El siguiente comando crea una carga para una aplicación de Android:

```
aws devicefarm create-upload --project-arn "arn:aws:devicefarm:us-
west-2:123456789012:project:070fc3ca-7ec1-4741-9c1f-d3e044efc506" --name app.apk --
type ANDROID_APP
```

Puede obtener el ARN del proyecto a partir de la salida de create-project o list-projects.

Salida:

```
{
    "upload": {
        "status": "INITIALIZED",
        "name": "app.apk",
        "created": 1503614408.769,
        "url": "https://prod-us-west-2-uploads.s3-us-west-2.amazonaws.com/
arn%3Aaws%3Adevicefarm%3Aus-west-2%3A123456789012%3Aproject%3A070fc3ca-
c7e1-4471-91cf-d3e4efc50604/uploads/arn%3Aaws%3Adevicefarm%3Aus-
west-2%3A123456789012%3Aupload%3A070fc3ca-7ec1-4741-9c1f-d3e044efc506/dd72723a-
ae9e-4087-09e6-f4cea3599514/app.apk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Date=20170824T224008Z&X-Amz-SignedHeaders=host&X-Amz-Expires=86400&X-Amz-
Credential=AKIAEXAMPLEPBUMBC3GA%2F20170824%2Fus-west-2%2Fs3%2Faws4_request&X-Amz-
Signature=05050370c38894ef5bd09f5d009f36fc8f96fa4bb04e1bba9aca71b8dbe49a0f",
        "type": "ANDROID_APP",
        "arn": "arn:aws:devicefarm:us-
west-2:123456789012:upload:070fc3ca-7ec1-4741-9c1f-d3e044efc506/dd72723a-
ae9e-4087-09e6-f4cea3599514"
    }
```

```
}
```

Utilizar la URL firmada en la salida para subir un archivo a Device Farm:

```
curl -T app.apk "https://prod-us-west-2-uploads.s3-us-west-2.amazonaws.com/
arn%3Aaws%3Adevicefarm%3Aus-west-2%3A123456789012%3Aproject%3A070fc3ca-
c7e1-4471-91cf-d3e4efc50604/uploads/arn%3Aaws%3Adevicefarm%3Aus-
west-2%3A123456789012%3Aupload%3A070fc3ca-7ec1-4741-9c1f-d3e044efc506/dd72723a-
ae9e-4087-09e6-f4cea3599514/app.apk?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Date=20170824T224008Z&X-Amz-SignedHeaders=host&X-Amz-Expires=86400&X-Amz-
Credential=AKIAEXAMPLEPBUMBC3GA%2F20170824%2Fus-west-2%2Fs3%2Faws4_request&X-Amz-
Signature=05050370c38894ef5bd09f5d009f36fc8f96fa4bb04e1bba9aca71b8dbe49a0f"
```

- Para obtener detalles sobre la API, consulte CreateUpload en la Referencia de comandos de la AWS CLI.

`get-upload`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-upload`.

AWS CLI

Visualización de una carga

El siguiente comando recupera información sobre una carga:

```
aws devicefarm get-upload --arn "arn:aws:devicefarm:us-
west-2:123456789012:upload:070fc3ca-7ec1-4741-9c1f-d3e044efc506/dd72723a-
ae9e-4087-09e6-f4cea3599514"
```

Puede obtener el ARN de carga de la salida de `create-upload`.

Salida:

```
{
    "upload": {
        "status": "SUCCEEDED",
        "name": "app.apk",
        "created": 1505262773.186,
        "type": "ANDROID_APP",
```

```
        "arn": "arn:aws:devicefarm:us-
west-2:123456789012:upload:070fc3ca-7ec1-4741-9c1f-d3e044efc506/dd72723a-
ae9e-4087-09e6-f4cea3599514",
        "metadata": "{\"device_admin\":false,\"activity_name\":
\"ccom.example.client.LauncherActivity\",\"version_name\":\"1.0.2.94\",\"screens
\":[\"small\",\"normal\",\"large\",\"xlarge\"],\"error_type\":null,\"sdk_version
\":\"16\",\"package_name\":\"com.example.client\",\"version_code\":\"20994\",
\"native_code\":[\"armeabi-v7a\"],\"target_sdk_version\":\"25\"}"
    }
}
```

- Para obtener detalles sobre la API, consulte GetUpload en la Referencia de comandos de la AWS CLI.

`list-projects`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-projects`.

AWS CLI

Para enumerar proyectos

A continuación, se recupera una lista de proyectos:

```
aws devicefarm list-projects
```

Salida:

```
{
    "projects": [
        {
            "name": "myproject",
            "arn": "arn:aws:devicefarm:us-
west-2:123456789012:project:070fc3ca-7ec1-4741-9c1f-d3e044efc506",
            "created": 1503612890.057
        },
        {
            "name": "otherproject",
            "arn": "arn:aws:devicefarm:us-
west-2:123456789012:project:a5f5b752-8098-49d1-86bf-5f7682c1c77e",
            "created": 1505257519.337
        }
```

```
    ]
}
```

- Para obtener detalles sobre la API, consulte ListProjects en la Referencia de comandos de la AWS CLI.

Direct Connect Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Direct Connect.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`accept-direct-connect-gateway-association-proposal`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-direct-connect-gateway-association-proposal`.

AWS CLI

Aceptación de una propuesta de asociación de puerta de enlace

En la siguiente `accept-direct-connect-gateway-association-proposal`, se acepta la propuesta especificada.

```
aws directconnect  accept-direct-connect-gateway-association-proposal \
    --direct-connect-gateway-id 11460968-4ac1-4fd3-bdb2-00599EXAMPLE \
    --proposal-id cb7f41cb-8128-43a5-93b1-dcaedEXAMPLE \
    --associated-gateway-owner-account 111122223333
```

```
{
    "directConnectGatewayAssociation": {
        "directConnectGatewayId": "11460968-4ac1-4fd3-bdb2-00599EXAMPLE",
        "directConnectGatewayOwnerAccount": "111122223333",
        "associationState": "associating",
        "associatedGateway": {
            "id": "tgw-02f776b1a7EXAMPLE",
            "type": "transitGateway",
            "ownerAccount": "111122223333",
            "region": "us-east-1"
        },
        "associationId": "6441f8bf-5917-4279-ade1-9708bEXAMPLE",
        "allowedPrefixesToDirectConnectGateway": [
            {
                "cidr": "192.168.1.0/30"
            }
        ]

  }
}
```

Para obtener más información, consulte Accepting or Rejecting a Transit Gateway Association Proposal en la Guía del usuario de AWS Direct Connect.

- Para obtener detalles sobre la API, consulte AcceptDirectConnectGatewayAssociationProposal en la Referencia de comandos de la AWS CLI.

`allocate-connection-on-interconnect`

En el siguiente ejemplo de código, se muestra cómo utilizar `allocate-connection-on-interconnect`.

AWS CLI

Creación de una conexión alojada en una interconexión

El siguiente comando `allocate-connection-on-interconnect` crea una conexión alojada en una interconexión:

```
aws directconnect allocate-connection-on-interconnect --bandwidth 500Mbps --
connection-name mydcinterconnect --owner-account 123456789012 --interconnect-
id dxcon-fgktov66 --vlan 101
```

Salida:

```
{
    "partnerName": "TIVIT",
    "vlan": 101,
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-ffzc51m1",
    "connectionState": "ordering",
    "bandwidth": "500Mbps",
    "location": "TIVIT",
    "connectionName": "mydcinterconnect",
    "region": "sa-east-1"
}
```

- Para obtener detalles sobre la API, consulte AllocateConnectionOnInterconnect en la Referencia de comandos de la AWS CLI.

`allocate-hosted-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `allocate-hosted-connection`.

AWS CLI

Creación de una conexión alojada en una interconexión

En el siguiente ejemplo de `allocate-hosted-connection`, se crea una conexión alojada en la interconexión especificada.

```
aws directconnect allocate-hosted-connection \
    --bandwidth 500Mbps \
    --connection-name mydcinterconnect \
    --owner-account 123456789012
    -connection-id dxcon-fgktov66
    -vlan 101
```

Salida:

```
{
    "partnerName": "TIVIT",
    "vlan": 101,
    "ownerAccount": "123456789012",
```

```
    "connectionId": "dxcon-ffzc51m1",
    "connectionState": "ordering",
    "bandwidth": "500Mbps",
    "location": "TIVIT",
    "connectionName": "mydcinterconnect",
    "region": "sa-east-1"
}
```

- Para obtener detalles sobre la API, consulte AllocateHostedConnection en la Referencia de comandos de la AWS CLI.

`allocate-private-virtual-interface`

En el siguiente ejemplo de código, se muestra cómo utilizar `allocate-private-virtual-interface`.

AWS CLI

Aprovisionamiento de una interfaz virtual privada

El siguiente comando `allocate-private-virtual-interface` aprovisiona una interfaz virtual privada para que sea propiedad de otro cliente:

```
aws directconnect allocate-private-virtual-interface --connection-id dxcon-
ffjrkx17 --owner-account 123456789012 --new-private-virtual-interface-
allocation virtualInterfaceName=PrivateVirtualInterface,vlan=1000,asn=65000,authKey=asdf34ex
```

Salida:

```
{
    "virtualInterfaceState": "confirming",
    "asn": 65000,
    "vlan": 1000,
    "customerAddress": "192.168.1.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-ffjrkx17",
    "virtualInterfaceId": "dxvif-fgy8orxu",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [],
    "location": "TIVIT",
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>\n  <logical_connection id=\"dxvif-fgy8orxu\">\n  <vlan>1000</
```

```
vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
 <amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>\n
 <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</amazon_bgp_asn>
\n  <connection_type>private</connection_type>\n</logical_connection>\n",
    "amazonAddress": "192.168.1.1/30",
    "virtualInterfaceType": "private",
    "virtualInterfaceName": "PrivateVirtualInterface"
}
```

- Para obtener detalles sobre la API, consulte AllocatePrivateVirtualInterface en la Referencia de comandos de la AWS CLI.

`allocate-public-virtual-interface`

En el siguiente ejemplo de código, se muestra cómo utilizar `allocate-public-virtual-interface`.

AWS CLI

Aprovisionamiento de una interfaz virtual pública

El siguiente comando `allocate-public-virtual-interface` aprovisiona una interfaz virtual pública para que sea propiedad de otro cliente:

```
aws directconnect allocate-public-virtual-interface --connection-id dxcon-
ffjrkx17 --owner-account 123456789012 --new-public-virtual-interface-
allocation virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,authKey=asdf34exa
{cidr=203.0.113.4/30}]
```

Salida:

```
{
    "virtualInterfaceState": "confirming",
    "asn": 65000,
    "vlan": 2000,
    "customerAddress": "203.0.113.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-ffjrkx17",
    "virtualInterfaceId": "dxvif-fg9xo9vp",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [
```

```
        {
            "cidr": "203.0.113.0/30"
        },
        {
            "cidr": "203.0.113.4/30"
        }
    ],
    "location": "TIVIT",
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>\n<logical_connection id=\"dxvif-fg9xo9vp\">\n  <vlan>2000</
vlan>\n  <customer_address>203.0.113.2/30</customer_address>\n
 <amazon_address>203.0.113.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>\n
 <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</amazon_bgp_asn>
\n  <connection_type>public</connection_type>\n</logical_connection>\n",
    "amazonAddress": "203.0.113.1/30",
    "virtualInterfaceType": "public",
    "virtualInterfaceName": "PublicVirtualInterface"
}
```

- Para obtener detalles sobre la API, consulte AllocatePublicVirtualInterface en la Referencia de comandos de la AWS CLI.

`allocate-transit-virtual-interface`

En el siguiente ejemplo de código, se muestra cómo utilizar `allocate-transit-virtual-interface`.

AWS CLI

Aprovisionamiento de una interfaz virtual de tránsito para que sea propiedad de la cuenta AWS especificada.

En el siguiente ejemplo de `allocate-transit-virtual-interface`, se proporciona una interfaz virtual de tránsito para la cuenta especificada.

```
aws directconnect allocate-transit-virtual-interface \
    --connection-id dxlag-fEXAMPLE \
    --owner-account 123456789012 \
    --new-transit-virtual-interface-allocation "virtualInterfaceName=Example Transit
 Virtual
 Interface,vlan=126,asn=65110,mtu=1500,authKey=0xzxgA9YoW9h58u8SEXAMPLE,amazonAddress=192.16
```

Salida:


```
{
    "virtualInterface": {
        "ownerAccount": "123456789012",
        "virtualInterfaceId": "dxvif-fEXAMPLE",
        "location": "loc1",
        "connectionId": "dxlag-fEXAMPLE",
        "virtualInterfaceType": "transit",
        "virtualInterfaceName": "Example Transit Virtual Interface",
        "vlan": 126,
        "asn": 65110,
        "amazonSideAsn": 7224,
        "authKey": "0xzxgA9YoW9h58u8SEXAMPLE",
        "amazonAddress": "192.168.1.1/30",
        "customerAddress": "192.168.1.2/30",
        "addressFamily": "ipv4",
        "virtualInterfaceState": "confirming",
        "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-fEXAMPLE\">\n  <vlan>126</
vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
 <amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65110</bgp_asn>\n
 <bgp_auth_key>0xzxgA9YoW9h58u8SEXAMPLE</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>transit</connection_type>\n</logical_connection>
\n",
        "mtu": 1500,
        "jumboFrameCapable": true,
        "virtualGatewayId": "",
        "directConnectGatewayId": "",
        "routeFilterPrefixes": [],
        "bgpPeers": [
            {
                "bgpPeerId": "dxpeer-fEXAMPLE",
                "asn": 65110,
                "authKey": "0xzxgA9YoW9h58u8EXAMPLE",
                "addressFamily": "ipv4",
                "amazonAddress": "192.168.1.1/30",
                "customerAddress": "192.168.1.2/30",
                "bgpPeerState": "pending",
                "bgpStatus": "down",
                "awsDeviceV2": "loc1-26wz6vEXAMPLE"
            }
        ],
        "region": "sa-east-1",
```

```
        "awsDeviceV2": "loc1-26wz6vEXAMPLE",
        "tags": [
            {
                "key": "Tag",
                "value": "Example"
            }
        ]
    }
}
```

Para obtener más información, consulte Creating a Hosted Transit Virtual Interface en la Guía del usuario de AWS Direct Connect.

- Para obtener detalles sobre la API, consulte AllocateTransitVirtualInterface en la Referencia de comandos de la AWS CLI.

`associate-connection-with-lag`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-connection-with-lag`.

AWS CLI

Asociación de una conexión a un LAG

En el siguiente ejemplo, se asocia la conexión especificada con el LAG especificado.

Comando:

```
aws directconnect associate-connection-with-lag --lag-id dxlag-fhccu14t --
connection-id dxcon-fg9607vm
```

Salida:

```
{
  "ownerAccount": "123456789012",
  "connectionId": "dxcon-fg9607vm",
  "lagId": "dxlag-fhccu14t",
  "connectionState": "requested",
  "bandwidth": "1Gbps",
  "location": "EqDC2",
  "connectionName": "Con2ForLag",
  "region": "us-east-1"
```

```
}
```

- Para obtener detalles sobre la API, consulte AssociateConnectionWithLag en la Referencia de comandos de la AWS CLI.

`associate-hosted-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-hosted-connection`.

AWS CLI

Asociación de una conexión alojada a un LAG

En el siguiente ejemplo, se asocia la conexión alojada especificada con el LAG especificado.

Comando:

```
aws directconnect associate-hosted-connection --parent-connection-id dxlag-fhccu14t
 --connection-id dxcon-fg9607vm
```

Salida:

```
{
  "partnerName": "TIVIT",
  "vlan": 101,
  "ownerAccount": "123456789012",
  "connectionId": "dxcon-fg9607vm",
  "lagId": "dxlag-fhccu14t",
  "connectionState": "ordering",
  "bandwidth": "500Mbps",
  "location": "TIVIT",
  "connectionName": "mydcinterconnect",
  "region": "sa-east-1"
}
```

- Para obtener detalles sobre la API, consulte AssociateHostedConnection en la Referencia de comandos de la AWS CLI.

`associate-virtual-interface`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-virtual-interface`.

AWS CLI

Asociación de una interfaz virtual a una conexión

En el siguiente ejemplo, se asocia la interfaz virtual especificada con el LAG especificado. Como alternativa, para asociar la interfaz virtual a una conexión, especifique el ID de una conexión de AWS Direct Connect para `--connection-id`; por ejemplo, `dxcon-ffnikghc`.

Comando:

```
aws directconnect associate-virtual-interface --connection-id dxlag-ffjhj9lx --
virtual-interface-id dxvif-fgputw0j
```

Salida:

```
{
  "virtualInterfaceState": "pending",
  "asn": 65000,
  "vlan": 123,
  "customerAddress": "169.254.255.2/30",
  "ownerAccount": "123456789012",
  "connectionId": "dxlag-ffjhj9lx",
  "addressFamily": "ipv4",
  "virtualGatewayId": "vgw-38e90b51",
  "virtualInterfaceId": "dxvif-fgputw0j",
  "authKey": "0x123pK5_VBqv.UQ3kJ4123_",
  "routeFilterPrefixes": [],
  "location": "CSVA1",
  "bgpPeers": [
      {
          "bgpStatus": "down",
          "customerAddress": "169.254.255.2/30",
          "addressFamily": "ipv4",
          "authKey": "0x123pK5_VBqv.UQ3kJ4123_",
          "bgpPeerState": "deleting",
          "amazonAddress": "169.254.255.1/30",
          "asn": 65000
      },
      {
          "bgpStatus": "down",
          "customerAddress": "169.254.255.2/30",
          "addressFamily": "ipv4",
          "authKey": "0x123pK5_VBqv.UQ3kJ4123_",
```

```
            "bgpPeerState": "pending",
            "amazonAddress": "169.254.255.1/30",
            "asn": 65000
        }
    ],
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>\n<logical_connection id=\"dxvif-fgputw0j\">\n  <vlan>123</vlan>
\n  <customer_address>169.254.255.2/30</customer_address>\n
 <amazon_address>169.254.255.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>\n
  <bgp_auth_key>0x123pK5_VBqv.UQ3kJ4123_</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>private</connection_type>\n</logical_connection>
\n",
    "amazonAddress": "169.254.255.1/30",
    "virtualInterfaceType": "private",
    "virtualInterfaceName": "VIF1A"
}
```

- Para obtener detalles sobre la API, consulte AssociateVirtualInterface en la Referencia de comandos de la AWS CLI.

`confirm-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `confirm-connection`.

AWS CLI

Confirmación de la creación de una conexión alojada en una interconexión

El siguiente comando `confirm-connection` confirma la creación de una conexión alojada en una interconexión:

```
aws directconnect confirm-connection --connection-id dxcon-fg2wi7hy
```

Salida:

```
{
    "connectionState": "pending"
}
```

- Para obtener detalles sobre la API, consulte ConfirmConnection en la Referencia de comandos de la AWS CLI.

`confirm-private-virtual-interface`

En el siguiente ejemplo de código, se muestra cómo utilizar `confirm-private-virtual-interface`.

AWS CLI

Aceptación de la propiedad de una interfaz virtual privada

El siguiente comando `confirm-private-virtual-interface` acepta la propiedad de una interfaz virtual privada creada por otro cliente:

```
aws directconnect confirm-private-virtual-interface --virtual-interface-id dxvif-fgy8orxu --virtual-gateway-id vgw-e4a47df9
```

Salida:

```
{
    "virtualInterfaceState": "pending"
}
```

- Para obtener detalles sobre la API, consulte ConfirmPrivateVirtualInterface en la Referencia de comandos de la AWS CLI.

`confirm-public-virtual-interface`

En el siguiente ejemplo de código, se muestra cómo utilizar `confirm-public-virtual-interface`.

AWS CLI

Aceptación de la propiedad de una interfaz virtual pública

El siguiente comando `confirm-public-virtual-interface` acepta la propiedad de una interfaz virtual pública creada por otro cliente:

```
aws directconnect confirm-public-virtual-interface --virtual-interface-id dxvif-fg9xo9vp
```

Salida:

```
{
    "virtualInterfaceState": "verifying"
}
```

- Para obtener detalles sobre la API, consulte ConfirmPublicVirtualInterface en la Referencia de comandos de la AWS CLI.

`confirm-transit-virtual-interface`

En el siguiente ejemplo de código, se muestra cómo utilizar `confirm-transit-virtual-interface`.

AWS CLI

Aceptación de la propiedad de una interfaz virtual de tránsito

La siguiente `confirm-transit-virtual-interface` acepta la propiedad de una interfaz virtual de tránsito creada por otro cliente.

```
aws directconnect confirm-transit-virtual-interface \
    --virtual-interface-id dxvif-fEXAMPLE \
    --direct-connect-gateway-id 4112ccf9-25e9-4111-8237-b6c5dEXAMPLE
```

Salida:

```
{
    "virtualInterfaceState": "pending"
}
```

Para obtener más información, consulte Accepting a Hosted Virtual Interface en la Guía del usuario de AWS Direct Connect.

- Para obtener detalles sobre la API, consulte ConfirmTransitVirtualInterface en la Referencia de comandos de la AWS CLI.

`create-bgp-peer`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-bgp-peer`.

AWS CLI

Creación de una sesión de emparejamiento de BGP IPv6

En el siguiente ejemplo, se crea una sesión de emparejamiento de BGP IPv6 en una interfaz virtual privada `dxvif-fg1vuj3d`. Amazon asigna automáticamente las direcciones IPv6 homólogas.

Comando:

```
aws directconnect create-bgp-peer --virtual-interface-id dxvif-fg1vuj3d --new-bgp-peer asn=64600,addressFamily=ipv6
```

Salida:

```
{
  "virtualInterface": {
      "virtualInterfaceState": "available",
      "asn": 65000,
      "vlan": 125,
      "customerAddress": "169.254.255.2/30",
      "ownerAccount": "123456789012",
      "connectionId": "dxcon-fguhmqlc",
      "addressFamily": "ipv4",
      "virtualGatewayId": "vgw-f9eb0c90",
      "virtualInterfaceId": "dxvif-fg1vuj3d",
      "authKey": "0xC_ukbCerl6EYA0example",
      "routeFilterPrefixes": [],
      "location": "EqDC2",
      "bgpPeers": [
          {
              "bgpStatus": "down",
              "customerAddress": "169.254.255.2/30",
              "addressFamily": "ipv4",
              "authKey": "0xC_ukbCerl6EYA0uexample",
              "bgpPeerState": "available",
              "amazonAddress": "169.254.255.1/30",
              "asn": 65000
          },
          {
              "bgpStatus": "down",
              "customerAddress": "2001:db8:1100:2f0:0:1:9cb4:4216/125",
              "addressFamily": "ipv6",
```

```
            "authKey": "0xS27kAIU_VHPjjAexample",
            "bgpPeerState": "pending",
            "amazonAddress": "2001:db8:1100:2f0:0:1:9cb4:4211/125",
            "asn": 64600
        }
    ],
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-fg1vuj3d\">\n  <vlan>125</
vlan>\n  <customer_address>169.254.255.2/30</customer_address>\n
 <amazon_address>169.254.255.1/30</amazon_address>\n  <bgp_asn>65000</
bgp_asn>\n  <bgp_auth_key>0xC_ukbCerl6EYA0uexample</bgp_auth_key>\n
 <ipv6_customer_address>2001:db8:1100:2f0:0:1:9cb4:4216/125</ipv6_customer_address>
\n  <ipv6_amazon_address>2001:db8:1100:2f0:0:1:9cb4:4211/125</ipv6_amazon_address>\n
  <ipv6_bgp_asn>64600</ipv6_bgp_asn>\n  <ipv6_bgp_auth_key>0xS27kAIU_VHPjjAexample</
ipv6_bgp_auth_key>\n  <amazon_bgp_asn>7224</amazon_bgp_asn>\n
 <connection_type>private</connection_type>\n</logical_connection>\n",
    "amazonAddress": "169.254.255.1/30",
    "virtualInterfaceType": "private",
    "virtualInterfaceName": "Test"
  }
}
```

- Para obtener detalles sobre la API, consulte CreateBgpPeer en la Referencia de comandos de la AWS CLI.

`create-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-connection`.

AWS CLI

Creación de una conexión de su red a una ubicación de AWS Direct Connect

El siguiente comando `create-connection` crea una conexión de su red a una ubicación de AWS Direct Connect:

```
aws directconnect create-connection --location TIVIT --bandwidth 1Gbps --connection-
name "Connection to AWS"
```

Salida:

```
{
```

```
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "connectionState": "requested",
    "bandwidth": "1Gbps",
    "location": "TIVIT",
    "connectionName": "Connection to AWS",
    "region": "sa-east-1"
}
```

- Para obtener más información sobre la API, consulte CreateConnection en la Referencia de comandos de la AWS CLI.

`create-direct-connect-gateway-association-proposal`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-direct-connect-gateway-association-proposal`.

AWS CLI

Creación de una propuesta para asociar la puerta de enlace de tránsito especificada con la puerta de enlace de Direct Connect especificada

En el siguiente ejemplo de `create-direct-connect-gateway-association-proposal`, se crea una propuesta para asociar la puerta de enlace de tránsito especificada con la puerta de enlace de Direct Connect especificada.

```
aws directconnect create-direct-connect-gateway-association-proposal \
    --direct-connect-gateway-id 11460968-4ac1-4fd3-bdb2-00599EXAMPLE \
    --direct-connect-gateway-owner-account 111122223333 \
    --gateway-id tgw-02f776b1a7EXAMPLE \
    --add-allowed-prefixes-to-direct-connect-gateway cidr=192.168.1.0/30
```

Salida:

```
{
    "directConnectGatewayAssociationProposal": {
        "proposalId": "cb7f41cb-8128-43a5-93b1-dcaedEXAMPLE",
        "directConnectGatewayId": "11460968-4ac1-4fd3-bdb2-00599EXAMPLE",
        "directConnectGatewayOwnerAccount": "111122223333",
        "proposalState": "requested",
        "associatedGateway": {
```

```
            "id": "tgw-02f776b1a7EXAMPLE",
            "type": "transitGateway",
            "ownerAccount": "111122223333",
            "region": "us-east-1"
        },
        "requestedAllowedPrefixesToDirectConnectGateway": [
            {
                "cidr": "192.168.1.0/30"
            }
        ]
    }
}
```

Para obtener más información, consulte Creating a Transit Gateway Association Proposal en la Guía del usuario de AWS Direct Connect.

- Para obtener detalles sobre la API, consulte CreateDirectConnectGatewayAssociationProposal en la Referencia de comandos de la AWS CLI.

`create-direct-connect-gateway-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-direct-connect-gateway-association`.

AWS CLI

Asociación de una puerta de enlace privada virtual con una puerta de enlace de Direct Connect

En el siguiente ejemplo, se asocia la puerta de enlace privada virtual `vgw-6efe725e` con la puerta de enlace Direct Connect `5f294f92-bafb-4011-916d-9b0bexample`. Debe ejecutar el comando en la región en la que se encuentra la puerta de enlace privada virtual.

Comando:

```
aws directconnect create-direct-connect-gateway-association --direct-connect-gateway-id 5f294f92-bafb-4011-916d-9b0bexample --virtual-gateway-id vgw-6efe725e
```

Salida:

```
{
  "directConnectGatewayAssociation": {
```

```
        "associationState": "associating",
        "virtualGatewayOwnerAccount": "123456789012",
        "directConnectGatewayId": "5f294f92-bafb-4011-916d-9b0bexample",
        "virtualGatewayId": "vgw-6efe725e",
        "virtualGatewayRegion": "us-east-2"
    }
}
```

- Para obtener detalles sobre la API, consulte CreateDirectConnectGatewayAssociation en la Referencia de comandos de la AWS CLI.

`create-direct-connect-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-direct-connect-gateway`.

AWS CLI

Creación de una puerta de enlace de Direct Connect

En el siguiente ejemplo, se crea una puerta de enlace de Direct Connect con el nombre`DxGateway1`.

Comando:

```
aws directconnect create-direct-connect-gateway --direct-connect-gateway-
name "DxGateway1"
```

Salida:

```
{
    "directConnectGateway": {
        "amazonSideAsn": 64512,
        "directConnectGatewayId": "5f294f92-bafb-4011-916d-9b0bdexample",
        "ownerAccount": "123456789012",
        "directConnectGatewayName": "DxGateway1",
        "directConnectGatewayState": "available"
    }
}
```

- Para obtener detalles sobre la API, consulte CreateDirectConnectGateway en la Referencia de comandos de la AWS CLI.

`create-interconnect`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-interconnect`.

AWS CLI

Creación de una interconexión entre la red de un socio y AWS

El siguiente comando `create-interconnect` crea una nueva interconexión entre la red de un socio de AWS Direct Connect y una ubicación de AWS Direct Connect específica.

```
aws directconnect create-interconnect --interconnect-name "1G Interconnect to AWS"
 --bandwidth 1Gbps --location TIVIT
```

Salida:

```
{
    "region": "sa-east-1",
    "bandwidth": "1Gbps",
    "location": "TIVIT",
    "interconnectName": "1G Interconnect to AWS",
    "interconnectId": "dxcon-fgktov66",
    "interconnectState": "requested"
}
```

- Para obtener detalles sobre la API, consulte CreateInterconnect en la Referencia de comandos de la AWS CLI.

`create-lag`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-lag`.

AWS CLI

Creación de un LAG con nuevas conexiones

En el siguiente ejemplo, se crea un LAG y se solicitan dos nuevas conexiones de AWS Direct Connect para el LAG con un ancho de banda de 1 Gbps.

Comando:

```
aws directconnect create-lag --location CSVA1 --number-of-connections 2 --
connections-bandwidth 1Gbps --lag-name 1GBLag
```

Salida:

```
{
  "awsDevice": "CSVA1-23u8tlpaz8iks",
  "numberOfConnections": 2,
  "lagState": "pending",
  "ownerAccount": "123456789012",
  "lagName": "1GBLag",
  "connections": [
      {
          "ownerAccount": "123456789012",
          "connectionId": "dxcon-ffqr6x5q",
          "lagId": "dxlag-ffjhj9lx",
          "connectionState": "requested",
          "bandwidth": "1Gbps",
          "location": "CSVA1",
          "connectionName": "Requested Connection 1 for Lag dxlag-ffjhj9lx",
          "region": "us-east-1"
      },
      {
          "ownerAccount": "123456789012",
          "connectionId": "dxcon-fflqyj95",
          "lagId": "dxlag-ffjhj9lx",
          "connectionState": "requested",
          "bandwidth": "1Gbps",
          "location": "CSVA1",
          "connectionName": "Requested Connection 2 for Lag dxlag-ffjhj9lx",
          "region": "us-east-1"
      }
  ],
  "lagId": "dxlag-ffjhj9lx",
  "minimumLinks": 0,
  "connectionsBandwidth": "1Gbps",
  "region": "us-east-1",
  "location": "CSVA1"
}
```

Creación de un LAG con una conexión existente

En el siguiente ejemplo, se crea un LAG a partir de una conexión existente en su cuenta y se solicita una segunda conexión nueva para el LAG con el mismo ancho de banda y la misma ubicación que la conexión existente.

Comando:

```
aws directconnect create-lag --location EqDC2 --number-of-connections 2 --
connections-bandwidth 1Gbps --lag-name 2ConnLAG --connection-id dxcon-fgk145dr
```

Salida:

```
{
  "awsDevice": "EqDC2-4h6ce2r1bes6",
  "numberOfConnections": 2,
  "lagState": "pending",
  "ownerAccount": "123456789012",
  "lagName": "2ConnLAG",
  "connections": [
      {
          "ownerAccount": "123456789012",
          "connectionId": "dxcon-fh6ljcvo",
          "lagId": "dxlag-fhccu14t",
          "connectionState": "requested",
          "bandwidth": "1Gbps",
          "location": "EqDC2",
          "connectionName": "Requested Connection 1 for Lag dxlag-fhccu14t",
          "region": "us-east-1"
      },
      {
          "ownerAccount": "123456789012",
          "connectionId": "dxcon-fgk145dr",
          "lagId": "dxlag-fhccu14t",
          "connectionState": "down",
          "bandwidth": "1Gbps",
          "location": "EqDC2",
          "connectionName": "VAConn1",
          "region": "us-east-1"
      }
  ],
  "lagId": "dxlag-fhccu14t",
  "minimumLinks": 0,
  "connectionsBandwidth": "1Gbps",
  "region": "us-east-1",
```

```
  "location": "EqDC2"
}
```

- Para obtener detalles sobre la API, consulte CreateLag en la Referencia de comandos de la AWS CLI.

`create-private-virtual-interface`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-private-virtual-interface`.

AWS CLI

Creación de una interfaz virtual privada

El siguiente comando `create-private-virtual-interface` crea una interfaz virtual privada:

```
aws directconnect create-private-virtual-interface --connection-id dxcon-ffjrkx17 --
new-private-virtual-
interface virtualInterfaceName=PrivateVirtualInterface,vlan=101,asn=65000,authKey=asdf34exam
aba37db6
```

Salida:

```
{
    "virtualInterfaceState": "pending",
    "asn": 65000,
    "vlan": 101,
    "customerAddress": "192.168.1.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-ffjrkx17",
    "virtualGatewayId": "vgw-aba37db6",
    "virtualInterfaceId": "dxvif-ffhhk74f",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [],
    "location": "TIVIT",
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-ffhhk74f\">\n  <vlan>101</
vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
 <amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>\n
```

```
 <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</amazon_bgp_asn>
\n  <connection_type>private</connection_type>\n</logical_connection>\n",
    "amazonAddress": "192.168.1.1/30",
    "virtualInterfaceType": "private",
    "virtualInterfaceName": "PrivateVirtualInterface"
}
```

- Para obtener detalles sobre la API, consulte CreatePrivateVirtualInterface en la Referencia de comandos de la AWS CLI.

`create-public-virtual-interface`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-public-virtual-interface`.

AWS CLI

Creación de una interfaz virtual pública

El siguiente comando `create-public-virtual-interface` crea una interfaz virtual pública:

```
aws directconnect create-public-virtual-interface --connection-id dxcon-ffjrkx17 --
new-public-virtual-
interface virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,authKey=asdf34exam
{cidr=203.0.113.4/30}]
```

Salida:

```
{
    "virtualInterfaceState": "verifying",
    "asn": 65000,
    "vlan": 2000,
    "customerAddress": "203.0.113.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-ffjrkx17",
    "virtualInterfaceId": "dxvif-fgh0hcrk",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [
        {
            "cidr": "203.0.113.0/30"
        },
        {
```

```
            "cidr": "203.0.113.4/30"
        }
    ],
    "location": "TIVIT",
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>\n<logical_connection id=\"dxvif-fgh0hcrk\">\n  <vlan>2000</
vlan>\n  <customer_address>203.0.113.2/30</customer_address>\n
 <amazon_address>203.0.113.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>\n
 <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</amazon_bgp_asn>
\n  <connection_type>public</connection_type>\n</logical_connection>\n",
    "amazonAddress": "203.0.113.1/30",
    "virtualInterfaceType": "public",
    "virtualInterfaceName": "PublicVirtualInterface"
}
```

- Para obtener detalles sobre la API, consulte CreatePublicVirtualInterface en la Referencia de comandos de la AWS CLI.

`create-transit-virtual-interface`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-transit-virtual-interface`.

AWS CLI

Creación de una interfaz virtual de tránsito

En el siguiente ejemplo de `create-transit-virtual-interface`, se crea una interfaz virtual de tránsito para la conexión especificada.

```
aws directconnect create-transit-virtual-interface \
    --connection-id dxlag-fEXAMPLE \
    --new-transit-virtual-interface "virtualInterfaceName=Example Transit Virtual
 Interface,vlan=126,asn=65110,mtu=1500,authKey=0xzxgA9YoW9h58u8SvEXAMPLE,amazonAddress=192.1
aada-5a1baEXAMPLE,tags=[{key=Tag,value=Example}]"
```

Salida:

```
{
    "virtualInterface": {
        "ownerAccount": "1111222233333",
        "virtualInterfaceId": "dxvif-fEXAMPLE",
```

```
        "location": "loc1",
        "connectionId": "dxlag-fEXAMPLE",
        "virtualInterfaceType": "transit",
        "virtualInterfaceName": "Example Transit Virtual Interface",
        "vlan": 126,
        "asn": 65110,
        "amazonSideAsn": 4200000000,
        "authKey": "0xzxgA9YoW9h58u8SEXAMPLE",
        "amazonAddress": "192.168.1.1/30",
        "customerAddress": "192.168.1.2/30",
        "addressFamily": "ipv4",
        "virtualInterfaceState": "pending",
        "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-fEXAMPLE\">\n  <vlan>126</
vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
 <amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65110</
bgp_asn>\n  <bgp_auth_key>0xzxgA9YoW9h58u8SvOmXRTw</bgp_auth_key>\n
 <amazon_bgp_asn>4200000000</amazon_bgp_asn>\n  <connection_type>transit</
connection_type>\n</logical_connection>\n",
        "mtu": 1500,
        "jumboFrameCapable": true,
        "virtualGatewayId": "",
        "directConnectGatewayId": "8384da05-13ce-4a91-aada-5a1baEXAMPLE",
        "routeFilterPrefixes": [],
        "bgpPeers": [
            {
                "bgpPeerId": "dxpeer-EXAMPLE",
                "asn": 65110,
                "authKey": "0xzxgA9YoW9h58u8SEXAMPLE",
                "addressFamily": "ipv4",
                "amazonAddress": "192.168.1.1/30",
                "customerAddress": "192.168.1.2/30",
                "bgpPeerState": "pending",
                "bgpStatus": "down",
                "awsDeviceV2": "loc1-26wz6vEXAMPLE"
            }
        ],
        "region": "sa-east-1",
        "awsDeviceV2": "loc1-26wz6vEXAMPLE",
        "tags": [
            {
                "key": "Tag",
                "value": "Example"
            }
```

```
        ]
    }
}
```

Para obtener más información, consulte Creating a Transit Virtual Interface to the Direct Connect Gateway en la AWSGuía del usuario de AWS Direct Connect.

- Para obtener detalles sobre la API, consulte CreateTransitVirtualInterface en la Referencia de comandos de la AWS CLI.

`delete-bgp-peer`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bgp-peer`.

AWS CLI

Eliminación de un par BGP de una interfaz virtual

En el siguiente ejemplo, se elimina el par BGP IPv6 de la interfaz virtual `dxvif-fg1vuj3d`.

Comando:

```
aws directconnect delete-bgp-peer --virtual-interface-id dxvif-fg1vuj3d --asn 64600
 --customer-address 2001:db8:1100:2f0:0:1:9cb4:4216/125
```

Salida:

```
{
  "virtualInterface": {
      "virtualInterfaceState": "available",
      "asn": 65000,
      "vlan": 125,
      "customerAddress": "169.254.255.2/30",
      "ownerAccount": "123456789012",
      "connectionId": "dxcon-fguhmqlc",
      "addressFamily": "ipv4",
      "virtualGatewayId": "vgw-f9eb0c90",
      "virtualInterfaceId": "dxvif-fg1vuj3d",
      "authKey": "0xC_ukbCerl6EYA0example",
      "routeFilterPrefixes": [],
      "location": "EqDC2",
      "bgpPeers": [
          {
```

```
            "bgpStatus": "down",
            "customerAddress": "169.254.255.2/30",
            "addressFamily": "ipv4",
            "authKey": "0xC_ukbCerl6EYA0uexample",
            "bgpPeerState": "available",
            "amazonAddress": "169.254.255.1/30",
            "asn": 65000
        },
        {
            "bgpStatus": "down",
            "customerAddress": "2001:db8:1100:2f0:0:1:9cb4:4216/125",
            "addressFamily": "ipv6",
            "authKey": "0xS27kAIU_VHPjjAexample",
            "bgpPeerState": "deleting",
            "amazonAddress": "2001:db8:1100:2f0:0:1:9cb4:4211/125",
            "asn": 64600
        }
    ],
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-fg1vuj3d\">\n  <vlan>125</
vlan>\n  <customer_address>169.254.255.2/30</customer_address>\n
 <amazon_address>169.254.255.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>\n
  <bgp_auth_key>0xC_ukbCerl6EYA0example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>private</connection_type>\n</logical_connection>
\n",
    "amazonAddress": "169.254.255.1/30",
    "virtualInterfaceType": "private",
    "virtualInterfaceName": "Test"
  }
}
```

- Para obtener detalles sobre la API, consulte DeleteBgpPeer en la Referencia de comandos de la AWS CLI.

`delete-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-connection`.

AWS CLI

Para eliminar una conexión

El siguiente comando `delete-connection` elimina la colección especificada:

```
aws directconnect delete-connection --connection-id dxcon-fg31dyv6
```

Salida:

```
{
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "connectionState": "deleted",
    "bandwidth": "1Gbps",
    "location": "TIVIT",
    "connectionName": "Connection to AWS",
    "region": "sa-east-1"
}
```

- Para obtener detalles sobre la API, consulte DeleteConnection en la Referencia de comandos de la AWS CLI.

`delete-direct-connect-gateway-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-direct-connect-gateway-association`.

AWS CLI

Eliminación de una asociación de puerta de enlace de Direct Connect

En el siguiente ejemplo de `delete-direct-connect-gateway-association`, se elimina la asociación de la puerta de enlace de Direct Connect con una puerta de enlace de tránsito que tiene el ID de asociación especificado.

```
aws directconnect delete-direct-connect-gateway-association --association-id
  be85116d-46eb-4b43-a27a-da0c2ad648de
```

Salida:

```
{
    "directConnectGatewayAssociation": {
        "directConnectGatewayId": "11460968-4ac1-4fd3-bdb2-00599EXAMPlE",
        "directConnectGatewayOwnerAccount": "123456789012",
        "associationState": "disassociating",
        "associatedGateway": {
```

```
            "id": "tgw-095b3b0b54EXAMPLE",
            "type": "transitGateway",
            "ownerAccount": "123456789012",
            "region": "us-east-1"
        },
         "associationId": " be85116d-46eb-4b43-a27a-da0c2ad648deEXAMPLE ",
         "allowedPrefixesToDirectConnectGateway": [
            {
                "cidr": "192.0.1.0/28"
            }
         ]
    }
}
```

Para obtener más información, consulte Associating and Disassociating Transit Gateways en la Guía del usuario de AWS Direct Connect.

- Para obtener detalles sobre la API, consulte DeleteDirectConnectGatewayAssociation en la Referencia de comandos de la AWS CLI.

`delete-direct-connect-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-direct-connect-gateway`.

AWS CLI

Eliminación de una puerta de enlace de Direct Connect

En el siguiente ejemplo, se elimina la puerta de enlace `5f294f92-bafb-4011-916d-9b0bexample` de Direct Connect.

Comando:

```
aws directconnect delete-direct-connect-gateway --direct-connect-gateway-
id 5f294f92-bafb-4011-916d-9b0bexample
```

Salida:

```
{
  "directConnectGateway": {
      "amazonSideAsn": 64512,
      "directConnectGatewayId": "5f294f92-bafb-4011-916d-9b0bexample",
```

```
      "ownerAccount": "123456789012",
      "directConnectGatewayName": "DxGateway1",
      "directConnectGatewayState": "deleting"
  }
}
```

- Para obtener detalles sobre la API, consulte DeleteDirectConnectGateway en la Referencia de comandos de la AWS CLI.

`delete-interconnect`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-interconnect`.

AWS CLI

Eliminación de una interconexión

El siguiente comando `delete-interconnect` elimina la interconexión especificada:

```
aws directconnect delete-interconnect --interconnect-id dxcon-fgktov66
```

Salida:

```
{
    "interconnectState": "deleted"
}
```

- Para obtener detalles sobre la API, consulte DeleteInterconnect en la Referencia de comandos de la AWS CLI.

`delete-lag`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-lag`.

AWS CLI

Eliminación de un LAG

En el siguiente ejemplo, se elimina el LAG especificado.

Comando:

```
aws directconnect delete-lag --lag-id dxlag-ffrhowd9
```

Salida:

```
{
  "awsDevice": "EqDC2-4h6ce2r1bes6",
  "numberOfConnections": 0,
  "lagState": "deleted",
  "ownerAccount": "123456789012",
  "lagName": "TestLAG",
  "connections": [],
  "lagId": "dxlag-ffrhowd9",
  "minimumLinks": 0,
  "connectionsBandwidth": "1Gbps",
  "region": "us-east-1",
  "location": "EqDC2"
}
```

- Para obtener detalles sobre la API, consulte DeleteLag en la Referencia de comandos de la AWS CLI.

`delete-virtual-interface`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-virtual-interface`.

AWS CLI

Eliminación de una interfaz virtual

El siguiente comando `delete-virtual-interface` elimina la interfaz virtual especificada:

```
aws directconnect delete-virtual-interface --virtual-interface-id dxvif-ffhhk74f
```

Salida:

```
{
    "virtualInterfaceState": "deleting"
}
```

- Para obtener detalles sobre la API, consulte DeleteVirtualInterface en la Referencia de comandos de la AWS CLI.

describe-connection-loa

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-connection-loa`.

AWS CLI

Descripción de su LOA-CFA para una conexión mediante Linux o Mac OS X

En el siguiente ejemplo, se describe el documento LOA-CFA para la conexión `dxcon-fh6ayh1d`. El contenido del documento LOA-CFA está codificado en base64. Este comando usa los parámetros `--output` y `--query` para controlar la salida y extraer el contenido de la estructura de `loaContent`. La última parte del comando decodifica el contenido mediante la utilidad `base64` y envía el resultado a un archivo PDF.

```
aws directconnect describe-connection-loa --connection-id dxcon-fh6ayh1d --
output text --query loa.loaContent|base64 --decode > myLoaCfa.pdf
```

Descripción de su documento LOA-CFA para una conexión mediante Windows

El ejemplo anterior requiere el uso de la utilidad `base64` para decodificar la salida. En un equipo con Windows, puede usar `certutil` en su lugar. En el siguiente ejemplo, el primer comando describe su documento LOA-CFA para la conexión `dxcon-fh6ayh1d` y utiliza los parámetros `--output` y `--query` para controlar la salida y extraer el contenido de la estructura de `loaContent` en un archivo llamado `myLoaCfa.base64`. El segundo comando utiliza la utilidad `certutil` para decodificar el archivo y enviar el resultado a un archivo PDF.

```
aws directconnect describe-connection-loa --connection-id dxcon-fh6ayh1d --
output text --query loa.loaContent > myLoaCfa.base64
```

```
certutil -decode myLoaCfa.base64 myLoaCfa.pdf
```

Para obtener más información acerca del control de la salida de la CLI de AWS, consulte Controlling Command Output from the AWS Command Line Interface en la Guía del usuario de la interfaz de la línea de comandos de AWS.

- Para obtener detalles sobre la API, consulte DescribeConnectionLoa en la Referencia de comandos de la AWS CLI.

`describe-connections-on-interconnect`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-connections-on-interconnect`.

AWS CLI

Para enumerar las conexiones de una interconexión

El siguiente comando `describe-connections-on-interconnect` enumera las conexiones que se han aprovisionado en la interconexión especificada:

```
aws directconnect describe-connections-on-interconnect --interconnect-id dxcon-fgktov66
```

Salida:

```
{
    "connections": [
        {
            "partnerName": "TIVIT",
            "vlan": 101,
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-ffzc51m1",
            "connectionState": "ordering",
            "bandwidth": "500Mbps",
            "location": "TIVIT",
            "connectionName": "mydcinterconnect",
            "region": "sa-east-1"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeConnectionsOnInterconnect en la Referencia de comandos de la AWS CLI.

`describe-connections`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-connections`.

AWS CLI

Para enumerar todas las conexiones de la región actual

El siguiente comando `describe-connections` muestra todas las conexiones de la región actual:

```
aws directconnect describe-connections
```

Salida:

```
{
  "connections": [
      {
          "awsDevice": "EqDC2-123h49s71dabc",
          "ownerAccount": "123456789012",
          "connectionId": "dxcon-fguhmqlc",
          "lagId": "dxlag-ffrz71kw",
          "connectionState": "down",
          "bandwidth": "1Gbps",
          "location": "EqDC2",
          "connectionName": "My_Connection",
          "loaIssueTime": 1491568964.0,
          "region": "us-east-1"
      }
  ]
}
```

- Para obtener detalles sobre la API, consulte DescribeConnections en la Referencia de comandos de la AWS CLI.

`describe-direct-connect-gateway-association-proposals`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-direct-connect-gateway-association-proposals`.

AWS CLI

Descripción de sus propuestas de asociación de puerta de enlace de Direct Connect

En el siguiente ejemplo de `describe-direct-connect-gateway-association-proposals`, se muestran detalles sobre sus propuestas de asociación de puertas de enlace de Direct Connect.

```
aws directconnect describe-direct-connect-gateway-association-proposals
```

Salida:

```
{
    "directConnectGatewayAssociationProposals": [
        {
            "proposalId": "c2ede9b4-bbc6-4d33-923c-bc4feEXAMPLE",
            "directConnectGatewayId": "11460968-4ac1-4fd3-bdb2-00599EXAMPLE",
            "directConnectGatewayOwnerAccount": "111122223333",
            "proposalState": "requested",
            "associatedGateway": {
                "id": "tgw-02f776b1a7EXAMPLE",
                "type": "transitGateway",
                "ownerAccount": "111122223333",
                "region": "us-east-1"
            },
            "existingAllowedPrefixesToDirectConnectGateway": [
                {
                    "cidr": "192.168.2.0/30"
                },
                {
                    "cidr": "192.168.1.0/30"
                }
            ],
            "requestedAllowedPrefixesToDirectConnectGateway": [
                {
                    "cidr": "192.168.1.0/30"
                }
            ]
        },
        {
            "proposalId": "cb7f41cb-8128-43a5-93b1-dcaedEXAMPLE",
            "directConnectGatewayId": "11560968-4ac1-4fd3-bcb2-00599EXAMPLE",
            "directConnectGatewayOwnerAccount": "111122223333",
            "proposalState": "accepted",
            "associatedGateway": {
                "id": "tgw-045776b1a7EXAMPLE",
                "type": "transitGateway",
```

```
                "ownerAccount": "111122223333",
                "region": "us-east-1"
            },
            "existingAllowedPrefixesToDirectConnectGateway": [
                {
                    "cidr": "192.168.4.0/30"
                },
                {
                    "cidr": "192.168.5.0/30"
                }
            ],
            "requestedAllowedPrefixesToDirectConnectGateway": [
                {
                    "cidr": "192.168.5.0/30"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Associating and Disassociating Transit Gateways en la Guía del usuario de AWS Direct Connect.

- Para obtener detalles sobre la API, consulte DescribeDirectConnectGatewayAssociationProposals en la Referencia de comandos de la AWS CLI.

`describe-direct-connect-gateway-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-direct-connect-gateway-associations`.

AWS CLI

Descripción de asociaciones de puertas de enlace de Direct Connect

En el siguiente ejemplo, se describen todas las asociaciones con una puerta de enlace de Direct Connect `5f294f92-bafb-4011-916d-9b0bexample`.

Comando:

```
aws directconnect describe-direct-connect-gateway-associations --direct-connect-
gateway-id 5f294f92-bafb-4011-916d-9b0bexample
```

Salida:

```
{
  "nextToken":
 "eyJ2IjoxLCJzIjoxLCJpIjoiOU83OTFodzdycnZCbkN4MExHeHVwQT09IiwiYyI6InIxTEN0UEVHV0I1UFlkaWFnNl
  "directConnectGatewayAssociations": [
      {
          "associationState": "associating",
          "virtualGatewayOwnerAccount": "123456789012",
          "directConnectGatewayId": "5f294f92-bafb-4011-916d-9b0bexample",
          "virtualGatewayId": "vgw-6efe725e",
          "virtualGatewayRegion": "us-east-2"
      },
      {
          "associationState": "disassociating",
          "virtualGatewayOwnerAccount": "123456789012",
          "directConnectGatewayId": "5f294f92-bafb-4011-916d-9b0bexample",
          "virtualGatewayId": "vgw-ebaa27db",
          "virtualGatewayRegion": "us-east-2"
      }
  ]
}
```

- Para obtener detalles sobre la API, consulte DescribeDirectConnectGatewayAssociations en la Referencia de comandos de la AWS CLI.

`describe-direct-connect-gateway-attachments`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-direct-connect-gateway-attachments`.

AWS CLI

Descripción de las vinculaciones de puertas de enlace de Direct Connect

El siguiente ejemplo describe las interfaces virtuales que están vinculadas a la puerta de enlace Direct Connect `5f294f92-bafb-4011-916d-9b0bexample`.

Comando:

```
aws directconnect describe-direct-connect-gateway-attachments --direct-connect-
gateway-id 5f294f92-bafb-4011-916d-9b0bexample
```

Salida:

```
{
  "directConnectGatewayAttachments": [
      {
          "virtualInterfaceOwnerAccount": "123456789012",
          "directConnectGatewayId": "5f294f92-bafb-4011-916d-9b0bexample",
          "virtualInterfaceRegion": "us-east-2",
          "attachmentState": "attaching",
          "virtualInterfaceId": "dxvif-fg9zyabc"
      }
  ],
  "nextToken":
 "eyJ2IjoxLCJzIjoxLCJpIjoibEhXdlNpUXF5RzhoL1JyUW52SlV2QT09IiwiYyI6Im5wQjFHQ0RyQUdRS3puNnNXcU
}
```

- Para obtener detalles sobre la API, consulte DescribeDirectConnectGatewayAttachments en la Referencia de comandos de la AWS CLI.

`describe-direct-connect-gateways`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-direct-connect-gateways`.

AWS CLI

Descripción de sus puertas de enlace de Direct Connect

En el siguiente ejemplo, se describen todas sus puertas de enlace de Direct Connect.

Comando:

```
aws directconnect describe-direct-connect-gateways
```

Salida:

```
{
```

```
  "directConnectGateways": [
      {
          "amazonSideAsn": 64512,
          "directConnectGatewayId": "cf68415c-f4ae-48f2-87a7-3b52cexample",
          "ownerAccount": "123456789012",
          "directConnectGatewayName": "DxGateway2",
          "directConnectGatewayState": "available"
      },
      {
          "amazonSideAsn": 64512,
          "directConnectGatewayId": "5f294f92-bafb-4011-916d-9b0bdexample",
          "ownerAccount": "123456789012",
          "directConnectGatewayName": "DxGateway1",
          "directConnectGatewayState": "available"
      }
  ]
}
```

- Para obtener detalles sobre la API, consulte DescribeDirectConnectGateways en la Referencia de comandos de la AWS CLI.

`describe-hosted-connections`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-hosted-connections`.

AWS CLI

Para enumerar las conexiones de una interconexión

El siguiente ejemplo enumera las conexiones que se han aprovisionado en la interconexión especificada:

Comando:

```
aws directconnect describe-hosted-connections --connection-id dxcon-fgktov66
```

Salida:

```
{
    "connections": [
        {
            "partnerName": "TIVIT",
```

```
            "vlan": 101,
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-ffzc51m1",
            "connectionState": "ordering",
            "bandwidth": "500Mbps",
            "location": "TIVIT",
            "connectionName": "mydcinterconnect",
            "region": "sa-east-1"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeHostedConnections en la Referencia de comandos de la AWS CLI.

`describe-interconnect-loa`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-interconnect-loa`.

AWS CLI

Descripción de su LOA-CFA para una conexión mediante Linux o Mac OS X

En el siguiente ejemplo, se describe el documento LOA-CFA para la interconexión `dxcon-fh6ayh1d`. El contenido del documento LOA-CFA está codificado en base64. Este comando usa los parámetros `--output` y `--query` para controlar la salida y extraer el contenido de la estructura de `loaContent`. La última parte del comando decodifica el contenido mediante la utilidad `base64` y envía el resultado a un archivo PDF.

```
aws directconnect describe-interconnect-loa --interconnect-id dxcon-fh6ayh1d --
output text --query loa.loaContent|base64 --decode > myLoaCfa.pdf
```

Descripción de su documento LOA-CFA para una interconexión mediante Windows

El ejemplo anterior requiere el uso de la utilidad `base64` para decodificar la salida. En un equipo con Windows, puede usar `certutil` en su lugar. En el siguiente ejemplo, el primer comando describe su documento LOA-CFA para la interconexión `dxcon-fh6ayh1d` y utiliza los parámetros `--output` y `--query` para controlar la salida y extraer el contenido de la estructura de `loaContent` en un archivo llamado `myLoaCfa.base64`. El segundo comando utiliza la utilidad `certutil` para decodificar el archivo y enviar el resultado a un archivo PDF.

```
aws directconnect describe-interconnect-loa --interconnect-id dxcon-fh6ayh1d --
output text --query loa.loaContent > myLoaCfa.base64
```

```
certutil -decode myLoaCfa.base64 myLoaCfa.pdf
```

Para obtener más información acerca del control de la salida de la CLI de AWS, consulte Controlling Command Output from the AWS Command Line Interface en la Guía del usuario de la interfaz de la línea de comandos de AWS.

- Para obtener detalles sobre la API, consulte DescribeInterconnectLoa en la Referencia de comandos de la AWS CLI.

`describe-interconnects`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-interconnects`.

AWS CLI

Para enumerar las interconexiones

El siguiente comando `describe-interconnects` muestra las interconexiones que pertenecen a su cuenta AWS:

```
aws directconnect describe-interconnects
```

Salida:

```
{
    "interconnects": [
        {
            "region": "sa-east-1",
            "bandwidth": "1Gbps",
            "location": "TIVIT",
            "interconnectName": "1G Interconnect to AWS",
            "interconnectId": "dxcon-fgktov66",
            "interconnectState": "down"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeInterconnects en la Referencia de comandos de la AWS CLI.

`describe-lags`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-lags`.

AWS CLI

Descripción de sus LAG

En el siguiente comando, se describen todos los LAG de la región actual.

Comando:

```
aws directconnect describe-lags
```

Salida:

```
{
  "lags": [
      {
          "awsDevice": "EqDC2-19y7z3m17xpuz",
          "numberOfConnections": 2,
          "lagState": "down",
          "ownerAccount": "123456789012",
          "lagName": "DA-LAG",
          "connections": [
              {
                  "ownerAccount": "123456789012",
                  "connectionId": "dxcon-ffnikghc",
                  "lagId": "dxlag-fgsu9erb",
                  "connectionState": "requested",
                  "bandwidth": "10Gbps",
                  "location": "EqDC2",
                  "connectionName": "Requested Connection 1 for Lag dxlag-fgsu9erb",
                  "region": "us-east-1"
              },
              {
                  "ownerAccount": "123456789012",
                  "connectionId": "dxcon-fglgbdea",
                  "lagId": "dxlag-fgsu9erb",
```

```
                "connectionState": "requested",
                "bandwidth": "10Gbps",
                "location": "EqDC2",
                "connectionName": "Requested Connection 2 for Lag dxlag-fgsu9erb",
                "region": "us-east-1"
            }
        ],
        "lagId": "dxlag-fgsu9erb",
        "minimumLinks": 0,
        "connectionsBandwidth": "10Gbps",
        "region": "us-east-1",
        "location": "EqDC2"
    }
  ]
}
```

- Para obtener detalles sobre la API, consulte DescribeLags en la Referencia de comandos de la AWS CLI.

`describe-loa`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-loa`.

AWS CLI

Descripción de su LOA-CFA para una conexión mediante Linux o Mac OS X

En el siguiente ejemplo, se describe el documento LOA-CFA para la conexión `dxcon-fh6ayh1d`. El contenido del documento LOA-CFA está codificado en base64. Este comando usa los parámetros `--output` y `--query` para controlar la salida y extraer el contenido de la estructura de `loaContent`. La última parte del comando decodifica el contenido mediante la utilidad `base64` y envía el resultado a un archivo PDF.

```
aws directconnect describe-loa --connection-id dxcon-fh6ayh1d --output text --
query loa.loaContent|base64 --decode > myLoaCfa.pdf
```

Descripción de su documento LOA-CFA para una conexión mediante Windows

El ejemplo anterior requiere el uso de la utilidad `base64` para decodificar la salida. En un equipo con Windows, puede usar `certutil` en su lugar. En el siguiente ejemplo, el primer comando describe su documento LOA-CFA para la conexión `dxcon-fh6ayh1d` y utiliza los

parámetros `--output` y `--query` para controlar la salida y extraer el contenido de la estructura de `loaContent` en un archivo llamado `myLoaCfa.base64`. El segundo comando utiliza la utilidad `certutil` para decodificar el archivo y enviar el resultado a un archivo PDF.

```
aws directconnect describe-loa --connection-id dxcon-fh6ayh1d --output text --
query loa.loaContent > myLoaCfa.base64
```

```
certutil -decode myLoaCfa.base64 myLoaCfa.pdf
```

Para obtener más información acerca del control de la salida de la CLI de AWS, consulte Controlling Command Output from the AWS Command Line Interface en la Guía del usuario de la interfaz de la línea de comandos de AWS.

- Para obtener detalles sobre la API, consulte DescribeLoa en la Referencia de comandos de la AWS CLI.

`describe-locations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-locations`.

AWS CLI

Para enumerar los socios y las ubicaciones de AWS Direct Connect

El siguiente comando `describe-locations` enumera los socios y las ubicaciones de AWS Direct Connect en la región actual:

```
aws directconnect describe-locations
```

Salida:

```
{
    "locations": [
        {
            "locationName": "NAP do Brasil, Barueri, Sao Paulo",
            "locationCode": "TNDB"
        },
        {
            "locationName": "Tivit - Site Transamerica (Sao Paulo)",
            "locationCode": "TIVIT"
```

```
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeLocations en la Referencia de comandos de la AWS CLI.

`describe-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-tags`.

AWS CLI

Descripción de las etiquetas de sus recursos de AWS Direct Connect

El siguiente comando describe las etiquetas de la conexión `dxcon-abcabc12`.

Comando:

```
aws directconnect describe-tags --resource-arns arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-abcabc12
```

Salida:

```
{
  "resourceTags": [
      {
          "resourceArn": "arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-
abcabc12",
          "tags": [
              {
                  "value": "VAConnection",
                  "key": "Name"
              }
          ]
      }
  ]
}
```

- Para obtener detalles sobre la API, consulte DescribeTags en la Referencia de comandos de la AWS CLI.

describe-virtual-gateways

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-virtual-gateways`.

AWS CLI

Para enumerar las puertas de enlace privadas virtuales

El siguiente comando `describe-virtual-gateways` enumera las puertas de enlace privadas virtuales que son propiedad de su cuenta de AWS:

```
aws directconnect describe-virtual-gateways
```

Salida:

```
{
    "virtualGateways": [
        {
            "virtualGatewayId": "vgw-aba37db6",
            "virtualGatewayState": "available"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeVirtualGateways en la Referencia de comandos de la AWS CLI.

describe-virtual-interfaces

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-virtual-interfaces`.

AWS CLI

Para enumerar todas las interfaces virtuales

El siguiente comando `describe-virtual-interfaces` muestra la información sobre todas las interfaces virtuales asociadas a su cuenta de AWS:

```
aws directconnect describe-virtual-interfaces --connection-id dxcon-ffjrkx17
```

Salida:


```
{
    "virtualInterfaces": [
        {
            "virtualInterfaceState": "down",
            "asn": 65000,
            "vlan": 101,
            "customerAddress": "192.168.1.2/30",
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-ffjrkx17",
            "virtualGatewayId": "vgw-aba37db6",
            "virtualInterfaceId": "dxvif-ffhhk74f",
            "authKey": "asdf34example",
            "routeFilterPrefixes": [],
            "location": "TIVIT",
            "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-ffhhk74f\">\n  <vlan>101</
vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
 <amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>\n
 <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</amazon_bgp_asn>
\n  <connection_type>private</connection_type>\n</logical_connection>\n",
            "amazonAddress": "192.168.1.1/30",
            "virtualInterfaceType": "private",
            "virtualInterfaceName": "PrivateVirtualInterface"
        },
        {
            "virtualInterfaceState": "verifying",
            "asn": 65000,
            "vlan": 2000,
            "customerAddress": "203.0.113.2/30",
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-ffjrkx17",
            "virtualGatewayId": "",
            "virtualInterfaceId": "dxvif-fgh0hcrk",
            "authKey": "asdf34example",
            "routeFilterPrefixes": [
                {
                    "cidr": "203.0.113.4/30"
                },
                {
                    "cidr": "203.0.113.0/30"
                }
            ],
```

```
            "location": "TIVIT",
            "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-fgh0hcrk\">\n  <vlan>2000</
vlan>\n  <customer_address>203.0.113.2/30</customer_address>\n
 <amazon_address>203.0.113.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>\n
 <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</amazon_bgp_asn>
\n  <connection_type>public</connection_type>\n</logical_connection>\n",
            "amazonAddress": "203.0.113.1/30",
            "virtualInterfaceType": "public",
            "virtualInterfaceName": "PublicVirtualInterface"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeVirtualInterfaces en la Referencia de comandos de la AWS CLI.

`disassociate-connection-from-lag`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-connection-from-lag`.

AWS CLI

Desasociar una conexión de un LAG

En el siguiente ejemplo, se desasocia la conexión especificada del LAG indicado.

Comando:

```
aws directconnect disassociate-connection-from-lag --lag-id dxlag-fhccu14t --
connection-id  dxcon-fg9607vm
```

Salida:

```
{
  "ownerAccount": "123456789012",
  "connectionId": "dxcon-fg9607vm",
  "connectionState": "requested",
  "bandwidth": "1Gbps",
  "location": "EqDC2",
```

```
  "connectionName": "Con2ForLag",
  "region": "us-east-1"
}
```

- Para obtener detalles sobre la API, consulte DisassociateConnectionFromLag en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Adición de una etiqueta a un recurso de AWS Direct Connect

El siguiente comando agrega una etiqueta con una clave de `Name` y un valor de `VAConnection` a la instancia `dxcon-abcabc12`. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws directconnect tag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-abcabc12 --tags "key=Name,value=VAConnection"
```

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de una etiqueta de un recurso de AWS Direct Connect

El siguiente comando elimina la etiqueta con la clave `Name` de la conexión `dxcon-abcabc12`. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws directconnect untag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-abcabc12 --tag-keys Name
```

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-direct-connect-gateway-association

En el siguiente ejemplo de código, se muestra cómo utilizar `update-direct-connect-gateway-association`.

AWS CLI

Actualización de los atributos especificados de la asociación de puertas de enlace de Direct Connect.

En el siguiente ejemplo `update-direct-connect-gateway-association`, se agrega el bloque de CIDR especificado a una asociación de puertas de enlace de Direct Connect.

```
aws directconnect update-direct-connect-gateway-association \
    --association-id 820a6e4f-5374-4004-8317-3f64bEXAMPLE \
    --add-allowed-prefixes-to-direct-connect-gateway cidr=192.168.2.0/30
```

Salida:

```
{
    "directConnectGatewayAssociation": {
        "directConnectGatewayId": "11460968-4ac1-4fd3-bdb2-00599EXAMPLE",
        "directConnectGatewayOwnerAccount": "111122223333",
        "associationState": "updating",
        "associatedGateway": {
            "id": "tgw-02f776b1a7EXAMPLE",
            "type": "transitGateway",
            "ownerAccount": "111122223333",
            "region": "us-east-1"
        },
        "associationId": "820a6e4f-5374-4004-8317-3f64bEXAMPLE",
        "allowedPrefixesToDirectConnectGateway": [
            {
                "cidr": "192.168.2.0/30"
```

```
            },
            {
                "cidr": "192.168.1.0/30"
            }
        ]
    }
}
```

Para obtener más información, consulte Working with Direct Connect Gateways en la Guía del usuario de AWS Direct Connect.

- Para obtener detalles sobre la API, consulte UpdateDirectConnectGatewayAssociation en la Referencia de comandos de la AWS CLI.

`update-lag`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-lag`.

AWS CLI

Actualización de un LAG

En el siguiente ejemplo, se cambia el nombre del LAG especificado.

Comando:

```
aws directconnect update-lag --lag-id dxlag-ffjhj9lx --lag-name 2ConnLag
```

Salida:

```
{
  "awsDevice": "CSVA1-23u8tlpaz8iks",
  "numberOfConnections": 2,
  "lagState": "down",
  "ownerAccount": "123456789012",
  "lagName": "2ConnLag",
  "connections": [
      {
          "ownerAccount": "123456789012",
          "connectionId": "dxcon-fflqyj95",
          "lagId": "dxlag-ffjhj9lx",
```

```
            "connectionState": "requested",
            "bandwidth": "1Gbps",
            "location": "CSVA1",
            "connectionName": "Requested Connection 2 for Lag dxlag-ffjhj9lx",
            "region": "us-east-1"
        },
        {
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-ffqr6x5q",
            "lagId": "dxlag-ffjhj9lx",
            "connectionState": "requested",
            "bandwidth": "1Gbps",
            "location": "CSVA1",
            "connectionName": "Requested Connection 1 for Lag dxlag-ffjhj9lx",
            "region": "us-east-1"
        }
    ],
    "lagId": "dxlag-ffjhj9lx",
    "minimumLinks": 0,
    "connectionsBandwidth": "1Gbps",
    "region": "us-east-1",
    "location": "CSVA1"
}
```

- Para obtener detalles sobre la API, consulte UpdateLag en la Referencia de comandos de la AWS CLI.

`update-virtual-interface-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-virtual-interface-attributes`.

AWS CLI

Actualización de la MTU de una interfaz virtual

En el siguiente ejemplo `update-virtual-interface-attributes`, se actualiza la MTU de la interfaz virtual especificada.

```
aws directconnect update-virtual-interface-attributes \
    --virtual-interface-id dxvif-fEXAMPLE \
    --mtu 1500
```

Salida:


```
{
    "ownerAccount": "1111222233333",
    "virtualInterfaceId": "dxvif-fEXAMPLE",
    "location": "loc1",
    "connectionId": "dxlag-fEXAMPLE",
    "virtualInterfaceType": "transit",
    "virtualInterfaceName": "example transit virtual interface",
    "vlan": 125,
    "asn": 650001,
    "amazonSideAsn": 64512,
    "authKey": "0xzxgA9YoW9h58u8SEXAMPLE",
    "amazonAddress": "169.254.248.1/30",
    "customerAddress": "169.254.248.2/30",
    "addressFamily": "ipv4",
    "virtualInterfaceState": "down",
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>\n<logical_connection id=\"dxvif-fEXAMPLE\">\n  <vlan>125</vlan>
\n  <customer_address>169.254.248.2/30</customer_address>\n
 <amazon_address>169.254.248.1/30</amazon_address>\n  <bgp_asn>650001</bgp_asn>\n
  <bgp_auth_key>0xzxgA9YoW9h58u8SEXAMPLE</bgp_auth_key>\n  <amazon_bgp_asn>64512</
amazon_bgp_asn>\n  <connection_type>transit</connection_type>\n</logical_connection>
\n",
    "mtu": 1500,
    "jumboFrameCapable": true,
    "virtualGatewayId": "",
    "directConnectGatewayId": "879b76a1-403d-4700-8b53-4a56ed85436e",
    "routeFilterPrefixes": [],
    "bgpPeers": [
        {
            "bgpPeerId": "dxpeer-fEXAMPLE",
            "asn": 650001,
            "authKey": "0xzxgA9YoW9h58u8SEXAMPLE",
            "addressFamily": "ipv4",
            "amazonAddress": "169.254.248.1/30",
            "customerAddress": "169.254.248.2/30",
            "bgpPeerState": "available",
            "bgpStatus": "down",
            "awsDeviceV2": "loc1-26wz6vEXAMPLE"
        }
    ],
    "region": "sa-east-1",
    "awsDeviceV2": "loc1-26wz6vEXAMPLE",
```

```
    "tags": []
}
```

Para obtener más información, consulte Setting Network MTU for Private Virtual Interfaces or Transit Virtual Interfaces en la Guía del usuario de AWS Direct Connect.

- Para obtener detalles sobre la API, consulte UpdateVirtualInterfaceAttributes en la Referencia de comandos de la AWS CLI.

Directory Service Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Directory Service.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`describe-directories`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-directories`.

AWS CLI

Obtención de información detallada acerca de sus directorios.

En el siguiente ejemplo de `describe-directories`, se muestran los detalles del directorio especificado.

```
aws ds describe-directories \
   --directory-id d-a1b2c3d4e5
```

Salida:


```
{
    "DirectoryDescriptions": [
        {
            "DirectoryId": "d-a1b2c3d4e5",
            "Name": "mydirectory.example.com",
            "ShortName": "mydirectory",
            "Size": "Small",
            "Edition": "Standard",
            "Alias": "d-a1b2c3d4e5",
            "AccessUrl": "d-a1b2c3d4e5.awsapps.com",
            "Stage": "Active",
            "ShareStatus": "Shared",
            "ShareMethod": "HANDSHAKE",
            "ShareNotes": "These are my share notes",
            "LaunchTime": "2019-07-08T15:33:46.327000-07:00",
            "StageLastUpdatedDateTime": "2019-07-08T15:59:12.307000-07:00",
            "Type": "SharedMicrosoftAD",
            "SsoEnabled": false,
            "DesiredNumberOfDomainControllers": 0,
            "OwnerDirectoryDescription": {
                "DirectoryId": "d-b2c3d4e5f6",
                "AccountId": "123456789111",
                "DnsIpAddrs": [
                    "203.113.0.248",
                    "203.113.0.253"
                ],
                "VpcSettings": {
                    "VpcId": "vpc-a1b2c3d4",
                    "SubnetIds": [
                        "subnet-a1b2c3d4",
                        "subnet-d4c3b2a1"
                    ],
                    "AvailabilityZones": [
                        "us-west-2a",
                        "us-west-2c"
                    ]
                }
            }
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeDirectories en la Referencia de comandos de la AWS CLI.

`describe-trusts`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-trusts`.

AWS CLI

Obtención de detalles sobre sus relaciones de confianza

En el siguiente ejemplo de `describe-trusts`, se muestran detalles sobre las relaciones de confianza del directorio especificado.

```
aws ds describe-trusts \
   --directory-id d-a1b2c3d4e5
```

Salida:

```
{
    "Trusts": [
        {
            "DirectoryId": "d-a1b2c3d4e5",
            "TrustId": "t-9a8b7c6d5e",
            "RemoteDomainName": "other.example.com",
            "TrustType": "Forest",
            "TrustDirection": "Two-Way",
            "TrustState": "Verified",
            "CreatedDateTime": "2017-06-20T18:08:45.614000-07:00",
            "LastUpdatedDateTime": "2019-06-04T10:52:12.410000-07:00",
            "StateLastUpdatedDateTime": "2019-06-04T10:52:12.410000-07:00",
            "SelectiveAuth": "Disabled"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeTrusts en la Referencia de comandos de la AWS CLI.

Ejemplos de datos de Directory Service que utilizan AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes mediante AWS Command Line Interface con datos de Directory Service.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-group-member`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-group-member`.

AWS CLI

Agregación de un miembro de grupo a un directorio

En el siguiente ejemplo de `add-group-member`, se agrega el usuario especificado al grupo especificado en el directorio especificado.

```
aws ds-data add-group-member \
    --directory-id d-1234567890 \
    --group-name 'sales' \
    --member-name 'john.doe'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adding or removing AWS Managed Microsoft AD members to groups and groups to groups en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte AddGroupMember en la Referencia de comandos de la AWS CLI.

`create-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-group`.

AWS CLI

Para enumerar los widgets disponibles

En el siguiente ejemplo de `create-group`, se crea un grupo en un directorio especificado.

```
aws ds-data create-group \
    --directory-id d-1234567890 \
    --sam-account-name "sales"
```

Salida:

```
{
    "DirectoryId": "d-1234567890",
    "SAMAccountName": "sales",
    "SID": "S-1-2-34-5567891234-5678912345-67891234567-8912"
}
```

Para obtener más información, consulte Creación de un grupo de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte CreateGroup en la Referencia de comandos de la AWS CLI.

`create-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-user`.

AWS CLI

Para crear un usuario

En el siguiente ejemplo de `create-user`, se crea un usuario en el directorio especificado.

```
aws ds-data create-user \
    --directory-id d-1234567890 \
    --sam-account-name 'john.doe'
```

Salida:

```
{
    "DirectoryId": "d-1234567890",
    "SAMAccountName": "john.doe",
    "SID": "S-1-2-34-5567891234-5678912345-67891234567-8912"
}
```

Para obtener más información, consulte Creación de un usuario de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte CreateUser en la Referencia de comandos de la AWS CLI.

`delete-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-group`.

AWS CLI

Para eliminar un grupo

En el siguiente ejemplo de `delete-group`, se elimina el grupo especificado del directorio especificado.

```
aws ds-data delete-group \
    --directory-id d-1234567890 \
    --sam-account-name 'sales'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de un grupo de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte DeleteGroup en la Referencia de comandos de la AWS CLI.

`delete-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-user`.

AWS CLI

Cómo eliminar un usuario

En el siguiente ejemplo de `delete-user`, se elimina el usuario especificado del directorio especificado.

```
aws ds-data delete-user \
    --directory-id d-1234567890 \
    --sam-account-name 'john.doe'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de un usuario de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte DeleteUser en la Referencia de comandos de la AWS CLI.

`describe-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-group`.

AWS CLI

Muestra de los detalles de un grupo

En el siguiente ejemplo de `describe-group`, se obtiene información del grupo especificado en el directorio especificado.

```
aws ds-data describe-group \
    --directory-id d-1234567890 \
    --sam-account-name 'sales'
```

Salida:

```
{
    "DirectoryId": "d-1234567890",
    "DistinguishedName": "CN=sales,OU=Users,OU=CORP,DC=corp,DC=example,DC=com",
    "GroupScope": "Global",
    "GroupType": "Security",
    "Realm": "corp.example.com",
    "SAMAccountName": "sales",
    "SID": "S-1-2-34-5567891234-5678912345-67891234567-8912"
}
```

Para obtener más información, consulte Visualización y actualización de los detalles de un grupo de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte DescribeGroup en la Referencia de comandos de la AWS CLI.

`describe-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-user`.

AWS CLI

Muestra de la información de un usuario

En el siguiente ejemplo de `describe-user`, se obtiene información del usuario especificado en el directorio especificado.

```
aws ds-data describe-user command-name \
    --directory-id d-1234567890 \
    --sam-account-name 'john.doe'
```

Salida:

```
{
    "DirectoryId": "d-1234567890",
    "DistinguishedName": "CN=john.doe,OU=Users,OU=CORP,DC=corp,DC=example,DC=com",
    "Enabled": false,
    "Realm": "corp.example.com",
    "SAMAccountName": "john.doe",
    "SID": "S-1-2-34-5678901234-5678901234-5678910123-4567",
    "UserPrincipalName": "john.doe@CORP.EXAMPLE.COM"
}
```

Para obtener más información, consulte Visualización y actualización de un usuario de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener detalles sobre la API, consulte DescribeUser en la Referencia de comandos de la AWS CLI.

`disable-directory-data-access`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-directory-data-access`.

AWS CLI

Desactivación de la API de Directory Service Data para un directorio

En el siguiente ejemplo de `disable-directory-data-access`, se desactiva la API de Directory Service Data para el directorio especificado.

```
aws ds disable-directory-data-access \
    --directory-id d-1234567890
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Habilitación o desactivación de la administración de usuarios y grupos o AWS Directory Service Data en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte DisableDirectoryDataAccess en la Referencia de comandos de la AWS CLI.

`disable-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-user`.

AWS CLI

Deshabilitación de un usuario

En el siguiente ejemplo de `disable-user`, se desactiva el usuario especificado del directorio especificado.

```
aws ds-data disable-user \
    --directory-id d-1234567890 \
    --sam-account-name 'john.doe'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Desactivación de un usuario de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte DisableUser en la Referencia de comandos de la AWS CLI.

`enable-directory-data-access`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-directory-data-access`.

AWS CLI

Habilitación de la API de Directory Service Data para un directorio

En el siguiente ejemplo de `enable-directory-data-access`, se habilita la API de Directory Service Data para el directorio especificado.

```
aws ds enable-directory-data-access \
    --directory-id d-1234567890
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Habilitación o desactivación de la administración de usuarios y grupos o AWS Directory Service Data en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte EnableDirectoryDataAccess en la Referencia de comandos de AWS CLI.

`list-group-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-group-members`.

AWS CLI

Muestra de los miembros del grupo de un directorio

En el siguiente ejemplo de `list-group-members`, se muestran los miembros del grupo especificado en el directorio especificado.

```
aws ds-data list-group-members \
    --directory-id d-1234567890 \
    --sam-account-name 'sales'
```

Salida:

```
{
    "Members": [
```

```
        {
            "MemberType": "USER",
            "SAMAccountName": "Jane Doe",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4568"
        },
        {
            "MemberType": "USER",
            "SAMAccountName": "John Doe",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4569"
        }
    ],
    "DirectoryId": "d-1234567890",
    "MemberRealm": "corp.example.com",
    "Realm": "corp.example.com"
}
```

Para obtener más información, consulte Visualización y actualización de los detalles de un grupo de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte ListGroupMembers en la Referencia de comandos de la AWS CLI.

`list-groups-for-member`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-groups-for-member`.

AWS CLI

Muestra de la pertenencia a grupos de un directorio

En el siguiente ejemplo de `list-groups-for-member`, se muestra la pertenencia a grupos de un usuario especificado en el directorio especificado.

```
aws ds-data list-groups-for-member \
    --directory-id d-1234567890 \
    --sam-account-name 'john.doe'
```

Salida:

```
{
    "Groups": [
        {
            "GroupScope": "Global",
```

```
            "GroupType": "Security",
            "SAMAccountName": "Domain Users",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4567"
        }
    ],
    "DirectoryId": "d-1234567890",
    "MemberRealm": "corp.example.com",
    "Realm": "corp.example.com"
}
```

Para obtener más información, consulte Visualización y actualización de un usuario de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte ListGroupsForMember en la Referencia de comandos de la AWS CLI.

`list-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-groups`.

AWS CLI

Muestra de los grupos de un directorio

En el siguiente ejemplo de `list-groups`, se muestran los grupos en el directorio especificado.

```
aws ds-data list-groups \
    --directory-id d-1234567890
```

Salida:

```
{
    "Groups": [
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Administrators",
            "SID": "S-1-2-33-441"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Users",
```

```
            "SID": "S-1-2-33-442"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Guests",
            "SID": "S-1-2-33-443"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Print Operators",
            "SID": "S-1-2-33-444"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Backup Operators",
            "SID": "S-1-2-33-445"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Replicator",
            "SID": "S-1-2-33-446"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Remote Desktop Users",
            "SID": "S-1-2-33-447"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Network Configuration Operators",
            "SID": "S-1-2-33-448"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Performance Monitor Users",
            "SID": "S-1-2-33-449"
        },
```

```
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Performance Log Users",
            "SID": "S-1-2-33-450"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Distributed COM Users",
            "SID": "S-1-2-33-451"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "IIS_IUSRS",
            "SID": "S-1-2-33-452"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Cryptographic Operators",
            "SID": "S-1-2-33-453"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Event Log Readers",
            "SID": "S-1-2-33-454"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Certificate Service DCOM Access",
            "SID": "S-1-2-33-456"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "RDS Remote Access Servers",
            "SID": "S-1-2-33-457"
        },
        {
            "GroupScope": "BuiltinLocal",
```

```
            "GroupType": "Security",
            "SAMAccountName": "RDS Endpoint Servers",
            "SID": "S-1-2-33-458"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "RDS Management Servers",
            "SID": "S-1-2-33-459"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Hyper-V Administrators",
            "SID": "S-1-2-33-460"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Access Control Assistance Operators",
            "SID": "S-1-2-33-461"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Remote Management Users",
            "SID": "S-1-2-33-462"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Storage Replica Administrators",
            "SID": "S-1-2-33-463"
        },
        {
            "GroupScope": "Global",
            "GroupType": "Security",
            "SAMAccountName": "Domain Computers",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-789"
        },
        {
            "GroupScope": "Global",
            "GroupType": "Security",
            "SAMAccountName": "Domain Controllers",
```

```
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-790"
        },
        {
            "GroupScope": "Universal",
            "GroupType": "Security",
            "SAMAccountName": "Schema Admins",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-791"
        },
        {
            "GroupScope": "Universal",
            "GroupType": "Security",
            "SAMAccountName": "Enterprise Admins",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-792"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "Cert Publishers",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-793"
        },
        {
            "GroupScope": "Global",
            "GroupType": "Security",
            "SAMAccountName": "Domain Admins",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-794"
        },
        {
            "GroupScope": "Global",
            "GroupType": "Security",
            "SAMAccountName": "Domain Users",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-795"
        },
        {
            "GroupScope": "Global",
            "GroupType": "Security",
            "SAMAccountName": "Domain Guests",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-796"
        },
        {
            "GroupScope": "Global",
            "GroupType": "Security",
            "SAMAccountName": "Group Policy Creator Owners",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-797"
        },
```

```
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "RAS and IAS Servers",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-798"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Server Operators",
            "SID": "S-1-2-33-464"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Account Operators",
            "SID": "S-1-2-33-465"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Pre-Windows 2000 Compatible Access",
            "SID": "S-1-2-33-466"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Incoming Forest Trust Builders",
            "SID": "S-1-2-33-467"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Windows Authorization Access Group",
            "SID": "S-1-2-33-468"
        },
        {
            "GroupScope": "BuiltinLocal",
            "GroupType": "Security",
            "SAMAccountName": "Terminal Server License Servers",
            "SID": "S-1-2-33-469"
        },
        {
            "GroupScope": "DomainLocal",
```

```
            "GroupType": "Security",
            "SAMAccountName": "Allowed RODC Password Replication Group",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-798"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "Denied RODC Password Replication Group",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-799"
        },
        {
            "GroupScope": "Global",
            "GroupType": "Security",
            "SAMAccountName": "Read-only Domain Controllers",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-800"
        },
        {
            "GroupScope": "Universal",
            "GroupType": "Security",
            "SAMAccountName": "Enterprise Read-only Domain Controllers",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-801"
        },
        {
            "GroupScope": "Global",
            "GroupType": "Security",
            "SAMAccountName": "Cloneable Domain Controllers",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-802"
        },
        {
            "GroupScope": "Global",
            "GroupType": "Security",
            "SAMAccountName": "Protected Users",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-803"
        },
        {
            "GroupScope": "Global",
            "GroupType": "Security",
            "SAMAccountName": "Key Admins",
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-804"
        },
        {
            "GroupScope": "Universal",
            "GroupType": "Security",
            "SAMAccountName": "Enterprise Key Admins",
```

```
            "SID": "S-1-2-34-56789123456-7891012345-6789123486-805"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "DnsAdmins",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4567"
        },
        {
            "GroupScope": "Global",
            "GroupType": "Security",
            "SAMAccountName": "DnsUpdateProxy",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4568"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "Admins",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4569"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWSAdministrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4570"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Object Management Service Accounts",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4571"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Private CA Connector for AD Delegated Group",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4572"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Application and Service Delegated Group",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4573"
        },
```

```
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4574"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated FSx Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4575"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Account Operators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4576"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Active Directory Based Activation
Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4577"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Allowed to Authenticate Objects",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4578"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Allowed to Authenticate to Domain
Controllers",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4579"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Deleted Object Lifetime
Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4580"
```

```
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Distributed File System
Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4581"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Dynamic Host Configuration Protocol
Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4582"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Enterprise Certificate Authority
Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4583"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Fine Grained Password Policy
Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4584"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Group Policy Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4585"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Managed Service Account
Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4586"
        },
        {
            "GroupScope": "DomainLocal",
```

```
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Read Foreign Security Principals",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4587"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Remote Access Service Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4588"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Replicate Directory Changes
Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4588"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Sites and Services Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4589"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated System Management Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4590"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Terminal Server Licensing
Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4591"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated User Principal Name Suffix
Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4592"
        },
        {
```

```
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Add Workstations To Domain Users",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4593"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Domain Name System Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4594"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Kerberos Delegation Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4595"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated Server Administrators",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4596"
        },
        {
            "GroupScope": "DomainLocal",
            "GroupType": "Security",
            "SAMAccountName": "AWS Delegated MS-NPRC Non-Compliant Devices",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4597"
        },
        {
            "GroupScope": "Global",
            "GroupType": "Security",
            "SAMAccountName": "Remote Access",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4598"
        },
        {
            "GroupScope": "Global",
            "GroupType": "Security",
            "SAMAccountName": "Accounting",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4599"
        },
        {
            "GroupScope": "Global",
            "GroupType": "Distribution",
```

```
            "SAMAccountName": "sales",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4567"
        }
    ],
    "DirectoryId": "d-1234567890",
    "Realm": "corp.example.com"
}
```

Para obtener más información, consulte Visualización y actualización de los detalles de un grupo de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte ListGroups en la Referencia de comandos de la AWS CLI.

`list-users`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-users`.

AWS CLI

Muestra de los usuarios de un directorio

En el siguiente ejemplo de `list-users`, se muestran los usuarios en el directorio especificado.

```
aws ds-data list-users \
    --directory-id d-1234567890
```

Salida:

```
{
    "Users": [
        {
            "Enabled": true,
            "SAMAccountName": "Administrator",
            "SID": "S-1-2-34-5678910123-4567895012-3456789012-345"
        },
        {
            "Enabled": false,
            "SAMAccountName": "Guest",
            "SID": "S-1-2-34-5678910123-4567895012-3456789012-345"
        },
        {
```

```
            "Enabled": false,
            "SAMAccountName": "krbtgt",
            "SID": "S-1-2-34-5678910123-4567895012-3456789012-346"
        },
        {
            "Enabled": true,
            "SAMAccountName": "Admin",
            "SID": "S-1-2-34-5678910123-4567895012-3456789012-347"
        },
        {
            "Enabled": true,
            "SAMAccountName": "Richard Roe",
            "SID": "S-1-2-34-5678910123-4567895012-3456789012-348"
        },
        {
            "Enabled": true,
            "SAMAccountName": "Jane Doe",
            "SID": "S-1-2-34-5678910123-4567895012-3456789012-349"
        },
        {
            "Enabled": true,
            "SAMAccountName": "AWS_WGnzYlN6YyY",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4567"
        },
        {
            "Enabled": true,
            "SAMAccountName": "john.doe",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4568"
        }
    ],
    "DirectoryId": "d-1234567890",
    "Realm": "corp.example.com"
}
```

Para obtener más información, consulte Visualización y actualización de un usuario de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte ListUsers en la Referencia de comandos de la AWS CLI.

`remove-group-member`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-group-member`.

AWS CLI

Eliminación de un miembro de un grupo de un directorio

En el siguiente ejemplo de `remove-group-member`, se elimina el miembro del grupo especificado en el directorio especificado.

```
aws ds-data remove-group-member \
    --directory-id d-1234567890 \
    --group-name 'sales' \
    --member-name 'john.doe'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adding or removing AWS Managed Microsoft AD members to groups and groups to groups en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte RemoveGroupMember en la Referencia de comandos de la AWS CLI.

`reset-user-password`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-user-password`.

AWS CLI

Restablecimiento de una contraseña de usuario en un directorio

En el siguiente ejemplo de `reset-user-password`, se restablece y habilita el usuario especificado del directorio especificado.

```
aws ds reset-user-password \
    --directory-id d-1234567890 \
    --user-name 'john.doe' \
    --new-password 'password'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Restablecimiento y habilitación de la contraseña de un usuario de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte ResetUserPassword en la Referencia de comandos de la AWS CLI.

`search-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-groups`.

AWS CLI

Búsqueda de un grupo en un directorio

En el siguiente ejemplo de `search-groups`, se busca el grupo especificado en el directorio especificado.

```
aws ds-data search-groups \
    --directory-id d-1234567890 \
    --search-attributes 'SamAccountName' \
    --search-string 'sales'
```

Salida:

```
{
    "Groups": [
        {
            "GroupScope": "Global",
            "GroupType": "Distribution",
            "SAMAccountName": "sales",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4567"
        }
    ],
    "DirectoryId": "d-1234567890",
    "Realm": "corp.example.com"
}
```

Para obtener más información, consulte Visualización y actualización de los detalles de un grupo de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte SearchGroups en la Referencia de comandos de la AWS CLI.

`search-users`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-users`.

AWS CLI

Búsqueda de un usuario en un directorio

En el siguiente ejemplo de `search-users`, se busca el usuario especificado en el directorio especificado.

```
aws ds-data search-users \
    --directory-id d-1234567890 \
    --search-attributes 'SamAccountName' \
    --Search-string 'john.doe'
```

Salida:

```
{
    "Users": [
        {
            "Enabled": true,
            "SAMAccountName": "john.doe",
            "SID": "S-1-2-34-5678901234-5678901234-5678910123-4567"
        }
    ],
    "DirectoryId": "d-1234567890",
    "Realm": "corp.example.com"
}
```

Para obtener más información, consulte Visualización y actualización de un usuario de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte SearchUsers en la Referencia de comandos de la AWS CLI.

`update-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-group`.

AWS CLI

Actualización del atributo de un grupo en un directorio

En el siguiente ejemplo de `update-group`, se actualiza el atributo especificado para el grupo especificado en el directorio especificado.

```
aws ds-data update-group \
    --directory-id d-1234567890 \
    --sam-account-name 'sales' \
    --update-type 'REPLACE' \
    --group-type 'Distribution'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Visualización y actualización de los detalles de un grupo de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte UpdateGroup en la Referencia de comandos de la AWS CLI.

`update-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-user`.

AWS CLI

Actualización del atributo de un usuario en un directorio

En el siguiente ejemplo de `update-user`, se actualiza el atributo especificado para el usuario especificado en el directorio especificado.

```
aws ds-data update-user \
    --directory-id d-1234567890 \
    --sam-account-name 'john.doe' \
    --update-type 'ADD' \
    --email-address 'example.corp.com'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Visualización y actualización de un usuario de Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

- Para obtener información sobre la API, consulte UpdateUser en la Referencia de comandos de la AWS CLI.

AWS DMS Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS DMS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-tags-to-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-tags-to-resource`.

AWS CLI

Para agregar etiquetas a un recurso

En el siguiente ejemplo de `add-tags-to-resource`, se añaden etiquetas a una instancia de replicación.

```
aws dms add-tags-to-resource \
    --resource-arn arn:aws:dms:us-east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE
 \
    --tags Key=Environment,Value=PROD Key=Project,Value=dbMigration
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging Resources en la Guía del usuario de AWS Database Migration Service.

- Para obtener información sobre la API, consulte AddTagsToResource en la Referencia de comandos de la AWS CLI.

`create-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-endpoint`.

AWS CLI

Creación de un punto de conexión

En el siguiente ejemplo de `create-endpoint`, se crea un punto de conexión para un origen de Amazon S3.

```
aws dms create-endpoint \
    --endpoint-type source \
    --engine-name s3 \
    --endpoint-identifier src-endpoint \
    --s3-settings file://s3-settings.json
```

Contenido de `s3-settings.json`:

```
{
    "BucketName":"my-corp-data",
    "BucketFolder":"sourcedata",
    "ServiceAccessRoleArn":"arn:aws:iam::123456789012:role/my-s3-access-role"
}
```

Salida:

```
{
    "Endpoint": {
        "EndpointIdentifier": "src-endpoint",
        "EndpointType": "SOURCE",
        "EngineName": "s3",
        "EngineDisplayName": "Amazon S3",
        "ExtraConnectionAttributes": "bucketFolder=sourcedata;bucketName=my-corp-
data;compressionType=NONE;csvDelimiter=,;csvRowDelimiter=\\n;",
        "Status": "active",
        "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:GUVAFG34EECUOJ6QVZ56DAHT3U",
        "SslMode": "none",
        "ServiceAccessRoleArn": "arn:aws:iam::123456789012:role/my-s3-access-role",
        "S3Settings": {
            "ServiceAccessRoleArn": "arn:aws:iam::123456789012:role/my-s3-access-
role",
```

```
            "CsvRowDelimiter": "\\n",
            "CsvDelimiter": ",",
            "BucketFolder": "sourcedata",
            "BucketName": "my-corp-data",
            "CompressionType": "NONE",
            "EnableStatistics": true
        }
    }
}
```

Para obtener más información, consulte Working with AWS DMS Endpoints en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte CreateEndpoint en la Referencia de comandos de la AWS CLI.

`create-event-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-event-subscription`.

AWS CLI

Para enumerar las suscripciones a eventos

En el siguiente ejemplo de `create-event-subscription`, se crea una suscripción de eventos a un tema de Amazon SNS (my-sns-topic).

```
aws dms create-event-subscription \
    --subscription-name my-dms-events \
    --sns-topic-arn arn:aws:sns:us-east-1:123456789012:my-sns-topic
```

Salida:

```
{
    "EventSubscription": {
        "CustomerAwsId": "123456789012",
        "CustSubscriptionId": "my-dms-events",
        "SnsTopicArn": "arn:aws:sns:us-east-1:123456789012:my-sns-topic",
        "Status": "creating",
        "SubscriptionCreationTime": "2020-05-21 21:58:38.598",
        "Enabled": true
    }
```

```
}
```

Para obtener más información, consulte Working with Events and Notifications en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte CreateEventSubscription en la Referencia de comandos de la AWS CLI.

`create-replication-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-replication-instance`.

AWS CLI

Creación de una instancia de replicación

En el siguiente ejemplo de `create-replication-instance`, se crea una instancia de replicación.

```
aws dms create-replication-instance \
    --replication-instance-identifier my-repl-instance \
    --replication-instance-class dms.t2.micro \
    --allocated-storage 5
```

Salida:

```
{
    "ReplicationInstance": {
        "ReplicationInstanceIdentifier": "my-repl-instance",
        "ReplicationInstanceClass": "dms.t2.micro",
        "ReplicationInstanceStatus": "creating",
        "AllocatedStorage": 5,
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-f839b688",
                "Status": "active"
            }
        ],
        "ReplicationSubnetGroup": {
            "ReplicationSubnetGroupIdentifier": "default",
            "ReplicationSubnetGroupDescription": "default",
            "VpcId": "vpc-136a4c6a",
            "SubnetGroupStatus": "Complete",
```

```
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-da327bf6",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1a"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-42599426",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1d"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-bac383e0",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1c"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-6746046b",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1f"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-d7c825e8",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1e"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-cbfff283",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1b"
                    },
                    "SubnetStatus": "Active"
                }
            ]
```

```
        },
        "PreferredMaintenanceWindow": "sat:12:35-sat:13:05",
        "PendingModifiedValues": {},
        "MultiAZ": false,
        "EngineVersion": "3.3.2",
        "AutoMinorVersionUpgrade": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/f7bc0f8e-1a3a-4ace-9faa-
e8494fa3921a",
        "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:ZK2VQBUWFDBAWHIXHAYG5G2PKY",
        "PubliclyAccessible": true
    }
}
```

Para obtener más información, consulte Working with an AWS DMS Replication Instance en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte CreateReplicationInstance en la Referencia de comandos de la AWS CLI.

`create-replication-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-replication-subnet-group`.

AWS CLI

Para crear un grupo de subredes

En el siguiente ejemplo de `create-replication-subnet-group`, se crea un grupo compuesto por tres subredes.

```
aws dms create-replication-subnet-group \
    --replication-subnet-group-identifier my-subnet-group \
    --replication-subnet-group-description "my subnet group" \
    --subnet-ids subnet-da327bf6 subnet-bac383e0 subnet-d7c825e8
```

Salida:

```
{
    "ReplicationSubnetGroup": {
```

```
        "ReplicationSubnetGroupIdentifier": "my-subnet-group",
        "ReplicationSubnetGroupDescription": "my subnet group",
        "VpcId": "vpc-136a4c6a",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-da327bf6",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1a"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-bac383e0",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-d7c825e8",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1e"
                },
                "SubnetStatus": "Active"
            }
        ]
    }
}
```

Para obtener más información, consulte Setting Up a Network for a Replication Instance en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte CreateReplicationSubnetGroup en la Referencia de comandos de la AWS CLI.

`create-replication-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-replication-task`.

AWS CLI

Creación de una tarea de replicación

En el siguiente ejemplo de `create-replication-task`, se crea una tarea de replicación.

```
aws dms create-replication-task \
    --replication-task-identifier movedata \
    --source-endpoint-arn arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA \
    --target-endpoint-arn arn:aws:dms:us-
east-1:123456789012:endpoint:EOM4SFKCZEYHZBFGAGZT3QEC5U \
    --replication-instance-arn $RI_ARN \
    --migration-type full-load \
    --table-mappings file://table-mappings.json
```

Contenido de `table-mappings.json`:

```
{
    "rules": [
        {
            "rule-type": "selection",
            "rule-id": "1",
            "rule-name": "1",
            "object-locator": {
                "schema-name": "prodrep",
                "table-name": "%"
            },
            "rule-action": "include",
            "filters": []
        }
    ]
}
```

Salida:

```
{
    "ReplicationTask": {
        "ReplicationTaskIdentifier": "moveit2",
        "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA",
        "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EOM4SFKCZEYHZBFGAGZT3QEC5U",
        "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE",
        "MigrationType": "full-load",
        "TableMappings": ...output omitted... ,
```

```
        "ReplicationTaskSettings": ...output omitted... ,
        "Status": "creating",
        "ReplicationTaskCreationDate": 1590524772.505,
        "ReplicationTaskArn": "arn:aws:dms:us-
east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII"
    }
}
```

Para obtener más información, consulte Working with AWS DMS Tasks en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte CreateReplicationTask en la Referencia de comandos de la AWS CLI.

`delete-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-connection`.

AWS CLI

Para eliminar una conexión

El siguiente ejemplo de `delete-connection`, se desasocia un punto de conexión de una instancia de replicación.

```
aws dms delete-connection \
    --endpoint-arn arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA \
    --replication-instance-arn arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE
```

Salida:

```
{
    "Connection": {
        "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE",
        "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA",
        "Status": "deleting",
        "EndpointIdentifier": "src-database-1",
        "ReplicationInstanceIdentifier": "my-repl-instance"
    }
```

```
}
```

Para obtener más información, consulte https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Endpoints.Creating.html en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DeleteConnection en la Referencia de comandos de la AWS CLI.

`delete-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-endpoint`.

AWS CLI

Para eliminar un punto de conexión

En el siguiente ejemplo de la `delete-endpoint`, se elimina un punto de conexión.

```
aws dms delete-endpoint \
    --endpoint-arn arn:aws:dms:us-east-1:123456789012:endpoint:OUJJVXO4XZ4CYTSEG5XGMN2R3Y
```

Salida:

```
{
    "Endpoint": {
        "EndpointIdentifier": "src-endpoint",
        "EndpointType": "SOURCE",
        "EngineName": "s3",
        "EngineDisplayName": "Amazon S3",
        "ExtraConnectionAttributes": "bucketFolder=sourcedata;bucketName=my-corp-data;compressionType=NONE;csvDelimiter=,;csvRowDelimiter=\\n;",
        "Status": "deleting",
        "EndpointArn": "arn:aws:dms:us-east-1:123456789012:endpoint:OUJJVXO4XZ4CYTSEG5XGMN2R3Y",
        "SslMode": "none",
        "ServiceAccessRoleArn": "arn:aws:iam::123456789012:role/my-s3-access-role",
        "S3Settings": {
            "ServiceAccessRoleArn": "arn:aws:iam::123456789012:role/my-s3-access-role",
            "CsvRowDelimiter": "\\n",
            "CsvDelimiter": ",",
            "BucketFolder": "sourcedata",
```

```
            "BucketName": "my-corp-data",
            "CompressionType": "NONE",
            "EnableStatistics": true
        }
    }
}
```

Para obtener más información, consulte Working with AWS DMS Endpoints en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DeleteEndpoint en la Referencia de comandos de la AWS CLI.

`delete-event-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-event-subscription`.

AWS CLI

Para eliminar la suscripción a un evento

En el siguiente ejemplo de `delete-event-subscription`, se elimina una suscripción a un tema de Amazon SNS.

```
aws dms delete-event-subscription \
    --subscription-name "my-dms-events"
```

Salida:

```
{
    "EventSubscription": {
        "CustomerAwsId": "123456789012",
        "CustSubscriptionId": "my-dms-events",
        "SnsTopicArn": "arn:aws:sns:us-east-1:123456789012:my-sns-topic",
        "Status": "deleting",
        "SubscriptionCreationTime": "2020-05-21 21:58:38.598",
        "Enabled": true
    }
}
```

Para obtener más información, consulte Working with Events and Notifications en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DeleteEventSubscription en la Referencia de comandos de la AWS CLI.

`delete-replication-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-replication-instance`.

AWS CLI

Eliminación de una instancia de replicación

En el siguiente ejemplo de la `delete-replication-instance`, se elimina una instancia de replicación.

```
aws dms delete-replication-instance \
    --replication-instance-arn arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE
```

Salida:

```
{
    "ReplicationInstance": {
        "ReplicationInstanceIdentifier": "my-repl-instance",
        "ReplicationInstanceClass": "dms.t2.micro",
        "ReplicationInstanceStatus": "deleting",
        "AllocatedStorage": 5,
        "InstanceCreateTime": 1590011235.952,
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-f839b688",
                "Status": "active"
            }
        ],
        "AvailabilityZone": "us-east-1e",
        "ReplicationSubnetGroup": {
            "ReplicationSubnetGroupIdentifier": "default",
            "ReplicationSubnetGroupDescription": "default",
            "VpcId": "vpc-136a4c6a",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-da327bf6",
```

```
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1a"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-42599426",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1d"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-bac383e0",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1c"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-6746046b",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1f"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-d7c825e8",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1e"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-cbfff283",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1b"
                    },
                    "SubnetStatus": "Active"
                }
            ]
        },
        "PreferredMaintenanceWindow": "wed:11:42-wed:12:12",
        "PendingModifiedValues": {},
```

```
        "MultiAZ": true,
        "EngineVersion": "3.3.2",
        "AutoMinorVersionUpgrade": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/f7bc0f8e-1a3a-4ace-9faa-
e8494fa3921a",
        "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE",
        "ReplicationInstancePublicIpAddress": "54.225.120.92",
        "ReplicationInstancePrivateIpAddress": "172.31.30.121",
        "ReplicationInstancePublicIpAddresses": [
            "54.225.120.92",
            "3.230.18.248"
        ],
        "ReplicationInstancePrivateIpAddresses": [
            "172.31.30.121",
            "172.31.75.90"
        ],
        "PubliclyAccessible": true,
        "SecondaryAvailabilityZone": "us-east-1b"
    }
}
```

Para obtener más información, consulte Working with an AWS DMS Replication Instance en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DeleteReplicationInstance en la Referencia de comandos de la AWS CLI.

`delete-replication-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-replication-subnet-group`.

AWS CLI

Para eliminar un grupo de subredes

En el siguiente ejemplo de `delete-replication-subnet-group`, se elimina el grupo de subredes:

```
aws dms delete-replication-subnet-group \
--replication-subnet-group-identifier my-subnet-group
```

Salida:

```
(none)
```

Para obtener más información, consulte Setting Up a Network for a Replication Instance en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DeleteReplicationSubnetGroup en la Referencia de comandos de la AWS CLI.

`delete-replication-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-replication-task`.

AWS CLI

Eliminación de una tarea de replicación

En el siguiente ejemplo de `delete-replication-task`, se elimina una tarea de replicación.

```
aws dms delete-replication-task \
    --replication-task-arn arn:aws:dms:us-
east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII
```

Salida:

```
{
    "ReplicationTask": {
        "ReplicationTaskIdentifier": "moveit2",
        "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA",
        "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EOM4SFKCZEYHZBFGAGZT3QEC5U",
        "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE",
        "MigrationType": "full-load",
        "TableMappings": ...output omitted...,
        "ReplicationTaskSettings": ...output omitted...,
        "Status": "deleting",
        "StopReason": "Stop Reason FULL_LOAD_ONLY_FINISHED",
        "ReplicationTaskCreationDate": 1590524772.505,
```

```
        "ReplicationTaskStartDate": 1590789988.677,
        "ReplicationTaskArn": "arn:aws:dms:us-
east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII"
    }
}
```

Para obtener más información, consulte Working with AWS DMS Tasks en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DeleteReplicationTask en la Referencia de comandos de la AWS CLI.

`describe-account-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-account-attributes`.

AWS CLI

Descripción de atributos de cuenta

En el siguiente ejemplo de `describe-account-attributes`, se enumeran los atributos de su cuenta de AWS.

```
aws dms describe-account-attributes
```

Salida:

```
{
    "AccountQuotas": [
        {
            "AccountQuotaName": "ReplicationInstances",
            "Used": 1,
            "Max": 20
        },
        {
            "AccountQuotaName": "AllocatedStorage",
            "Used": 5,
            "Max": 10000
        },

        ...remaining output omitted...
```

```
    ],
    "UniqueAccountIdentifier": "cqahfbfy5xee"
}
```

- Para obtener información sobre la API, consulte DescribeAccountAttributes en la Referencia de comandos de la AWS CLI.

`describe-certificates`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-certificates`.

AWS CLI

Para enumerar los certificados disponibles

En el siguiente ejemplo de `describe-certificates`, se enumeran los certificados registrados en su cuenta de AWS.

```
aws dms describe-certificates
```

Salida:

```
{
    "Certificates": [
        {
            "CertificateIdentifier": "my-cert",
            "CertificateCreationDate": 1543259542.506,
            "CertificatePem": "-----BEGIN CERTIFICATE-----
\nMIID9DCCAtygAwIBAgIBQjANBgkqhkiG9w0BAQ ...U"

            ... remaining output omittted ...

        }
    ]
}
```

Para obtener más información, consulte Using SSL en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DescribeCertificates en la Referencia de comandos de la AWS CLI.

`describe-connections`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-connections`.

AWS CLI

Descripción de conexiones

El siguiente ejemplo de `describe-connections`, se muestra una lista de las conexiones que ha probado entre una instancia de replicación y un punto de conexión.

```
aws dms describe-connections
```

Salida:

```
{
    "Connections": [
        {
            "Status": "successful",
            "ReplicationInstanceIdentifier": "test",
            "EndpointArn": "arn:aws:dms:us-east-arn:aws:dms:us-
east-1:123456789012:endpoint:ZW5UAN6P4E77EC7YWHK4RZZ3BE",
            "EndpointIdentifier": "testsrc1",
            "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:6UTDJGBOUS3VI3SUWA66XFJCJQ"
        }
    ]
}
```

Para obtener más información, consulte Creating Source and Target Endpoints en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DescribeConnections en la Referencia de comandos de la AWS CLI.

`describe-endpoint-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-endpoint-types`.

AWS CLI

Para enumerar los tipos de puntos de conexión disponibles

En el siguiente ejemplo de `describe-endpoint-types`, se enumeran los tipos de puntos de conexión de MySQL que están disponibles.

```
aws dms describe-endpoint-types \
    --filters "Name=engine-name,Values=mysql"
```

Salida:

```
{
    "SupportedEndpointTypes": [
        {
            "EngineName": "mysql",
            "SupportsCDC": true,
            "EndpointType": "source",
            "EngineDisplayName": "MySQL"
        },
        {
            "EngineName": "mysql",
            "SupportsCDC": true,
            "EndpointType": "target",
            "EngineDisplayName": "MySQL"
        }
    ]
}
```

Para obtener más información, consulte Working with AWS DMS Endpoints <https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Endpoints.html>`__ en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DescribeEndpointTypes en la Referencia de comandos de la AWS CLI.

`describe-endpoints`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-endpoints`.

AWS CLI

Descripción de puntos de conexión

En el siguiente ejemplo de `describe-endpoints`, se enumeran los puntos de conexión para su cuenta de AWS.

```
aws dms describe-endpoints
```

Salida:

```
{
    "Endpoints": [
        {
            "Username": "dms",
            "Status": "active",
            "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:SF2WOFLWYWKVEOHID2EKLP3SJI",
            "ServerName": "ec2-52-32-48-61.us-west-2.compute.amazonaws.com",
            "EndpointType": "SOURCE",
            "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/94d5c4e7-4e4c-44be-
b58a-c8da7adf57cd",
            "DatabaseName": "test",
            "EngineName": "mysql",
            "EndpointIdentifier": "pri100",
            "Port": 8193
        },
        {
            "Username": "admin",
            "Status": "active",
            "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TJJZCIH3CJ24TJRU4VC32WEWFR",
            "ServerName": "test.example.com",
            "EndpointType": "SOURCE",
            "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/2431021b-1cf2-
a2d4-77b2-59a9e4bce323",
            "DatabaseName": "EMPL",
            "EngineName": "oracle",
            "EndpointIdentifier": "test",
            "Port": 1521
        }
    ]
}
```

Para obtener más información, consulte Working with AWS DMS Endpoints en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DescribeEndpoints en la Referencia de comandos de la AWS CLI.

`describe-event-categories`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-event-categories`.

AWS CLI

Para describir las categorías de eventos

En el siguiente ejemplo de `describe-event-categories`, se enumeran las categorías de eventos disponibles.

```
aws dms describe-event-categories
```

Salida:

```
{
    "EventCategoryGroupList": [
        {
            "SourceType": "replication-instance",
            "EventCategories": [
                "low storage",
                "configuration change",
                "maintenance",
                "deletion",
                "creation",
                "failover",
                "failure"
            ]
        },
        {
            "SourceType": "replication-task",
            "EventCategories": [
                "configuration change",
                "state change",
                "deletion",
                "creation",
                "failure"
            ]
        }
    ]
}
```

Para obtener más información, consulte Working with Events and Notifications en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DescribeEventCategories en la Referencia de comandos de la AWS CLI.

`describe-event-subscriptions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-event-subscriptions`.

AWS CLI

Para describir suscripciones a eventos

En el siguiente ejemplo de `describe-event-subscriptions`, se enumeran las suscripciones a eventos para un tema de Amazon SNS.

```
aws dms describe-event-subscriptions
```

Salida:

```
{
    "EventSubscriptionsList": [
        {
            "CustomerAwsId": "123456789012",
            "CustSubscriptionId": "my-dms-events",
            "SnsTopicArn": "arn:aws:sns:us-east-1:123456789012:my-sns-topic",
            "Status": "deleting",
            "SubscriptionCreationTime": "2020-05-21 22:28:51.924",
            "Enabled": true
        }
    ]
}
```

Para obtener más información, consulte Working with Events and Notifications en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DescribeEventSubscriptions en la Referencia de comandos de la AWS CLI.

`describe-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-events`.

AWS CLI

Para enumerar los eventos de DMS

En el siguiente ejemplo de `describe-events`, se enumeran los eventos que se originaron en una instancia de replicación.

```
aws dms describe-events \
    --source-type "replication-instance"
```

Salida:

```
{
    "Events": [
        {
            "SourceIdentifier": "my-repl-instance",
            "SourceType": "replication-instance",
            "Message": "Replication application shutdown",
            "EventCategories": [],
            "Date": 1590771645.776
        }
    ]
}
```

Para obtener más información, consulte Working with Events and Notifications en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DescribeEvents en la Referencia de comandos de la AWS CLI.

`describe-orderable-replication-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-orderable-replication-instances`.

AWS CLI

Descripción de las instancias de replicación que se pueden solicitar

En el siguiente ejemplo de `describe-orderable-replication-instances`, se enumeran los tipos de instancias de replicación que puede solicitar.

```
aws dms describe-orderable-replication-instances
```

Salida:

```
{
    "OrderableReplicationInstances": [
        {
            "EngineVersion": "3.3.2",
            "ReplicationInstanceClass": "dms.c4.2xlarge",
            "StorageType": "gp2",
            "MinAllocatedStorage": 5,
            "MaxAllocatedStorage": 6144,
            "DefaultAllocatedStorage": 100,
            "IncludedAllocatedStorage": 100,
            "AvailabilityZones": [
                "us-east-1a",
                "us-east-1b",
                "us-east-1c",
                "us-east-1d",
                "us-east-1e",
                "us-east-1f"
            ]
        },
        {
            "EngineVersion": "3.3.2",
            "ReplicationInstanceClass": "dms.c4.4xlarge",
            "StorageType": "gp2",
            "MinAllocatedStorage": 5,
            "MaxAllocatedStorage": 6144,
            "DefaultAllocatedStorage": 100,
            "IncludedAllocatedStorage": 100,
            "AvailabilityZones": [
                "us-east-1a",
                "us-east-1b",
                "us-east-1c",
                "us-east-1d",
                "us-east-1e",
                "us-east-1f"
            ]
        },
```

```
        ...remaining output omitted...

    }
```

Para obtener más información, consulte Working with an AWS DMS Replication Instance en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DescribeOrderableReplicationInstances en la Referencia de comandos de la AWS CLI.

`describe-refresh-schemas-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-refresh-schemas-status`.

AWS CLI

Para enumerar el estado de actualización de un punto de conexión

El siguiente ejemplo de `describe-refresh-schemas-status` devuelve el estado de una solicitud de actualización anterior.

```
aws dms describe-refresh-schemas-status \
    --endpoint-arn arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA
```

Salida:

```
{
    "RefreshSchemasStatus": {
        "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA",
        "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE",
        "Status": "successful",
        "LastRefreshDate": 1590786544.605
    }
}
```

- Para obtener detalles sobre la API, consulte DescribeRefreshSchemasStatus en la Referencia de comandos de la AWS CLI.

describe-replication-instances

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-replication-instances`.

AWS CLI

Descripción de las instancias de replicación

En el siguiente ejemplo de `describe-replication-instances`, se enumeran las instancias de replicación de su cuenta de AWS.

```
aws dms describe-replication-instances
```

Salida:

```
{
    "ReplicationInstances": [
        {
            "ReplicationInstanceIdentifier": "my-repl-instance",
            "ReplicationInstanceClass": "dms.t2.micro",
            "ReplicationInstanceStatus": "available",
            "AllocatedStorage": 5,
            "InstanceCreateTime": 1590011235.952,
            "VpcSecurityGroups": [
                {
                    "VpcSecurityGroupId": "sg-f839b688",
                    "Status": "active"
                }
            ],
            "AvailabilityZone": "us-east-1e",
            "ReplicationSubnetGroup": {
                "ReplicationSubnetGroupIdentifier": "default",
                "ReplicationSubnetGroupDescription": "default",
                "VpcId": "vpc-136a4c6a",
                "SubnetGroupStatus": "Complete",
                "Subnets": [
                    {
                        "SubnetIdentifier": "subnet-da327bf6",
                        "SubnetAvailabilityZone": {
                            "Name": "us-east-1a"
                        },
                        "SubnetStatus": "Active"
                    },
```

```
                {
                    "SubnetIdentifier": "subnet-42599426",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1d"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-bac383e0",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1c"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-6746046b",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1f"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-d7c825e8",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1e"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-cbfff283",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1b"
                    },
                    "SubnetStatus": "Active"
                }
            ]
        },
        "PreferredMaintenanceWindow": "wed:11:42-wed:12:12",
        "PendingModifiedValues": {
            "MultiAZ": true
        },
        "MultiAZ": false,
        "EngineVersion": "3.3.2",
        "AutoMinorVersionUpgrade": true,
```

```
            "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/
f7bc0f8e-1a3a-4ace-9faa-e8494fa3921a",
            "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE",
            "ReplicationInstancePublicIpAddress": "3.230.18.248",
            "ReplicationInstancePrivateIpAddress": "172.31.75.90",
            "ReplicationInstancePublicIpAddresses": [
                "3.230.18.248"
            ],
            "ReplicationInstancePrivateIpAddresses": [
                "172.31.75.90"
            ],
            "PubliclyAccessible": true,
            "FreeUntil": 1590194829.267
        }
    ]
}
```

Para obtener más información, consulte Working with an AWS DMS Replication Instance en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DescribeReplicationInstances en la Referencia de comandos de la AWS CLI.

`describe-replication-subnet-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-replication-subnet-groups`.

AWS CLI

Visualización de los grupos de subredes disponibles

En el siguiente ejemplo de `describe-replication-subnet-groups`, se enumeran los grupos de subredes disponibles.

```
aws dms describe-replication-subnet-groups \
    --filter "Name=replication-subnet-group-id,Values=my-subnet-group"
```

Salida:

```
{
```

```
    "ReplicationSubnetGroups": [
        {
            "ReplicationSubnetGroupIdentifier": "my-subnet-group",
            "ReplicationSubnetGroupDescription": "my subnet group",
            "VpcId": "vpc-136a4c6a",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-da327bf6",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1a"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-bac383e0",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1c"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-d7c825e8",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1e"
                    },
                    "SubnetStatus": "Active"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Setting Up a Network for a Replication Instance en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DescribeReplicationSubnetGroups en la Referencia de comandos de la AWS CLI.

`describe-replication-task-assessment-results`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-replication-task-assessment-results`.

AWS CLI

Para enumerar los resultados de las evaluaciones de las tareas de replicación

En el siguiente ejemplo de `describe-replication-task-assessment-results`, se enumeran los resultados de una evaluación de tareas anterior.

```
aws dms describe-replication-task-assessment-results
```

Salida:

```
{
    "ReplicationTaskAssessmentResults": [
        {
            "ReplicationTaskIdentifier": "moveit2",
            "ReplicationTaskArn": "arn:aws:dms:us-
east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII",
            "ReplicationTaskLastAssessmentDate": 1590790230.0,
            "AssessmentStatus": "No issues found",
            "AssessmentResultsFile": "moveit2/2020-05-29-22-10"
        }
    ]
}
```

Para obtener más información, consulte Creating a Task Assessment Report en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DescribeReplicationTaskAssessmentResults en la Referencia de comandos de la AWS CLI.

`describe-replication-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-replication-tasks`.

AWS CLI

Descripción de una tarea de replicación

En el siguiente ejemplo de `describe-replication-tasks`, se describen las tareas de replicación actuales.

```
aws dms describe-replication-tasks
```

Salida:

```
{
    "ReplicationTasks": [
        {
            "ReplicationTaskIdentifier": "moveit2",
            "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA",
            "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EOM4SFKCZEYHZBFGAGZT3QEC5U",
            "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE",
            "MigrationType": "full-load",
            "TableMappings": ...output omitted... ,
            "ReplicationTaskSettings": ...output omitted... ,
            "Status": "stopped",
            "StopReason": "Stop Reason FULL_LOAD_ONLY_FINISHED",
            "ReplicationTaskCreationDate": 1590524772.505,
            "ReplicationTaskStartDate": 1590619805.212,
            "ReplicationTaskArn": "arn:aws:dms:us-
east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII",
            "ReplicationTaskStats": {
                "FullLoadProgressPercent": 100,
                "ElapsedTimeMillis": 0,
                "TablesLoaded": 0,
                "TablesLoading": 0,
                "TablesQueued": 0,
                "TablesErrored": 0,
                "FreshStartDate": 1590619811.528,
                "StartDate": 1590619811.528,
                "StopDate": 1590619842.068
            }
        }
    ]
}
```

Para obtener más información, consulte Working with AWS DMS Tasks en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DescribeReplicationTasks en la Referencia de comandos de la AWS CLI.

`describe-schemas`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-schemas`.

AWS CLI

Descripción de los esquemas de bases de datos

En el siguiente ejemplo de `describe-schemas`, se enumeran las tablas que están disponibles en un punto de conexión.

```
aws dms describe-schemas \
    --endpoint-arn "arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA"
```

Salida:

```
{
    "Schemas": [
        "prodrep"
    ]
}
```

Para obtener más información, consulte This is the topic title en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte DescribeSchemas en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se añaden etiquetas a una instancia de replicación.

```
aws dms list-tags-for-resource \
    --resource-arn arn:aws:dms:us-east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE
```

Salida:

```
{
    "TagList": [
        {
            "Key": "Project",
            "Value": "dbMigration"
        },
        {
            "Key": "Environment",
            "Value": "PROD"
        }
    ]
}
```

Para obtener más información, consulte Tagging Resources en la Guía del usuario de AWS Database Migration Service.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`modify-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-endpoint`.

AWS CLI

Modificación de un punto de conexión

En el siguiente ejemplo de `modify-endpoint`, se añade un atributo de conexión adicional a un punto de conexión.

```
aws dms modify-endpoint \
    --endpoint-arn "arn:aws:dms:us-
east-1:123456789012:endpoint:GUVAFG34EECUOJ6QVZ56DAHT3U" \
    --extra-connection-attributes "compressionType=GZIP"
```

Salida:

```
{
    "Endpoint": {
        "EndpointIdentifier": "src-endpoint",
```

```
        "EndpointType": "SOURCE",
        "EngineName": "s3",
        "EngineDisplayName": "Amazon S3",
        "ExtraConnectionAttributes":
 "compressionType=GZIP;csvDelimiter=,;csvRowDelimiter=\\n;",
        "Status": "active",
        "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:GUVAFG34EECUOJ6QVZ56DAHT3U",
        "SslMode": "none",
        "ServiceAccessRoleArn": "arn:aws:iam::123456789012:role/my-s3-access-role",
        "S3Settings": {
            "ServiceAccessRoleArn": "arn:aws:iam::123456789012:role/my-s3-access-
role",
            "CsvRowDelimiter": "\\n",
            "CsvDelimiter": ",",
            "BucketFolder": "",
            "BucketName": "",
            "CompressionType": "GZIP",
            "EnableStatistics": true
        }
    }
}
```

Para obtener más información, consulte Working with AWS DMS Endpoints <https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Endpoints.html>`__ en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte ModifyEndpoint en la Referencia de comandos de la AWS CLI.

`modify-event-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-event-subscription`.

AWS CLI

Para modificar una suscripción a un evento

En el siguiente ejemplo de `modify-event-subscription`, se cambia el tipo de origen de una suscripción a un evento.

```
aws dms modify-event-subscription \
    --subscription-name "my-dms-events" \
```

```
    --source-type replication-task
```

Salida:

```
{
    "EventSubscription": {
        "CustomerAwsId": "123456789012",
        "CustSubscriptionId": "my-dms-events",
        "SnsTopicArn": "arn:aws:sns:us-east-1:123456789012:my-sns-topic",
        "Status": "modifying",
        "SubscriptionCreationTime": "2020-05-29 17:04:40.262",
        "SourceType": "replication-task",
        "Enabled": true
    }
}
```

Para obtener más información, consulte Working with Events and Notifications en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte ModifyEventSubscription en la Referencia de comandos de la AWS CLI.

`modify-replication-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-replication-instance`.

AWS CLI

Modificación de una instancia de replicación

En el siguiente ejemplo de `modify-replication-instance`, se modifica una instancia de replicación para que utilice una implementación Multi-AZ.

```
aws dms modify-replication-instance \
     --replication-instance-arn arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE \
     --multi-az
```

Salida:

```
{
```

```
    "ReplicationInstance": {
        "ReplicationInstanceIdentifier": "my-repl-instance",
        "ReplicationInstanceClass": "dms.t2.micro",
        "ReplicationInstanceStatus": "available",
        "AllocatedStorage": 5,
        "InstanceCreateTime": 1590011235.952,

        ...output omitted...

        "PendingModifiedValues": {
            "MultiAZ": true
        },
        "MultiAZ": false,
        "EngineVersion": "3.3.2",
        "AutoMinorVersionUpgrade": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/f7bc0f8e-1a3a-4ace-9faa-
e8494fa3921a",

        ...output omitted...

    }
}
```

Para obtener más información, consulte Working with an AWS DMS Replication Instance en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte ModifyReplicationInstance en la Referencia de comandos de la AWS CLI.

`modify-replication-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-replication-subnet-group`.

AWS CLI

Modificación de un grupo de subredes

En el siguiente ejemplo de `modify-replication-subnet-group`, se cambian las listas de subredes asociadas a un grupo de subredes.

```
aws dms modify-replication-subnet-group \
    --replication-subnet-group-identifier my-subnet-group \
```

```
    --subnet-id subnet-da327bf6 subnet-bac383e0
```

Salida:

```
{
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "my-subnet-group",
        "ReplicationSubnetGroupDescription": "my subnet group",
        "VpcId": "vpc-136a4c6a",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-da327bf6",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1a"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-bac383e0",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetStatus": "Active"
            }
        ]
    }
}
```

Para obtener más información, consulte Setting Up a Network for a Replication Instance en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte ModifyReplicationSubnetGroup en la Referencia de comandos de la AWS CLI.

`modify-replication-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-replication-task`.

AWS CLI

Modificación de una tarea de replicación

En el siguiente ejemplo de `modify-replication-task`, se cambian las asignaciones de tablas de una tarea.

```
aws dms modify-replication-task \
    --replication-task-arn "arn:aws:dms:us-
east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII" \
    --table-mappings file://table-mappings.json
```

Contenido de `table-mappings.json`:

```
{
    "rules": [
        {
            "rule-type": "selection",
            "rule-id": "1",
            "rule-name": "1",
            "object-locator": {
                "schema-name": "prodrep",
                "table-name": "ACCT_%"
            },
            "rule-action": "include",
            "filters": []
        }
    ]
}
```

Salida:

```
{
    "ReplicationTask": {
        "ReplicationTaskIdentifier": "moveit2",
        "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA",
        "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EOM4SFKCZEYHZBFGAGZT3QEC5U",
        "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE",
        "MigrationType": "full-load",
        "TableMappings": ...output omitted...,
        "ReplicationTaskSettings": ...output omitted...,
        "Status": "modifying",
        "StopReason": "Stop Reason FULL_LOAD_ONLY_FINISHED",
```

```
        "ReplicationTaskCreationDate": 1590524772.505,
        "ReplicationTaskStartDate": 1590789424.653,
        "ReplicationTaskArn": "arn:aws:dms:us-
east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII"
    }
}
```

Para obtener más información, consulte Working with AWS DMS Tasks en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte ModifyReplicationTask en la Referencia de comandos de la AWS CLI.

`reboot-replication-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `reboot-replication-instance`.

AWS CLI

Reinicio de una instancia de replicación

En el siguiente ejemplo de la `reboot-replication-instance`, se reinicia una instancia de replicación.

```
aws dms reboot-replication-instance \
    --replication-instance-arn arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE
```

Salida:

```
{
    "ReplicationInstance": {
        "ReplicationInstanceIdentifier": "my-repl-instance",
        "ReplicationInstanceClass": "dms.t2.micro",
        "ReplicationInstanceStatus": "rebooting",
        "AllocatedStorage": 5,
        "InstanceCreateTime": 1590011235.952,
    ... output omitted ...
    }
}
```

Para obtener más información, consulte Working with an AWS DMS Replication Instance en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte RebootReplicationInstance en la Referencia de comandos de la AWS CLI.

`refresh-schemas`

En el siguiente ejemplo de código, se muestra cómo utilizar `refresh-schemas`.

AWS CLI

Actualización de los esquemas de bases de datos

En el siguiente ejemplo de `refresh-schemas`, se solicita que AWS DMS actualice la lista de esquemas en un punto de conexión.

```
aws dms refresh-schemas \
    --replication-instance-arn arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE \
    --endpoint-arn "arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA"
```

Salida:

```
{
    "RefreshSchemasStatus": {
        "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA",
        "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE",
        "Status": "refreshing",
        "LastRefreshDate": 1590019949.103
    }
}
```

- Para obtener detalles sobre la API, consulte RefreshSchemas en la Referencia de comandos de la AWS CLI.

`reload-tables`

En el siguiente ejemplo de código, se muestra cómo utilizar `reload-tables`.

AWS CLI

Actualización de la lista de tablas disponibles en un punto de conexión

En el siguiente ejemplo de `reload-tables`, se vuelve a cargar la lista de tablas que están disponibles en un punto de conexión.

```
aws dms reload-tables \
    --replication-task-arn "arn:aws:dms:us-
east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII" \
    --tables-to-reload "SchemaName=prodrep,TableName=ACCT_BAL"
```

Salida:

```
{
    "ReplicationTaskArn": "arn:aws:dms:us-
east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII"
}
```

- Para obtener detalles sobre la API, consulte ReloadTables en la Referencia de comandos de la AWS CLI.

`remove-tags-from-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-tags-from-resource`.

AWS CLI

Eliminación de etiquetas de una instancia de replicación

En el siguiente ejemplo de `remove-tags-from-resource`, se eliminan etiquetas de una instancia de replicación.

```
aws dms remove-tags-from-resource \
    --resource-arn arn:aws:dms:us-east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE
 \
    --tag-keys Environment Project
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging Resources en la Guía del usuario de AWS Database Migration Service.

- Para obtener información sobre la API, consulte RemoveTagsFromResource en la Referencia de comandos de la AWS CLI.

`start-replication-task-assessment`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-replication-task-assessment`.

AWS CLI

Inicio de una evaluación de tareas

En el siguiente ejemplo de `start-replication-task-assessment`, se inicia una evaluación de la tarea de replicación.

```
aws dms start-replication-task-assessment \
    --replication-task-arn arn:aws:dms:us-
east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII
```

Salida:

```
{
    "ReplicationTask": {
        "ReplicationTaskIdentifier": "moveit2",
        "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA",
        "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EOM4SFKCZEYHZBFGAGZT3QEC5U",
        "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE",
        "MigrationType": "full-load",
        "TableMappings": ...output omitted...,
        "ReplicationTaskSettings": ...output omitted...,
        "Status": "testing",
        "StopReason": "Stop Reason FULL_LOAD_ONLY_FINISHED",
        "ReplicationTaskCreationDate": 1590524772.505,
        "ReplicationTaskStartDate": 1590789988.677,
        "ReplicationTaskArn": "arn:aws:dms:us-
east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII"
    }
}
```

Para obtener más información, consulte Creating a Task Assessment Report en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte StartReplicationTaskAssessment en la Referencia de comandos de la AWS CLI.

`start-replication-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-replication-task`.

AWS CLI

Inicio de una tarea de replicación

En el siguiente ejemplo de `command-name`, se genera una lista de los widgets disponibles en la cuenta de AWS.

```
aws dms start-replication-task \
    --replication-task-arn arn:aws:dms:us-
east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII \
    --start-replication-task-type reload-target
```

Salida:

```
{
    "ReplicationTask": {
        "ReplicationTaskIdentifier": "moveit2",
        "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA",
        "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EOM4SFKCZEYHZBFGAGZT3QEC5U",
        "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE",
        "MigrationType": "full-load",
        "TableMappings": ...output omitted... ,
        "ReplicationTaskSettings": ...output omitted... ,
        "Status": "starting",
        "ReplicationTaskCreationDate": 1590524772.505,
        "ReplicationTaskStartDate": 1590619805.212,
        "ReplicationTaskArn": "arn:aws:dms:us-
east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII"
    }
```

```
}
```

Para obtener más información, consulte Working with AWS DMS Tasks en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte StartReplicationTask en la Referencia de comandos de la AWS CLI.

`stop-replication-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-replication-task`.

AWS CLI

Para detener una tarea

En el siguiente ejemplo de `stop-replication-task`, se detiene una tarea.

```
aws dms stop-replication-task \
    --replication-task-arn arn:aws:dms:us-
east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII
```

Salida:

```
{
    "ReplicationTask": {
        "ReplicationTaskIdentifier": "moveit2",
        "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA",
        "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EOM4SFKCZEYHZBFGAGZT3QEC5U",
        "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE",
        "MigrationType": "full-load",
        "TableMappings": ...output omitted...,
        "ReplicationTaskSettings": ...output omitted...,
        "Status": "stopping",
        "ReplicationTaskCreationDate": 1590524772.505,
        "ReplicationTaskStartDate": 1590789424.653,
        "ReplicationTaskArn": "arn:aws:dms:us-
east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII"
    }
```

```
}
```

Para obtener más información, consulte Working with AWS DMS Tasks en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte StopReplicationTask en la Referencia de comandos de la AWS CLI.

`test-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `test-connection`.

AWS CLI

Prueba de una conexión a un punto de conexión

En el siguiente ejemplo de `test-connection`, se comprueba si se puede acceder a un punto de conexión desde una instancia de replicación.

```
aws dms test-connection \
    --replication-instance-arn arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE \
    --endpoint-arn arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA
```

Salida:

```
{
    "Connection": {
        "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T3OM7OUB5NM2LCVZF7JPGJRNUE",
        "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:6GGI6YPWWGAYUVLKIB732KEVWA",
        "Status": "testing",
        "EndpointIdentifier": "src-database-1",
        "ReplicationInstanceIdentifier": "my-repl-instance"
    }
}
```

Para obtener más información, consulte Creating source and target endpoints en la Guía del usuario de AWS Database Migration Service.

- Para obtener detalles sobre la API, consulte TestConnection en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon DocumentDB que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando la AWS Command Line Interface con Amazon DocumentDB.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-tags-to-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-tags-to-resource`.

AWS CLI

Adición de una o varias etiquetas a un recurso especificado

En el siguiente ejemplo `add-tags-to-resource`, se agregan tres etiquetas a `sample-cluster`. Una etiqueta (`CropB`) tiene un nombre de clave pero no un valor.

```
aws docdb add-tags-to-resource \
    --resource-name arn:aws:rds:us-west-2:123456789012:cluster:sample-cluster \
    --tags Key="CropA",Value="Apple" Key="CropB" Key="CropC",Value="Corn"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging Amazon DocumentDB Resources en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener información sobre la API, consulte AddTagsToResource en la Referencia de comandos de la AWS CLI.

`apply-pending-maintenance-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `apply-pending-maintenance-action`.

AWS CLI

Acciones de mantenimiento pendientes: cómo hacer que se lleven a cabo durante el siguiente período de mantenimiento

El ejemplo `apply-pending-maintenance-action` siguiente hace que todas las acciones de actualización del sistema se realicen durante el siguiente período de mantenimiento programado.

```
aws docdb apply-pending-maintenance-action \
--resource-identifier arn:aws:rds:us-west-2:123456789012:cluster:sample-cluster \
--apply-action system-update \
--opt-in-type next-maintenance
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Applying Amazon DocumentDB Updates en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte ApplyPendingMaintenanceAction en la Referencia de comandos de la AWS CLI.

`copy-db-cluster-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-db-cluster-parameter-group`.

AWS CLI

Duplicación de un grupo de parámetros de clúster de DB existente

En el siguiente ejemplo de `copy-db-cluster-parameter-group`, se crea una copia de `custom-docdb3-6` llamada `custom-docdb3-6-copy`. Al realizar la copia, se añaden etiquetas al nuevo grupo de parámetros.

```
aws docdb copy-db-cluster-parameter-group \
    --source-db-cluster-parameter-group-identifier custom-docdb3-6 \
    --target-db-cluster-parameter-group-identifier custom-docdb3-6-copy \
    --target-db-cluster-parameter-group-description "Copy of custom-docdb3-6" \
    --tags Key="CopyNumber",Value="1" Key="Modifiable",Value="Yes"
```

Salida:

```
{
    "DBClusterParameterGroup": {
        "DBParameterGroupFamily": "docdb3.6",
        "DBClusterParameterGroupArn": "arn:aws:rds:us-east-1:12345678901:cluster-
pg:custom-docdb3-6-copy",
        "DBClusterParameterGroupName": "custom-docdb3-6-copy",
        "Description": "Copy of custom-docdb3-6"
    }
}
```

Para obtener más información, consulte Copying an Amazon DocumentDB Cluster Parameter Group en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte CopyDbClusterParameterGroup en la Referencia de comandos de la AWS CLI.

`copy-db-cluster-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-db-cluster-snapshot`.

AWS CLI

Creación de una copia de una instantánea

En el siguiente ejemplo de la `copy-db-cluster-snapshot` se crea una copia de `sample-cluster-snapshot` llamada `sample-cluster-snapshot-copy`. La copia tiene todas las etiquetas del original más una etiqueta nueva con el `CopyNumber` del nombre de la clave.

```
aws docdb copy-db-cluster-snapshot \
    --source-db-cluster-snapshot-identifier sample-cluster-snapshot \
    --target-db-cluster-snapshot-identifier sample-cluster-snapshot-copy \
    --copy-tags \
    --tags Key="CopyNumber",Value="1"
```

Este comando no genera ninguna salida.

Para obtener más información sobre estas opciones, consulte Copying a Cluster Snapshot en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte CopyDbClusterSnapshot en la Referencia de comandos de la AWS CLI.

`create-db-cluster-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-cluster-parameter-group`.

AWS CLI

Creación de grupos de parámetros del clúster de Amazon DocumentDB

En el siguiente ejemplo de `create-db-cluster-parameter-group`, se crea el grupo de parámetros del clúster de DB `sample-parameter-group` usando la familia `docdb3.6`.

```
aws docdb create-db-cluster-parameter-group \
    --db-cluster-parameter-group-name sample-parameter-group \
    --db-parameter-group-family docdb3.6 \
    --description "Sample parameter group based on docdb3.6"
```

Salida:

```
{
    "DBClusterParameterGroup": {
        "Description": "Sample parameter group based on docdb3.6",
        "DBParameterGroupFamily": "docdb3.6",
        "DBClusterParameterGroupArn": "arn:aws:rds:us-west-2:123456789012:cluster-
pg:sample-parameter-group",
        "DBClusterParameterGroupName": "sample-parameter-group"
    }
}
```

Para obtener más información, consulte Creating an Amazon DocumentDB Cluster Parameter Group en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte CreateDbClusterParameterGroup en la Referencia de comandos de la AWS CLI.

`create-db-cluster-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-cluster-snapshot`.

AWS CLI

Creación manual de una instantánea del clúster de Amazon DocumentDB

En el siguiente ejemplo de `create-db-cluster-snapshot`, se crea una instantánea de un clúster de Amazon DB denominada sample-cluster-snapshot.

```
aws docdb create-db-cluster-snapshot \
   --db-cluster-identifier sample-cluster \
   --db-cluster-snapshot-identifier sample-cluster-snapshot
```

Salida:

```
{
    "DBClusterSnapshot": {
        "MasterUsername": "master-user",
        "SnapshotCreateTime": "2019-03-18T18:27:14.794Z",
        "AvailabilityZones": [
            "us-west-2a",
            "us-west-2b",
            "us-west-2c",
            "us-west-2d",
            "us-west-2e",
            "us-west-2f"
        ],
        "SnapshotType": "manual",
        "DBClusterSnapshotArn": "arn:aws:rds:us-west-2:123456789012:cluster-
snapshot:sample-cluster-snapshot",
        "EngineVersion": "3.6.0",
        "PercentProgress": 0,
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot",
        "Engine": "docdb",
        "DBClusterIdentifier": "sample-cluster",
        "Status": "creating",
        "ClusterCreateTime": "2019-03-15T20:29:58.836Z",
        "Port": 0,
        "StorageEncrypted": false,
        "VpcId": "vpc-91280df6"
    }
```

```
}
```

Para obtener más información, consulte Creating a Manual Cluster Snapshot en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte CreateDbClusterSnapshot en la Referencia de comandos de la AWS CLI.

`create-db-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-cluster`.

AWS CLI

Creación de un clúster de Amazon DocumentDB

En el siguiente ejemplo de `create-db-cluster`, se crea un clúster de Amazon DocumentDB denominado `sample-cluster` con el intervalo de mantenimiento preferido los domingos entre las 20:30 y las 11:00.

```
aws docdb create-db-cluster \
    --db-cluster-identifier sample-cluster \
    --engine docdb \
    --master-username master-user \
    --master-user-password password \
    --preferred-maintenance-window Sun:20:30-Sun:21:00
```

Salida:

```
{
    "DBCluster": {
        "DBClusterParameterGroup": "default.docdb3.6",
        "AssociatedRoles": [],
        "DBSubnetGroup": "default",
        "ClusterCreateTime": "2019-03-18T18:06:34.616Z",
        "Status": "creating",
        "Port": 27017,
        "PreferredMaintenanceWindow": "sun:20:30-sun:21:00",
        "HostedZoneId": "ZNKXH85TT8WVW",
        "DBClusterMembers": [],
        "Engine": "docdb",
```

```
        "DBClusterIdentifier": "sample-cluster",
        "PreferredBackupWindow": "10:12-10:42",
        "AvailabilityZones": [
            "us-west-2d",
            "us-west-2f",
            "us-west-2e"
        ],
        "MasterUsername": "master-user",
        "BackupRetentionPeriod": 1,
        "ReaderEndpoint": "sample-cluster.cluster-ro-corcjozrlsfc.us-
west-2.docdb.amazonaws.com",
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-77186e0d",
                "Status": "active"
            }
        ],
        "StorageEncrypted": false,
        "DBClusterArn": "arn:aws:rds:us-west-2:123456789012:cluster:sample-cluster",
        "DbClusterResourceId": "cluster-L3R4YRSBUYDP4GLMTJ2WF5GH5Q",
        "MultiAZ": false,
        "Endpoint": "sample-cluster.cluster-corcjozrlsfc.us-
west-2.docdb.amazonaws.com",
        "EngineVersion": "3.6.0"
    }
}
```

Para obtener más información, consulte Creating an Amazon DocumentDB Cluster en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte CreateDbCluster en la Referencia de comandos de la AWS CLI.

`create-db-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-instance`.

AWS CLI

Creación de una instancia de un clúster de Amazon DocumentDB

En el siguiente código de ejemplo de `create-db-instance`, se crean las instancias `sample-cluster-instance-2` de un clúster de Amazon DocumentDB `sample-cluster`.

```
aws docdb create-db-instance \
    --db-cluster-identifier sample-cluster \
    --db-instance-class db.r4.xlarge \
    --db-instance-identifier sample-cluster-instance-2 \
    --engine docdb
```

Salida:

```
{
    "DBInstance": {
        "DBInstanceStatus": "creating",
        "PendingModifiedValues": {
            "PendingCloudwatchLogsExports": {
                "LogTypesToEnable": [
                    "audit"
                ]
            }
        },
        "PubliclyAccessible": false,
        "PreferredBackupWindow": "00:00-00:30",
        "PromotionTier": 1,
        "EngineVersion": "3.6.0",
        "BackupRetentionPeriod": 3,
        "DBInstanceIdentifier": "sample-cluster-instance-2",
        "PreferredMaintenanceWindow": "tue:10:28-tue:10:58",
        "StorageEncrypted": false,
        "Engine": "docdb",
        "DBClusterIdentifier": "sample-cluster",
        "DBSubnetGroup": {
            "Subnets": [
                {
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2a"
                    },
                    "SubnetStatus": "Active",
                    "SubnetIdentifier": "subnet-4e26d263"
                },
                {
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2c"
                    },
                    "SubnetStatus": "Active",
                    "SubnetIdentifier": "subnet-afc329f4"
```

```
                },
                {
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2d"
                    },
                    "SubnetStatus": "Active",
                    "SubnetIdentifier": "subnet-53ab3636"
                },
                {
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2b"
                    },
                    "SubnetStatus": "Active",
                    "SubnetIdentifier": "subnet-991cb8d0"
                }
            ],
            "DBSubnetGroupDescription": "default",
            "SubnetGroupStatus": "Complete",
            "VpcId": "vpc-91280df6",
            "DBSubnetGroupName": "default"
        },
        "DBInstanceClass": "db.r4.xlarge",
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-77186e0d"
            }
        ],
        "DBInstanceArn": "arn:aws:rds:us-west-2:123456789012:db:sample-cluster-
instance-2",
        "DbiResourceId": "db-XEKJLEMGRV5ZKCARUVA4HO3ITE"
    }
}
```

Para obtener más información, consulte Adding an Amazon DocumentDB Instance to a Cluster en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte CreateDbInstance en la Referencia de comandos de la AWS CLI.

`create-db-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-subnet-group`.

AWS CLI

Creación de un grupo de subredes de Amazon DocumentDB

En el siguiente ejemplo de `create-db-subnet-group`, se crea un grupo de subredes de Amazon DocumentDB denominado `sample-subnet-group`.

```
aws docdb create-db-subnet-group \
    --db-subnet-group-description "a sample subnet group" \
    --db-subnet-group-name sample-subnet-group \
    --subnet-ids "subnet-29ab1025" "subnet-991cb8d0" "subnet-53ab3636"
```

Salida:

```
{
    "DBSubnetGroup": {
        "SubnetGroupStatus": "Complete",
        "DBSubnetGroupName": "sample-subnet-group",
        "DBSubnetGroupDescription": "a sample subnet group",
        "VpcId": "vpc-91280df6",
        "DBSubnetGroupArn": "arn:aws:rds:us-west-2:123456789012:subgrp:sample-
subnet-group",
        "Subnets": [
            {
                "SubnetStatus": "Active",
                "SubnetIdentifier": "subnet-53ab3636",
                "SubnetAvailabilityZone": {
                    "Name": "us-west-2d"
                }
            },
            {
                "SubnetStatus": "Active",
                "SubnetIdentifier": "subnet-991cb8d0",
                "SubnetAvailabilityZone": {
                    "Name": "us-west-2b"
                }
            },
            {
                "SubnetStatus": "Active",
                "SubnetIdentifier": "subnet-29ab1025",
                "SubnetAvailabilityZone": {
                    "Name": "us-west-2c"
                }
```

```
            }
        ]
    }
}
```

Para obtener más información, consulte Creating an Amazon DocumentDB Subnet Group en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte CreateDbSubnetGroup en la Referencia de comandos de la AWS CLI.

`delete-db-cluster-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-cluster-parameter-group`.

AWS CLI

Eliminación de grupos de parámetros del clúster de Amazon DocumentDB

En el siguiente ejemplo de `delete-db-cluster-parameter-group`, se elimina un grupo de parámetros de Amazon DocumentDB `sample-parameter-group`.

```
aws docdb delete-db-cluster-parameter-group \
    --db-cluster-parameter-group-name sample-parameter-group
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting an Amazon DocumentDB Cluster Parameter Group en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DeleteDbClusterParameterGroup en la Referencia de comandos de la AWS CLI.

`delete-db-cluster-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-cluster-snapshot`.

AWS CLI

Eliminación de una instantánea de un clúster de Amazon DocumentDB

En el siguiente ejemplo de `delete-db-cluster-snapshot`, se elimina la instantánea del clúster de Amazon DocumentDB `sample-cluster-snapshot`.

```
aws docdb delete-db-cluster-snapshot \
    --db-cluster-snapshot-identifier sample-cluster-snapshot
```

Salida:

```
{
    "DBClusterSnapshot": {
        "DBClusterIdentifier": "sample-cluster",
        "AvailabilityZones": [
            "us-west-2a",
            "us-west-2b",
            "us-west-2c",
            "us-west-2d"
        ],
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot",
        "VpcId": "vpc-91280df6",
        "DBClusterSnapshotArn": "arn:aws:rds:us-west-2:123456789012:cluster-
snapshot:sample-cluster-snapshot",
        "EngineVersion": "3.6.0",
        "Engine": "docdb",
        "SnapshotCreateTime": "2019-03-18T18:27:14.794Z",
        "Status": "available",
        "MasterUsername": "master-user",
        "ClusterCreateTime": "2019-03-15T20:29:58.836Z",
        "PercentProgress": 100,
        "StorageEncrypted": false,
        "SnapshotType": "manual",
        "Port": 0
    }
}
```

Para obtener más información, consulte Deleting a Cluster Snapshot en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DeleteDbClusterSnapshot en la Referencia de comandos de la AWS CLI.

`delete-db-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-cluster`.

AWS CLI

Eliminación de un clúster de Amazon DocumentDB

En el siguiente ejemplo de `delete-db-cluster`, se elimina la instantánea del clúster de Amazon DocumentDB `sample-cluster`. No se realiza ninguna copia de seguridad del clúster antes de eliminarlo. NOTA: Debe eliminar todas las instancias asociadas al clúster antes de poder eliminarlo.

```
aws docdb delete-db-cluster \
    --db-cluster-identifier sample-cluster \
    --skip-final-snapshot
```

Salida:

```
{
    "DBCluster": {
        "DBClusterIdentifier": "sample-cluster",
        "DBSubnetGroup": "default",
        "EngineVersion": "3.6.0",
        "Engine": "docdb",
        "LatestRestorableTime": "2019-03-18T18:07:24.610Z",
        "PreferredMaintenanceWindow": "sun:20:30-sun:21:00",
        "StorageEncrypted": false,
        "EarliestRestorableTime": "2019-03-18T18:07:24.610Z",
        "Port": 27017,
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-77186e0d"
            }
        ],
        "MultiAZ": false,
        "MasterUsername": "master-user",
        "DBClusterArn": "arn:aws:rds:us-west-2:123456789012:cluster:sample-cluster",
        "Status": "available",
        "PreferredBackupWindow": "10:12-10:42",
        "ReaderEndpoint": "sample-cluster.cluster-ro-corcjozrlsfc.us-
west-2.docdb.amazonaws.com",
```

```
        "AvailabilityZones": [
            "us-west-2c",
            "us-west-2b",
            "us-west-2a"
        ],
        "Endpoint": "sample-cluster.cluster-corcjozrlsfc.us-
west-2.docdb.amazonaws.com",
        "DbClusterResourceId": "cluster-L3R4YRSBUYDP4GLMTJ2WF5GH5Q",
        "ClusterCreateTime": "2019-03-18T18:06:34.616Z",
        "AssociatedRoles": [],
        "DBClusterParameterGroup": "default.docdb3.6",
        "HostedZoneId": "ZNKXH85TT8WVW",
        "BackupRetentionPeriod": 1,
        "DBClusterMembers": []
    }
}
```

Para obtener más información, consulte Deleting an Amazon DocumentDB Cluster en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DeleteDbCluster en la Referencia de comandos de la AWS CLI.

`delete-db-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-instance`.

AWS CLI

Eliminación de una instancia de Amazon DocumentDB

En el siguiente ejemplo de `delete-db-instance`, se elimina la instancia de Amazon DocumentDB `sample-cluster-instance-2`.

```
aws docdb delete-db-instance \
    --db-instance-identifier sample-cluster-instance-2
```

Salida:

```
{
    "DBInstance": {
        "DBSubnetGroup": {
            "Subnets": [
```

```
                {
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2a"
                    },
                    "SubnetStatus": "Active",
                    "SubnetIdentifier": "subnet-4e26d263"
                },
                {
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2c"
                    },
                    "SubnetStatus": "Active",
                    "SubnetIdentifier": "subnet-afc329f4"
                },
                {
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2d"
                    },
                    "SubnetStatus": "Active",
                    "SubnetIdentifier": "subnet-53ab3636"
                },
                {
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2b"
                    },
                    "SubnetStatus": "Active",
                    "SubnetIdentifier": "subnet-991cb8d0"
                }
            ],
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-91280df6",
            "SubnetGroupStatus": "Complete"
        },
        "PreferredBackupWindow": "00:00-00:30",
        "InstanceCreateTime": "2019-03-18T18:37:33.709Z",
        "DBInstanceClass": "db.r4.xlarge",
        "DbiResourceId": "db-XEKJLEMGRV5ZKCARUVA4HO3ITE",
        "BackupRetentionPeriod": 3,
        "Engine": "docdb",
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-77186e0d"
```

```
            }
        ],
        "AutoMinorVersionUpgrade": true,
        "PromotionTier": 1,
        "EngineVersion": "3.6.0",
        "Endpoint": {
            "Address": "sample-cluster-instance-2.corcjozrlsfc.us-
west-2.docdb.amazonaws.com",
            "HostedZoneId": "ZNKXH85TT8WVW",
            "Port": 27017
        },
        "DBInstanceIdentifier": "sample-cluster-instance-2",
        "PreferredMaintenanceWindow": "tue:10:28-tue:10:58",
        "EnabledCloudwatchLogsExports": [
            "audit"
        ],
        "PendingModifiedValues": {},
        "DBInstanceStatus": "deleting",
        "PubliclyAccessible": false,
        "DBInstanceArn": "arn:aws:rds:us-west-2:123456789012:db:sample-cluster-
instance-2",
        "DBClusterIdentifier": "sample-cluster",
        "AvailabilityZone": "us-west-2c",
        "StorageEncrypted": false
    }
}
```

Para obtener más información, consulte Deleting an Amazon DocumentDB Instance en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DeleteDbInstance en la Referencia de comandos de la AWS CLI.

`delete-db-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-subnet-group`.

AWS CLI

Eliminación de un grupo de subredes de Amazon DocumentDB

En el siguiente ejemplo de `delete-db-subnet-group`, se elimina un grupo de subredes de Amazon DocumentDB `sample-subnet-group`.

```
aws docdb delete-db-subnet-group \
    --db-subnet-group-name sample-subnet-group
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting an Amazon DocumentDB Subnet Group en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DeleteDbSubnetGroup en la Referencia de comandos de la AWS CLI.

`describe-db-cluster-parameter-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-cluster-parameter-groups`.

AWS CLI

Visualización de detalles de uno o más grupos de parámetros del clúster de Amazon DocumentDB

En el siguiente ejemplo de `describe-db-cluster-parameter-groups`, se muestran los detalles de un grupo de parámetros del clúster de Amazon DocumentDB `custom3-6-param-grp`.

```
aws docdb describe-db-cluster-parameter-groups \
    --db-cluster-parameter-group-name custom3-6-param-grp
```

Salida:

```
{
    "DBClusterParameterGroups": [
        {
            "DBParameterGroupFamily": "docdb3.6",
            "DBClusterParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:cluster-pg:custom3-6-param-grp",
            "Description": "Custom docdb3.6 parameter group",
            "DBClusterParameterGroupName": "custom3-6-param-grp"
        }
    ]
}
```

Para obtener más información, consulte Viewing Amazon DocumentDB Cluster Parameter Groups en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DescribeDbClusterParameterGroups en la Referencia de comandos de la AWS CLI.

`describe-db-cluster-parameters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-cluster-parameters`.

AWS CLI

Visualización de la lista detallada de parámetros para un grupo de parámetros de clúster de Amazon DocumentDB.

En el siguiente ejemplo de `describe-db-cluster-parameters`, se enumeran los parámetros del grupo de parámetros custom3-6-param-grp de Amazon DocumentDB.

```
aws docdb describe-db-cluster-parameters \
     --db-cluster-parameter-group-name custom3-6-param-grp
```

Salida:

```
{
    "Parameters": [
        {
            "DataType": "string",
            "ParameterName": "audit_logs",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot",
            "Source": "system",
            "ApplyType": "dynamic",
            "AllowedValues": "enabled,disabled",
            "Description": "Enables auditing on cluster.",
            "ParameterValue": "disabled"
        },
        {
            "DataType": "string",
            "ParameterName": "tls",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot",
            "Source": "system",
```

```
            "ApplyType": "static",
            "AllowedValues": "disabled,enabled",
            "Description": "Config to enable/disable TLS",
            "ParameterValue": "enabled"
        },
        {
            "DataType": "string",
            "ParameterName": "ttl_monitor",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot",
            "Source": "user",
            "ApplyType": "dynamic",
            "AllowedValues": "disabled,enabled",
            "Description": "Enables TTL Monitoring",
            "ParameterValue": "enabled"
        }
    ]
}
```

Para obtener más información, consulte Viewing Amazon DocumentDB Cluster Parameters en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DescribeDbClusterParameters en la Referencia de comandos de la AWS CLI.

`describe-db-cluster-snapshot-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-cluster-snapshot-attributes`.

AWS CLI

Para enumerar los nombres y los valores de los atributos de una instantánea de Amazon DocumentDB

En el siguiente ejemplo de `describe-db-cluster-snapshot-attributes`, se enumeran los nombres y los valores de los atributos de la instantánea de Amazon DocumentDB `sample-cluster-snapshot`.

```
aws docdb describe-db-cluster-snapshot-attributes \
    --db-cluster-snapshot-identifier sample-cluster-snapshot
```

Salida:

```
{
    "DBClusterSnapshotAttributesResult": {
        "DBClusterSnapshotAttributes": [
            {
                "AttributeName": "restore",
                "AttributeValues": []
            }
        ],
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot"
    }
}
```

Para obtener más información, consulte DescribeDBClusterSnapshotAttributes en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DescribeDbClusterSnapshotAttributes en la Referencia de comandos de la AWS CLI.

`describe-db-cluster-snapshots`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-cluster-snapshots`.

AWS CLI

Descripción de las instantáneas de Amazon DocumentDB

En el siguiente ejemplo de `describe-db-cluster-snapshots`, se muestran los detalles de la instantánea de Amazon DocumentDB `sample-cluster-snapshot`.

```
aws docdb describe-db-cluster-snapshots \
    --db-cluster-snapshot-identifier sample-cluster-snapshot
```

Salida:

```
{
    "DBClusterSnapshots": [
        {
            "AvailabilityZones": [
                "us-west-2a",
                "us-west-2b",
```

```
                "us-west-2c",
                "us-west-2d"
            ],
            "Status": "available",
            "DBClusterSnapshotArn": "arn:aws:rds:us-west-2:123456789012:cluster-
snapshot:sample-cluster-snapshot",
            "SnapshotCreateTime": "2019-03-15T20:41:26.515Z",
            "SnapshotType": "manual",
            "DBClusterSnapshotIdentifier": "sample-cluster-snapshot",
            "DBClusterIdentifier": "sample-cluster",
            "MasterUsername": "master-user",
            "StorageEncrypted": false,
            "VpcId": "vpc-91280df6",
            "EngineVersion": "3.6.0",
            "PercentProgress": 100,
            "Port": 0,
            "Engine": "docdb",
            "ClusterCreateTime": "2019-03-15T20:29:58.836Z"
        }
    ]
}
```

Para obtener más información, consulte DescribeDBClusterSnapshots en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DescribeDbClusterSnapshots en la Referencia de comandos de la AWS CLI.

`describe-db-clusters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-clusters`.

AWS CLI

Obtención de información detallada sobre uno o más clústeres de Amazon DocumentDB.

En el siguiente ejemplo de `describe-db-clusters`, se muestran los detalles del clúster de Amazon DocumentDB `sample-cluster`. Al omitir el parámetro `--db-cluster-identifier`, puede obtener información de hasta 100 clústeres.

```
aws docdb describe-db-clusters
    --db-cluster-identifier sample-cluster
```

Salida:


```
{
    "DBClusters": [
        {
            "DBClusterParameterGroup": "default.docdb3.6",
            "Endpoint": "sample-cluster.cluster-corcjozrlsfc.us-
west-2.docdb.amazonaws.com",
            "PreferredBackupWindow": "00:00-00:30",
            "DBClusterIdentifier": "sample-cluster",
            "ClusterCreateTime": "2019-03-15T20:29:58.836Z",
            "LatestRestorableTime": "2019-03-18T20:28:03.239Z",
            "MasterUsername": "master-user",
            "DBClusterMembers": [
                {
                    "PromotionTier": 1,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "IsClusterWriter": false,
                    "DBInstanceIdentifier": "sample-cluster"
                },
                {
                    "PromotionTier": 1,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "IsClusterWriter": true,
                    "DBInstanceIdentifier": "sample-cluster2"
                }
            ],
            "PreferredMaintenanceWindow": "sat:04:30-sat:05:00",
            "VpcSecurityGroups": [
                {
                    "VpcSecurityGroupId": "sg-77186e0d",
                    "Status": "active"
                }
            ],
            "Engine": "docdb",
            "ReaderEndpoint": "sample-cluster.cluster-ro-corcjozrlsfc.us-
west-2.docdb.amazonaws.com",
            "DBSubnetGroup": "default",
            "MultiAZ": true,
            "AvailabilityZones": [
                "us-west-2a",
                "us-west-2c",
                "us-west-2b"
            ],
```

```
            "EarliestRestorableTime": "2019-03-15T20:30:47.020Z",
            "DbClusterResourceId": "cluster-UP4EF2PVDDFVHHDJQTYDAIGHLE",
            "DBClusterArn": "arn:aws:rds:us-west-2:123456789012:cluster:sample-
cluster",
            "BackupRetentionPeriod": 3,
            "HostedZoneId": "ZNKXH85TT8WVW",
            "StorageEncrypted": false,
            "EnabledCloudwatchLogsExports": [
                "audit"
            ],
            "AssociatedRoles": [],
            "EngineVersion": "3.6.0",
            "Port": 27017,
            "Status": "available"
        }
    ]
}
```

Para obtener más información, consulte Describing Amazon DocumentDB Clusters en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DescribeDbClusters en la Referencia de comandos de la AWS CLI.

`describe-db-engine-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-engine-versions`.

AWS CLI

Para enumerar las versiones disponibles del motor de Amazon DocumentDB

En el siguiente ejemplo de `describe-db-engine-versions`, se enumeran todas las versiones disponibles del motor de Amazon DocumentDB.

```
aws docdb describe-db-engine-versions \
    --engine docdb
```

Salida:

```
{
    "DBEngineVersions": [
        {
```

```
            "DBEngineVersionDescription": "DocDB version 1.0.200837",
            "DBParameterGroupFamily": "docdb3.6",
            "EngineVersion": "3.6.0",
            "ValidUpgradeTarget": [],
            "DBEngineDescription": "Amazon DocumentDB (with MongoDB compatibility)",
            "SupportsLogExportsToCloudwatchLogs": true,
            "Engine": "docdb",
            "ExportableLogTypes": [
                "audit"
            ]
        }
    ]
}
```

Para obtener más información, consulte DescribeDBEngineVersions en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DescribeDbEngineVersions en la Referencia de comandos de la AWS CLI.

`describe-db-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-instances`.

AWS CLI

Búsqueda de información acerca de las instancias de Amazon DocumentDB aprovisionadas

En el siguiente ejemplo de `describe-db-instances`, se muestran los detalles de la instancia de Amazon DocumentDB `sample-cluster-instance`. Al omitir el parámetro `--db-instance-identifier`, obtiene información de hasta 100 instancias.

```
aws docdb describe-db-instances \
    --db-instance-identifier sample-cluster-instance
```

Salida:

```
{
    "DBInstances": [
        {
            "Endpoint": {
                "HostedZoneId": "ZNKXH85TT8WVW",
```

```
                "Address": "sample-cluster-instance.corcjozrlsfc.us-
west-2.docdb.amazonaws.com",
                "Port": 27017
            },
            "PreferredBackupWindow": "00:00-00:30",
            "DBInstanceStatus": "available",
            "DBInstanceClass": "db.r4.large",
            "EnabledCloudwatchLogsExports": [
                "audit"
            ],
            "DBInstanceIdentifier": "sample-cluster-instance",
            "DBSubnetGroup": {
                "Subnets": [
                    {
                        "SubnetStatus": "Active",
                        "SubnetIdentifier": "subnet-4e26d263",
                        "SubnetAvailabilityZone": {
                            "Name": "us-west-2a"
                        }
                    },
                    {
                        "SubnetStatus": "Active",
                        "SubnetIdentifier": "subnet-afc329f4",
                        "SubnetAvailabilityZone": {
                            "Name": "us-west-2c"
                        }
                    },
                    {
                        "SubnetStatus": "Active",
                        "SubnetIdentifier": "subnet-53ab3636",
                        "SubnetAvailabilityZone": {
                            "Name": "us-west-2d"
                        }
                    },
                    {
                        "SubnetStatus": "Active",
                        "SubnetIdentifier": "subnet-991cb8d0",
                        "SubnetAvailabilityZone": {
                            "Name": "us-west-2b"
                        }
                    }
                ],
                "DBSubnetGroupName": "default",
                "SubnetGroupStatus": "Complete",
```

```
                "DBSubnetGroupDescription": "default",
                "VpcId": "vpc-91280df6"
            },
            "InstanceCreateTime": "2019-03-15T20:36:06.338Z",
            "Engine": "docdb",
            "StorageEncrypted": false,
            "AutoMinorVersionUpgrade": true,
            "DBInstanceArn": "arn:aws:rds:us-west-2:123456789012:db:sample-cluster-
instance",
            "PreferredMaintenanceWindow": "tue:08:39-tue:09:09",
            "VpcSecurityGroups": [
                {
                    "Status": "active",
                    "VpcSecurityGroupId": "sg-77186e0d"
                }
            ],
            "DBClusterIdentifier": "sample-cluster",
            "PendingModifiedValues": {},
            "BackupRetentionPeriod": 3,
            "PubliclyAccessible": false,
            "EngineVersion": "3.6.0",
            "PromotionTier": 1,
            "AvailabilityZone": "us-west-2c",
            "DbiResourceId": "db-A2GIKUV6KPOHITGGKI2NHVISZA"
        }
    ]
}
```

Para obtener más información, consulte Describing Amazon DocumentDB Instances en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DescribeDbInstances en la Referencia de comandos de la AWS CLI.

`describe-db-subnet-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-subnet-groups`.

AWS CLI

Recuperación de una lista de descripciones de subredes de Amazon DocumentDB

En el siguiente ejemplo de `describe-db-subnet-groups`, se describen los detalles de la subred de Amazon DocumentDB denominada `default`.

```
aws docdb describe-db-subnet-groups \
    --db-subnet-group-name default
```

Salida:

```
{
    "DBSubnetGroups": [
        {
            "VpcId": "vpc-91280df6",
            "DBSubnetGroupArn": "arn:aws:rds:us-west-2:123456789012:subgrp:default",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-4e26d263",
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2a"
                    }
                },
                {
                    "SubnetIdentifier": "subnet-afc329f4",
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2c"
                    }
                },
                {
                    "SubnetIdentifier": "subnet-53ab3636",
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2d"
                    }
                },
                {
                    "SubnetIdentifier": "subnet-991cb8d0",
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2b"
                    }
                }
            ],
```

```
            "DBSubnetGroupName": "default",
            "SubnetGroupStatus": "Complete",
            "DBSubnetGroupDescription": "default"
        }
    ]
}
```

Para obtener más información, consulte Describing Subnet Groups en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DescribeDbSubnetGroups en la Referencia de comandos de la AWS CLI.

`describe-engine-default-cluster-parameters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-engine-default-cluster-parameters`.

AWS CLI

Descripción de información sobre el motor y los parámetros del sistema predeterminados para Amazon DocumentDB

El siguiente ejemplo de `describe-engine-default-cluster-parameters` muestra información sobre el motor y los parámetros del sistema predeterminados para el grupo de parámetros de Amazon DocumentDB `docdb3.6`.

```
aws docdb describe-engine-default-cluster-parameters \
    --db-parameter-group-family docdb3.6
```

Salida:

```
{
    "EngineDefaults": {
        "DBParameterGroupFamily": "docdb3.6",
        "Parameters": [
            {
                "ApplyType": "dynamic",
                "ParameterValue": "disabled",
                "Description": "Enables auditing on cluster.",
                "Source": "system",
```

```
                "DataType": "string",
                "MinimumEngineVersion": "3.6.0",
                "AllowedValues": "enabled,disabled",
                "ParameterName": "audit_logs",
                "IsModifiable": true
            },
            {
                "ApplyType": "static",
                "ParameterValue": "enabled",
                "Description": "Config to enable/disable TLS",
                "Source": "system",
                "DataType": "string",
                "MinimumEngineVersion": "3.6.0",
                "AllowedValues": "disabled,enabled",
                "ParameterName": "tls",
                "IsModifiable": true
            },
            {
                "ApplyType": "dynamic",
                "ParameterValue": "enabled",
                "Description": "Enables TTL Monitoring",
                "Source": "system",
                "DataType": "string",
                "MinimumEngineVersion": "3.6.0",
                "AllowedValues": "disabled,enabled",
                "ParameterName": "ttl_monitor",
                "IsModifiable": true
            }
        ]
    }
}
```

Para obtener más información, consulte DescribeEngineDefaultClusterParameters en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DescribeEngineDefaultClusterParameters en la Referencia de comandos de la AWS CLI.

`describe-event-categories`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-event-categories`.

AWS CLI

Descripción de todas las categorías de eventos de Amazon DocumentDB

En el siguiente ejemplo de `describe-event-categories`, se muestran todas las categorías para el tipo de origen de eventos de Amazon DocumentDB `db-instance`.

```
aws docdb describe-event-categories \
    --source-type db-cluster
```

Salida:

```
{
    "EventCategoriesMapList": [
        {
            "SourceType": "db-cluster",
            "EventCategories": [
                "failover",
                "maintenance",
                "notification",
                "failure"
            ]
        }
    ]
}
```

Para obtener más información, consulte Viewing Event Categories en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DescribeEventCategories en la Referencia de comandos de la AWS CLI.

`describe-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-events`.

AWS CLI

Para enumerar los eventos de Amazon DocumentDB

En el siguiente ejemplo de `describe-events`, se muestran todos los eventos de Amazon DocumentDB de las últimas 24 horas (1440 minutos).

```
aws docdb describe-events \
    --duration 1440
```

Este comando no genera ninguna salida. Salida:

```
{
    "Events": [
        {
            "EventCategories": [
                "failover"
            ],
            "Message": "Started cross AZ failover to DB instance: sample-cluster",
            "Date": "2019-03-18T21:36:29.807Z",
            "SourceArn": "arn:aws:rds:us-west-2:123456789012:cluster:sample-
cluster",
            "SourceIdentifier": "sample-cluster",
            "SourceType": "db-cluster"
        },
        {
            "EventCategories": [
                "availability"
            ],
            "Message": "DB instance restarted",
            "Date": "2019-03-18T21:36:40.793Z",
            "SourceArn": "arn:aws:rds:us-west-2:123456789012:db:sample-cluster",
            "SourceIdentifier": "sample-cluster",
            "SourceType": "db-instance"
        },
        {
            "EventCategories": [],
            "Message": "A new writer was promoted. Restarting database as a
 reader.",
            "Date": "2019-03-18T21:36:43.873Z",
            "SourceArn": "arn:aws:rds:us-west-2:123456789012:db:sample-cluster2",
            "SourceIdentifier": "sample-cluster2",
            "SourceType": "db-instance"
        },
        {
            "EventCategories": [
                "availability"
            ],
            "Message": "DB instance restarted",
            "Date": "2019-03-18T21:36:51.257Z",
```

```
            "SourceArn": "arn:aws:rds:us-west-2:123456789012:db:sample-cluster2",
            "SourceIdentifier": "sample-cluster2",
            "SourceType": "db-instance"
        },
        {
            "EventCategories": [
                "failover"
            ],
            "Message": "Completed failover to DB instance: sample-cluster",
            "Date": "2019-03-18T21:36:53.462Z",
            "SourceArn": "arn:aws:rds:us-west-2:123456789012:cluster:sample-
cluster",
            "SourceIdentifier": "sample-cluster",
            "SourceType": "db-cluster"
        },
        {
            "Date": "2019-03-19T16:51:48.847Z",
            "EventCategories": [
                "configuration change"
            ],
            "Message": "Updated parameter audit_logs to enabled with apply method
 pending-reboot",
            "SourceIdentifier": "custom3-6-param-grp",
            "SourceType": "db-parameter-group"
        },
        {
            "EventCategories": [
                "configuration change"
            ],
            "Message": "Applying modification to database instance class",
            "Date": "2019-03-19T17:55:20.095Z",
            "SourceArn": "arn:aws:rds:us-west-2:123456789012:db:sample-cluster2",
            "SourceIdentifier": "sample-cluster2",
            "SourceType": "db-instance"
        },
        {
            "EventCategories": [
                "availability"
            ],
            "Message": "DB instance shutdown",
            "Date": "2019-03-19T17:56:31.127Z",
            "SourceArn": "arn:aws:rds:us-west-2:123456789012:db:sample-cluster2",
            "SourceIdentifier": "sample-cluster2",
            "SourceType": "db-instance"
```

```
        },
        {
            "EventCategories": [
                "configuration change"
            ],
            "Message": "Finished applying modification to DB instance class",
            "Date": "2019-03-19T18:00:45.822Z",
            "SourceArn": "arn:aws:rds:us-west-2:123456789012:db:sample-cluster2",
            "SourceIdentifier": "sample-cluster2",
            "SourceType": "db-instance"
        },
        {
            "EventCategories": [
                "availability"
            ],
            "Message": "DB instance restarted",
            "Date": "2019-03-19T18:00:53.397Z",
            "SourceArn": "arn:aws:rds:us-west-2:123456789012:db:sample-cluster2",
            "SourceIdentifier": "sample-cluster2",
            "SourceType": "db-instance"
        },
        {
            "EventCategories": [
                "availability"
            ],
            "Message": "DB instance shutdown",
            "Date": "2019-03-19T18:23:36.045Z",
            "SourceArn": "arn:aws:rds:us-west-2:123456789012:db:sample-cluster2",
            "SourceIdentifier": "sample-cluster2",
            "SourceType": "db-instance"
        },
        {
            "EventCategories": [
                "availability"
            ],
            "Message": "DB instance restarted",
            "Date": "2019-03-19T18:23:46.209Z",
            "SourceArn": "arn:aws:rds:us-west-2:123456789012:db:sample-cluster2",
            "SourceIdentifier": "sample-cluster2",
            "SourceType": "db-instance"
        },
        {
            "Date": "2019-03-19T18:39:05.822Z",
            "EventCategories": [
```

```
                "configuration change"
            ],
            "Message": "Updated parameter ttl_monitor to enabled with apply method
 immediate",
            "SourceIdentifier": "custom3-6-param-grp",
            "SourceType": "db-parameter-group"
        },
        {
            "Date": "2019-03-19T18:39:48.067Z",
            "EventCategories": [
                "configuration change"
            ],
            "Message": "Updated parameter audit_logs to disabled with apply method
 immediate",
            "SourceIdentifier": "custom3-6-param-grp",
            "SourceType": "db-parameter-group"
        }
    ]
}
```

Para obtener más información, consulte Viewing Amazon DocumentDB Events en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DescribeEvents en la Referencia de comandos de la AWS CLI.

`describe-orderable-db-instance-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-orderable-db-instance-options`.

AWS CLI

Búsqueda de las opciones de instancia de Amazon DocumentDB que puede solicitar

En el siguiente ejemplo de `describe-orderable-db-instance-options`, se enumeran todas las opciones de instancia de Amazon DocumentDB para una región.

```
aws docdb describe-orderable-db-instance-options \
    --engine docdb \
    --region us-east-1
```

Salida:


```
{
    "OrderableDBInstanceOptions": [
        {
            "Vpc": true,
            "AvailabilityZones": [
                {
                    "Name": "us-east-1a"
                },
                {
                    "Name": "us-east-1b"
                },
                {
                    "Name": "us-east-1c"
                },
                {
                    "Name": "us-east-1d"
                }
            ],
            "EngineVersion": "3.6.0",
            "DBInstanceClass": "db.r4.16xlarge",
            "LicenseModel": "na",
            "Engine": "docdb"
        },
        {
            "Vpc": true,
            "AvailabilityZones": [
                {
                    "Name": "us-east-1a"
                },
                {
                    "Name": "us-east-1b"
                },
                {
                    "Name": "us-east-1c"
                },
                {
                    "Name": "us-east-1d"
                }
                }
            ],
            "EngineVersion": "3.6.0",
            "DBInstanceClass": "db.r4.2xlarge",
```

```
            "LicenseModel": "na",
            "Engine": "docdb"
        },
        {
            "Vpc": true,
            "AvailabilityZones": [
                {
                    "Name": "us-east-1a"
                },
                {
                    "Name": "us-east-1b"
                },
                {
                    "Name": "us-east-1c"
                },
                {
                    "Name": "us-east-1d"
                }
            ],
            "EngineVersion": "3.6.0",
            "DBInstanceClass": "db.r4.4xlarge",
            "LicenseModel": "na",
            "Engine": "docdb"
        },
        {
            "Vpc": true,
            "AvailabilityZones": [
                {
                    "Name": "us-east-1a"
                },
                {
                    "Name": "us-east-1b"
                },
                {
                    "Name": "us-east-1c"
                },
                {
                    "Name": "us-east-1d"
                }
            ],
            "EngineVersion": "3.6.0",
            "DBInstanceClass": "db.r4.8xlarge",
            "LicenseModel": "na",
            "Engine": "docdb"
```

```
        },
        {
            "Vpc": true,
            "AvailabilityZones": [
                {
                    "Name": "us-east-1a"
                },
                {
                    "Name": "us-east-1b"
                },
                {
                    "Name": "us-east-1c"
                },
                {
                    "Name": "us-east-1d"
                }
            ],
            "EngineVersion": "3.6.0",
            "DBInstanceClass": "db.r4.large",
            "LicenseModel": "na",
            "Engine": "docdb"
        },
        {
            "Vpc": true,
            "AvailabilityZones": [
                {
                    "Name": "us-east-1a"
                },
                {
                    "Name": "us-east-1b"
                },
                {
                    "Name": "us-east-1c"
                },
                {
                    "Name": "us-east-1d"
                }
            ],
            "EngineVersion": "3.6.0",
            "DBInstanceClass": "db.r4.xlarge",
            "LicenseModel": "na",
            "Engine": "docdb"
        }
    ]
```

```
}
```

Para obtener más información, consulte Adding an Amazon DocumentDB Instance to a Cluster en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DescribeOrderableDbInstanceOptions en la Referencia de comandos de la AWS CLI.

`describe-pending-maintenance-actions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-pending-maintenance-actions`.

AWS CLI

Para enumerar las acciones de mantenimiento pendientes de Amazon DocumentDB

En el siguiente ejemplo de `describe-pending-maintenance-actions`, se enumeran todas las acciones de mantenimiento pendientes de Amazon DocumentDB.

```
aws docdb describe-pending-maintenance-actions
```

Salida:

```
{
    "PendingMaintenanceActions": []
}
```

Para obtener más información, consulte las Maintaining Amazon DocumentDB en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte DescribePendingMaintenanceActions en la Referencia de comandos de la AWS CLI.

`failover-db-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `failover-db-cluster`.

AWS CLI

Conmutación por error forzada a una réplica por parte de un clúster de Amazon DocumentDB

En el siguiente ejemplo de `failover-db-cluster`, se obliga a la instancia principal del clúster sample-cluster de Amazon DocumentDB a realizar una conmutación por error a una réplica.

```
aws docdb failover-db-cluster \
    --db-cluster-identifier sample-cluster
```

Salida:

```
{
    "DBCluster": {
        "AssociatedRoles": [],
        "DBClusterIdentifier": "sample-cluster",
        "EngineVersion": "3.6.0",
        "DBSubnetGroup": "default",
        "MasterUsername": "master-user",
        "EarliestRestorableTime": "2019-03-15T20:30:47.020Z",
        "Endpoint": "sample-cluster.cluster-corcjozrlsfc.us-
west-2.docdb.amazonaws.com",
        "AvailabilityZones": [
            "us-west-2a",
            "us-west-2c",
            "us-west-2b"
        ],
        "LatestRestorableTime": "2019-03-18T21:35:23.548Z",
        "PreferredMaintenanceWindow": "sat:04:30-sat:05:00",
        "PreferredBackupWindow": "00:00-00:30",
        "Port": 27017,
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-77186e0d",
                "Status": "active"
            }
        ],
        "StorageEncrypted": false,
        "ClusterCreateTime": "2019-03-15T20:29:58.836Z",
        "MultiAZ": true,
        "Status": "available",
        "DBClusterMembers": [
            {
                "DBClusterParameterGroupStatus": "in-sync",
                "IsClusterWriter": false,
                "DBInstanceIdentifier": "sample-cluster",
                "PromotionTier": 1
```

```
            },
            {
                "DBClusterParameterGroupStatus": "in-sync",
                "IsClusterWriter": true,
                "DBInstanceIdentifier": "sample-cluster2",
                "PromotionTier": 2
            }
        ],
        "EnabledCloudwatchLogsExports": [
            "audit"
        ],
        "DBClusterParameterGroup": "default.docdb3.6",
        "HostedZoneId": "ZNKXH85TT8WVW",
        "DBClusterArn": "arn:aws:rds:us-west-2:123456789012:cluster:sample-cluster",
        "BackupRetentionPeriod": 3,
        "DbClusterResourceId": "cluster-UP4EF2PVDDFVHHDJQTYDAIGHLE",
        "ReaderEndpoint": "sample-cluster.cluster-ro-corcjozrlsfc.us-
west-2.docdb.amazonaws.com",
        "Engine": "docdb"
    }
}
```

Para obtener más información, consulte las Amazon DocumentDB Failover en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte FailoverDbCluster en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar todas las etiquetas en un recurso de Amazon DocumentDB

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran todas las etiquetas de un clúster `sample-cluster` de Amazon DocumentDB.

```
aws docdb list-tags-for-resource \
    --resource-name arn:aws:rds:us-west-2:123456789012:cluster:sample-cluster
```

Salida:

```
{
    "TagList": [
        {
            "Key": "A",
            "Value": "ALPHA"
        },
        {
            "Key": "B",
            "Value": ""
        },
        {
            "Key": "C",
            "Value": "CHARLIE"
        }
    ]
}
```

Para obtener más información, consulte Listing Tags on an Amazon DocumentDB Resource en la Guía para desarrolladores de Amazon DocumentDB.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`modify-db-cluster-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-cluster-parameter-group`.

AWS CLI

Modificación de un grupo de parámetros de clúster de Amazon DocumentDB

En el siguiente ejemplo de `modify-db-cluster-parameter-group`, se modifica el grupo de parámetros del clúster `custom3-6-param-grp` de Amazon DocumentDB estableciendo los dos parámetros `audit_logs` y `ttl_monitor` como habilitados. Los cambios se aplican en el siguiente reinicio.

```
aws docdb modify-db-cluster-parameter-group \
    --db-cluster-parameter-group-name custom3-6-param-grp \
    --
parameters ParameterName=audit_logs,ParameterValue=enabled,ApplyMethod=pending-
reboot \
```

```
  ParameterName=ttl_monitor,ParameterValue=enabled,ApplyMethod=pending-reboot
```

Salida:

```
{
    "DBClusterParameterGroupName": "custom3-6-param-grp"
}
```

Para obtener más información, consulte Modifying an Amazon DocumentDB Cluster Parameter Group en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte ModifyDbClusterParameterGroup en la Referencia de comandos de la AWS CLI.

`modify-db-cluster-snapshot-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-cluster-snapshot-attribute`.

AWS CLI

Ejemplo 1: añadir un atributo a una instantánea de Amazon DocumentDB

En el siguiente ejemplo de `modify-db-cluster-snapshot-attribute`, se añaden cuatro valores de atributo a una instantánea de clúster de Amazon DocumentDB.

```
aws docdb modify-db-cluster-snapshot-attribute \
    --db-cluster-snapshot-identifier sample-cluster-snapshot \
    --attribute-name restore \
    --values-to-add 123456789011 123456789012 123456789013
```

Salida:

```
{
    "DBClusterSnapshotAttributesResult": {
        "DBClusterSnapshotAttributes": [
            {
                "AttributeName": "restore",
                "AttributeValues": [
```

```
                    "123456789011",
                    "123456789012",
                    "123456789013"
                ]
            }
        ],
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot"
    }
}
```

Ejemplo 2: eliminación de atributos de una instantánea de Amazon DocumentDB

En el siguiente ejemplo de `modify-db-cluster-snapshot-attribute`, se eliminan dos valores de atributo de una instantánea de clúster de Amazon DocumentDB.

```
aws docdb modify-db-cluster-snapshot-attribute \
    --db-cluster-snapshot-identifier sample-cluster-snapshot \
    --attribute-name restore \
    --values-to-remove 123456789012
```

Salida:

```
{
    "DBClusterSnapshotAttributesResult": {
        "DBClusterSnapshotAttributes": [
            {
                "AttributeName": "restore",
                "AttributeValues": [
                    "123456789011",
                    "123456789013"
                ]
            }
        ],
        "DBClusterSnapshotIdentifier": "sample-cluster-snapshot"
    }
}
```

Para obtener más información, consulte ModifyDBClusterSnapshotAttribute en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte ModifyDbClusterSnapshotAttribute en la Referencia de comandos de la AWS CLI.

`modify-db-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-cluster`.

AWS CLI

Modificación de un clúster de Amazon DocumentDB

En el siguiente ejemplo de `modify-db-cluster`, se modifica el clúster `sample-cluster` de Amazon DocumentDB estableciendo en siete días el período de retención de las copias de seguridad automáticas y cambiando los plazos preferidos tanto para las copias de seguridad como para el mantenimiento. Todos estos cambios se aplican durante el siguiente plazo de mantenimiento.

```
aws docdb modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --no-apply-immediately \
    --backup-retention-period 7 \
    --preferred-backup-window 18:00-18:30 \
    --preferred-maintenance-window sun:20:00-sun:20:30
```

Salida:

```
{
    "DBCluster": {
        "Endpoint": "sample-cluster.cluster-corcjozrlsfc.us-
west-2.docdb.amazonaws.com",
        "DBClusterMembers": [
            {
                "DBClusterParameterGroupStatus": "in-sync",
                "DBInstanceIdentifier": "sample-cluster",
                "IsClusterWriter": true,
                "PromotionTier": 1
            },
            {
                "DBClusterParameterGroupStatus": "in-sync",
                "DBInstanceIdentifier": "sample-cluster2",
                "IsClusterWriter": false,
                "PromotionTier": 2
            }
        ],
        "HostedZoneId": "ZNKXH85TT8WVW",
```

```
        "StorageEncrypted": false,
        "PreferredBackupWindow": "18:00-18:30",
        "MultiAZ": true,
        "EngineVersion": "3.6.0",
        "MasterUsername": "master-user",
        "ReaderEndpoint": "sample-cluster.cluster-ro-corcjozrlsfc.us-
west-2.docdb.amazonaws.com",
        "DBSubnetGroup": "default",
        "LatestRestorableTime": "2019-03-18T22:08:13.408Z",
        "EarliestRestorableTime": "2019-03-15T20:30:47.020Z",
        "PreferredMaintenanceWindow": "sun:20:00-sun:20:30",
        "AssociatedRoles": [],
        "EnabledCloudwatchLogsExports": [
            "audit"
        ],
        "Engine": "docdb",
        "DBClusterParameterGroup": "default.docdb3.6",
        "DBClusterArn": "arn:aws:rds:us-west-2:123456789012:cluster:sample-cluster",
        "BackupRetentionPeriod": 7,
        "DBClusterIdentifier": "sample-cluster",
        "AvailabilityZones": [
            "us-west-2a",
            "us-west-2c",
            "us-west-2b"
        ],
        "Status": "available",
        "DbClusterResourceId": "cluster-UP4EF2PVDDFVHHDJQTYDAIGHLE",
        "ClusterCreateTime": "2019-03-15T20:29:58.836Z",
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-77186e0d",
                "Status": "active"
            }
        ],
        "Port": 27017
    }
}
```

Para obtener más información, consulte Modifying an Amazon DocumentDB Cluster en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte ModifyDbCluster en la Referencia de comandos de la AWS CLI.

`modify-db-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-instance`.

AWS CLI

Modificación de una instancia de Amazon DocumentDB

En el siguiente ejemplo de `modify-db-instance`, se modifica la instancia de Amazon DocumentDB `sample-cluster2` cambiando su clase de instancia a `db.r4.4xlarge` y su nivel de promoción a 5. Los cambios se aplican inmediatamente, pero solo se pueden ver una vez que la instancia se encuentre en estado disponible.

```
aws docdb modify-db-instance \
    --db-instance-identifier sample-cluster2 \
    --apply-immediately \
    --db-instance-class db.r4.4xlarge \
    --promotion-tier 5
```

Salida:

```
{
    "DBInstance": {
        "EngineVersion": "3.6.0",
        "StorageEncrypted": false,
        "DBInstanceClass": "db.r4.large",
        "PreferredMaintenanceWindow": "mon:08:39-mon:09:09",
        "AutoMinorVersionUpgrade": true,
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-77186e0d",
                "Status": "active"
            }
        ],
        "PreferredBackupWindow": "18:00-18:30",
        "EnabledCloudwatchLogsExports": [
            "audit"
        ],
        "AvailabilityZone": "us-west-2f",
        "DBInstanceIdentifier": "sample-cluster2",
        "InstanceCreateTime": "2019-03-15T20:36:06.338Z",
        "Engine": "docdb",
        "BackupRetentionPeriod": 7,
```

```
        "DBSubnetGroup": {
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-4e26d263",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2a"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-afc329f4",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2c"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-53ab3636",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2d"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-991cb8d0",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2b"
                    },
                    "SubnetStatus": "Active"
                }
            ],
            "VpcId": "vpc-91280df6"
        },
        "PromotionTier": 2,
        "Endpoint": {
            "Address": "sample-cluster2.corcjozrlsfc.us-west-2.docdb.amazonaws.com",
            "HostedZoneId": "ZNKXH85TT8WVW",
            "Port": 27017
        },
        "DbiResourceId": "db-A2GIKUV6KPOHITGGKI2NHVISZA",
        "DBClusterIdentifier": "sample-cluster",
```

```
        "DBInstanceArn": "arn:aws:rds:us-west-2:123456789012:db:sample-cluster2",
        "PendingModifiedValues": {
            "DBInstanceClass": "db.r4.4xlarge"
        },
        "PubliclyAccessible": false,
        "DBInstanceStatus": "available"
    }
}
```

Para obtener más información, consulte Modifying an Amazon DocumentDB Instance en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte ModifyDbInstance en la Referencia de comandos de la AWS CLI.

`modify-db-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-subnet-group`.

AWS CLI

Modificación de un grupo de subredes de Amazon DocumentDB

En el siguiente ejemplo de `modify-db-subnet-group`, se modifica el grupo de subredes `sample-subnet-group` añadiendo las subredes especificadas y una nueva descripción.

```
aws docdb modify-db-subnet-group \
    --db-subnet-group-name sample-subnet-group \
    --subnet-ids subnet-b3806e8f subnet-53ab3636 subnet-991cb8d0 \
    --db-subnet-group-description "New subnet description"
```

Salida:

```
{
    "DBSubnetGroup": {
        "DBSubnetGroupName": "sample-subnet-group",
        "SubnetGroupStatus": "Complete",
        "DBSubnetGroupArn": "arn:aws:rds:us-west-2:123456789012:subgrp:sample-
subnet-group",
        "VpcId": "vpc-91280df6",
        "DBSubnetGroupDescription": "New subnet description",
        "Subnets": [
```

```
            {
                "SubnetIdentifier": "subnet-b3806e8f",
                "SubnetStatus": "Active",
                "SubnetAvailabilityZone": {
                    "Name": "us-west-2a"
                }
            },
            {
                "SubnetIdentifier": "subnet-53ab3636",
                "SubnetStatus": "Active",
                "SubnetAvailabilityZone": {
                    "Name": "us-west-2c"
                }
            },
            {
                "SubnetIdentifier": "subnet-991cb8d0",
                "SubnetStatus": "Active",
                "SubnetAvailabilityZone": {
                    "Name": "us-west-2b"
                }
            }
        ]
    }
}
```

Para obtener más información, consulte Modifying an Amazon DocumentDB Subnet Group en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte ModifyDbSubnetGroup en la Referencia de comandos de la AWS CLI.

`reboot-db-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `reboot-db-instance`.

AWS CLI

Reinicio de la instancia de Amazon DocumentDB

En el siguiente ejemplo de `reboot-db-instance`, se reinicia la instancia de Amazon DocumentDB `sample-cluster2`.

```
aws docdb reboot-db-instance \
```

```
    --db-instance-identifier sample-cluster2
```

Este comando no genera ninguna salida. Salida:

```
{
    "DBInstance": {
        "PreferredBackupWindow": "18:00-18:30",
        "DBInstanceIdentifier": "sample-cluster2",
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-77186e0d"
            }
        ],
        "DBSubnetGroup": {
            "VpcId": "vpc-91280df6",
            "Subnets": [
                {
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2a"
                    },
                    "SubnetIdentifier": "subnet-4e26d263"
                },
                {
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2c"
                    },
                    "SubnetIdentifier": "subnet-afc329f4"
                },
                {
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2d"
                    },
                    "SubnetIdentifier": "subnet-53ab3636"
                },
                {
                    "SubnetStatus": "Active",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2b"
                    },
```

```
                    "SubnetIdentifier": "subnet-991cb8d0"
                }
            ],
            "SubnetGroupStatus": "Complete",
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default"
        },
        "PendingModifiedValues": {},
        "Endpoint": {
            "Address": "sample-cluster2.corcjozrlsfc.us-west-2.docdb.amazonaws.com",
            "HostedZoneId": "ZNKXH85TT8WVW",
            "Port": 27017
        },
        "EnabledCloudwatchLogsExports": [
            "audit"
        ],
        "StorageEncrypted": false,
        "DbiResourceId": "db-A2GIKUV6KPOHITGGKI2NHVISZA",
        "AutoMinorVersionUpgrade": true,
        "Engine": "docdb",
        "InstanceCreateTime": "2019-03-15T20:36:06.338Z",
        "EngineVersion": "3.6.0",
        "PromotionTier": 5,
        "BackupRetentionPeriod": 7,
        "DBClusterIdentifier": "sample-cluster",
        "PreferredMaintenanceWindow": "mon:08:39-mon:09:09",
        "PubliclyAccessible": false,
        "DBInstanceClass": "db.r4.4xlarge",
        "AvailabilityZone": "us-west-2d",
        "DBInstanceArn": "arn:aws:rds:us-west-2:123456789012:db:sample-cluster2",
        "DBInstanceStatus": "rebooting"
    }
}
```

Para obtener más información, consulte las Rebooting an Amazon DocumentDB ILnstance en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte RebootDbInstance en la Referencia de comandos de la AWS CLI.

`remove-tags-from-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-tags-from-resource`.

AWS CLI

Eliminación de las etiquetas de metadatos de un recurso de Amazon DocumentDB

En el siguiente ejemplo de `remove-tags-from-resource`, se elimina la etiqueta la clave denominada B del clúster de Amazon DocumentDB `sample-cluster`.

```
aws docdb remove-tags-from-resource \
    --resource-name arn:aws:rds:us-west-2:123456789012:cluster:sample-cluster \
    --tag-keys B
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Removing Tags from an Amazon DocumentDBResource en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener información sobre la API, consulte RemoveTagsFromResource en la Referencia de comandos de la AWS CLI.

`reset-db-cluster-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-db-cluster-parameter-group`.

AWS CLI

Restablecimiento del valor del parámetro especificado a sus valores predeterminados en un grupo de parámetros de Amazon DocumentDB

En el siguiente ejemplo de `reset-db-cluster-parameter-group`, se restablece el parámetro `ttl_monitor` en el grupo de parámetros `custom3-6-param-grp` de Amazon DocumentDB a su valor predeterminado.

```
aws docdb reset-db-cluster-parameter-group \
    --db-cluster-parameter-group-name custom3-6-param-grp \
    --parameters ParameterName=ttl_monitor,ApplyMethod=immediate
```

Salida:

```
{
    "DBClusterParameterGroupName": "custom3-6-param-grp"
```

```
}
```

Para obtener más información, consulte el título en la Guía para desarrolladores de Amazon DocumentDB.

Restablecimiento de todos los valores de los parámetros o solo los especificados a sus valores predeterminados en un grupo de parámetros de Amazon DocumentDB

En el siguiente ejemplo de `reset-db-cluster-parameter-group`, se restablecen todos los parámetros en el grupo de parámetros `custom3-6-param-grp` de Amazon DocumentDB a su valor predeterminado.

```
aws docdb reset-db-cluster-parameter-group \
    --db-cluster-parameter-group-name custom3-6-param-grp \
    --reset-all-parameters
```

Salida:

```
{
    "DBClusterParameterGroupName": "custom3-6-param-grp"
}
```

Para obtener más información, consulte Resetting an Amazon DocumentDB Cluster Parameter Group en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte ResetDbClusterParameterGroup en la Referencia de comandos de la AWS CLI.

`restore-db-cluster-from-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-db-cluster-from-snapshot`.

AWS CLI

Restauración de un clúster de Amazon DocumentDB desde una instantánea manual o automática

En el siguiente ejemplo de `restore-db-cluster-from-snapshot`, se crea un nuevo clúster de Amazon DocumentDB denominado `sample-cluster-2019-03-16-00-01-restored` a partir de la instantánea `rds:sample-cluster-2019-03-16-00-01`.

```
aws docdb restore-db-cluster-from-snapshot \
    --db-cluster-identifier sample-cluster-2019-03-16-00-01-restored \
    --engine docdb \
    --snapshot-identifier rds:sample-cluster-2019-03-16-00-01
```

Salida:

```
{
    "DBCluster": {
        "ClusterCreateTime": "2019-03-19T18:45:01.857Z",
        "HostedZoneId": "ZNKXH85TT8WVW",
        "Engine": "docdb",
        "DBClusterMembers": [],
        "MultiAZ": false,
        "AvailabilityZones": [
            "us-west-2a",
            "us-west-2c",
            "us-west-2b"
        ],
        "StorageEncrypted": false,
        "ReaderEndpoint": "sample-cluster-2019-03-16-00-01-restored.cluster-ro-
corcjozrlsfc.us-west-2.docdb.amazonaws.com",
        "Endpoint": "sample-cluster-2019-03-16-00-01-restored.cluster-
corcjozrlsfc.us-west-2.docdb.amazonaws.com",
        "Port": 27017,
        "PreferredBackupWindow": "00:00-00:30",
        "DBSubnetGroup": "default",
        "DBClusterIdentifier": "sample-cluster-2019-03-16-00-01-restored",
        "PreferredMaintenanceWindow": "sat:04:30-sat:05:00",
        "DBClusterArn": "arn:aws:rds:us-west-2:123456789012:cluster:sample-
cluster-2019-03-16-00-01-restored",
        "DBClusterParameterGroup": "default.docdb3.6",
        "DbClusterResourceId": "cluster-XOO46Q3RH4LWSYNH3NMZKXPISU",
        "MasterUsername": "master-user",
        "EngineVersion": "3.6.0",
        "BackupRetentionPeriod": 3,
        "AssociatedRoles": [],
        "Status": "creating",
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-77186e0d"
            }
```

```
        ]
    }
}
```

Para obtener más información, consulte Restoring from a Cluster Snapshot en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte RestoreDbClusterFromSnapshot en la Referencia de comandos de la AWS CLI.

`restore-db-cluster-to-point-in-time`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-db-cluster-to-point-in-time`.

AWS CLI

Restauración de un clúster de Amazon DocumentDB a un momento dado a partir de una instantánea manual

En el siguiente ejemplo de `restore-db-cluster-to-point-in-time`, se utiliza `sample-cluster-snapshot` para crear un nuevo clúster de Amazon DocumentDB`sample-cluster-pit` utilizando el punto de restauración más reciente.

```
aws docdb restore-db-cluster-to-point-in-time \
    --db-cluster-identifier sample-cluster-pit \
    --source-db-cluster-identifier arn:aws:rds:us-
west-2:123456789012:cluster:sample-cluster \
    --use-latest-restorable-time
```

Salida:

```
{
    "DBCluster": {
        "StorageEncrypted": false,
        "BackupRetentionPeriod": 3,
        "MasterUsername": "master-user",
        "HostedZoneId": "ZNKXH85TT8WVW",
        "PreferredBackupWindow": "00:00-00:30",
        "MultiAZ": false,
        "DBClusterIdentifier": "sample-cluster-pit",
        "DBSubnetGroup": "default",
```

```
        "ClusterCreateTime": "2019-04-03T15:55:21.320Z",
        "AssociatedRoles": [],
        "DBClusterParameterGroup": "default.docdb3.6",
        "DBClusterMembers": [],
        "Status": "creating",
        "AvailabilityZones": [
            "us-west-2a",
            "us-west-2d",
            "us-west-2b"
        ],
        "ReaderEndpoint": "sample-cluster-pit.cluster-ro-corcjozrlsfc.us-
west-2.docdb.amazonaws.com",
        "Port": 27017,
        "Engine": "docdb",
        "EngineVersion": "3.6.0",
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-77186e0d",
                "Status": "active"
            }
        ],
        "PreferredMaintenanceWindow": "sat:04:30-sat:05:00",
        "Endpoint": "sample-cluster-pit.cluster-corcjozrlsfc.us-
west-2.docdb.amazonaws.com",
        "DbClusterResourceId": "cluster-NLCABBXOSE2QPQ4GOLZIFWEPLM",
        "DBClusterArn": "arn:aws:rds:us-west-2:123456789012:cluster:sample-cluster-
pit"
    }
}
```

Para obtener más información, consulte Restoring a Snapshot to a Point in Time en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte RestoreDbClusterToPointInTime en la Referencia de comandos de la AWS CLI.

`start-db-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-db-cluster`.

AWS CLI

Inicio o detención de un clúster de Amazon DocumentDB

En el siguiente ejemplo de `start-db-cluster`, se inicia el clúster de Amazon DocumentDB especificado.

```
aws docdb start-db-cluster \
    --db-cluster-identifier sample-cluster
```

Salida:

```
{
    "DBCluster": {
        "ClusterCreateTime": "2019-03-19T18:45:01.857Z",
        "HostedZoneId": "ZNKXH85TT8WVW",
        "Engine": "docdb",
        "DBClusterMembers": [],
        "MultiAZ": false,
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1c",
            "us-east-1f"
        ],
        "StorageEncrypted": false,
        "ReaderEndpoint": "sample-cluster-2019-03-16-00-01-restored.cluster-ro-
corcjozrlsfc.us-east-1.docdb.amazonaws.com",
        "Endpoint": "sample-cluster-2019-03-16-00-01-restored.cluster-
corcjozrlsfc.us-east-1.docdb.amazonaws.com",
        "Port": 27017,
        "PreferredBackupWindow": "00:00-00:30",
        "DBSubnetGroup": "default",
        "DBClusterIdentifier": "sample-cluster-2019-03-16-00-01-restored",
        "PreferredMaintenanceWindow": "sat:04:30-sat:05:00",
        "DBClusterArn": "arn:aws:rds:us-east-1:123456789012:cluster:sample-
cluster-2019-03-16-00-01-restored",
        "DBClusterParameterGroup": "default.docdb3.6",
        "DbClusterResourceId": "cluster-XOO46Q3RH4LWSYNH3NMZKXPISU",
        "MasterUsername": "master-user",
        "EngineVersion": "3.6.0",
        "BackupRetentionPeriod": 3,
        "AssociatedRoles": [],
        "Status": "creating",
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-77186e0d"
```

```
            }
        ]
    }
}
```

Para obtener más información, consulte Stopping and Starting an Amazon DocumentDB Cluster en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte StartDbCluster en la Referencia de comandos de la AWS CLI.

`stop-db-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-db-cluster`.

AWS CLI

Detención de un clúster de Amazon DocumentDB que está ejecutándose

En el siguiente ejemplo de `stop-db-cluster`, se detiene el clúster de Amazon DocumentDB especificado.

```
aws docdb stop-db-cluster \
    --db-cluster-identifier sample-cluster
```

Salida:

```
{
    "DBCluster": {
        "ClusterCreateTime": "2019-03-19T18:45:01.857Z",
        "HostedZoneId": "ZNKXH85TT8WVW",
        "Engine": "docdb",
        "DBClusterMembers": [],
        "MultiAZ": false,
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1c",
            "us-east-1f"
        ],
        "StorageEncrypted": false,
        "ReaderEndpoint": "sample-cluster-2019-03-16-00-01-restored.cluster-ro-
corcjozrlsfc.us-east-1.docdb.amazonaws.com",
```

```
        "Endpoint": "sample-cluster-2019-03-16-00-01-restored.cluster-
corcjozrlsfc.us-east-1.docdb.amazonaws.com",
        "Port": 27017,
        "PreferredBackupWindow": "00:00-00:30",
        "DBSubnetGroup": "default",
        "DBClusterIdentifier": "sample-cluster-2019-03-16-00-01-restored",
        "PreferredMaintenanceWindow": "sat:04:30-sat:05:00",
        "DBClusterArn": "arn:aws:rds:us-east-1:123456789012:cluster:sample-
cluster-2019-03-16-00-01-restored",
        "DBClusterParameterGroup": "default.docdb3.6",
        "DbClusterResourceId": "cluster-XOO46Q3RH4LWSYNH3NMZKXPISU",
        "MasterUsername": "master-user",
        "EngineVersion": "3.6.0",
        "BackupRetentionPeriod": 3,
        "AssociatedRoles": [],
        "Status": "creating",
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "sg-77186e0d"
            }
        ]
    }
}
```

Para obtener más información, consulte Stopping and Starting an Amazon DocumentDB Cluster en la Guía para desarrolladores de Amazon DocumentDB.

- Para obtener detalles sobre la API, consulte StopDbCluster en la Referencia de comandos de la AWS CLI.

Ejemplos de DynamoDB que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con DynamoDB.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`batch-get-item`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-item`.

AWS CLI

Recuperación de varios elementos de una tabla

En el siguiente ejemplo `batch-get-items`, se leen varios elementos de la tabla `MusicCollection` mediante un lote de tres solicitudes `GetItem` y se solicita el número de unidades de capacidad de lectura consumidas por la operación. El comando devuelve solo el atributo `AlbumTitle`.

```
aws dynamodb batch-get-item \
    --request-items file://request-items.json \
    --return-consumed-capacity TOTAL
```

Contenido de `request-items.json`:

```
{
    "MusicCollection": {
        "Keys": [
            {
                "Artist": {"S": "No One You Know"},
                "SongTitle": {"S": "Call Me Today"}
            },
            {
                "Artist": {"S": "Acme Band"},
                "SongTitle": {"S": "Happy Day"}
            },
            {
                "Artist": {"S": "No One You Know"},
                "SongTitle": {"S": "Scared of My Shadow"}
            }
        ],
        "ProjectionExpression":"AlbumTitle"
    }
```

```
}
```

Salida:

```
{
    "Responses": {
        "MusicCollection": [
            {
                "AlbumTitle": {
                    "S": "Somewhat Famous"
                }
            },
            {
                "AlbumTitle": {
                    "S": "Blue Sky Blues"
                }
            },
            {
                "AlbumTitle": {
                    "S": "Louder Than Ever"
                }
            }
        ]
    },
    "UnprocessedKeys": {},
    "ConsumedCapacity": [
        {
            "TableName": "MusicCollection",
            "CapacityUnits": 1.5
        }
    ]
}
```

Para obtener más información, consulte Operaciones por lotes en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información de la API, consulte BatchGetItem en la Referencia de comandos de la AWS CLI.

`batch-write-item`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-write-item`.

AWS CLI

Adición de varios elementos a una tabla

En el siguiente ejemplo de `batch-write-item`, se añaden tres elementos nuevos a la tabla `MusicCollection` mediante un lote de tres solicitudes `PutItem`. También solicita información sobre el número de unidades de capacidad de escritura consumidas por la operación y cualquier colección de elementos modificada por la operación.

```
aws dynamodb batch-write-item \
    --request-items file://request-items.json \
    --return-consumed-capacity INDEXES \
    --return-item-collection-metrics SIZE
```

Contenido de `request-items.json`:

```
{
    "MusicCollection": [
        {
            "PutRequest": {
                "Item": {
                    "Artist": {"S": "No One You Know"},
                    "SongTitle": {"S": "Call Me Today"},
                    "AlbumTitle": {"S": "Somewhat Famous"}
                }
            }
        },
        {
            "PutRequest": {
                "Item": {
                    "Artist": {"S": "Acme Band"},
                    "SongTitle": {"S": "Happy Day"},
                    "AlbumTitle": {"S": "Songs About Life"}
                }
            }
        },
        {
            "PutRequest": {
                "Item": {
                    "Artist": {"S": "No One You Know"},
                    "SongTitle": {"S": "Scared of My Shadow"},
                    "AlbumTitle": {"S": "Blue Sky Blues"}
                }
```

```
            }
        }
    ]
}
```

Salida:

```
{
    "UnprocessedItems": {},
    "ItemCollectionMetrics": {
        "MusicCollection": [
            {
                "ItemCollectionKey": {
                    "Artist": {
                        "S": "No One You Know"
                    }
                },
                "SizeEstimateRangeGB": [
                    0.0,
                    1.0
                ]
            },
            {
                "ItemCollectionKey": {
                    "Artist": {
                        "S": "Acme Band"
                    }
                },
                "SizeEstimateRangeGB": [
                    0.0,
                    1.0
                ]
            }
        ]
    },
    "ConsumedCapacity": [
        {
            "TableName": "MusicCollection",
            "CapacityUnits": 6.0,
            "Table": {
                "CapacityUnits": 3.0
            },
            "LocalSecondaryIndexes": {
```

```
                "AlbumTitleIndex": {
                    "CapacityUnits": 3.0
                }
            }
        }
    ]
}
```

Para obtener más información, consulte Operaciones por lotes en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información de la API, consulte BatchWriteItem en la Referencia de comandos de la AWS CLI.

`create-backup`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-backup`.

AWS CLI

Creación de una copia de seguridad de una tabla de DynamoDB existente

En el siguiente ejemplo de `create-backup`, se crea una copia de seguridad de la tabla `MusicCollection`.

```
aws dynamodb create-backup \
    --table-name MusicCollection \
    --backup-name MusicCollectionBackup
```

Salida:

```
{
    "BackupDetails": {
        "BackupArn": "arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection/
backup/01576616366715-b4e58d3a",
        "BackupName": "MusicCollectionBackup",
        "BackupSizeBytes": 0,
        "BackupStatus": "CREATING",
        "BackupType": "USER",
        "BackupCreationDateTime": 1576616366.715
    }
}
```

Para obtener más información, consulte On-Demand Backup and Restore for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte CreateBackup en la Referencia de comandos de la AWS CLI.

`create-global-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-global-table`.

AWS CLI

Creación de una tabla global

En el siguiente ejemplo de `create-global-table`, se crea una tabla global a partir de dos tablas idénticas en las distintas regiones de AWS especificadas.

```
aws dynamodb create-global-table \
    --global-table-name MusicCollection \
    --replication-group RegionName=us-east-2 RegionName=us-east-1 \
    --region us-east-2
```

Salida:

```
{
    "GlobalTableDescription": {
        "ReplicationGroup": [
            {
                "RegionName": "us-east-2"
            },
            {
                "RegionName": "us-east-1"
            }
        ],
        "GlobalTableArn": "arn:aws:dynamodb::123456789012:global-table/
MusicCollection",
        "CreationDateTime": 1576625818.532,
        "GlobalTableStatus": "CREATING",
        "GlobalTableName": "MusicCollection"
    }
}
```

Para obtener más información, consulte Tablas globales de Amazon DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte CreateGlobalTable en la Referencia de comandos de la AWS CLI.

`create-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-table`.

AWS CLI

Ejemplo 1: Creación de una tabla con etiquetas

En el siguiente ejemplo `create-table`, se utilizan los atributos y el esquema de claves especificados para crear una tabla denominada `MusicCollection`. Esta tabla utiliza el rendimiento aprovisionado y se cifrará en reposo con la CMK predeterminada propiedad de AWS. El comando también aplica una etiqueta a la tabla, con una clave de `Owner` y un valor de `blueTeam`.

```
aws dynamodb create-table \
    --table-name MusicCollection \
    --attribute-
definitions AttributeName=Artist,AttributeType=S AttributeName=SongTitle,AttributeType=S
 \
    --key-
schema AttributeName=Artist,KeyType=HASH AttributeName=SongTitle,KeyType=RANGE \
    --provisioned-throughput ReadCapacityUnits=5,WriteCapacityUnits=5 \
    --tags Key=Owner,Value=blueTeam
```

Salida:

```
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "Artist",
                "AttributeType": "S"
            },
            {
                "AttributeName": "SongTitle",
                "AttributeType": "S"
```

```
            }
        ],
        "ProvisionedThroughput": {
            "NumberOfDecreasesToday": 0,
            "WriteCapacityUnits": 5,
            "ReadCapacityUnits": 5
        },
        "TableSizeBytes": 0,
        "TableName": "MusicCollection",
        "TableStatus": "CREATING",
        "KeySchema": [
            {
                "KeyType": "HASH",
                "AttributeName": "Artist"
            },
            {
                "KeyType": "RANGE",
                "AttributeName": "SongTitle"
            }
        ],
        "ItemCount": 0,
        "CreationDateTime": "2020-05-26T16:04:41.627000-07:00",
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection",
        "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    }
}
```

Para obtener más información, consulte Operaciones básicas con tablas en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 2: Creación de una tabla en modo bajo demanda

En el siguiente ejemplo, se crea una tabla denominada `MusicCollection` mediante el modo bajo demanda, en lugar del modo de rendimiento aprovisionado. Esto resulta útil para tablas con cargas de trabajo impredecibles.

```
aws dynamodb create-table \
    --table-name MusicCollection \
    --attribute-
definitions AttributeName=Artist,AttributeType=S AttributeName=SongTitle,AttributeType=S
 \
    --key-
schema AttributeName=Artist,KeyType=HASH AttributeName=SongTitle,KeyType=RANGE \
```

```
    --billing-mode PAY_PER_REQUEST
```

Salida:

```
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "Artist",
                "AttributeType": "S"
            },
            {
                "AttributeName": "SongTitle",
                "AttributeType": "S"
            }
        ],
        "TableName": "MusicCollection",
        "KeySchema": [
            {
                "AttributeName": "Artist",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "SongTitle",
                "KeyType": "RANGE"
            }
        ],
        "TableStatus": "CREATING",
        "CreationDateTime": "2020-05-27T11:44:10.807000-07:00",
        "ProvisionedThroughput": {
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 0,
            "WriteCapacityUnits": 0
        },
        "TableSizeBytes": 0,
        "ItemCount": 0,
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection",
        "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "BillingModeSummary": {
            "BillingMode": "PAY_PER_REQUEST"
        }
    }
}
```

Para obtener más información, consulte Operaciones básicas con tablas en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 3: creación de una tabla y cifrarla con una CMK administrada por el cliente

En el siguiente ejemplo, se crea una tabla denominada `MusicCollection` y se cifra mediante una CMK administrada por el cliente.

```
aws dynamodb create-table \
    --table-name MusicCollection \
    --attribute-
definitions AttributeName=Artist,AttributeType=S AttributeName=SongTitle,AttributeType=S
 \
    --key-
schema AttributeName=Artist,KeyType=HASH AttributeName=SongTitle,KeyType=RANGE \
    --provisioned-throughput ReadCapacityUnits=5,WriteCapacityUnits=5 \
    --sse-specification Enabled=true,SSEType=KMS,KMSMasterKeyId=abcd1234-abcd-1234-
a123-ab1234a1b234
```

Salida:

```
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "Artist",
                "AttributeType": "S"
            },
            {
                "AttributeName": "SongTitle",
                "AttributeType": "S"
            }
        ],
        "TableName": "MusicCollection",
        "KeySchema": [
            {
                "AttributeName": "Artist",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "SongTitle",
                "KeyType": "RANGE"
            }
```

```
        ],
        "TableStatus": "CREATING",
        "CreationDateTime": "2020-05-27T11:12:16.431000-07:00",
        "ProvisionedThroughput": {
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 5,
            "WriteCapacityUnits": 5
        },
        "TableSizeBytes": 0,
        "ItemCount": 0,
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection",
        "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "SSEDescription": {
            "Status": "ENABLED",
            "SSEType": "KMS",
            "KMSMasterKeyArn": "arn:aws:kms:us-west-2:123456789012:key/abcd1234-
abcd-1234-a123-ab1234a1b234"
        }
    }
}
```

Para obtener más información, consulte Operaciones básicas con tablas en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 4: creación de una tabla con un índice secundario local

En el siguiente ejemplo, se utilizan los atributos y el esquema de claves especificados para crear una tabla denominada `MusicCollection` con un índice secundario local denominado `AlbumTitleIndex`.

```
aws dynamodb create-table \
    --table-name MusicCollection \
    --attribute-
definitions AttributeName=Artist,AttributeType=S AttributeName=SongTitle,AttributeType=S Att
 \
    --key-
schema AttributeName=Artist,KeyType=HASH AttributeName=SongTitle,KeyType=RANGE \
    --provisioned-throughput ReadCapacityUnits=10,WriteCapacityUnits=5 \
    --local-secondary-indexes \
        "[
            {
                \"IndexName\": \"AlbumTitleIndex\",
                \"KeySchema\": [
```

```
                    {\"AttributeName\": \"Artist\",\"KeyType\":\"HASH\"},
                    {\"AttributeName\": \"AlbumTitle\",\"KeyType\":\"RANGE\"}
                ],
                \"Projection\": {
                    \"ProjectionType\": \"INCLUDE\",
                    \"NonKeyAttributes\": [\"Genre\", \"Year\"]
                }
            }
        ]"
```

Salida:

```
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "AlbumTitle",
                "AttributeType": "S"
            },
            {
                "AttributeName": "Artist",
                "AttributeType": "S"
            },
            {
                "AttributeName": "SongTitle",
                "AttributeType": "S"
            }
        ],
        "TableName": "MusicCollection",
        "KeySchema": [
            {
                "AttributeName": "Artist",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "SongTitle",
                "KeyType": "RANGE"
            }
        ],
        "TableStatus": "CREATING",
        "CreationDateTime": "2020-05-26T15:59:49.473000-07:00",
        "ProvisionedThroughput": {
            "NumberOfDecreasesToday": 0,
```

```
            "ReadCapacityUnits": 10,
            "WriteCapacityUnits": 5
        },
        "TableSizeBytes": 0,
        "ItemCount": 0,
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection",
        "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "LocalSecondaryIndexes": [
            {
                "IndexName": "AlbumTitleIndex",
                "KeySchema": [
                    {
                        "AttributeName": "Artist",
                        "KeyType": "HASH"
                    },
                    {
                        "AttributeName": "AlbumTitle",
                        "KeyType": "RANGE"
                    }
                ],
                "Projection": {
                    "ProjectionType": "INCLUDE",
                    "NonKeyAttributes": [
                        "Genre",
                        "Year"
                    ]
                },
                "IndexSizeBytes": 0,
                "ItemCount": 0,
                "IndexArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/index/AlbumTitleIndex"
            }
        ]
    }
}
```

Para obtener más información, consulte Operaciones básicas con tablas en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 5: creación de una tabla con un índice secundario global

En el siguiente ejemplo, se crea una tabla llamada `GameScores` con un índice secundario global denominado `GameTitleIndex`. La tabla base tiene una clave de partición de `UserId`

y una clave de ordenación de `GameTitle`, lo que le permite encontrar eficientemente la mejor puntuación de un usuario individual para un juego específico, mientras que el GSI tiene una clave de partición de `GameTitle` y una clave de ordenación de `TopScore`, lo que te permite encontrar rápidamente la puntuación más alta en general para un juego en particular.

```
aws dynamodb create-table \
    --table-name GameScores \
    --attribute-
definitions AttributeName=UserId,AttributeType=S AttributeName=GameTitle,AttributeType=S Att
 \
    --key-schema AttributeName=UserId,KeyType=HASH \
                 AttributeName=GameTitle,KeyType=RANGE \
    --provisioned-throughput ReadCapacityUnits=10,WriteCapacityUnits=5 \
    --global-secondary-indexes \
        "[
            {
                \"IndexName\": \"GameTitleIndex\",
                \"KeySchema\": [
                    {\"AttributeName\":\"GameTitle\",\"KeyType\":\"HASH\"},
                    {\"AttributeName\":\"TopScore\",\"KeyType\":\"RANGE\"}
                ],
                \"Projection\": {
                    \"ProjectionType\":\"INCLUDE\",
                    \"NonKeyAttributes\":[\"UserId\"]
                },
                \"ProvisionedThroughput\": {
                    \"ReadCapacityUnits\": 10,
                    \"WriteCapacityUnits\": 5
                }
            }
        ]"
```

Salida:

```
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "GameTitle",
                "AttributeType": "S"
            },
            {
```

```
                "AttributeName": "TopScore",
                "AttributeType": "N"
            },
            {
                "AttributeName": "UserId",
                "AttributeType": "S"
            }
        ],
        "TableName": "GameScores",
        "KeySchema": [
            {
                "AttributeName": "UserId",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "GameTitle",
                "KeyType": "RANGE"
            }
        ],
        "TableStatus": "CREATING",
        "CreationDateTime": "2020-05-26T17:28:15.602000-07:00",
        "ProvisionedThroughput": {
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 10,
            "WriteCapacityUnits": 5
        },
        "TableSizeBytes": 0,
        "ItemCount": 0,
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/GameScores",
        "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "GlobalSecondaryIndexes": [
            {
                "IndexName": "GameTitleIndex",
                "KeySchema": [
                    {
                        "AttributeName": "GameTitle",
                        "KeyType": "HASH"
                    },
                    {
                        "AttributeName": "TopScore",
                        "KeyType": "RANGE"
                    }
                ],
                "Projection": {
```

```
                    "ProjectionType": "INCLUDE",
                    "NonKeyAttributes": [
                        "UserId"
                    ]
                },
                "IndexStatus": "CREATING",
                "ProvisionedThroughput": {
                    "NumberOfDecreasesToday": 0,
                    "ReadCapacityUnits": 10,
                    "WriteCapacityUnits": 5
                },
                "IndexSizeBytes": 0,
                "ItemCount": 0,
                "IndexArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
GameScores/index/GameTitleIndex"
            }
        ]
    }
}
```

Para obtener más información, consulte Operaciones básicas con tablas en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 6: creación de una tabla con varios índices secundarios globales a la vez

En el siguiente ejemplo, se crea una tabla denominada `GameScores` con dos índices secundarios globales. Los esquemas GSI se transfieren mediante un archivo, en lugar de hacerlo a través de la línea de comandos.

```
aws dynamodb create-table \
    --table-name GameScores \
    --attribute-
definitions AttributeName=UserId,AttributeType=S AttributeName=GameTitle,AttributeType=S Att
 \
    --key-
schema AttributeName=UserId,KeyType=HASH AttributeName=GameTitle,KeyType=RANGE \
    --provisioned-throughput ReadCapacityUnits=10,WriteCapacityUnits=5 \
    --global-secondary-indexes file://gsi.json
```

Contenido de `gsi.json`:

```
[
```

```
    {
        "IndexName": "GameTitleIndex",
        "KeySchema": [
            {
                "AttributeName": "GameTitle",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "TopScore",
                "KeyType": "RANGE"
            }
        ],
        "Projection": {
            "ProjectionType": "ALL"
        },
        "ProvisionedThroughput": {
            "ReadCapacityUnits": 10,
            "WriteCapacityUnits": 5
        }
    },
    {
        "IndexName": "GameDateIndex",
        "KeySchema": [
            {
                "AttributeName": "GameTitle",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "Date",
                "KeyType": "RANGE"
            }
        ],
        "Projection": {
            "ProjectionType": "ALL"
        },
        "ProvisionedThroughput": {
            "ReadCapacityUnits": 5,
            "WriteCapacityUnits": 5
        }
    }
]
```

Salida:

```
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "Date",
                "AttributeType": "S"
            },
            {
                "AttributeName": "GameTitle",
                "AttributeType": "S"
            },
            {
                "AttributeName": "TopScore",
                "AttributeType": "N"
            },
            {
                "AttributeName": "UserId",
                "AttributeType": "S"
            }
        ],
        "TableName": "GameScores",
        "KeySchema": [
            {
                "AttributeName": "UserId",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "GameTitle",
                "KeyType": "RANGE"
            }
        ],
        "TableStatus": "CREATING",
        "CreationDateTime": "2020-08-04T16:40:55.524000-07:00",
        "ProvisionedThroughput": {
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 10,
            "WriteCapacityUnits": 5
        },
        "TableSizeBytes": 0,
        "ItemCount": 0,
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/GameScores",
        "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "GlobalSecondaryIndexes": [
```

```
            {
                "IndexName": "GameTitleIndex",
                "KeySchema": [
                    {
                        "AttributeName": "GameTitle",
                        "KeyType": "HASH"
                    },
                    {
                        "AttributeName": "TopScore",
                        "KeyType": "RANGE"
                    }
                ],
                "Projection": {
                    "ProjectionType": "ALL"
                },
                "IndexStatus": "CREATING",
                "ProvisionedThroughput": {
                    "NumberOfDecreasesToday": 0,
                    "ReadCapacityUnits": 10,
                    "WriteCapacityUnits": 5
                },
                "IndexSizeBytes": 0,
                "ItemCount": 0,
                "IndexArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
GameScores/index/GameTitleIndex"
            },
            {
                "IndexName": "GameDateIndex",
                "KeySchema": [
                    {
                        "AttributeName": "GameTitle",
                        "KeyType": "HASH"
                    },
                    {
                        "AttributeName": "Date",
                        "KeyType": "RANGE"
                    }
                ],
                "Projection": {
                    "ProjectionType": "ALL"
                },
                "IndexStatus": "CREATING",
                "ProvisionedThroughput": {
                    "NumberOfDecreasesToday": 0,
```

```
                    "ReadCapacityUnits": 5,
                    "WriteCapacityUnits": 5
                },
                "IndexSizeBytes": 0,
                "ItemCount": 0,
                "IndexArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
GameScores/index/GameDateIndex"
            }
        ]
    }
}
```

Para obtener más información, consulte Operaciones básicas con tablas en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 7: creación de una tabla que tiene habilitado Streams

En el siguiente ejemplo, se crea una tabla denominada `GameScores` con DynamoDB Streams habilitado. En el flujo se escribirán tanto las imágenes nuevas como las antiguas de cada elemento.

```
aws dynamodb create-table \
    --table-name GameScores \
    --attribute-
definitions AttributeName=UserId,AttributeType=S AttributeName=GameTitle,AttributeType=S
 \
    --key-
schema AttributeName=UserId,KeyType=HASH AttributeName=GameTitle,KeyType=RANGE \
    --provisioned-throughput ReadCapacityUnits=10,WriteCapacityUnits=5 \
    --stream-specification StreamEnabled=TRUE,StreamViewType=NEW_AND_OLD_IMAGES
```

Salida:

```
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "GameTitle",
                "AttributeType": "S"
            },
            {
                "AttributeName": "UserId",
                "AttributeType": "S"
```

```
            }
        ],
        "TableName": "GameScores",
        "KeySchema": [
            {
                "AttributeName": "UserId",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "GameTitle",
                "KeyType": "RANGE"
            }
        ],
        "TableStatus": "CREATING",
        "CreationDateTime": "2020-05-27T10:49:34.056000-07:00",
        "ProvisionedThroughput": {
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 10,
            "WriteCapacityUnits": 5
        },
        "TableSizeBytes": 0,
        "ItemCount": 0,
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/GameScores",
        "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "StreamSpecification": {
            "StreamEnabled": true,
            "StreamViewType": "NEW_AND_OLD_IMAGES"
        },
        "LatestStreamLabel": "2020-05-27T17:49:34.056",
        "LatestStreamArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
GameScores/stream/2020-05-27T17:49:34.056"
    }
}
```

Para obtener más información, consulte Operaciones básicas con tablas en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 8: creación de una tabla con un flujo habilitado solo de claves

En el siguiente ejemplo, se crea una tabla denominada `GameScores` con DynamoDB Streams habilitado. Solo se escriben en el flujo los atributos de clave del elementos modificados.

```
aws dynamodb create-table \
```

```
    --table-name GameScores \
    --attribute-
definitions AttributeName=UserId,AttributeType=S AttributeName=GameTitle,AttributeType=S
 \
    --key-
schema AttributeName=UserId,KeyType=HASH AttributeName=GameTitle,KeyType=RANGE \
    --provisioned-throughput ReadCapacityUnits=10,WriteCapacityUnits=5 \
    --stream-specification StreamEnabled=TRUE,StreamViewType=KEYS_ONLY
```

Salida:

```
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "GameTitle",
                "AttributeType": "S"
            },
            {
                "AttributeName": "UserId",
                "AttributeType": "S"
            }
        ],
        "TableName": "GameScores",
        "KeySchema": [
            {
                "AttributeName": "UserId",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "GameTitle",
                "KeyType": "RANGE"
            }
        ],
        "TableStatus": "CREATING",
        "CreationDateTime": "2023-05-25T18:45:34.140000+00:00",
        "ProvisionedThroughput": {
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 10,
            "WriteCapacityUnits": 5
        },
        "TableSizeBytes": 0,
        "ItemCount": 0,
```

```
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/GameScores",
        "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "StreamSpecification": {
            "StreamEnabled": true,
            "StreamViewType": "KEYS_ONLY"
        },
        "LatestStreamLabel": "2023-05-25T18:45:34.140",
        "LatestStreamArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
GameScores/stream/2023-05-25T18:45:34.140",
        "DeletionProtectionEnabled": false
    }
}
```

Para obtener más información, consulte Captura de datos de cambios para DynamoDB Streams en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 9: creación de una tabla mediante la clase de tabla de acceso poco frecuente estándar de DynamoDB

En el siguiente ejemplo se crea una tabla denominada `GameScores` y asigna la clase de tabla Estándar - Acceso poco frecuente (DynamoDB Standard-IA). Esta clase de tabla está optimizada para que el almacenamiento sea el costo dominante.

```
aws dynamodb create-table \
    --table-name GameScores \
    --attribute-
definitions AttributeName=UserId,AttributeType=S AttributeName=GameTitle,AttributeType=S
 \
    --key-
schema AttributeName=UserId,KeyType=HASH AttributeName=GameTitle,KeyType=RANGE \
    --provisioned-throughput ReadCapacityUnits=10,WriteCapacityUnits=5 \
    --table-class STANDARD_INFREQUENT_ACCESS
```

Salida:

```
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "GameTitle",
                "AttributeType": "S"
            },
```

```
            {
                "AttributeName": "UserId",
                "AttributeType": "S"
            }
        ],
        "TableName": "GameScores",
        "KeySchema": [
            {
                "AttributeName": "UserId",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "GameTitle",
                "KeyType": "RANGE"
            }
        ],
        "TableStatus": "CREATING",
        "CreationDateTime": "2023-05-25T18:33:07.581000+00:00",
        "ProvisionedThroughput": {
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 10,
            "WriteCapacityUnits": 5
        },
        "TableSizeBytes": 0,
        "ItemCount": 0,
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/GameScores",
        "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "TableClassSummary": {
            "TableClass": "STANDARD_INFREQUENT_ACCESS"
        },
        "DeletionProtectionEnabled": false
    }
}
```

Para obtener más información, consulte Clases de tabla en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 10: creación de una tabla con la protección contra eliminación habilitada

En el siguiente ejemplo, se crea una tabla denominada `GameScores` y habilita la protección contra eliminación.

```
aws dynamodb create-table \
```

```
    --table-name GameScores \
    --attribute-
definitions AttributeName=UserId,AttributeType=S AttributeName=GameTitle,AttributeType=S
 \
    --key-
schema AttributeName=UserId,KeyType=HASH AttributeName=GameTitle,KeyType=RANGE \
    --provisioned-throughput ReadCapacityUnits=10,WriteCapacityUnits=5 \
    --deletion-protection-enabled
```

Salida:

```
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "GameTitle",
                "AttributeType": "S"
            },
            {
                "AttributeName": "UserId",
                "AttributeType": "S"
            }
        ],
        "TableName": "GameScores",
        "KeySchema": [
            {
                "AttributeName": "UserId",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "GameTitle",
                "KeyType": "RANGE"
            }
        ],
        "TableStatus": "CREATING",
        "CreationDateTime": "2023-05-25T23:02:17.093000+00:00",
        "ProvisionedThroughput": {
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 10,
            "WriteCapacityUnits": 5
        },
        "TableSizeBytes": 0,
        "ItemCount": 0,
```

```
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/GameScores",
        "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "DeletionProtectionEnabled": true
    }
}
```

Para obtener más información, consulte Uso de la protección contra eliminación en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte CreateTable en la Referencia de comandos de la AWS CLI.

`delete-backup`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-backup`.

AWS CLI

Creación de una copia de seguridad de DynamoDB existente

En el siguiente ejemplo de `delete-backup`, se elimina una copia de seguridad especificada existente.

```
aws dynamodb delete-backup \
    --backup-arn arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection/
backup/01576616366715-b4e58d3a
```

Salida:

```
{
    "BackupDescription": {
        "BackupDetails": {
            "BackupArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/backup/01576616366715-b4e58d3a",
            "BackupName": "MusicCollectionBackup",
            "BackupSizeBytes": 0,
            "BackupStatus": "DELETED",
            "BackupType": "USER",
            "BackupCreationDateTime": 1576616366.715
        },
        "SourceTableDetails": {
            "TableName": "MusicCollection",
```

```
            "TableId": "b0c04bcc-309b-4352-b2ae-9088af169fe2",
            "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection",
            "TableSizeBytes": 0,
            "KeySchema": [
                {
                    "AttributeName": "Artist",
                    "KeyType": "HASH"
                },
                {
                    "AttributeName": "SongTitle",
                    "KeyType": "RANGE"
                }
            ],
            "TableCreationDateTime": 1576615228.571,
            "ProvisionedThroughput": {
                "ReadCapacityUnits": 5,
                "WriteCapacityUnits": 5
            },
            "ItemCount": 0,
            "BillingMode": "PROVISIONED"
        },
        "SourceTableFeatureDetails": {}
    }
}
```

Para obtener más información, consulte On-Demand Backup and Restore for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte DeleteBackup en la Referencia de comandos de la AWS CLI.

`delete-item`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-item`.

AWS CLI

Ejemplo 1: Eliminación de un elemento

En el siguiente ejemplo `delete-item`, se elimina un elemento de la tabla `MusicCollection` y se solicitan detalles sobre el elemento que se ha eliminado y la capacidad utilizada por la solicitud.

```
aws dynamodb delete-item \
    --table-name MusicCollection \
    --key file://key.json \
    --return-values ALL_OLD \
    --return-consumed-capacity TOTAL \
    --return-item-collection-metrics SIZE
```

Contenido de `key.json`:

```
{
    "Artist": {"S": "No One You Know"},
    "SongTitle": {"S": "Scared of My Shadow"}
}
```

Salida:

```
{
    "Attributes": {
        "AlbumTitle": {
            "S": "Blue Sky Blues"
        },
        "Artist": {
            "S": "No One You Know"
        },
        "SongTitle": {
            "S": "Scared of My Shadow"
        }
    },
    "ConsumedCapacity": {
        "TableName": "MusicCollection",
        "CapacityUnits": 2.0
    },
    "ItemCollectionMetrics": {
        "ItemCollectionKey": {
            "Artist": {
                "S": "No One You Know"
            }
        },
        "SizeEstimateRangeGB": [
            0.0,
            1.0
        ]
```

```
    }
}
```

Para obtener más información, consulte Escritura de un elemento en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 2: Eliminación de un elemento de forma condicional

En el siguiente ejemplo, se elimina un elemento de la tabla `ProductCatalog` solo si `ProductCategory` es `Sporting Goods` o `Gardening Supplies` y su precio está comprendido entre 500 y 600. Devuelve detalles sobre el elemento que se ha eliminado.

```
aws dynamodb delete-item \
    --table-name ProductCatalog \
    --key '{"Id":{"N":"456"}}' \
    --condition-expression "(ProductCategory IN (:cat1, :cat2)) and (#P between :lo
 and :hi)" \
    --expression-attribute-names file://names.json \
    --expression-attribute-values file://values.json \
    --return-values ALL_OLD
```

Contenido de `names.json`:

```
{
    "#P": "Price"
}
```

Contenido de `values.json`:

```
{
    ":cat1": {"S": "Sporting Goods"},
    ":cat2": {"S": "Gardening Supplies"},
    ":lo": {"N": "500"},
    ":hi": {"N": "600"}
}
```

Salida:

```
{
    "Attributes": {
        "Id": {
```

```
            "N": "456"
        },
        "Price": {
            "N": "550"
        },
        "ProductCategory": {
            "S": "Sporting Goods"
        }
    }
}
```

Para obtener más información, consulte Escritura de un elemento en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte DeleteItem en la Referencia de comandos de la AWS CLI.

`delete-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-table`.

AWS CLI

Eliminación de una tabla

En el siguiente ejemplo de `delete-table` se elimina la tabla `MusicCollection`.

```
aws dynamodb delete-table \
    --table-name MusicCollection
```

Salida:

```
{
    "TableDescription": {
        "TableStatus": "DELETING",
        "TableSizeBytes": 0,
        "ItemCount": 0,
        "TableName": "MusicCollection",
        "ProvisionedThroughput": {
            "NumberOfDecreasesToday": 0,
            "WriteCapacityUnits": 5,
            "ReadCapacityUnits": 5
        }
```

```
    }
}
```

Para obtener más información, consulte Eliminación de una tabla en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte DeleteTable en la Referencia de comandos de la AWS CLI.

`describe-backup`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-backup`.

AWS CLI

Obtención de información sobre una copia de seguridad existente de una tabla

En el siguiente ejemplo de `describe-backup`, se muestra información sobre la copia de seguridad existente especificada.

```
aws dynamodb describe-backup \
    --backup-arn arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection/
backup/01576616366715-b4e58d3a
```

Salida:

```
{
    "BackupDescription": {
        "BackupDetails": {
            "BackupArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/backup/01576616366715-b4e58d3a",
            "BackupName": "MusicCollectionBackup",
            "BackupSizeBytes": 0,
            "BackupStatus": "AVAILABLE",
            "BackupType": "USER",
            "BackupCreationDateTime": 1576616366.715
        },
        "SourceTableDetails": {
            "TableName": "MusicCollection",
            "TableId": "b0c04bcc-309b-4352-b2ae-9088af169fe2",
            "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection",
```

```
            "TableSizeBytes": 0,
            "KeySchema": [
                {
                    "AttributeName": "Artist",
                    "KeyType": "HASH"
                },
                {
                    "AttributeName": "SongTitle",
                    "KeyType": "RANGE"
                }
            ],
            "TableCreationDateTime": 1576615228.571,
            "ProvisionedThroughput": {
                "ReadCapacityUnits": 5,
                "WriteCapacityUnits": 5
            },
            "ItemCount": 0,
            "BillingMode": "PROVISIONED"
        },
        "SourceTableFeatureDetails": {}
    }
}
```

Para obtener más información, consulte On-Demand Backup and Restore for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte DescribeBackup en la Referencia de comandos de la AWS CLI.

`describe-continuous-backups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-continuous-backups`.

AWS CLI

Obtención de información sobre las copias de seguridad continuas de una tabla de DynamoDB

En el siguiente ejemplo de `describe-continuous-backups`, se muestran detalles sobre la configuración de copias de seguridad continuas para la tabla `MusicCollection`.

```
aws dynamodb describe-continuous-backups \
    --table-name MusicCollection
```

Salida:

```
{
    "ContinuousBackupsDescription": {
        "ContinuousBackupsStatus": "ENABLED",
        "PointInTimeRecoveryDescription": {
            "PointInTimeRecoveryStatus": "DISABLED"
        }
    }
}
```

Para obtener más información, consulte Point-in-Time Recovery for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte DescribeContinuousBackups en la Referencia de comandos de la AWS CLI.

`describe-contributor-insights`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-contributor-insights`.

AWS CLI

Visualización de la configuración de Contributor Insights de una tabla de DynamoDB

En el siguiente ejemplo de `describe-contributor-insights`, se muestra la configuración de Contributor Insights para la tabla `MusicCollection` y el índice secundario global de `AlbumTitle-index`.

```
aws dynamodb describe-contributor-insights \
    --table-name MusicCollection \
    --index-name AlbumTitle-index
```

Salida:

```
{
    "TableName": "MusicCollection",
    "IndexName": "AlbumTitle-index",
    "ContributorInsightsRuleList": [
        "DynamoDBContributorInsights-PKC-MusicCollection-1576629651520",
        "DynamoDBContributorInsights-SKC-MusicCollection-1576629651520",
```

```
        "DynamoDBContributorInsights-PKT-MusicCollection-1576629651520",
        "DynamoDBContributorInsights-SKT-MusicCollection-1576629651520"
    ],
    "ContributorInsightsStatus": "ENABLED",
    "LastUpdateDateTime": 1576629654.78
}
```

Para obtener más información, consulte Análisis del acceso a los datos mediante CloudWatch contributor insights for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte DescribeContributorInsights en la Referencia de comandos de la AWS CLI.

`describe-endpoints`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-endpoints`.

AWS CLI

Visualización de la información de los puntos de conexión regionales

En el siguiente ejemplo de `describe-endpoints`, se muestran detalles sobre los puntos de conexión de la región de AWS actual.

```
aws dynamodb describe-endpoints
```

Salida:

```
{
    "Endpoints": [
        {
            "Address": "dynamodb.us-west-2.amazonaws.com",
            "CachePeriodInMinutes": 1440
        }
    ]
}
```

Para obtener más información, consulte Amazon DynamoDB Endpoints and Quotas en la Referencia general de AWS.

- Para obtener detalles sobre la API, consulte DescribeEndpoints en la Referencia de comandos de la AWS CLI.

describe-global-table-settings

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-global-table-settings`.

AWS CLI

Obtención de información sobre la configuración de una tabla global de DynamoDB

En el siguiente ejemplo de `describe-global-table-settings`, se muestra la configuración de la tabla global de `MusicCollection`.

```
aws dynamodb describe-global-table-settings \
    --global-table-name MusicCollection
```

Salida:

```
{
    "GlobalTableName": "MusicCollection",
    "ReplicaSettings": [
        {
            "RegionName": "us-east-1",
            "ReplicaStatus": "ACTIVE",
            "ReplicaProvisionedReadCapacityUnits": 10,
            "ReplicaProvisionedReadCapacityAutoScalingSettings": {
                "AutoScalingDisabled": true
            },
            "ReplicaProvisionedWriteCapacityUnits": 5,
            "ReplicaProvisionedWriteCapacityAutoScalingSettings": {
                "AutoScalingDisabled": true
            }
        },
        {
            "RegionName": "us-east-2",
            "ReplicaStatus": "ACTIVE",
            "ReplicaProvisionedReadCapacityUnits": 10,
            "ReplicaProvisionedReadCapacityAutoScalingSettings": {
                "AutoScalingDisabled": true
            },
            "ReplicaProvisionedWriteCapacityUnits": 5,
            "ReplicaProvisionedWriteCapacityAutoScalingSettings": {
                "AutoScalingDisabled": true
            }
        }
```

```
    ]
}
```

Para obtener más información, consulte Tablas globales de Amazon DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte DescribeGlobalTableSettings en la Referencia de comandos de la AWS CLI.

`describe-global-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-global-table`.

AWS CLI

Visualización de información sobre una tabla global de DynamoDB

En el siguiente ejemplo de `describe-global-table`, se muestran detalles sobre la tabla global de `MusicCollection`.

```
aws dynamodb describe-global-table \
    --global-table-name MusicCollection
```

Salida:

```
{
    "GlobalTableDescription": {
        "ReplicationGroup": [
            {
                "RegionName": "us-east-2"
            },
            {
                "RegionName": "us-east-1"
            }
        ],
        "GlobalTableArn": "arn:aws:dynamodb::123456789012:global-table/
MusicCollection",
        "CreationDateTime": 1576625818.532,
        "GlobalTableStatus": "ACTIVE",
        "GlobalTableName": "MusicCollection"
    }
}
```

Para obtener más información, consulte Tablas globales de Amazon DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte DescribeGlobalTable en la Referencia de comandos de la AWS CLI.

`describe-limits`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-limits`.

AWS CLI

Visualización de los límites de capacidad aprovisionada

En el siguiente ejemplo de `describe-limits`, se muestran los límites de capacidad aprovisionada de su cuenta en la región actual de AWS.

```
aws dynamodb describe-limits
```

Salida:

```
{
    "AccountMaxReadCapacityUnits": 80000,
    "AccountMaxWriteCapacityUnits": 80000,
    "TableMaxReadCapacityUnits": 40000,
    "TableMaxWriteCapacityUnits": 40000
}
```

Para obtener más información, consulte Límites en DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte DescribeLimits en la Referencia de comandos de la AWS CLI.

`describe-table-replica-auto-scaling`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-table-replica-auto-scaling`.

AWS CLI

Visualización de la configuración de escalado automático en las réplicas de una tabla global

En el siguiente ejemplo de `describe-table-replica-auto-scaling`, se muestra la configuración de escalado automático en todas las réplicas de la tabla global de `MusicCollection`.

```
aws dynamodb describe-table-replica-auto-scaling \
    --table-name MusicCollection
```

Salida:

```
{
    "TableAutoScalingDescription": {
        "TableName": "MusicCollection",
        "TableStatus": "ACTIVE",
        "Replicas": [
            {
                "RegionName": "us-east-1",
                "GlobalSecondaryIndexes": [],
                "ReplicaProvisionedReadCapacityAutoScalingSettings": {
                    "MinimumUnits": 5,
                    "MaximumUnits": 40000,
                    "AutoScalingRoleArn": "arn:aws:iam::123456789012:role/
aws-service-role/dynamodb.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable",
                    "ScalingPolicies": [
                        {
                            "PolicyName": "DynamoDBReadCapacityUtilization:table/
MusicCollection",
                            "TargetTrackingScalingPolicyConfiguration": {
                                "TargetValue": 70.0
                            }
                        }
                    ]
                },
                "ReplicaProvisionedWriteCapacityAutoScalingSettings": {
                    "MinimumUnits": 5,
                    "MaximumUnits": 40000,
                    "AutoScalingRoleArn": "arn:aws:iam::123456789012:role/
aws-service-role/dynamodb.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable",
                    "ScalingPolicies": [
                        {
                            "PolicyName": "DynamoDBWriteCapacityUtilization:table/
MusicCollection",
```

```
                            "TargetTrackingScalingPolicyConfiguration": {
                                "TargetValue": 70.0
                            }
                        }
                    ]
                },
                "ReplicaStatus": "ACTIVE"
            },
            {
                "RegionName": "us-east-2",
                "GlobalSecondaryIndexes": [],
                "ReplicaProvisionedReadCapacityAutoScalingSettings": {
                    "MinimumUnits": 5,
                    "MaximumUnits": 40000,
                    "AutoScalingRoleArn": "arn:aws:iam::123456789012:role/
aws-service-role/dynamodb.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable",
                    "ScalingPolicies": [
                        {
                            "PolicyName": "DynamoDBReadCapacityUtilization:table/
MusicCollection",
                            "TargetTrackingScalingPolicyConfiguration": {
                                "TargetValue": 70.0
                            }
                        }
                    ]
                },
                "ReplicaProvisionedWriteCapacityAutoScalingSettings": {
                    "MinimumUnits": 5,
                    "MaximumUnits": 40000,
                    "AutoScalingRoleArn": "arn:aws:iam::123456789012:role/
aws-service-role/dynamodb.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable",
                    "ScalingPolicies": [
                        {
                            "PolicyName": "DynamoDBWriteCapacityUtilization:table/
MusicCollection",
                            "TargetTrackingScalingPolicyConfiguration": {
                                "TargetValue": 70.0
                            }
                        }
                    ]
                },
                "ReplicaStatus": "ACTIVE"
```

```
            }
        ]
    }
}
```

Para obtener más información, consulte Tablas globales de Amazon DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte DescribeTableReplicaAutoScaling en la Referencia de comandos de la AWS CLI.

`describe-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-table`.

AWS CLI

Descripción de una tabla

En el siguiente ejemplo `describe-table`, se describe la tabla `MusicCollection`.

```
aws dynamodb describe-table \
    --table-name MusicCollection
```

Salida:

```
{
    "Table": {
        "AttributeDefinitions": [
            {
                "AttributeName": "Artist",
                "AttributeType": "S"
            },
            {
                "AttributeName": "SongTitle",
                "AttributeType": "S"
            }
        ],
        "ProvisionedThroughput": {
            "NumberOfDecreasesToday": 0,
            "WriteCapacityUnits": 5,
            "ReadCapacityUnits": 5
```

```
        },
        "TableSizeBytes": 0,
        "TableName": "MusicCollection",
        "TableStatus": "ACTIVE",
        "KeySchema": [
            {
                "KeyType": "HASH",
                "AttributeName": "Artist"
            },
            {
                "KeyType": "RANGE",
                "AttributeName": "SongTitle"
            }
        ],
        "ItemCount": 0,
        "CreationDateTime": 1421866952.062
    }
}
```

Para obtener más información, consulte Descripción de una tabla en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte DescribeTable en la Referencia de comandos de la AWS CLI.

`describe-time-to-live`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-time-to-live`.

AWS CLI

Visualización de la configuración de tiempo de vida de una tabla

En el siguiente ejemplo de `describe-time-to-live`, se muestra la configuración de tiempo de vida de la tabla `MusicCollection`.

```
aws dynamodb describe-time-to-live \
    --table-name MusicCollection
```

Salida:

```
{
```

```
    "TimeToLiveDescription": {
        "TimeToLiveStatus": "ENABLED",
        "AttributeName": "ttl"
    }
}
```

Para obtener más información, consulte Tiempo de vida en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte DescribeTimeToLive en la Referencia de comandos de la AWS CLI.

`get-item`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-item`.

AWS CLI

Ejemplo 1: Lectura de un elemento de una tabla

En el siguiente ejemplo `get-item`, se recupera un elemento de la tabla `MusicCollection`. La tabla tiene una clave principal hash y de rango (`Artist` y `SongTitle`), por lo que debe especificar ambos atributos. El comando también solicita información sobre la capacidad de lectura consumida por la operación.

```
aws dynamodb get-item \
    --table-name MusicCollection \
    --key file://key.json \
    --return-consumed-capacity TOTAL
```

Contenido de `key.json`:

```
{
    "Artist": {"S": "Acme Band"},
    "SongTitle": {"S": "Happy Day"}
}
```

Salida:

```
{
    "Item": {
```

```
        "AlbumTitle": {
            "S": "Songs About Life"
        },
        "SongTitle": {
            "S": "Happy Day"
        },
        "Artist": {
            "S": "Acme Band"
        }
    },
    "ConsumedCapacity": {
        "TableName": "MusicCollection",
        "CapacityUnits": 0.5
    }
}
```

Para obtener más información, consulte Lectura de un elemento en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 2: Lectura de un elemento mediante una lectura coherente

En el siguiente ejemplo, se recupera un elemento de la tabla `MusicCollection` con lecturas altamente coherentes.

```
aws dynamodb get-item \
    --table-name MusicCollection \
    --key file://key.json \
    --consistent-read \
    --return-consumed-capacity TOTAL
```

Contenido de `key.json`:

```
{
    "Artist": {"S": "Acme Band"},
    "SongTitle": {"S": "Happy Day"}
}
```

Salida:

```
{
    "Item": {
        "AlbumTitle": {
```

```
            "S": "Songs About Life"
        },
        "SongTitle": {
            "S": "Happy Day"
        },
        "Artist": {
            "S": "Acme Band"
        }
    },
    "ConsumedCapacity": {
        "TableName": "MusicCollection",
        "CapacityUnits": 1.0
    }
}
```

Para obtener más información, consulte Lectura de un elemento en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 3: recuperación de atributos específicos de un elemento

En el siguiente ejemplo, se utiliza una expresión de proyección para recuperar solo tres atributos del elemento deseado.

```
aws dynamodb get-item \
    --table-name ProductCatalog \
    --key '{"Id": {"N": "102"}}' \
    --projection-expression "#T, #C, #P" \
    --expression-attribute-names file://names.json
```

Contenido de `names.json`:

```
{
    "#T": "Title",
    "#C": "ProductCategory",
    "#P": "Price"
}
```

Salida:

```
{
    "Item": {
        "Price": {
```

```
            "N": "20"
        },
        "Title": {
            "S": "Book 102 Title"
        },
        "ProductCategory": {
            "S": "Book"
        }
    }
}
```

Para obtener más información, consulte Lectura de un elemento en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte GetItem en la Referencia de comandos de la AWS CLI.

`list-backups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-backups`.

AWS CLI

Ejemplo 1: enumerar todas las copias de seguridad de DynamoDB existentes

En el siguiente ejemplo de `list-backups`, se enumeran todas sus copias de seguridad existentes.

```
aws dynamodb list-backups
```

Salida:

```
{
    "BackupSummaries": [
        {
            "TableName": "MusicCollection",
            "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection",
            "BackupArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/backup/01234567890123-a1bcd234",
            "BackupName": "MusicCollectionBackup1",
```

```
            "BackupCreationDateTime": "2020-02-12T14:41:51.617000-08:00",
            "BackupStatus": "AVAILABLE",
            "BackupType": "USER",
            "BackupSizeBytes": 170
        },
        {
            "TableName": "MusicCollection",
            "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection",
            "BackupArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/backup/01234567890123-b2abc345",
            "BackupName": "MusicCollectionBackup2",
            "BackupCreationDateTime": "2020-06-26T11:08:35.431000-07:00",
            "BackupStatus": "AVAILABLE",
            "BackupType": "USER",
            "BackupSizeBytes": 400
        }
    ]
}
```

Para obtener más información, consulte On-Demand Backup and Restore for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 2: lista de las copias de seguridad creadas por los usuarios en un intervalo de tiempo específico

En el siguiente ejemplo, se muestran solo las copias de seguridad de la tabla `MusicCollection` que ha creado el usuario (no las que DynamoDB ha creado automáticamente) con una fecha de creación entre el 1 de enero de 2020 y el 1 de marzo de 2020.

```
aws dynamodb list-backups \
    --table-name MusicCollection \
    --time-range-lower-bound 1577836800 \
    --time-range-upper-bound 1583020800 \
    --backup-type USER
```

Salida:

```
{
    "BackupSummaries": [
        {
```

```
            "TableName": "MusicCollection",
            "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection",
            "BackupArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/backup/01234567890123-a1bcd234",
            "BackupName": "MusicCollectionBackup1",
            "BackupCreationDateTime": "2020-02-12T14:41:51.617000-08:00",
            "BackupStatus": "AVAILABLE",
            "BackupType": "USER",
            "BackupSizeBytes": 170
        }
    ]
}
```

Para obtener más información, consulte On-Demand Backup and Restore for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 3: limitación del tamaño de la página

En el siguiente ejemplo, se devuelve una lista de todas las copias de seguridad existentes, pero recupera solo un elemento en cada llamada y, si es necesario, realiza varias llamadas para obtener la lista completa. Limitar el tamaño de página resulta útil cuando se ejecutan comandos de la lista en un gran número de recursos, lo que puede provocar un error de “tiempo de espera” cuando se utiliza el tamaño de página predeterminado de 1000.

```
aws dynamodb list-backups \
    --page-size 1
```

Salida:

```
{
    "BackupSummaries": [
        {
            "TableName": "MusicCollection",
            "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection",
            "BackupArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/backup/01234567890123-a1bcd234",
            "BackupName": "MusicCollectionBackup1",
            "BackupCreationDateTime": "2020-02-12T14:41:51.617000-08:00",
```

```
            "BackupStatus": "AVAILABLE",
            "BackupType": "USER",
            "BackupSizeBytes": 170
        },
        {
            "TableName": "MusicCollection",
            "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection",
            "BackupArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/backup/01234567890123-b2abc345",
            "BackupName": "MusicCollectionBackup2",
            "BackupCreationDateTime": "2020-06-26T11:08:35.431000-07:00",
            "BackupStatus": "AVAILABLE",
            "BackupType": "USER",
            "BackupSizeBytes": 400
        }
    ]
}
```

Para obtener más información, consulte On-Demand Backup and Restore for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 4: limitación del número de elementos devueltos

En el siguiente ejemplo, se limita el número de elementos devueltos a 1. La respuesta incluye un valor `NextToken` con el que recuperar la siguiente página de resultados.

```
aws dynamodb list-backups \
    --max-items 1
```

Salida:

```
{
    "BackupSummaries": [
        {
            "TableName": "MusicCollection",
            "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection",
            "BackupArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/backup/01234567890123-a1bcd234",
            "BackupName": "MusicCollectionBackup1",
```

```
            "BackupCreationDateTime": "2020-02-12T14:41:51.617000-08:00",
            "BackupStatus": "AVAILABLE",
            "BackupType": "USER",
            "BackupSizeBytes": 170
        }
    ],
    "NextToken":
 "abCDeFGhiJKlmnOPqrSTuvwxYZ1aBCdEFghijK7LM51nOpqRSTuv3WxY3ZabC5dEFGhI2Jk3LmnoPQ6RST9"
}
```

Para obtener más información, consulte On-Demand Backup and Restore for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 5: recuperar la siguiente página de resultados

El comando siguiente utiliza el valor `NextToken` de una llamada anterior al comando `list-backups` para recuperar otra página de resultados. Puesto que la respuesta en este caso no incluye ningún valor `NextToken`, sabemos que hemos llegado al final de los resultados.

```
aws dynamodb list-backups \
    --starting-
token abCDeFGhiJKlmnOPqrSTuvwxYZ1aBCdEFghijK7LM51nOpqRSTuv3WxY3ZabC5dEFGhI2Jk3LmnoPQ6RST9
```

Output

```
{
    "BackupSummaries": [
        {
            "TableName": "MusicCollection",
            "TableId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection",
            "BackupArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/backup/01234567890123-b2abc345",
            "BackupName": "MusicCollectionBackup2",
            "BackupCreationDateTime": "2020-06-26T11:08:35.431000-07:00",
            "BackupStatus": "AVAILABLE",
            "BackupType": "USER",
            "BackupSizeBytes": 400
        }
    ]
}
```

Para obtener más información, consulte On-Demand Backup and Restore for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte ListBackups en la Referencia de comandos de la AWS CLI.

`list-contributor-insights`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-contributor-insights`.

AWS CLI

Ejemplo 1: ver una lista de resúmenes de Contributor Insights

En el siguiente ejemplo de `list-contributor-insights`, se muestra una lista de resúmenes de Contributor Insights.

```
aws dynamodb list-contributor-insights
```

Salida:

```
{
    "ContributorInsightsSummaries": [
        {
            "TableName": "MusicCollection",
            "IndexName": "AlbumTitle-index",
            "ContributorInsightsStatus": "ENABLED"
        },
        {
            "TableName": "ProductCatalog",
            "ContributorInsightsStatus": "ENABLED"
        },
        {
            "TableName": "Forum",
            "ContributorInsightsStatus": "ENABLED"
        },
        {
            "TableName": "Reply",
            "ContributorInsightsStatus": "ENABLED"
        },
        {
            "TableName": "Thread",
```

```
            "ContributorInsightsStatus": "ENABLED"
        }
    ]
}
```

Para obtener más información, consulte Análisis del acceso a los datos mediante CloudWatch contributor insights for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 2: limitación del número de elementos devueltos

En el siguiente ejemplo, se limita el número de filas devueltas a cuatro. La respuesta incluye un valor `NextToken` con el que recuperar la siguiente página de resultados.

```
aws dynamodb list-contributor-insights \
    --max-results 4
```

Salida:

```
{
    "ContributorInsightsSummaries": [
        {
            "TableName": "MusicCollection",
            "IndexName": "AlbumTitle-index",
            "ContributorInsightsStatus": "ENABLED"
        },
        {
            "TableName": "ProductCatalog",
            "ContributorInsightsStatus": "ENABLED"
        },
        {
            "TableName": "Forum",
            "ContributorInsightsStatus": "ENABLED"
        }
    ],
    "NextToken":
 "abCDeFGhiJKlmnOPqrSTuvwxYZ1aBCdEFghijK7LM51nOpqRSTuv3WxY3ZabC5dEFGhI2Jk3LmnoPQ6RST9"
}
```

Para obtener más información, consulte Análisis del acceso a los datos mediante CloudWatch contributor insights for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 3: recuperar la siguiente página de resultados

El comando siguiente utiliza el valor `NextToken` de una llamada anterior al comando `list-contributor-insights` para recuperar otra página de resultados. Puesto que la respuesta en este caso no incluye ningún valor `NextToken`, sabemos que hemos llegado al final de los resultados.

```
aws dynamodb list-contributor-insights \
    --max-results 4 \
    --next-
token abCDeFGhiJKlmnOPqrSTuvwxYZ1aBCdEFghijK7LM51nOpqRSTuv3WxY3ZabC5dEFGhI2Jk3LmnoPQ6RST9
```

Salida:

```
{
    "ContributorInsightsSummaries": [
        {
            "TableName": "Reply",
            "ContributorInsightsStatus": "ENABLED"
        },
        {
            "TableName": "Thread",
            "ContributorInsightsStatus": "ENABLED"
        }
    ]
}
```

Para obtener más información, consulte Análisis del acceso a los datos mediante CloudWatch contributor insights for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte ListContributorInsights en la Referencia de comandos de la AWS CLI.

`list-global-tables`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-global-tables`.

AWS CLI

Para enumerar las tablas globales de DynamoDB existentes

En el siguiente ejemplo de `list-global-tables`, se enumeran todas sus tablas globales existentes.

```
aws dynamodb list-global-tables
```

Salida:

```
{
    "GlobalTables": [
        {
            "GlobalTableName": "MusicCollection",
            "ReplicationGroup": [
                {
                    "RegionName": "us-east-2"
                },
                {
                    "RegionName": "us-east-1"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Tablas globales de Amazon DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte ListGlobalTables en la Referencia de comandos de la AWS CLI.

`list-tables`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tables`.

AWS CLI

Ejemplo 1: Creación de una lista de tablas

En el siguiente ejemplo `list-tables`, se enumeran las tablas asociadas a la cuenta y región de AWS.

```
aws dynamodb list-tables
```

Salida:

```
{
    "TableNames": [
        "Forum",
        "ProductCatalog",
        "Reply",
        "Thread"
    ]
}
```

Para obtener más información, consulte Enumeración de nombres de tablas en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 2: Limitación del tamaño de la página

En el siguiente ejemplo, se devuelve una lista de todas las tablas existentes, pero recupera solo un elemento en cada llamada y, si es necesario, realiza varias llamadas para obtener la lista completa. Limitar el tamaño de página resulta útil cuando se ejecutan comandos de la lista en un gran número de recursos, lo que puede provocar un error de "tiempo de espera" cuando se utiliza el tamaño de página predeterminado de 1000.

```
aws dynamodb list-tables \
    --page-size 1
```

Salida:

```
{
    "TableNames": [
        "Forum",
        "ProductCatalog",
        "Reply",
        "Thread"
    ]
}
```

Para obtener más información, consulte Enumeración de nombres de tablas en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 3: limitación del número de elementos devueltos

En el siguiente ejemplo, se limita el número de elementos devueltos a 2. La respuesta incluye un valor `NextToken` con el que recuperar la siguiente página de resultados.

```
aws dynamodb list-tables \
    --max-items 2
```

Salida:

```
{
    "TableNames": [
        "Forum",
        "ProductCatalog"
    ],
    "NextToken":
 "abCDeFGhiJKlmnOPqrSTuvwxYZ1aBCdEFghijK7LM51nOpqRSTuv3WxY3ZabC5dEFGhI2Jk3LmnoPQ6RST9"
}
```

Para obtener más información, consulte Enumeración de nombres de tablas en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 4: recuperación de la siguiente página de resultados

El comando siguiente utiliza el valor `NextToken` de una llamada anterior al comando `list-tables` para recuperar otra página de resultados. Puesto que la respuesta en este caso no incluye ningún valor `NextToken`, sabemos que hemos llegado al final de los resultados.

```
aws dynamodb list-tables \
    --starting-
token abCDeFGhiJKlmnOPqrSTuvwxYZ1aBCdEFghijK7LM51nOpqRSTuv3WxY3ZabC5dEFGhI2Jk3LmnoPQ6RST9
```

Salida:

```
{
    "TableNames": [
        "Reply",
        "Thread"
    ]
}
```

Para obtener más información, consulte Enumeración de nombres de tablas en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte ListTables en la Referencia de comandos de la AWS CLI.

`list-tags-of-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-of-resource`.

AWS CLI

Ejemplo 1: enumerar las etiquetas de un recurso de DynamoDB

En el siguiente ejemplo de `list-tags-of-resource`, se muestran las etiquetas de la tabla `MusicCollection`.

```
aws dynamodb list-tags-of-resource \
    --resource-arn arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection
```

Salida:

```
{
    "Tags": [
        {
            "Key": "Owner",
            "Value": "blueTeam"
        },
        {
            "Key": "Environment",
            "Value": "Production"
        }
    ]
}
```

Para obtener más información, consulte Etiquetado para DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 2: limitación del número de etiquetas devueltas

En el siguiente ejemplo, se limita el número de etiquetas devueltas a 1. La respuesta incluye un valor `NextToken` con el que recuperar la siguiente página de resultados.

```
aws dynamodb list-tags-of-resource \
    --resource-arn arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection \
    --max-items 1
```

Salida:

```
{
    "Tags": [
        {
            "Key": "Owner",
            "Value": "blueTeam"
        }
    ],
    "NextToken":
 "abCDeFGhiJKlmnOPqrSTuvwxYZ1aBCdEFghijK7LM51nOpqRSTuv3WxY3ZabC5dEFGhI2Jk3LmnoPQ6RST9"
}
```

Para obtener más información, consulte Etiquetado para DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 3: recuperar la siguiente página de resultados

El comando siguiente utiliza el valor `NextToken` de una llamada anterior al comando `list-tags-of-resource` para recuperar otra página de resultados. Puesto que la respuesta en este caso no incluye ningún valor `NextToken`, sabemos que hemos llegado al final de los resultados.

```
aws dynamodb list-tags-of-resource \
    --resource-arn arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection \
    --starting-
token abCDeFGhiJKlmnOPqrSTuvwxYZ1aBCdEFghijK7LM51nOpqRSTuv3WxY3ZabC5dEFGhI2Jk3LmnoPQ6RST9
```

Salida:

```
{
    "Tags": [
        {
            "Key": "Environment",
            "Value": "Production"
        }
    ]
}
```

Para obtener más información, consulte Etiquetado para DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte ListTagsOfResource en la Referencia de comandos de la AWS CLI.

`put-item`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-item`.

AWS CLI

Ejemplo 1: Adición de un elemento a una tabla

En el siguiente ejemplo `put-item`, se añade un elemento nuevo a la tabla MusicCollection.

```
aws dynamodb put-item \
    --table-name MusicCollection \
    --item file://item.json \
    --return-consumed-capacity TOTAL \
    --return-item-collection-metrics SIZE
```

Contenido de `item.json`:

```
{
    "Artist": {"S": "No One You Know"},
    "SongTitle": {"S": "Call Me Today"},
    "AlbumTitle": {"S": "Greatest Hits"}
}
```

Salida:

```
{
    "ConsumedCapacity": {
        "TableName": "MusicCollection",
        "CapacityUnits": 1.0
    },
    "ItemCollectionMetrics": {
        "ItemCollectionKey": {
            "Artist": {
                "S": "No One You Know"
            }
        },
        "SizeEstimateRangeGB": [
            0.0,
```

```
            1.0
        ]
    }
}
```

Para obtener más información, consulte Escritura de un elemento en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 2: Sobrescritura condicional de un elemento de una tabla

En el siguiente ejemplo de `put-item` se sobrescribe un elemento existente de la tabla `MusicCollection` solo si ese elemento existente tiene un atributo `AlbumTitle` con un valor de `Greatest Hits`. El comando devuelve el valor anterior del elemento.

```
aws dynamodb put-item \
    --table-name MusicCollection \
    --item file://item.json \
    --condition-expression "#A = :A" \
    --expression-attribute-names file://names.json \
    --expression-attribute-values file://values.json \
    --return-values ALL_OLD
```

Contenido de `item.json`:

```
{
    "Artist": {"S": "No One You Know"},
    "SongTitle": {"S": "Call Me Today"},
    "AlbumTitle": {"S": "Somewhat Famous"}
}
```

Contenido de `names.json`:

```
{
    "#A": "AlbumTitle"
}
```

Contenido de `values.json`:

```
{
    ":A": {"S": "Greatest Hits"}
}
```

Salida:

```
{
    "Attributes": {
        "AlbumTitle": {
            "S": "Greatest Hits"
        },
        "Artist": {
            "S": "No One You Know"
        },
        "SongTitle": {
            "S": "Call Me Today"
        }
    }
}
```

Si la clave ya existe, debería ver el siguiente resultado:

```
A client error (ConditionalCheckFailedException) occurred when calling the PutItem
 operation: The conditional request failed.
```

Para obtener más información, consulte Escritura de un elemento en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte PutItem en la Referencia de comandos de la AWS CLI.

`query`

En el siguiente ejemplo de código, se muestra cómo utilizar `query`.

AWS CLI

Ejemplo 1: Consulta de una tabla

En el siguiente ejemplo de `query` se consultan elementos de la tabla `MusicCollection`. La tabla tiene una clave principal hash y de rango (`Artist` y `SongTitle`), pero esta consulta solo especifica el valor de la clave hash. Devuelve los títulos de las canciones del artista llamado “No One You Know”.

```
aws dynamodb query \
```

```
    --table-name MusicCollection \
    --projection-expression "SongTitle" \
    --key-condition-expression "Artist = :v1" \
    --expression-attribute-values file://expression-attributes.json \
    --return-consumed-capacity TOTAL
```

Contenido de `expression-attributes.json`:

```
{
    ":v1": {"S": "No One You Know"}
}
```

Salida:

```
{
    "Items": [
        {
            "SongTitle": {
                "S": "Call Me Today"
            },
            "SongTitle": {
                "S": "Scared of My Shadow"
            }
        }
    ],
    "Count": 2,
    "ScannedCount": 2,
    "ConsumedCapacity": {
        "TableName": "MusicCollection",
        "CapacityUnits": 0.5
    }
}
```

Para obtener más información, consulte Uso de consultas en DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 2: Consulta de una tabla con lecturas altamente coherentes y recorrer el índice en orden descendente

En el siguiente ejemplo se realiza la misma consulta que en el primer ejemplo, pero se devuelven los resultados en orden inverso y se utilizan lecturas altamente coherentes.

```
aws dynamodb query \
    --table-name MusicCollection \
    --projection-expression "SongTitle" \
    --key-condition-expression "Artist = :v1" \
    --expression-attribute-values file://expression-attributes.json \
    --consistent-read \
    --no-scan-index-forward \
    --return-consumed-capacity TOTAL
```

Contenido de `expression-attributes.json`:

```
{
    ":v1": {"S": "No One You Know"}
}
```

Salida:

```
{
    "Items": [
        {
            "SongTitle": {
                "S": "Scared of My Shadow"
            }
        },
        {
            "SongTitle": {
                "S": "Call Me Today"
            }
        }
    ],
    "Count": 2,
    "ScannedCount": 2,
    "ConsumedCapacity": {
        "TableName": "MusicCollection",
        "CapacityUnits": 1.0
    }
}
```

Para obtener más información, consulte Uso de consultas en DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 3: filtrado de resultados específicos

En el siguiente ejemplo se consulta `MusicCollection` pero se excluyen los resultados con valores específicos en el atributo `AlbumTitle`. Tenga en cuenta que esto no afecta a `ScannedCount` o `ConsumedCapacity`, ya que el filtro se aplica después de leer los elementos.

```
aws dynamodb query \
    --table-name MusicCollection \
    --key-condition-expression "#n1 = :v1" \
    --filter-expression "NOT (#n2 IN (:v2, :v3))" \
    --expression-attribute-names file://names.json \
    --expression-attribute-values file://values.json \
    --return-consumed-capacity TOTAL
```

Contenido de `values.json`:

```
{
    ":v1": {"S": "No One You Know"},
    ":v2": {"S": "Blue Sky Blues"},
    ":v3": {"S": "Greatest Hits"}
}
```

Contenido de `names.json`:

```
{
    "#n1": "Artist",
    "#n2": "AlbumTitle"
}
```

Salida:

```
{
    "Items": [
        {
            "AlbumTitle": {
                "S": "Somewhat Famous"
            },
            "Artist": {
                "S": "No One You Know"
            },
            "SongTitle": {
                "S": "Call Me Today"
            }
```

```
        }
    ],
    "Count": 1,
    "ScannedCount": 2,
    "ConsumedCapacity": {
        "TableName": "MusicCollection",
        "CapacityUnits": 0.5
    }
}
```

Para obtener más información, consulte Uso de consultas en DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 4: Recuperación de un solo recuento de elementos

En el siguiente ejemplo, se recupera un recuento de los elementos que coinciden con la consulta, pero no recupera ninguno de los elementos en sí.

```
aws dynamodb query \
    --table-name MusicCollection \
    --select COUNT \
    --key-condition-expression "Artist = :v1" \
    --expression-attribute-values file://expression-attributes.json
```

Contenido de `expression-attributes.json`:

```
{
    ":v1": {"S": "No One You Know"}
}
```

Salida:

```
{
    "Count": 2,
    "ScannedCount": 2,
    "ConsumedCapacity": null
}
```

Para obtener más información, consulte Uso de consultas en DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 5: consulta de un índice

El siguiente ejemplo consulta el índice secundario global `AlbumTitleIndex`. La consulta devuelve todos los atributos de la tabla base que se han proyectado en el índice secundario local. Tenga en cuenta que, al consultar un índice secundario local o un índice secundario global, también debe proporcionar el nombre de la tabla base mediante el parámetro `table-name`.

```
aws dynamodb query \
    --table-name MusicCollection \
    --index-name AlbumTitleIndex \
    --key-condition-expression "Artist = :v1" \
    --expression-attribute-values file://expression-attributes.json \
    --select ALL_PROJECTED_ATTRIBUTES \
    --return-consumed-capacity INDEXES
```

Contenido de `expression-attributes.json`:

```
{
    ":v1": {"S": "No One You Know"}
}
```

Salida:

```
{
    "Items": [
        {
            "AlbumTitle": {
                "S": "Blue Sky Blues"
            },
            "Artist": {
                "S": "No One You Know"
            },
            "SongTitle": {
                "S": "Scared of My Shadow"
            }
        },
        {
            "AlbumTitle": {
                "S": "Somewhat Famous"
            },
            "Artist": {
```

```
                "S": "No One You Know"
            },
            "SongTitle": {
                "S": "Call Me Today"
            }
        }
    ],
    "Count": 2,
    "ScannedCount": 2,
    "ConsumedCapacity": {
        "TableName": "MusicCollection",
        "CapacityUnits": 0.5,
        "Table": {
            "CapacityUnits": 0.0
        },
        "LocalSecondaryIndexes": {
            "AlbumTitleIndex": {
                "CapacityUnits": 0.5
            }
        }
    }
}
```

Para obtener más información, consulte Uso de consultas en DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte Query en la Referencia de comandos de la AWS CLI.

`restore-table-from-backup`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-table-from-backup`.

AWS CLI

Creación de una tabla de DynamoDB a partir de una copia de seguridad existente

En el siguiente ejemplo de `restore-table-from-backup`, se restaura la tabla especificada a partir de una copia de seguridad existente.

```
aws dynamodb restore-table-from-backup \
    --target-table-name MusicCollection \
```

```
    --backup-arnarn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection/
backup/01576616366715-b4e58d3a
```

Salida:

```
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "Artist",
                "AttributeType": "S"
            },
            {
                "AttributeName": "SongTitle",
                "AttributeType": "S"
            }
        ],
        "TableName": "MusicCollection2",
        "KeySchema": [
            {
                "AttributeName": "Artist",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "SongTitle",
                "KeyType": "RANGE"
            }
        ],
        "TableStatus": "CREATING",
        "CreationDateTime": 1576618274.326,
        "ProvisionedThroughput": {
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 5,
            "WriteCapacityUnits": 5
        },
        "TableSizeBytes": 0,
        "ItemCount": 0,
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection2",
        "TableId": "114865c9-5ef3-496c-b4d1-c4cbdd2d44fb",
        "BillingModeSummary": {
            "BillingMode": "PROVISIONED"
        },
```

```
        "RestoreSummary": {
            "SourceBackupArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/backup/01576616366715-b4e58d3a",
            "SourceTableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection",
            "RestoreDateTime": 1576616366.715,
            "RestoreInProgress": true
        }
    }
}
```

Para obtener más información, consulte On-Demand Backup and Restore for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte RestoreTableFromBackup en la Referencia de comandos de la AWS CLI.

`restore-table-to-point-in-time`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-table-to-point-in-time`.

AWS CLI

Restauración de una tabla de DynamoDB a un momento específico

En el siguiente ejemplo de `restore-table-to-point-in-time`, se restaura la tabla `MusicCollection` al momento especificado.

```
aws dynamodb restore-table-to-point-in-time \
    --source-table-name MusicCollection \
    --target-table-name MusicCollectionRestore \
    --restore-date-time 1576622404.0
```

Salida:

```
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "Artist",
                "AttributeType": "S"
            },
            {
```

```
                "AttributeName": "SongTitle",
                "AttributeType": "S"
            }
        ],
        "TableName": "MusicCollectionRestore",
        "KeySchema": [
            {
                "AttributeName": "Artist",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "SongTitle",
                "KeyType": "RANGE"
            }
        ],
        "TableStatus": "CREATING",
        "CreationDateTime": 1576623311.86,
        "ProvisionedThroughput": {
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 5,
            "WriteCapacityUnits": 5
        },
        "TableSizeBytes": 0,
        "ItemCount": 0,
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollectionRestore",
        "TableId": "befd9e0e-1843-4dc6-a147-d6d00e85cb1f",
        "BillingModeSummary": {
            "BillingMode": "PROVISIONED"
        },
        "RestoreSummary": {
            "SourceTableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection",
            "RestoreDateTime": 1576622404.0,
            "RestoreInProgress": true
        }
    }
}
```

Para obtener más información, consulte Point-in-Time Recovery for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte RestoreTableToPointInTime en la Referencia de comandos de la AWS CLI.

`scan`

En el siguiente ejemplo de código, se muestra cómo utilizar `scan`.

AWS CLI

Análisis de una tabla

En el siguiente ejemplo de `scan` se escanea toda la tabla `MusicCollection` y, a continuación, se reducen los resultados a las canciones del artista “No One You Know”. Para cada elemento, solo se devuelven el título del álbum y el título de la canción.

```
aws dynamodb scan \
    --table-name MusicCollection \
    --filter-expression "Artist = :a" \
    --projection-expression "#ST, #AT" \
    --expression-attribute-names file://expression-attribute-names.json \
    --expression-attribute-values file://expression-attribute-values.json
```

Contenido de `expression-attribute-names.json`:

```
{
    "#ST": "SongTitle",
    "#AT":"AlbumTitle"
}
```

Contenido de `expression-attribute-values.json`:

```
{
    ":a": {"S": "No One You Know"}
}
```

Salida:

```
{
    "Count": 2,
    "Items": [
        {
            "SongTitle": {
                "S": "Call Me Today"
            },
```

```
            "AlbumTitle": {
                "S": "Somewhat Famous"
            }
        },
        {
            "SongTitle": {
                "S": "Scared of My Shadow"
            },
            "AlbumTitle": {
                "S": "Blue Sky Blues"
            }
        }
    ],
    "ScannedCount": 3,
    "ConsumedCapacity": null
}
```

Para obtener más información, consulte Uso de operaciones de análisis en DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte Scan en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Adición de etiquetas a un recurso de DynamoDB

En el siguiente ejemplo de `tag-resource`, se agrega una etiqueta con el par clave-valor a una tabla de `MusicCollection`.

```
aws dynamodb tag-resource \
    --resource-arn arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection \
    --tags Key=Owner,Value=blueTeam
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado para DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`transact-get-items`

En el siguiente ejemplo de código, se muestra cómo utilizar `transact-get-items`.

AWS CLI

Recuperación de varios elementos de manera granular de una o más tablas

En el siguiente ejemplo de `transact-get-items`, se recuperan varios elementos de manera granular.

```
aws dynamodb transact-get-items \
    --transact-items file://transact-items.json \
    --return-consumed-capacity TOTAL
```

Contenido de `transact-items.json`:

```
[
    {
        "Get": {
            "Key": {
                "Artist": {"S": "Acme Band"},
                "SongTitle": {"S": "Happy Day"}
            },
            "TableName": "MusicCollection"
        }
    },
    {
        "Get": {
            "Key": {
                "Artist": {"S": "No One You Know"},
                "SongTitle": {"S": "Call Me Today"}
            },
            "TableName": "MusicCollection"
        }
    }
]
```

Salida:

```
{
    "ConsumedCapacity": [
        {
            "TableName": "MusicCollection",
            "CapacityUnits": 4.0,
            "ReadCapacityUnits": 4.0
        }
    ],
    "Responses": [
        {
            "Item": {
                "AlbumTitle": {
                    "S": "Songs About Life"
                },
                "Artist": {
                    "S": "Acme Band"
                },
                "SongTitle": {
                    "S": "Happy Day"
                }
            }
        },
        {
            "Item": {
                "AlbumTitle": {
                    "S": "Somewhat Famous"
                },
                "Artist": {
                    "S": "No One You Know"
                },
                "SongTitle": {
                    "S": "Call Me Today"
                }
            }
        }
    ]
}
```

Para obtener más información, consulte Administración de flujos de trabajo complejos con transacciones de DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte TransactGetItems en la Referencia de comandos de la AWS CLI.

`transact-write-items`

En el siguiente ejemplo de código, se muestra cómo utilizar `transact-write-items`.

AWS CLI

Ejemplo 1: escritura de elementos de manera granular en una o más tablas

En el siguiente ejemplo de `transact-write-items`, se actualiza un elemento y se elimina otro. La operación da error si alguna de las operaciones falla o si alguno de los elementos contiene un atributo `Rating`.

```
aws dynamodb transact-write-items \
    --transact-items file://transact-items.json \
    --return-consumed-capacity TOTAL \
    --return-item-collection-metrics SIZE
```

Contenido del archivo `transact-items.json`:

```
[
    {
        "Update": {
            "Key": {
                "Artist": {"S": "Acme Band"},
                "SongTitle": {"S": "Happy Day"}
            },
            "UpdateExpression": "SET AlbumTitle = :newval",
            "ExpressionAttributeValues": {
                ":newval": {"S": "Updated Album Title"}
            },
            "TableName": "MusicCollection",
            "ConditionExpression": "attribute_not_exists(Rating)"
        }
    },
    {
        "Delete": {
            "Key": {
                "Artist": {"S": "No One You Know"},
                "SongTitle": {"S": "Call Me Today"}
            },
            "TableName": "MusicCollection",
            "ConditionExpression": "attribute_not_exists(Rating)"
        }
```

```
    }
]
```

Salida:

```
{
    "ConsumedCapacity": [
        {
            "TableName": "MusicCollection",
            "CapacityUnits": 10.0,
            "WriteCapacityUnits": 10.0
        }
    ],
    "ItemCollectionMetrics": {
        "MusicCollection": [
            {
                "ItemCollectionKey": {
                    "Artist": {
                        "S": "No One You Know"
                    }
                },
                "SizeEstimateRangeGB": [
                    0.0,
                    1.0
                ]
            },
            {
                "ItemCollectionKey": {
                    "Artist": {
                        "S": "Acme Band"
                    }
                },
                "SizeEstimateRangeGB": [
                    0.0,
                    1.0
                ]
            }
        ]
    }
}
```

Para obtener más información, consulte Administración de flujos de trabajo complejos con transacciones de DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 2: cómo escribir elementos de manera granular mediante un token de solicitud del cliente

El siguiente comando usa un token de solicitud de cliente para hacer que la llamada a `transact-write-items` sea idempotente, lo que significa que la llamada produce el mismo resultado tanto si se ejecuta una como varias veces.

```
aws dynamodb transact-write-items \
    --transact-items file://transact-items.json \
    --client-request-token abc123
```

Contenido del archivo `transact-items.json`:

```
[
    {
        "Update": {
            "Key": {
                "Artist": {"S": "Acme Band"},
                "SongTitle": {"S": "Happy Day"}
            },
            "UpdateExpression": "SET AlbumTitle = :newval",
            "ExpressionAttributeValues": {
                ":newval": {"S": "Updated Album Title"}
            },
            "TableName": "MusicCollection",
            "ConditionExpression": "attribute_not_exists(Rating)"
        }
    },
    {
        "Delete": {
            "Key": {
                "Artist": {"S": "No One You Know"},
                "SongTitle": {"S": "Call Me Today"}
            },
            "TableName": "MusicCollection",
            "ConditionExpression": "attribute_not_exists(Rating)"
        }
    }
]
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración de flujos de trabajo complejos con transacciones de DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte TransactWriteItems en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de una etiqueta de un recurso de DynamoDB

En el siguiente ejemplo de `untag-resource`, se elimina la etiqueta con la clave `Owner` de la tabla `MusicCollection`.

```
aws dynamodb untag-resource \
    --resource-arn arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection \
    --tag-keys Owner
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado para DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-continuous-backups`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-continuous-backups`.

AWS CLI

Actualización de la configuración de copia de seguridad continua de una tabla de DynamoDB

En el siguiente ejemplo de `update-continuous-backups`, se habilita la recuperación en un momento dado para la tabla `MusicCollection`.

```
aws dynamodb update-continuous-backups \
    --table-name MusicCollection \
```

```
    --point-in-time-recovery-specification PointInTimeRecoveryEnabled=true
```

Salida:

```
{
    "ContinuousBackupsDescription": {
        "ContinuousBackupsStatus": "ENABLED",
        "PointInTimeRecoveryDescription": {
            "PointInTimeRecoveryStatus": "ENABLED",
            "EarliestRestorableDateTime": 1576622404.0,
            "LatestRestorableDateTime": 1576622404.0
        }
    }
}
```

Para obtener más información, consulte Point-in-Time Recovery for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte UpdateContinuousBackups en la Referencia de comandos de la AWS CLI.

`update-contributor-insights`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-contributor-insights`.

AWS CLI

Habilitación de Contributor Insights en una tabla

En el siguiente ejemplo de `update-contributor-insights`, se habilita la configuración de Contributor Insights para la tabla `MusicCollection` y el índice secundario global de `AlbumTitle-index`.

```
aws dynamodb update-contributor-insights \
    --table-name MusicCollection \
    --index-name AlbumTitle-index \
    --contributor-insights-action ENABLE
```

Salida:

```
{
```

```
    "TableName": "MusicCollection",
    "IndexName": "AlbumTitle-index",
    "ContributorInsightsStatus": "ENABLING"
}
```

Para obtener más información, consulte Análisis del acceso a los datos mediante CloudWatch contributor insights for DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte UpdateContributorInsights en la Referencia de comandos de la AWS CLI.

`update-global-table-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-global-table-settings`.

AWS CLI

Actualización de la configuración de la capacidad de escritura aprovisionada en una tabla global de DynamoDB

El siguiente ejemplo de `update-global-table-settings`, se establece la capacidad de escritura aprovisionada de la tabla global `MusicCollection` en 15.

```
aws dynamodb update-global-table-settings \
    --global-table-name MusicCollection \
    --global-table-provisioned-write-capacity-units 15
```

Salida:

```
{
    "GlobalTableName": "MusicCollection",
    "ReplicaSettings": [
        {
            "RegionName": "eu-west-1",
            "ReplicaStatus": "UPDATING",
            "ReplicaProvisionedReadCapacityUnits": 10,
            "ReplicaProvisionedReadCapacityAutoScalingSettings": {
                "AutoScalingDisabled": true
            },
            "ReplicaProvisionedWriteCapacityUnits": 10,
            "ReplicaProvisionedWriteCapacityAutoScalingSettings": {
```

```
                "AutoScalingDisabled": true
            }
        },
        {
            "RegionName": "us-east-1",
            "ReplicaStatus": "UPDATING",
            "ReplicaProvisionedReadCapacityUnits": 10,
            "ReplicaProvisionedReadCapacityAutoScalingSettings": {
                "AutoScalingDisabled": true
            },
            "ReplicaProvisionedWriteCapacityUnits": 10,
            "ReplicaProvisionedWriteCapacityAutoScalingSettings": {
                "AutoScalingDisabled": true
            }
        },
        {
            "RegionName": "us-east-2",
            "ReplicaStatus": "UPDATING",
            "ReplicaProvisionedReadCapacityUnits": 10,
            "ReplicaProvisionedReadCapacityAutoScalingSettings": {
                "AutoScalingDisabled": true
            },
            "ReplicaProvisionedWriteCapacityUnits": 10,
            "ReplicaProvisionedWriteCapacityAutoScalingSettings": {
                "AutoScalingDisabled": true
            }
        }
    ]
}
```

Para obtener más información, consulte Tablas globales de Amazon DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte UpdateGlobalTableSettings en la Referencia de comandos de la AWS CLI.

`update-global-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-global-table`.

AWS CLI

Actualización de una tabla global de DynamoDB

En el siguiente ejemplo de `update-global-table`, se agrega una réplica de la región especificada a la tabla global `MusicCollection`.

```
aws dynamodb update-global-table \
    --global-table-name MusicCollection \
    --replica-updates Create={RegionName=eu-west-1}
```

Salida:

```
{
    "GlobalTableDescription": {
        "ReplicationGroup": [
            {
                "RegionName": "eu-west-1"
            },
            {
                "RegionName": "us-east-2"
            },
            {
                "RegionName": "us-east-1"
            }
        ],
        "GlobalTableArn": "arn:aws:dynamodb::123456789012:global-table/
MusicCollection",
        "CreationDateTime": 1576625818.532,
        "GlobalTableStatus": "ACTIVE",
        "GlobalTableName": "MusicCollection"
    }
}
```

Para obtener más información, consulte Tablas globales de Amazon DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte UpdateGlobalTable en la Referencia de comandos de la AWS CLI.

`update-item`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-item`.

AWS CLI

Ejemplo 1: Actualización de un elemento de una tabla

En el siguiente ejemplo de `update-item`, se actualiza un elemento de la tabla `MusicCollection`. Añade un nuevo atributo (`Year`) y modifica el atributo `AlbumTitle`. En la respuesta se muestran todos los atributos del elemento, tal como aparecen después de la actualización.

```
aws dynamodb update-item \
    --table-name MusicCollection \
    --key file://key.json \
    --update-expression "SET #Y = :y, #AT = :t" \
    --expression-attribute-names file://expression-attribute-names.json \
    --expression-attribute-values file://expression-attribute-values.json  \
    --return-values ALL_NEW \
    --return-consumed-capacity TOTAL \
    --return-item-collection-metrics SIZE
```

Contenido de `key.json`:

```
{
    "Artist": {"S": "Acme Band"},
    "SongTitle": {"S": "Happy Day"}
}
```

Contenido de `expression-attribute-names.json`:

```
{
    "#Y":"Year", "#AT":"AlbumTitle"
}
```

Contenido de `expression-attribute-values.json`:

```
{
    ":y":{"N": "2015"},
    ":t":{"S": "Louder Than Ever"}
}
```

Salida:

```
{
    "Attributes": {
        "AlbumTitle": {
            "S": "Louder Than Ever"
        },
        "Awards": {
            "N": "10"
        },
        "Artist": {
            "S": "Acme Band"
        },
        "Year": {
            "N": "2015"
        },
        "SongTitle": {
            "S": "Happy Day"
        }
    },
    "ConsumedCapacity": {
        "TableName": "MusicCollection",
        "CapacityUnits": 3.0
    },
    "ItemCollectionMetrics": {
        "ItemCollectionKey": {
            "Artist": {
                "S": "Acme Band"
            }
        },
        "SizeEstimateRangeGB": [
            0.0,
            1.0
        ]
    }
}
```

Para obtener más información, consulte Escritura de un elemento en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 2: actualización de un elemento de forma condicional

En el siguiente ejemplo se actualiza un elemento de la tabla `MusicCollection`, pero solo si el elemento existente aún no tiene un atributo `Year`.

```
aws dynamodb update-item \
    --table-name MusicCollection \
    --key file://key.json \
    --update-expression "SET #Y = :y, #AT = :t" \
    --expression-attribute-names file://expression-attribute-names.json \
    --expression-attribute-values file://expression-attribute-values.json  \
    --condition-expression "attribute_not_exists(#Y)"
```

Contenido de `key.json`:

```
{
    "Artist": {"S": "Acme Band"},
    "SongTitle": {"S": "Happy Day"}
}
```

Contenido de `expression-attribute-names.json`:

```
{
    "#Y":"Year",
    "#AT":"AlbumTitle"
}
```

Contenido de `expression-attribute-values.json`:

```
{
    ":y":{"N": "2015"},
    ":t":{"S": "Louder Than Ever"}
}
```

Si el elemento ya tiene un atributo `Year`, DynamoDB devuelve el siguiente resultado.

```
An error occurred (ConditionalCheckFailedException) when calling the UpdateItem
 operation: The conditional request failed
```

Para obtener más información, consulte Escritura de un elemento en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte UpdateItem en la Referencia de comandos de la AWS CLI.

update-table-replica-auto-scaling

En el siguiente ejemplo de código, se muestra cómo utilizar `update-table-replica-auto-scaling`.

AWS CLI

Actualización de la configuración de escalado automático en las réplicas de una tabla global

En el siguiente ejemplo de `update-table-replica-auto-scaling`, se actualiza la configuración de escalado automático de la capacidad en todas las réplicas de la tabla global especificada.

```
aws dynamodb update-table-replica-auto-scaling \
    --table-name MusicCollection \
    --provisioned-write-capacity-auto-scaling-update file://auto-scaling-policy.json
```

Contenido de `auto-scaling-policy.json`:

```
{
    "MinimumUnits": 10,
    "MaximumUnits": 100,
    "AutoScalingDisabled": false,
    "ScalingPolicyUpdate": {
        "PolicyName": "DynamoDBWriteCapacityUtilization:table/MusicCollection",
        "TargetTrackingScalingPolicyConfiguration": {
            "TargetValue": 80
        }
    }
}
```

Salida:

```
{
    "TableAutoScalingDescription": {
        "TableName": "MusicCollection",
        "TableStatus": "ACTIVE",
        "Replicas": [
            {
                "RegionName": "eu-central-1",
                "GlobalSecondaryIndexes": [],
                "ReplicaProvisionedReadCapacityAutoScalingSettings": {
```

```
                    "MinimumUnits": 5,
                    "MaximumUnits": 40000,
                    "AutoScalingRoleArn": "arn:aws:iam::123456789012:role/
aws-service-role/dynamodb.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable",
                    "ScalingPolicies": [
                        {
                            "PolicyName": "DynamoDBReadCapacityUtilization:table/
MusicCollection",
                            "TargetTrackingScalingPolicyConfiguration": {
                                "TargetValue": 70.0
                            }
                        }
                    ]
                },
                "ReplicaProvisionedWriteCapacityAutoScalingSettings": {
                    "MinimumUnits": 10,
                    "MaximumUnits": 100,
                    "AutoScalingRoleArn": "arn:aws:iam::123456789012:role/
aws-service-role/dynamodb.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable",
                    "ScalingPolicies": [
                        {
                            "PolicyName": "DynamoDBWriteCapacityUtilization:table/
MusicCollection",
                            "TargetTrackingScalingPolicyConfiguration": {
                                "TargetValue": 80.0
                            }
                        }
                    ]
                },
                "ReplicaStatus": "ACTIVE"
            },
            {
                "RegionName": "us-east-1",
                "GlobalSecondaryIndexes": [],
                "ReplicaProvisionedReadCapacityAutoScalingSettings": {
                    "MinimumUnits": 5,
                    "MaximumUnits": 40000,
                    "AutoScalingRoleArn": "arn:aws:iam::123456789012:role/
aws-service-role/dynamodb.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable",
                    "ScalingPolicies": [
                        {
```

```
                            "PolicyName": "DynamoDBReadCapacityUtilization:table/
MusicCollection",
                            "TargetTrackingScalingPolicyConfiguration": {
                                "TargetValue": 70.0
                            }
                        }
                    ]
                },
                "ReplicaProvisionedWriteCapacityAutoScalingSettings": {
                    "MinimumUnits": 10,
                    "MaximumUnits": 100,
                    "AutoScalingRoleArn": "arn:aws:iam::123456789012:role/
aws-service-role/dynamodb.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable",
                    "ScalingPolicies": [
                        {
                            "PolicyName": "DynamoDBWriteCapacityUtilization:table/
MusicCollection",
                            "TargetTrackingScalingPolicyConfiguration": {
                                "TargetValue": 80.0
                            }
                        }
                    ]
                },
                "ReplicaStatus": "ACTIVE"
            },
            {
                "RegionName": "us-east-2",
                "GlobalSecondaryIndexes": [],
                "ReplicaProvisionedReadCapacityAutoScalingSettings": {
                    "MinimumUnits": 5,
                    "MaximumUnits": 40000,
                    "AutoScalingRoleArn": "arn:aws:iam::123456789012:role/
aws-service-role/dynamodb.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable",
                    "ScalingPolicies": [
                        {
                            "PolicyName": "DynamoDBReadCapacityUtilization:table/
MusicCollection",
                            "TargetTrackingScalingPolicyConfiguration": {
                                "TargetValue": 70.0
                            }
                        }
                    ]
```

```
                },
                "ReplicaProvisionedWriteCapacityAutoScalingSettings": {
                    "MinimumUnits": 10,
                    "MaximumUnits": 100,
                    "AutoScalingRoleArn": "arn:aws:iam::123456789012:role/
aws-service-role/dynamodb.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable",
                    "ScalingPolicies": [
                        {
                            "PolicyName": "DynamoDBWriteCapacityUtilization:table/
MusicCollection",
                            "TargetTrackingScalingPolicyConfiguration": {
                                "TargetValue": 80.0
                            }
                        }
                    ]
                },
                "ReplicaStatus": "ACTIVE"
            }
        ]
    }
}
```

Para obtener más información, consulte Tablas globales de Amazon DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte UpdateTableReplicaAutoScaling en la Referencia de comandos de la AWS CLI.

`update-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-table`.

AWS CLI

Ejemplo 1: modificar el modo de facturación de una tabla

El siguiente ejemplo de `update-table` aumenta la capacidad de lectura y escritura aprovisionada en la tabla `MusicCollection`.

```
aws dynamodb update-table \
    --table-name MusicCollection \
    --billing-mode PROVISIONED \
```

```
    --provisioned-throughput ReadCapacityUnits=15,WriteCapacityUnits=10
```

Salida:

```
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "AlbumTitle",
                "AttributeType": "S"
            },
            {
                "AttributeName": "Artist",
                "AttributeType": "S"
            },
            {
                "AttributeName": "SongTitle",
                "AttributeType": "S"
            }
        ],
        "TableName": "MusicCollection",
        "KeySchema": [
            {
                "AttributeName": "Artist",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "SongTitle",
                "KeyType": "RANGE"
            }
        ],
        "TableStatus": "UPDATING",
        "CreationDateTime": "2020-05-26T15:59:49.473000-07:00",
        "ProvisionedThroughput": {
            "LastIncreaseDateTime": "2020-07-28T13:18:18.921000-07:00",
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 15,
            "WriteCapacityUnits": 10
        },
        "TableSizeBytes": 182,
        "ItemCount": 2,
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection",
        "TableId": "abcd0123-01ab-23cd-0123-abcdef123456",
```

```
        "BillingModeSummary": {
            "BillingMode": "PROVISIONED",
            "LastUpdateToPayPerRequestDateTime": "2020-07-28T13:14:48.366000-07:00"
        }
    }
}
```

Para obtener más información, consulte Actualización de una tabla en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 5: crear un índice secundario global

En el siguiente ejemplo se añade un índice secundario global a la tabla `MusicCollection`.

```
aws dynamodb update-table \
    --table-name MusicCollection \
    --attribute-definitions AttributeName=AlbumTitle,AttributeType=S \
    --global-secondary-index-updates file://gsi-updates.json
```

Contenido de `gsi-updates.json`:

```
[
    {
        "Create": {
            "IndexName": "AlbumTitle-index",
            "KeySchema": [
                {
                    "AttributeName": "AlbumTitle",
                    "KeyType": "HASH"
                }
            ],
            "ProvisionedThroughput": {
                "ReadCapacityUnits": 10,
                "WriteCapacityUnits": 10
            },
            "Projection": {
                "ProjectionType": "ALL"
            }
        }
    }
]
```

Salida:

```
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "AlbumTitle",
                "AttributeType": "S"
            },
            {
                "AttributeName": "Artist",
                "AttributeType": "S"
            },
            {
                "AttributeName": "SongTitle",
                "AttributeType": "S"
            }
        ],
        "TableName": "MusicCollection",
        "KeySchema": [
            {
                "AttributeName": "Artist",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "SongTitle",
                "KeyType": "RANGE"
            }
        ],
        "TableStatus": "UPDATING",
        "CreationDateTime": "2020-05-26T15:59:49.473000-07:00",
        "ProvisionedThroughput": {
            "LastIncreaseDateTime": "2020-07-28T12:59:17.537000-07:00",
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 15,
            "WriteCapacityUnits": 10
        },
        "TableSizeBytes": 182,
        "ItemCount": 2,
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection",
        "TableId": "abcd0123-01ab-23cd-0123-abcdef123456",
        "BillingModeSummary": {
            "BillingMode": "PROVISIONED",
            "LastUpdateToPayPerRequestDateTime": "2020-07-28T13:14:48.366000-07:00"
        },
```

```
        "GlobalSecondaryIndexes": [
            {
                "IndexName": "AlbumTitle-index",
                "KeySchema": [
                    {
                        "AttributeName": "AlbumTitle",
                        "KeyType": "HASH"
                    }
                ],
                "Projection": {
                    "ProjectionType": "ALL"
                },
                "IndexStatus": "CREATING",
                "Backfilling": false,
                "ProvisionedThroughput": {
                    "NumberOfDecreasesToday": 0,
                    "ReadCapacityUnits": 10,
                    "WriteCapacityUnits": 10
                },
                "IndexSizeBytes": 0,
                "ItemCount": 0,
                "IndexArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/index/AlbumTitle-index"
            }
        ]
    }
}
```

Para obtener más información, consulte Actualización de una tabla en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 3: activar DynamoDB Streams en una tabla

El siguiente comando activa DynamoDB Streams en la tabla `MusicCollection`.

```
aws dynamodb update-table \
    --table-name MusicCollection \
    --stream-specification StreamEnabled=true,StreamViewType=NEW_IMAGE
```

Salida:

```
{
    "TableDescription": {
```

```
        "AttributeDefinitions": [
            {
                "AttributeName": "AlbumTitle",
                "AttributeType": "S"
            },
            {
                "AttributeName": "Artist",
                "AttributeType": "S"
            },
            {
                "AttributeName": "SongTitle",
                "AttributeType": "S"
            }
        ],
        "TableName": "MusicCollection",
        "KeySchema": [
            {
                "AttributeName": "Artist",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "SongTitle",
                "KeyType": "RANGE"
            }
        ],
        "TableStatus": "UPDATING",
        "CreationDateTime": "2020-05-26T15:59:49.473000-07:00",
        "ProvisionedThroughput": {
            "LastIncreaseDateTime": "2020-07-28T12:59:17.537000-07:00",
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 15,
            "WriteCapacityUnits": 10
        },
        "TableSizeBytes": 182,
        "ItemCount": 2,
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection",
        "TableId": "abcd0123-01ab-23cd-0123-abcdef123456",
        "BillingModeSummary": {
            "BillingMode": "PROVISIONED",
            "LastUpdateToPayPerRequestDateTime": "2020-07-28T13:14:48.366000-07:00"
        },
        "LocalSecondaryIndexes": [
            {
                "IndexName": "AlbumTitleIndex",
```

```
                "KeySchema": [
                    {
                        "AttributeName": "Artist",
                        "KeyType": "HASH"
                    },
                    {
                        "AttributeName": "AlbumTitle",
                        "KeyType": "RANGE"
                    }
                ],
                "Projection": {
                    "ProjectionType": "INCLUDE",
                    "NonKeyAttributes": [
                        "Year",
                        "Genre"
                    ]
                },
                "IndexSizeBytes": 139,
                "ItemCount": 2,
                "IndexArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/index/AlbumTitleIndex"
            }
        ],
        "GlobalSecondaryIndexes": [
            {
                "IndexName": "AlbumTitle-index",
                "KeySchema": [
                    {
                        "AttributeName": "AlbumTitle",
                        "KeyType": "HASH"
                    }
                ],
                "Projection": {
                    "ProjectionType": "ALL"
                },
                "IndexStatus": "ACTIVE",
                "ProvisionedThroughput": {
                    "NumberOfDecreasesToday": 0,
                    "ReadCapacityUnits": 10,
                    "WriteCapacityUnits": 10
                },
                "IndexSizeBytes": 0,
                "ItemCount": 0,
```

```
                "IndexArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/index/AlbumTitle-index"
            }
        ],
        "StreamSpecification": {
            "StreamEnabled": true,
            "StreamViewType": "NEW_IMAGE"
        },
        "LatestStreamLabel": "2020-07-28T21:53:39.112",
        "LatestStreamArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/stream/2020-07-28T21:53:39.112"
    }
}
```

Para obtener más información, consulte Actualización de una tabla en la Guía para desarrolladores de Amazon DynamoDB.

Ejemplo 4: activar el cifrado en el lado del servidor

El siguiente ejemplo activa el cifrado del lado del servidor en la tabla `MusicCollection`.

```
aws dynamodb update-table \
    --table-name MusicCollection \
    --sse-specification Enabled=true,SSEType=KMS
```

Salida:

```
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "AlbumTitle",
                "AttributeType": "S"
            },
            {
                "AttributeName": "Artist",
                "AttributeType": "S"
            },
            {
                "AttributeName": "SongTitle",
                "AttributeType": "S"
            }
        ],
```

```
        "TableName": "MusicCollection",
        "KeySchema": [
            {
                "AttributeName": "Artist",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "SongTitle",
                "KeyType": "RANGE"
            }
        ],
        "TableStatus": "ACTIVE",
        "CreationDateTime": "2020-05-26T15:59:49.473000-07:00",
        "ProvisionedThroughput": {
            "LastIncreaseDateTime": "2020-07-28T12:59:17.537000-07:00",
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 15,
            "WriteCapacityUnits": 10
        },
        "TableSizeBytes": 182,
        "ItemCount": 2,
        "TableArn": "arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection",
        "TableId": "abcd0123-01ab-23cd-0123-abcdef123456",
        "BillingModeSummary": {
            "BillingMode": "PROVISIONED",
            "LastUpdateToPayPerRequestDateTime": "2020-07-28T13:14:48.366000-07:00"
        },
        "LocalSecondaryIndexes": [
            {
                "IndexName": "AlbumTitleIndex",
                "KeySchema": [
                    {
                        "AttributeName": "Artist",
                        "KeyType": "HASH"
                    },
                    {
                        "AttributeName": "AlbumTitle",
                        "KeyType": "RANGE"
                    }
                ],
                "Projection": {
                    "ProjectionType": "INCLUDE",
                    "NonKeyAttributes": [
                        "Year",
```

```
                        "Genre"
                    ]
                },
                "IndexSizeBytes": 139,
                "ItemCount": 2,
                "IndexArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/index/AlbumTitleIndex"
            }
        ],
        "GlobalSecondaryIndexes": [
            {
                "IndexName": "AlbumTitle-index",
                "KeySchema": [
                    {
                        "AttributeName": "AlbumTitle",
                        "KeyType": "HASH"
                    }
                ],
                "Projection": {
                    "ProjectionType": "ALL"
                },
                "IndexStatus": "ACTIVE",
                "ProvisionedThroughput": {
                    "NumberOfDecreasesToday": 0,
                    "ReadCapacityUnits": 10,
                    "WriteCapacityUnits": 10
                },
                "IndexSizeBytes": 0,
                "ItemCount": 0,
                "IndexArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/index/AlbumTitle-index"
            }
        ],
        "StreamSpecification": {
            "StreamEnabled": true,
            "StreamViewType": "NEW_IMAGE"
        },
        "LatestStreamLabel": "2020-07-28T21:53:39.112",
        "LatestStreamArn": "arn:aws:dynamodb:us-west-2:123456789012:table/
MusicCollection/stream/2020-07-28T21:53:39.112",
        "SSEDescription": {
            "Status": "UPDATING"
        }
    }
```

```
}
```

Para obtener más información, consulte Actualización de una tabla en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte UpdateTable en la AWS CLI Command Reference.

`update-time-to-live`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-time-to-live`.

AWS CLI

Actualización de la configuración de tiempo de vida en una tabla

El siguiente ejemplo de `update-time-to-live` activa Tiempo de vida en la tabla especificada.

```
aws dynamodb update-time-to-live \
    --table-name MusicCollection \
    --time-to-live-specification Enabled=true,AttributeName=ttl
```

Salida:

```
{
    "TimeToLiveSpecification": {
        "Enabled": true,
        "AttributeName": "ttl"
    }
}
```

Para obtener más información, consulte Tiempo de vida en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte UpdateTimeToLive en la Referencia de comandos de la AWS CLI.

Ejemplos de DynamoDB que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con DynamoDB Streams.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`describe-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stream`.

AWS CLI

Obtención de información sobre un flujo de DynamoDB

El siguiente comando de `describe-stream` muestra información sobre el flujo de DynamoDB específico.

```
aws dynamodbstreams describe-stream \
    --stream-arn arn:aws:dynamodb:us-west-1:123456789012:table/Music/
stream/2019-10-22T18:02:01.576
```

Salida:

```
{
    "StreamDescription": {
        "StreamArn": "arn:aws:dynamodb:us-west-1:123456789012:table/Music/
stream/2019-10-22T18:02:01.576",
        "StreamLabel": "2019-10-22T18:02:01.576",
        "StreamStatus": "ENABLED",
        "StreamViewType": "NEW_AND_OLD_IMAGES",
        "CreationRequestDateTime": 1571767321.571,
        "TableName": "Music",
        "KeySchema": [
            {
```

```
                "AttributeName": "Artist",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "SongTitle",
                "KeyType": "RANGE"
            }
        ],
        "Shards": [
            {
                "ShardId": "shardId-00000001571767321804-697ce3d2",
                "SequenceNumberRange": {
                    "StartingSequenceNumber": "400000000000642977831",
                    "EndingSequenceNumber": "400000000000642977831"
                }
            },
            {
                "ShardId": "shardId-00000001571780995058-40810d86",
                "SequenceNumberRange": {
                    "StartingSequenceNumber": "757400000000005655171150"
                },
                "ParentShardId": "shardId-00000001571767321804-697ce3d2"
            }
        ]
    }
}
```

Para obtener más información, consulte Capturing Table Activity with DynamoDB Streams en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte DescribeStream en la Referencia de comandos de la AWS CLI.

`get-records`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-records`.

AWS CLI

Obtención de registros de un flujo de Dynamodb

El siguiente `get-records` comando recupera los registros mediante el iterador de fragmentos de Amazon DynamoDB especificado.

```
aws dynamodbstreams get-records \
    --shard-iterator "arn:aws:dynamodb:us-west-1:123456789012:table/Music/
stream/2019-10-22T18:02:01.576|1|
AAAAAAAAAAGgM3YZ89vLZZxjmoQeo33r9M4x3+zmmTLsiL86MfrF4+B4EbsByi52InVmiONmy6xVW4IRcIIbs1zO7MNI
+CjNPlqQjnyRSAnfOwWmKhL1/KNParWSfz2odf780oOObIDIWRRMkt7+Hyzh9SD
+hFxFAWR5C7QIlOXPc8mRBfNIazfrVCjJK8/jsjCzsqNyXKzJbhh+GXCoxYN
+Kpmg4nyj1EAsYhbGL35muvHFoHjcyuynbsczbWaXNfThDwRAyvoTmc8XhHKtAWUbJiaVd8ZPtQwDsThCrmDRPIdmTRG
+w/lEGS05ha1qNP+Vl4+tuhz2TRnhnJo/pny9GI/yGpce97mWvSPr5KPwy+Dtcm5BHayBs
+PVYHITaTliInFlT
+LCwvaz1QH3MY3b8A05Z800wjpktm60iQqtMeDwN4NX6FrcxR34JoFKGsgR8XkHVJzz2xr1xqSJ12ycpNTyHnndusw==
```

Salida:

```
{
    "Records": [
        {
            "eventID": "c3b5d798eef6215d42f8137b19a88e50",
            "eventName": "INSERT",
            "eventVersion": "1.1",
            "eventSource": "aws:dynamodb",
            "awsRegion": "us-west-1",
            "dynamodb": {
                "ApproximateCreationDateTime": 1571849028.0,
                "Keys": {
                    "Artist": {
                        "S": "No One You Know"
                    },
                    "SongTitle": {
                        "S": "Call Me Today"
                    }
                },
                "NewImage": {
                    "AlbumTitle": {
                        "S": "Somewhat Famous"
                    },
                    "Artist": {
                        "S": "No One You Know"
                    },
                    "Awards": {
                        "N": "1"
                    },
                    "SongTitle": {
                        "S": "Call Me Today"
```

```
                }
            },
            "SequenceNumber": "700000000013256296913",
            "SizeBytes": 119,
            "StreamViewType": "NEW_AND_OLD_IMAGES"
        }
    },
    {
        "eventID": "878960a6967867e2da16b27380a27328",
        "eventName": "INSERT",
        "eventVersion": "1.1",
        "eventSource": "aws:dynamodb",
        "awsRegion": "us-west-1",
        "dynamodb": {
            "ApproximateCreationDateTime": 1571849029.0,
            "Keys": {
                "Artist": {
                    "S": "Acme Band"
                },
                "SongTitle": {
                    "S": "Happy Day"
                }
            },
            "NewImage": {
                "AlbumTitle": {
                    "S": "Songs About Life"
                },
                "Artist": {
                    "S": "Acme Band"
                },
                "Awards": {
                    "N": "10"
                },
                "SongTitle": {
                    "S": "Happy Day"
                }
            },
            "SequenceNumber": "800000000013256297217",
            "SizeBytes": 100,
            "StreamViewType": "NEW_AND_OLD_IMAGES"
        }
    },
    {
        "eventID": "520fabde080e159fc3710b15ee1d4daa",
```

```
            "eventName": "MODIFY",
            "eventVersion": "1.1",
            "eventSource": "aws:dynamodb",
            "awsRegion": "us-west-1",
            "dynamodb": {
                "ApproximateCreationDateTime": 1571849734.0,
                "Keys": {
                    "Artist": {
                        "S": "Acme Band"
                    },
                    "SongTitle": {
                        "S": "Happy Day"
                    }
                },
                "NewImage": {
                    "AlbumTitle": {
                        "S": "Updated Album Title"
                    },
                    "Artist": {
                        "S": "Acme Band"
                    },
                    "Awards": {
                        "N": "10"
                    },
                    "SongTitle": {
                        "S": "Happy Day"
                    }
                },
                "OldImage": {
                    "AlbumTitle": {
                        "S": "Songs About Life"
                    },
                    "Artist": {
                        "S": "Acme Band"
                    },
                    "Awards": {
                        "N": "10"
                    },
                    "SongTitle": {
                        "S": "Happy Day"
                    }
                },
                "SequenceNumber": "900000000013256687845",
                "SizeBytes": 170,
```

```
                "StreamViewType": "NEW_AND_OLD_IMAGES"
            }
        }
    ],
    "NextShardIterator": "arn:aws:dynamodb:us-west-1:123456789012:table/
Music/stream/2019-10-23T16:41:08.740|1|AAAAAAAAAAEhEI04jkFLW
+LKOwivjT8d/IHEh3iExV2xK00aTxEzVy1C1C7Kbb5+ZOW6bT9VQ2n1/
mrs7+PRiaOZCHJu7JHJVW7zlsqOi/ges3fw8GYEymyL+piEk35cx67rQqwKKyq
+Q6w9JyjreIOj4F2lWLV26lBwRTrIYC4IB7C3BZZK4715QwYdDxNdVHiSBRZX8UqoS6WOt0F87xZLNB9F/
NhYBLXi/wcGvAcBcC0TNIOH+N0NqwtoB/
FGCkNrf8YZ0xRoNN6RgGuVWHF3pxOhxEJeFZoSoJTIKeG9YcYxzi5Ci/
mhdtm7tBXnbw5c6xmsGsBqTirNjlDyJLcWl8Cl0UOLX63Ufo/5QliztcjEbKsQe28x8LM8o7VH1Is0fF/
ITt8awSA4igyJS0P87GN8Qri8kj8iaE35805jBHWF2wvwT6Iy2xGrR2r2HzYps9dwGOarVdEITaJfWzNoL4HajMhmREZ
+V04i1YIeHMXJfcwetNRuIbdQXfJht2NQZa4PVV6iknY6d19MrdbSTMKoqAuvp6g3Q2jH4t7GKCLWgodcPAn8g5+43Da
}
```

Para obtener más información, consulte Capturing Table Activity with DynamoDB Streams en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte GetRecords en la Referencia de comandos de la AWS CLI.

`get-shard-iterator`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-shard-iterator`.

AWS CLI

Obtención de un iterador de fragmentos

El siguiente comando de `get-shard-iterator` recupera un iterador de fragmentos para el fragmento especificado.

```
aws dynamodbstreams get-shard-iterator \
    --stream-arn arn:aws:dynamodb:us-west-1:12356789012:table/Music/
stream/2019-10-22T18:02:01.576 \
    --shard-id shardId-00000001571780995058-40810d86 \
    --shard-iterator-type LATEST
```

Salida:

```
{
```

```
    "ShardIterator": "arn:aws:dynamodb:us-west-1:123456789012:table/Music/
stream/2019-10-22T18:02:01.576|1|
AAAAAAAAAAGgM3YZ89vLZZxjmoQeo33r9M4x3+zmmTLsiL86MfrF4+B4EbsByi52InVmiONmy6xVW4IRcIIbs1zO7MNI
+CjNPlqQjnyRSAnfOwWmKhL1/KNParWSfz2odf780oOObIDIWRRMkt7+Hyzh9SD
+hFxFAWR5C7QIlOXPc8mRBfNIazfrVCjJK8/jsjCzsqNyXKzJbhh+GXCoxYN
+Kpmg4nyj1EAsYhbGL35muvHFoHjcyuynbsczbWaXNfThDwRAyvoTmc8XhHKtAWUbJiaVd8ZPtQwDsThCrmDRPIdmTRG
+w/lEGS05ha1qNP+Vl4+tuhz2TRnhnJo/pny9GI/yGpce97mWvSPr5KPwy+Dtcm5BHayBs
+PVYHITaTliInFlT
+LCwvaz1QH3MY3b8A05Z800wjpktm60iQqtMeDwN4NX6FrcxR34JoFKGsgR8XkHVJzz2xr1xqSJ12ycpNTyHnndusw==
}
```

Para obtener más información, consulte Capturing Table Activity with DynamoDB Streams en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener detalles sobre la API, consulte GetShardIterator en la Referencia de comandos de la AWS CLI.

`list-streams`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-streams`.

AWS CLI

Para enumerar flujos de DynamoDB

El siguiente comando de `list-streams` muestra todas los flujos de Amazon DynamoDB existentes en la región de AWS predeterminada.

```
aws dynamodbstreams list-streams
```

Salida:

```
{
    "Streams": [
        {
            "StreamArn": "arn:aws:dynamodb:us-west-1:123456789012:table/Music/
stream/2019-10-22T18:02:01.576",
            "TableName": "Music",
            "StreamLabel": "2019-10-22T18:02:01.576"
        }
    ]
```

```
}
```

Para obtener más información, consulte Capturing Table Activity with DynamoDB Streams en la Guía para desarrolladores de Amazon DynamoDB.

- Para obtener información sobre la API, consulte ListStreams en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon EC2 que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon EC2.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`accept-address-transfer`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-address-transfer`.

AWS CLI

Para aceptar una dirección IP elástica transferida a su cuenta

En el siguiente ejemplo de `accept-address-transfer` se acepta la transferencia de la dirección IP elástica especificada a su cuenta.

```
aws ec2 accept-address-transfer \
    --address 100.21.184.216
```

Salida:

```
{
    "AddressTransfer": {
        "PublicIp": "100.21.184.216",
        "AllocationId": "eipalloc-09ad461b0d03f6aaf",
        "TransferAccountId": "123456789012",
        "TransferOfferExpirationTimestamp": "2023-02-22T20:51:10.000Z",
        "TransferOfferAcceptedTimestamp": "2023-02-22T22:52:54.000Z",
        "AddressTransferStatus": "accepted"
    }
}
```

Para obtener más información, consulte Transfer Elastic IP addresses en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte AcceptAddressTransfer en la Referencia de comandos de la AWS CLI.

`accept-reserved-instances-exchange-quote`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-reserved-instances-exchange-quote`.

AWS CLI

Para realizar un intercambio de instancias reservadas convertibles

En este ejemplo se realiza un intercambio de las instancias reservadas convertibles especificadas.

Comando:

```
aws ec2 accept-reserved-instances-exchange-quote --reserved-
instance-ids 7b8750c3-397e-4da4-bbcb-a45ebexample --target-
configurations OfferingId=b747b472-423c-48f3-8cee-679bcexample
```

Salida:

```
{
```

```
  "ExchangeId": "riex-e68ed3c1-8bc8-4c17-af77-811afexample"
}
```

- Para obtener información sobre la API, consulte AcceptReservedInstancesExchangeQuote en la Referencia de comandos de la AWS CLI.

`accept-transit-gateway-peering-attachment`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-transit-gateway-peering-attachment`.

AWS CLI

Para aceptar conexión de emparejamiento de puerta de enlace de tránsito

En el siguiente ejemplo de `accept-transit-gateway-peering-attachment`, se acepta la conexión de emparejamiento de puerta de enlace de tránsito especificada. El parámetro `--region` especifica la región en la que se encuentra la puerta de enlace de tránsito aceptadora.

```
aws ec2 accept-transit-gateway-peering-attachment \
    --transit-gateway-attachment-id tgw-attach-4455667788aabbccd \
    --region us-east-2
```

Salida:

```
{
    "TransitGatewayPeeringAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-4455667788aabbccd",
        "RequesterTgwInfo": {
            "TransitGatewayId": "tgw-123abc05e04123abc",
            "OwnerId": "123456789012",
            "Region": "us-west-2"
        },
        "AccepterTgwInfo": {
            "TransitGatewayId": "tgw-11223344aabbcc112",
            "OwnerId": "123456789012",
            "Region": "us-east-2"
        },
        "State": "pending",
        "CreationTime": "2019-12-09T11:38:31.000Z"
    }
```

```
}
```

Para obtener más información, consulte Transit Gateway Peering Attachments en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte AcceptTransitGatewayPeeringAttachment en la Referencia de comandos de la AWS CLI.

`accept-transit-gateway-vpc-attachment`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-transit-gateway-vpc-attachment`.

AWS CLI

Para aceptar una solicitud de conexión de una VPC a una puerta de enlace de tránsito

En el siguiente ejemplo de `accept-transit-gateway-vpc-attachment`, se acepta la solicitud de la conexión especificada.

```
aws ec2 accept-transit-gateway-vpc-attachment \
    --transit-gateway-attachment-id tgw-attach-0a34fe6b4fEXAMPLE
```

Salida:

```
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-0a34fe6b4fEXAMPLE",
        "TransitGatewayId": "tgw-0262a0e521EXAMPLE",
        "VpcId": "vpc-07e8ffd50fEXAMPLE",
        "VpcOwnerId": "123456789012",
        "State": "pending",
        "SubnetIds": [
            "subnet-0752213d59EXAMPLE"
        ],
        "CreationTime": "2019-07-10T17:33:46.000Z",
        "Options": {
            "DnsSupport": "enable",
            "Ipv6Support": "disable"
        }
    }
}
```

Para obtener más información, consulte Transit Gateway Attachments to a VPC en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte AcceptTransitGatewayVpcAttachment en la Referencia de comandos de la AWS CLI.

`accept-vpc-endpoint-connections`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-vpc-endpoint-connections`.

AWS CLI

Para aceptar una solicitud de conexión de punto de conexión de interfaz

En este ejemplo se acepta la solicitud de conexión de punto de conexión especificada para el servicio de punto de conexión especificado.

Comando:

```
aws ec2 accept-vpc-endpoint-connections --service-id vpce-svc-03d5ebb7d9579a2b3 --vpc-endpoint-ids vpce-0c1308d7312217abc
```

Salida:

```
{
  "Unsuccessful": []
}
```

- Para obtener información sobre la API, consulte AcceptVpcEndpointConnections en la Referencia de comandos de la AWS CLI.

`accept-vpc-peering-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-vpc-peering-connection`.

AWS CLI

Para aceptar una conexión de emparejamiento de VPC

En este ejemplo, se acepta la solicitud de conexión de emparejamiento de VPC especificada.

Comando:

```
aws ec2 accept-vpc-peering-connection --vpc-peering-connection-id pcx-1a2b3c4d
```

Salida:

```
{
  "VpcPeeringConnection": {
    "Status": {
      "Message": "Provisioning",
      "Code": "provisioning"
    },
    "Tags": [],
    "AccepterVpcInfo": {
      "OwnerId": "444455556666",
      "VpcId": "vpc-44455566",
      "CidrBlock": "10.0.1.0/28"
    },
    "VpcPeeringConnectionId": "pcx-1a2b3c4d",
    "RequesterVpcInfo": {
      "OwnerId": "444455556666",
      "VpcId": "vpc-111abc45",
      "CidrBlock": "10.0.0.0/28"
    }
  }
}
```

- Para obtener información sobre la API, consulte AcceptVpcPeeringConnection en la Referencia de comandos de la AWS CLI.

`advertise-byoip-cidr`

En el siguiente ejemplo de código, se muestra cómo utilizar `advertise-byoip-cidr`.

AWS CLI

Para anunciar un rango de direcciones

En el siguiente ejemplo de `advertise-byoip-cidr` se anuncia el rango de direcciones IPv4 públicas especificado.

```
aws ec2 advertise-byoip-cidr \
```

```
    --cidr 203.0.113.25/24
```

Salida:

```
{
    "ByoipCidr": {
        "Cidr": "203.0.113.25/24",
        "StatusMessage": "ipv4pool-ec2-1234567890abcdef0",
        "State": "provisioned"
    }
}
```

- Para obtener información sobre la API, consulte AdvertiseByoipCidr en la Referencia de comandos de la AWS CLI.

`allocate-address`

En el siguiente ejemplo de código, se muestra cómo utilizar `allocate-address`.

AWS CLI

Ejemplo 1: Asignar una dirección IP elástica del grupo de direcciones de Amazon

En el siguiente ejemplo de `allocate-address`, se asigna una dirección IP elástica. Amazon EC2 selecciona la dirección del conjunto de direcciones de Amazon.

```
aws ec2 allocate-address
```

Salida:

```
{
    "PublicIp": "70.224.234.241",
    "AllocationId": "eipalloc-01435ba59eEXAMPLE",
    "PublicIpv4Pool": "amazon",
    "NetworkBorderGroup": "us-west-2",
    "Domain": "vpc"
}
```

Para obtener más información, consulte Direcciones IP elásticas en la Guía del usuario de Amazon EC2.

Ejemplo 2: Asignar una dirección IP elástica y asociarla a un grupo fronterizo de red

En el siguiente ejemplo de `allocate-address`, se asigna una dirección IP elástica y se la asocia al grupo fronterizo de red especificado.

```
aws ec2 allocate-address \
    --network-border-group us-west-2-lax-1
```

Salida:

```
{
    "PublicIp": "70.224.234.241",
    "AllocationId": "eipalloc-e03dd489ceEXAMPLE",
    "PublicIpv4Pool": "amazon",
    "NetworkBorderGroup": "us-west-2-lax-1",
    "Domain": "vpc"
}
```

Para obtener más información, consulte Direcciones IP elásticas en la Guía del usuario de Amazon EC2.

Ejemplo 3: asignación de una dirección IP elástica desde un grupo de direcciones propio

En el siguiente ejemplo de `allocate-address`, se asigna una dirección IP elástica desde un grupo de direcciones que usted trajo a su cuenta de Amazon Web Services. Amazon EC2 selecciona la dirección del conjunto de direcciones.

```
aws ec2 allocate-address \
    --public-ipv4-pool ipv4pool-ec2-1234567890abcdef0
```

Salida:

```
{
    "AllocationId": "eipalloc-02463d08ceEXAMPLE",
    "NetworkBorderGroup": "us-west-2",
    "CustomerOwnedIp": "18.218.95.81",
    "CustomerOwnedIpv4Pool": "ipv4pool-ec2-1234567890abcdef0",
    "Domain": "vpc"
    "NetworkBorderGroup": "us-west-2",
}
```

Para obtener más información, consulte Direcciones IP elásticas en la Guía del usuario de Amazon EC2.

Ejemplo 4: asignación de una dirección IP elástica de un grupo de IPAM

En el siguiente ejemplo de `allocate-address`, se asigna una dirección IP elástica específica/32 desde un grupo del Administrador de direcciones IP (IPAM) de Amazon VPC.

```
aws ec2 allocate-address \
    --region us-east-1 \
    --ipam-pool-id ipam-pool-1234567890abcdef0 \
    --address 192.0.2.0
```

Salida:

```
{
    "PublicIp": "192.0.2.0",
    "AllocationId": "eipalloc-abcdef01234567890",
    "PublicIpv4Pool": "ipam-pool-1234567890abcdef0",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

Para obtener más información, consulte Asignación de direcciones IP elásticas secuenciales de un grupo del IPAM en la Guía del usuario del Administrador de direcciones IP de Amazon VPC.

- Para obtener información sobre la API, consulte AllocateAddress en la Referencia de comandos de la AWS CLI.

`allocate-hosts`

En el siguiente ejemplo de código, se muestra cómo utilizar `allocate-hosts`.

AWS CLI

Ejemplo 1: asignación de un host dedicado

En el siguiente ejemplo de `allocate-hosts`, se asigna un host dedicado único de la zona de disponibilidad `eu-west-1a` en el que se pueden lanzar instancias de `m5.large`. De forma predeterminada, el host dedicado solo acepta el lanzamiento de instancias de destino y no admite la recuperación del host.

```
aws ec2 allocate-hosts \
    --instance-type m5.large \
    --availability-zone eu-west-1a \
    --quantity 1
```

Salida:

```
{
    "HostIds": [
        "h-07879acf49EXAMPLE"
    ]
}
```

Ejemplo 2: asignación de un host dedicado con la ubicación automática y la recuperación del host habilitadas

El siguiente ejemplo de `allocate-hosts`, se asigna un host dedicado único de la zona de disponibilidad `eu-west-1a` con la ubicación automática y la recuperación del host habilitadas.

```
aws ec2 allocate-hosts \
    --instance-type m5.large \
    --availability-zone eu-west-1a \
    --auto-placement on \
    --host-recovery on \
    --quantity 1
```

Salida:

```
{
     "HostIds": [
         "h-07879acf49EXAMPLE"
     ]
}
```

Ejemplo 3: asignación de un host dedicado con etiquetas

En el siguiente ejemplo de `allocate-hosts`, se asigna un host dedicado único y se aplica una etiqueta con una clave denominada `purpose` y el valor `production`.

```
aws ec2 allocate-hosts \
```

```
    --instance-type m5.large \
    --availability-zone eu-west-1a \
    --quantity 1 \
    --tag-specifications 'ResourceType=dedicated-
host,Tags={Key=purpose,Value=production}'
```

Salida:

```
{
    "HostIds": [
        "h-07879acf49EXAMPLE"
    ]
}
```

Para obtener más información, consulte Asignar un host dedicado en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte AllocateHosts en la Referencia de comandos de la AWS CLI.

`allocate-ipam-pool-cidr`

En el siguiente ejemplo de código, se muestra cómo utilizar `allocate-ipam-pool-cidr`.

AWS CLI

Para asignar un CIDR desde un grupo de IPAM

En el siguiente ejemplo de `allocate-ipam-pool-cidr`, se asigna un CIDR desde un grupo de IPAM.

(Linux):

```
aws ec2 allocate-ipam-pool-cidr \
    --ipam-pool-id ipam-pool-0533048da7d823723 \
    --netmask-length 24
```

(Windows):

```
aws ec2 allocate-ipam-pool-cidr ^
   --ipam-pool-id ipam-pool-0533048da7d823723 ^
```

```
    --netmask-length 24
```

Salida:

```
{
    "IpamPoolAllocation": {
        "Cidr": "10.0.0.0/24",
        "IpamPoolAllocationId": "ipam-pool-alloc-018ecc28043b54ba38e2cd99943cebfbd",
        "ResourceType": "custom",
        "ResourceOwner": "123456789012"
    }
}
```

Para obtener más información, consulte Asignar de forma manual un CIDR a un grupo para reservar espacio de direcciones IP en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte AllocateIpamPoolCidr en la Referencia de comandos de la AWS CLI.

`apply-security-groups-to-client-vpn-target-network`

En el siguiente ejemplo de código, se muestra cómo utilizar `apply-security-groups-to-client-vpn-target-network`.

AWS CLI

Para aplicar grupos de seguridad a una red de destino para un punto de conexión de Client VPN

En el siguiente ejemplo de `apply-security-groups-to-client-vpn-target-network`, se aplica un grupo de seguridad `sg-01f6e627a89f4db32` a la asociación entre la red de destino especificada y el punto de conexión de Client VPN.

```
aws ec2 apply-security-groups-to-client-vpn-target-network \
    --security-group-ids sg-01f6e627a89f4db32 \
    --vpc-id vpc-0e2110c2f324332e0 \
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde
```

Salida:

```
{
```

```
    "SecurityGroupIds": [
        "sg-01f6e627a89f4db32"
    ]
}
```

Para obtener más información, consulte Target Networks en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte ApplySecurityGroupsToClientVpnTargetNetwork en la Referencia de comandos de la AWS CLI.

`assign-ipv6-addresses`

En el siguiente ejemplo de código, se muestra cómo utilizar `assign-ipv6-addresses`.

AWS CLI

Para asignar direcciones IPv6 específicas a una interfaz de red

En este ejemplo, se asignan las direcciones IPv6 especificadas a la interfaz de red especificada.

Comando:

```
aws ec2 assign-ipv6-addresses --network-interface-id eni-38664473 --ipv6-
addresses 2001:db8:1234:1a00:3304:8879:34cf:4071 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Salida:

```
{
  "AssignedIpv6Addresses": [
      "2001:db8:1234:1a00:3304:8879:34cf:4071",
      "2001:db8:1234:1a00:9691:9503:25ad:1761"
  ],
  "NetworkInterfaceId": "eni-38664473"
}
```

Para asignar a una interfaz de red direcciones IPv6 que Amazon selecciona

En este ejemplo, se asignan dos direcciones IPv6 a la interfaz de red especificada. Amazon asigna automáticamente estas direcciones IPv6 de entre las direcciones IPv6 disponibles en el rango de bloques de CIDR de IPv6 de la subred.

Comando:

```
aws ec2 assign-ipv6-addresses --network-interface-id eni-38664473 --ipv6-address-
count 2
```

Salida:

```
{
  "AssignedIpv6Addresses": [
      "2001:db8:1234:1a00:3304:8879:34cf:4071",
      "2001:db8:1234:1a00:9691:9503:25ad:1761"
  ],
  "NetworkInterfaceId": "eni-38664473"
}
```

- Para obtener información sobre la API, consulte AssignIpv6Addresses en la Referencia de comandos de la AWS CLI.

`assign-private-ip-addresses`

En el siguiente ejemplo de código, se muestra cómo utilizar `assign-private-ip-addresses`.

AWS CLI

Para asignar una dirección IP privada secundaria a una interfaz de red

En este ejemplo, se asignan las direcciones IP especificadas a la interfaz de red especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 assign-private-ip-addresses --network-interface-id eni-e5aa89a3 --private-
ip-addresses 10.0.0.82
```

Para asignar a una interfaz de red direcciones IP privadas secundarias que Amazon EC2 selecciona

En este ejemplo, se asignan dos direcciones IP privadas secundarias a la interfaz de red especificada. Amazon EC2 asigna automáticamente estas direcciones IP de entre las direcciones

IP disponibles en el rango de bloques de CIDR de la subred a la que está asociada la interfaz de red. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 assign-private-ip-addresses --network-interface-id eni-e5aa89a3 --secondary-private-ip-address-count 2
```

- Para obtener información sobre la API, consulte AssignPrivateIpAddresses en la Referencia de comandos de la AWS CLI.

`assign-private-nat-gateway-address`

En el siguiente ejemplo de código, se muestra cómo utilizar `assign-private-nat-gateway-address`.

AWS CLI

Para asignar direcciones IP privadas a la puerta de enlace de NAT privada

En el siguiente ejemplo de `assign-private-nat-gateway-address`, se asignan dos direcciones IP privadas a la puerta de enlace de NAT privada especificada.

```
aws ec2 assign-private-nat-gateway-address \
    --nat-gateway-id nat-1234567890abcdef0 \
    --private-ip-address-count 2
```

Salida:

```
{
    "NatGatewayId": "nat-1234567890abcdef0",
    "NatGatewayAddresses": [
        {
            "NetworkInterfaceId": "eni-0065a61b324d1897a",
            "IsPrimary": false,
            "Status": "assigning"
        },
        {
            "NetworkInterfaceId": "eni-0065a61b324d1897a",
            "IsPrimary": false,
            "Status": "assigning"
```

```
        }
    ]
}
```

Para obtener información, consulte Gateways NAT en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte AssignPrivateNatGatewayAddress en la Referencia de comandos de la AWS CLI.

`associate-address`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-address`.

AWS CLI

Ejemplo 1: asociación de una dirección IP elástica a una instancia

En el siguiente ejemplo de `associate-address`, se asocia una dirección IP elástica con la instancia de EC2 especificada.

```
aws ec2 associate-address \
    --instance-id i-0b263919b6498b123 \
    --allocation-id eipalloc-64d5890a
```

Salida:

```
{
    "AssociationId": "eipassoc-2bebb745"
}
```

Ejemplo 2: asociación de una dirección IP elástica con una interfaz de red

En el siguiente ejemplo de `associate-address`, se asocia la dirección IP elástica especificada con la interfaz de red especificada.

```
aws ec2 associate-address
    --allocation-id eipalloc-64d5890a \
    --network-interface-id eni-1a2b3c4d
```

Salida:

```
{
    "AssociationId": "eipassoc-2bebb745"
}
```

Ejemplo 3: asociación de una dirección IP elástica con una dirección IP privada

En el siguiente ejemplo de `associate-address`, se asocia la dirección IP elástica especificada con la dirección IP privada especificada en la interfaz de red especificada.

```
aws ec2 associate-address \
    --allocation-id eipalloc-64d5890a \
    --network-interface-id eni-1a2b3c4d \
    --private-ip-address 10.0.0.85
```

Salida:

```
{
    "AssociationId": "eipassoc-2bebb745"
}
```

Para obtener más información, consulte Direcciones IP elásticas en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte AssociateAddress en la Referencia de comandos de la AWS CLI.

`associate-client-vpn-target-network`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-client-vpn-target-network`.

AWS CLI

Para asociar una red de destino a un punto de conexión de Client VPN

En el siguiente ejemplo de `associate-client-vpn-target-network`, se asocia una subred al punto de conexión de Client VPN especificado.

```
aws ec2 associate-client-vpn-target-network \
    --subnet-id subnet-0123456789abcabca \
```

```
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde
```

Salida:

```
{
    "AssociationId": "cvpn-assoc-12312312312312312",
    "Status": {
        "Code": "associating"
    }
}
```

Para obtener más información, consulte Target Networks en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte AssociateClientVpnTargetNetwork en la Referencia de comandos de la AWS CLI.

`associate-dhcp-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-dhcp-options`.

AWS CLI

Para asociar un conjunto de opciones de DHCP a la VPC

En este ejemplo, se asocia el conjunto de opciones de DHCP especificado a la VPC especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 associate-dhcp-options --dhcp-options-id dopt-d9070ebb --vpc-id vpc-a01106c2
```

Para asociar el conjunto de opciones de DHCP predeterminado a la VPC

En este ejemplo, se asocia el conjunto de opciones de DHCP predeterminado a la VPC especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 associate-dhcp-options --dhcp-options-id default --vpc-id vpc-a01106c2
```

- Para obtener información sobre la API, consulte AssociateDhcpOptions en la Referencia de comandos de la AWS CLI.

`associate-iam-instance-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-iam-instance-profile`.

AWS CLI

Para crear un perfil de instancia de IAM a una instancia

En este ejemplo, se asocia un perfil de instancia de IAM denominado `admin-role` a la instancia `i-123456789abcde123`.

Comando:

```
aws ec2 associate-iam-instance-profile --instance-id i-123456789abcde123 --iam-instance-profile Name=admin-role
```

Salida:

```
{
  "IamInstanceProfileAssociation": {
      "InstanceId": "i-123456789abcde123",
      "State": "associating",
      "AssociationId": "iip-assoc-0e7736511a163c209",
      "IamInstanceProfile": {
          "Id": "AIPAJBLK7RKJKWDXVHIEC",
          "Arn": "arn:aws:iam::123456789012:instance-profile/admin-role"
      }
  }
}
```

- Para obtener información sobre la API, consulte AssociateIamInstanceProfile en la Referencia de comandos de la AWS CLI.

`associate-instance-event-window`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-instance-event-window`.

AWS CLI

Ejemplo 1: asociación de una o varias instancias a un período de evento

En el siguiente ejemplo de `associate-instance-event-window`, se asocian una o varias instancias a un período de evento.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Salida:

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-1234567890abcdef0",
                "i-0598c7d356eba48d7"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Para conocer las restricciones de los períodos de eventos, consulte Consideraciones en la sección sobre eventos programados de la Guía del usuario de Amazon EC2.

Ejemplo 2: asociación de etiquetas de instancia a un período de evento

En el siguiente ejemplo de `associate-instance-event-window`, se asocian etiquetas de instancias a un período de evento. Introduzca un parámetro `instance-event-window-id` para especificar el período de evento. Para asociar las etiquetas de instancia, especifique el parámetro `association-target` y, para el valor del parámetro, especifique una o varias etiquetas.

```
aws ec2 associate-instance-event-window \
```

```
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Salida:

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [
                {
                    "Key": "k2",
                    "Value": "v2"
                },
                {
                    "Key": "k1",
                    "Value": "v1"
                }
            ],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Para conocer las restricciones de los períodos de eventos, consulte Consideraciones en la sección sobre eventos programados de la Guía del usuario de Amazon EC2.

Ejemplo 3: asociación de un host dedicado a un período de evento

En el siguiente ejemplo de `associate-instance-event-window` se asocia un host dedicado a un período de evento. Introduzca un parámetro `instance-event-window-id` para especificar el período de evento. Para asociar un host dedicado, especifique el parámetro `--association-target` y, para los valores del parámetro, especifique uno o varios ID de host dedicado.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
```

```
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "DedicatedHostIds=h-029fa35a02b99801d"
```

Salida:

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": [
                "h-029fa35a02b99801d"
            ]
        },
        "State": "creating"
    }
}
```

Para conocer las restricciones de los períodos de eventos, consulte Consideraciones en la sección sobre eventos programados de la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte AssociateInstanceEventWindow en la Referencia de comandos de la AWS CLI.

`associate-ipam-resource-discovery`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-ipam-resource-discovery`.

AWS CLI

Para asociar una detección de recursos a un IPAM

En este ejemplo, usted es un administrador delegado de IPAM y otra cuenta de AWS ha creado y compartido con usted una detección de recursos, de forma que pueda utilizar IPAM para administrar y supervisar los CIDR de recursos propiedad de esa otra cuenta.

Nota

Para completar esta solicitud, necesitará el ID de detección de recursos, que puede obtener mediante describe-ipam-resource-discoveries, así como el ID de IPAM, que puede obtener mediante describe-ipams. La detección de recursos que se va a asociar debe haberse compartido primero con su cuenta mediante AWS RAM. El valor de `--region` que introduzca debe coincidir con la región de origen del IPAM al que se va a asociar.

En el siguiente ejemplo de `associate-ipam-resource-discovery`, se asocia un recurso de detección de recursos a un IPAM.

```
aws ec2 associate-ipam-resource-discovery \
    --ipam-id ipam-005f921c17ebd5107 \
    --ipam-resource-discovery-id ipam-res-disco-03e0406de76a044ee \
    --tag-specifications 'ResourceType=ipam-resource-discovery,Tags=[{Key=cost-
center,Value=cc123}]' \
    --region us-east-1
```

Salida:

```
{
    {
        "IpamResourceDiscoveryAssociation": {
            "OwnerId": "320805250157",
            "IpamResourceDiscoveryAssociationId": "ipam-res-disco-
assoc-04382a6346357cf82",
            "IpamResourceDiscoveryAssociationArn": "arn:aws:ec2::320805250157:ipam-
resource-discovery-association/ipam-res-disco-assoc-04382a6346357cf82",
            "IpamResourceDiscoveryId": "ipam-res-disco-0365d2977fc1672fe",
            "IpamId": "ipam-005f921c17ebd5107",
            "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-005f921c17ebd5107",
            "IpamRegion": "us-east-1",
            "IsDefault": false,
            "ResourceDiscoveryStatus": "active",
            "State": "associate-in-progress",
            "Tags": []
        }
    }
}
```

Una vez asociada la detección de recursos, puede supervisar o administrar las direcciones IP de los recursos creados por las otras cuentas. Para obtener más información, consulte Integración de IPAM con cuentas ajenas a su organización en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte AssociateIpamResourceDiscovery en la Referencia de comandos de la AWS CLI.

`associate-nat-gateway-address`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-nat-gateway-address`.

AWS CLI

Para asociar una dirección IP elástica a una puerta de enlace de NAT pública

En el siguiente `associate-nat-gateway-address` ejemplo se asocia la dirección IP elástica especificada a la puerta de enlace de NAT pública especificada. AWS asigna automáticamente una dirección IPv4 privada secundaria.

```
aws ec2 associate-nat-gateway-address \
    --nat-gateway-id nat-1234567890abcdef0 \
    --allocation-ids eipalloc-0be6ecac95EXAMPLE
```

Salida:

```
{
    "NatGatewayId": "nat-1234567890abcdef0",
    "NatGatewayAddresses": [
        {
            "AllocationId": "eipalloc-0be6ecac95EXAMPLE",
            "NetworkInterfaceId": "eni-09cc4b2558794f7f9",
            "IsPrimary": false,
            "Status": "associating"
        }
    ]
}
```

Para obtener información, consulte Gateways NAT en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte AssociateNatGatewayAddress en la Referencia de comandos de la AWS CLI.

`associate-route-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-route-table`.

AWS CLI

Para asociar una tabla de enrutamiento a una subred

En este ejemplo, se asocia la tabla de enrutamiento especificada a la subred especificada.

Comando:

```
aws ec2 associate-route-table --route-table-id rtb-22574640 --subnet-
id subnet-9d4a7b6c
```

Salida:

```
{
    "AssociationId": "rtbassoc-781d0d1a"
}
```

- Para obtener información sobre la API, consulte AssociateRouteTable en la Referencia de comandos de la AWS CLI.

`associate-security-group-vpc`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-security-group-vpc`.

AWS CLI

Asociación de un grupo de seguridad a otra VPC

En el siguiente ejemplo de `associate-security-group-vpc`, se asocia el grupo de seguridad especificado a la VPC especificada.

```
aws ec2 associate-security-group-vpc \
    --group-id sg-04dbb43907d3f8a78 \
    --vpc-id vpc-0bf4c2739bc05a694
```

Salida:

```
{
    "State": "associating"
}
```

Para obtener más información, consulte Asociación de grupos de seguridad a varias VPC en la Guía del usuario de Amazon VPC.

- Para obtener detalles sobre la API, consulte AssociateSecurityGroupVpc en la Referencia de comandos de la AWS CLI.

`associate-subnet-cidr-block`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-subnet-cidr-block`.

AWS CLI

Para asociar un bloque de CIDR de IPv6 a una subred

En este ejemplo, se asocia un bloque de CIDR de IPv6 a la subred especificada.

Comando:

```
aws ec2 associate-subnet-cidr-block --subnet-id subnet-5f46ec3b --ipv6-cidr-
block 2001:db8:1234:1a00::/64
```

Salida:

```
{
  "SubnetId": "subnet-5f46ec3b",
  "Ipv6CidrBlockAssociation": {
      "Ipv6CidrBlock": "2001:db8:1234:1a00::/64",
      "AssociationId": "subnet-cidr-assoc-3aa54053",
      "Ipv6CidrBlockState": {
          "State": "associating"
      }
  }
}
```

- Para obtener información sobre la API, consulte AssociateSubnetCidrBlock en la Referencia de comandos de la AWS CLI.

`associate-transit-gateway-multicast-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-transit-gateway-multicast-domain`.

AWS CLI

Para asociar una puerta de enlace de tránsito a un dominio de multidifusión

En el siguiente ejemplo de `associate-transit-gateway-multicast-domain`, se asocian la subred y la conexión especificadas al dominio de multidifusión especificado.

```
aws ec2 associate-transit-gateway-multicast-domain \
    --transit-gateway-multicast-domain-id tgw-mcast-domain-0c4905cef79d6e597 \
    --transit-gateway-attachment-id tgw-attach-028c1dd0f8f5cbe8e \
    --subnet-ids subnet-000de86e3b49c932a \
    --transit-gateway-multicast-domain-id tgw-mcast-domain-0c4905cef7EXAMPLE
```

Salida:

```
{
    "Associations": {
        "TransitGatewayMulticastDomainId": "tgw-mcast-domain-0c4905cef79d6e597",
        "TransitGatewayAttachmentId": "tgw-attach-028c1dd0f8f5cbe8e",
        "ResourceId": "vpc-01128d2c240c09bd5",
        "ResourceType": "vpc",
        "Subnets": [
            {
                "SubnetId": "subnet-000de86e3b49c932a",
                "State": "associating"
            }
        ]
    }
}
```

Para obtener más información, consulte Dominios de multidifusión en la Guía de puertas de enlace de tránsito.

- Para obtener información sobre la API, consulte AssociateTransitGatewayMulticastDomain en la Referencia de comandos de la AWS CLI.

`associate-transit-gateway-route-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-transit-gateway-route-table`.

AWS CLI

Para asociar una tabla de enrutamiento de puerta de enlace de tránsito a una conexión de puerta de enlace de tránsito

En el siguiente ejemplo, se asocia la tabla de enrutamiento de puerta de enlace especificada a la conexión de VPC especificada.

```
aws ec2 associate-transit-gateway-route-table \
    --transit-gateway-route-table-id tgw-rtb-002573ed1eEXAMPLE \
    --transit-gateway-attachment-id tgw-attach-0b5968d3b6EXAMPLE
```

Salida:

```
{
    "Association": {
        "TransitGatewayRouteTableId": "tgw-rtb-002573ed1eEXAMPLE",
        "TransitGatewayAttachmentId": "tgw-attach-0b5968d3b6EXAMPLE",
        "ResourceId": "vpc-0065acced4EXAMPLE",
        "ResourceType": "vpc",
        "State": "associating"
    }
}
```

Para obtener más información, consulte Associate a Transit Gateway Route Table en la Guía de AWS Transit Gateway.

- Para obtener información sobre la API, consulte AssociateTransitGatewayRouteTable en la Referencia de comandos de la AWS CLI.

`associate-vpc-cidr-block`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-vpc-cidr-block`.

AWS CLI

Ejemplo 1: asociación a una VPC de un bloque de CIDR de IPv6 proporcionado por Amazon

En el siguiente ejemplo de `associate-vpc-cidr-block` se asocia un bloque de CIDR de IPv6 con la VPC especificada.

```
aws ec2 associate-vpc-cidr-block \
```

```
    --amazon-provided-ipv6-cidr-block \
    --ipv6-cidr-block-network-border-group us-west-2-lax-1  \
    --vpc-id vpc-8EXAMPLE
```

Salida:

```
{
    "Ipv6CidrBlockAssociation": {
        "AssociationId": "vpc-cidr-assoc-0838ce7d9dEXAMPLE",
        "Ipv6CidrBlockState": {
            "State": "associating"
        },
        "NetworkBorderGroup": "us-west-2-lax-1"
    },
    "VpcId": "vpc-8EXAMPLE"
}
```

Ejemplo 2: asociación a una VPC de un bloque de CIDR de IPv4 adicional

En el siguiente ejemplo de `associate-vpc-cidr-block` se asocia a la VPC especificada el bloque de CIDR de IPv4 `10.2.0.0/16`.

```
aws ec2 associate-vpc-cidr-block \
    --vpc-id vpc-1EXAMPLE \
    --cidr-block 10.2.0.0/16
```

Salida:

```
{
    "CidrBlockAssociation": {
        "AssociationId": "vpc-cidr-assoc-2EXAMPLE",
        "CidrBlock": "10.2.0.0/16",
        "CidrBlockState": {
            "State": "associating"
        }
    },
    "VpcId": "vpc-1EXAMPLE"
}
```

- Para obtener información sobre la API, consulte AssociateVpcCidrBlock en la Referencia de comandos de la AWS CLI.

`attach-classic-link-vpc`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-classic-link-vpc`.

AWS CLI

Para vincular (asociar) una instancia de EC2-Classic a una VPC

En este ejemplo, se vincula la instancia i-1234567890abcdef0 a la VPC vpc-88888888 a través del grupo de seguridad de VPC sg-12312312.

Comando:

```
aws ec2 attach-classic-link-vpc --instance-id  i-1234567890abcdef0 --vpc-
id vpc-88888888 --groups sg-12312312
```

Salida:

```
{
  "Return": true
}
```

- Para obtener información sobre la API, consulte AttachClassicLinkVpc en la Referencia de comandos de la AWS CLI.

`attach-internet-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-internet-gateway`.

AWS CLI

Para asociar una puerta de enlace de Internet a la VPC

En el siguiente ejemplo de `attach-internet-gateway`, se asocia la puerta de enlace de Internet especificada a la VPC específica.

```
aws ec2 attach-internet-gateway \
    --internet-gateway-id igw-0d0fb496b3EXAMPLE \
    --vpc-id vpc-0a60eb65b4EXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Puertas de enlace de Internet en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte AttachInternetGateway en la Referencia de comandos de la AWS CLI.

`attach-network-interface`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-network-interface`.

AWS CLI

Ejemplo 1: asociación de una interfaz de red a una instancia

En el siguiente ejemplo de `attach-network-interface`, se asocia la interfaz de red especificada a la instancia especificada.

```
aws ec2 attach-network-interface \
    --network-interface-id eni-0dc56a8d4640ad10a \
    --instance-id i-1234567890abcdef0 \
    --device-index 1
```

Salida:

```
{
    "AttachmentId": "eni-attach-01a8fc87363f07cf9"
}
```

Para obtener más información, consulte Interfaces de red elásticas en la Guía del usuario de Amazon EC2.

Ejemplo 2: asociación de una interfaz de red a una instancia con varias tarjetas de red

En el siguiente ejemplo de `attach-network-interface`, se asocia la interfaz de red especificada a la instancia y tarjeta de red especificadas.

```
aws ec2 attach-network-interface \
    --network-interface-id eni-07483b1897541ad83 \
    --instance-id i-01234567890abcdef \
    --network-card-index 1 \
```

```
    --device-index 1
```

Salida:

```
{
    "AttachmentId": "eni-attach-0fbd7ee87a88cd06c"
}
```

Para obtener más información, consulte Interfaces de red elásticas en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte AttachNetworkInterface en la Referencia de comandos de la AWS CLI.

`attach-verified-access-trust-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-verified-access-trust-provider`.

AWS CLI

Para asociar un proveedor de confianza a una instancia

En el siguiente ejemplo de `attach-verified-access-trust-provider`, se asocia el proveedor de confianza de Acceso verificado especificado a la instancia de Acceso verificado especificada.

```
aws ec2 attach-verified-access-trust-provider \
    --verified-access-instance-id vai-0ce000c0b7643abea \
    --verified-access-trust-provider-id vatp-0bb32de759a3e19e7
```

Salida:

```
{
    "VerifiedAccessTrustProvider": {
        "VerifiedAccessTrustProviderId": "vatp-0bb32de759a3e19e7",
        "Description": "",
        "TrustProviderType": "user",
        "UserTrustProviderType": "iam-identity-center",
        "PolicyReferenceName": "idc",
        "CreationTime": "2023-08-25T19:00:38",
```

```
        "LastUpdatedTime": "2023-08-25T19:00:38"
    },
    "VerifiedAccessInstance": {
        "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
        "Description": "",
        "VerifiedAccessTrustProviders": [
            {
                "VerifiedAccessTrustProviderId": "vatp-0bb32de759a3e19e7",
                "TrustProviderType": "user",
                "UserTrustProviderType": "iam-identity-center"
            }
        ],
        "CreationTime": "2023-08-25T18:27:56",
        "LastUpdatedTime": "2023-08-25T18:27:56"
    }
}
```

Para obtener más información, consulte Verified Access instances en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte AttachVerifiedAccessTrustProvider en la Referencia de comandos de la AWS CLI.

`attach-volume`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-volume`.

AWS CLI

Para asociar un volumen a una instancia

En este ejemplo de comando se asocia un volumen (`vol-1234567890abcdef0`) a una instancia (`i-01474ef662b89480`) como `/dev/sdf`.

Comando:

```
aws ec2 attach-volume --volume-id vol-1234567890abcdef0 --instance-
id i-01474ef662b89480 --device /dev/sdf
```

Salida:

```
{
```

```
    "AttachTime": "YYYY-MM-DDTHH:MM:SS.000Z",
    "InstanceId": "i-01474ef662b89480",
    "VolumeId": "vol-1234567890abcdef0",
    "State": "attaching",
    "Device": "/dev/sdf"
}
```

- Para obtener información sobre la API, consulte AttachVolume en la Referencia de comandos de la AWS CLI.

`attach-vpn-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-vpn-gateway`.

AWS CLI

Para asociar una puerta de enlace privada virtual a una VPC

En el siguiente ejemplo de `attach-vpn-gateway`, se asocia la puerta de enlace privada virtual especificada a la VPC especificada.

```
aws ec2 attach-vpn-gateway \
    --vpn-gateway-id vgw-9a4cacf3 \
    --vpc-id vpc-a01106c2
```

Salida:

```
{
    "VpcAttachment": {
        "State": "attaching",
        "VpcId": "vpc-a01106c2"
    }
}
```

- Para obtener información sobre la API, consulte AttachVpnGateway en la Referencia de comandos de la AWS CLI.

`authorize-client-vpn-ingress`

En el siguiente ejemplo de código, se muestra cómo utilizar `authorize-client-vpn-ingress`.

AWS CLI

Para agregar una regla de autorización a un punto de conexión de Client VPN

En el siguiente ejemplo de `authorize-client-vpn-ingress`, se agrega una regla de autorización de entrada que permite a todos los clientes obtener acceso a Internet (`0.0.0.0/0`).

```
aws ec2 authorize-client-vpn-ingress \
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde \
    --target-network-cidr 0.0.0.0/0 \
    --authorize-all-groups
```

Salida:

```
{
    "Status": {
        "Code": "authorizing"
    }
}
```

Para obtener más información, consulte Authorization Rules en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte AuthorizeClientVpnIngress en la Referencia de comandos de la AWS CLI.

`authorize-security-group-egress`

En el siguiente ejemplo de código, se muestra cómo utilizar `authorize-security-group-egress`.

AWS CLI

Ejemplo 1: agregación de una regla que permita el tráfico saliente a un rango de direcciones específico

En el siguiente ejemplo de `authorize-security-group-egress`, se agrega una regla que otorga acceso en el puerto TCP 80 a los rangos de direcciones especificados.

```
aws ec2 authorize-security-group-egress \
```

```
    --group-id sg-1234567890abcdef0 \
    --ip-permissions
 'IpProtocol=tcp,FromPort=80,ToPort=80,IpRanges=[{CidrIp=10.0.0.0/16}]'
```

Salida:

```
{
    "Return": true,
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-0b15794cdb17bf29c",
            "GroupId": "sg-1234567890abcdef0",
            "GroupOwnerId": "123456789012",
            "IsEgress": true,
            "IpProtocol": "tcp",
            "FromPort": 80,
            "ToPort": 80,
            "CidrIpv4": "10.0.0.0/16"
        }
    ]
}
```

Ejemplo 2: agregación de una regla que permita el tráfico saliente a un grupo de seguridad específico

En el siguiente ejemplo de `authorize-security-group-egress`, se agrega una regla que otorga acceso en el puerto TCP 80 al grupo de seguridad especificado.

```
aws ec2 authorize-security-group-egress \
    --group-id sg-1234567890abcdef0 \
    --ip-permissions
 'IpProtocol=tcp,FromPort=80,ToPort=80,UserIdGroupPairs=[{GroupId=sg-0aad1c26bbeec5c22}]'
```

Salida:

```
{
    "Return": true,
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-0b5dd815afcea9cc3",
            "GroupId": "sg-1234567890abcdef0",
```

```
            "GroupOwnerId": "123456789012",
            "IsEgress": true,
            "IpProtocol": "tcp",
            "FromPort": 80,
            "ToPort": 80,
            "ReferencedGroupInfo": {
                "GroupId": "sg-0aad1c26bbeec5c22",
                "UserId": "123456789012"
            }
        }
    ]
}
```

Para obtener más información, consulte Grupo de seguridad en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte AuthorizeSecurityGroupEgress en la Referencia de comandos de la AWS CLI.

`authorize-security-group-ingress`

En el siguiente ejemplo de código, se muestra cómo utilizar `authorize-security-group-ingress`.

AWS CLI

Ejemplo 1: Agregar una regla que permita el tráfico SSH entrante

En el siguiente ejemplo de `authorize-security-group-ingress`, se agrega una regla que permite el tráfico entrante en un puerto TCP 22 (SSH).

```
aws ec2 authorize-security-group-ingress \
    --group-id sg-1234567890abcdef0 \
    --protocol tcp \
    --port 22 \
    --cidr 203.0.113.0/24
```

Salida:

```
{
    "Return": true,
```

```
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-01afa97ef3e1bedfc",
            "GroupId": "sg-1234567890abcdef0",
            "GroupOwnerId": "123456789012",
            "IsEgress": false,
            "IpProtocol": "tcp",
            "FromPort": 22,
            "ToPort": 22,
            "CidrIpv4": "203.0.113.0/24"
        }
    ]
}
```

Ejemplo 2: Agregar una regla que permita el tráfico HTTP entrante desde otro grupo de seguridad

En el siguiente ejemplo de `authorize-security-group-ingress`, se agrega una regla que permite el acceso entrante al puerto TCP 80 desde el grupo de seguridad de origen `sg-1a2b3c4d`. El grupo de origen debe estar en la misma VPC o en una VPC del mismo nivel (requiere una conexión de emparejamiento de VPC). Se permite el tráfico entrante según las direcciones IP privadas de las instancias asociadas al grupo de seguridad de origen (y no la dirección IP pública o la dirección IP elástica).

```
aws ec2 authorize-security-group-ingress \
    --group-id sg-1234567890abcdef0 \
    --protocol tcp \
    --port 80 \
    --source-group sg-1a2b3c4d
```

Salida:

```
{
    "Return": true,
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-01f4be99110f638a7",
            "GroupId": "sg-1234567890abcdef0",
            "GroupOwnerId": "123456789012",
            "IsEgress": false,
            "IpProtocol": "tcp",
            "FromPort": 80,
            "ToPort": 80,
```

```
            "ReferencedGroupInfo": {
                "GroupId": "sg-1a2b3c4d",
                "UserId": "123456789012"
            }
        }
    ]
}
```

Ejemplo 3: agregar varias reglas en la misma llamada

En el siguiente ejemplo de `authorize-security-group-ingress`, se usa el parámetro `ip-permissions` para agregar dos reglas de entrada, una que habilita el acceso entrante en el puerto TCP 3389 (RDP) y la otra que habilita ping/ICMP.

```
aws ec2 authorize-security-group-ingress \
    --group-id sg-1234567890abcdef0 \
    --ip-permissions
 'IpProtocol=tcp,FromPort=3389,ToPort=3389,IpRanges=[{CidrIp=172.31.0.0/16}]"
 "IpProtocol=icmp,FromPort=-1,ToPort=-1,IpRanges=[{CidrIp=172.31.0.0/16}]'
```

Salida:

```
{
    "Return": true,
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-00e06e5d3690f29f3",
            "GroupId": "sg-1234567890abcdef0",
            "GroupOwnerId": "123456789012",
            "IsEgress": false,
            "IpProtocol": "tcp",
            "FromPort": 3389,
            "ToPort": 3389,
            "CidrIpv4": "172.31.0.0/16"
        },
        {
            "SecurityGroupRuleId": "sgr-0a133dd4493944b87",
            "GroupId": "sg-1234567890abcdef0",
            "GroupOwnerId": "123456789012",
            "IsEgress": false,
            "IpProtocol": "tcp",
            "FromPort": -1,
```

```
            "ToPort": -1,
            "CidrIpv4": "172.31.0.0/16"
        }
    ]
}
```

Ejemplo 4: agregar una regla para el tráfico ICMP

En el siguiente ejemplo de `authorize-security-group-ingress`, se usa el parámetro `ip-permissions` para agregar una regla de entrada que permita enviar el mensaje ICMP `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (tipo 3, código 4) desde cualquier lugar.

```
aws ec2 authorize-security-group-ingress \
    --group-id sg-1234567890abcdef0 \
    --ip-permissions
 'IpProtocol=icmp,FromPort=3,ToPort=4,IpRanges=[{CidrIp=0.0.0.0/0}]'
```

Salida:

```
{
    "Return": true,
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-0de3811019069b787",
            "GroupId": "sg-1234567890abcdef0",
            "GroupOwnerId": "123456789012",
            "IsEgress": false,
            "IpProtocol": "icmp",
            "FromPort": 3,
            "ToPort": 4,
            "CidrIpv4": "0.0.0.0/0"
        }
    ]
}
```

Ejemplo 5: agregar una regla para el tráfico IPv

En el siguiente ejemplo de `authorize-security-group-ingress`, se usa el parámetro `ip-permissions` para agregar una regla de entrada que permita el acceso SSH (puerto 22) desde el intervalo IPv6 `2001:db8:1234:1a00::/64`.

```
aws ec2 authorize-security-group-ingress \
    --group-id sg-1234567890abcdef0 \
    --ip-permissions
 'IpProtocol=tcp,FromPort=22,ToPort=22,Ipv6Ranges=[{CidrIpv6=2001:db8:1234:1a00::/64}]'
```

Salida:

```
{
    "Return": true,
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-0455bc68b60805563",
            "GroupId": "sg-1234567890abcdef0",
            "GroupOwnerId": "123456789012",
            "IsEgress": false,
            "IpProtocol": "tcp",
            "FromPort": 22,
            "ToPort": 22,
            "CidrIpv6": "2001:db8:1234:1a00::/64"
        }
    ]
}
```

Ejemplo 6: Agregar una regla para el tráfico ICMPv

En el siguiente ejemplo de `authorize-security-group-ingress`, se usa el parámetro `ip-permissions` para agregar una regla de entrada que permita el tráfico ICMPv6 desde cualquier lugar.

```
aws ec2 authorize-security-group-ingress \
    --group-id sg-1234567890abcdef0 \
    --ip-permissions 'IpProtocol=icmpv6,Ipv6Ranges=[{CidrIpv6=::/0}]'
```

Salida:

```
{
    "Return": true,
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-04b612d9363ab6327",
            "GroupId": "sg-1234567890abcdef0",
```

```
            "GroupOwnerId": "123456789012",
            "IsEgress": false,
            "IpProtocol": "icmpv6",
            "FromPort": -1,
            "ToPort": -1,
            "CidrIpv6": "::/0"
        }
    ]
}
```

Ejemplo 7: agregar una regla con una descripción

En el siguiente ejemplo de `authorize-security-group-ingress`, se usa el parámetro `ip-permissions` para agregar una regla de entrada que permita el tráfico RDP desde el intervalo de direcciones IPv4 especificado. La regla incluye una descripción que lo ayudará a identificarla posteriormente.

```
aws ec2 authorize-security-group-ingress \
    --group-id sg-1234567890abcdef0 \
    --ip-permissions
 'IpProtocol=tcp,FromPort=3389,ToPort=3389,IpRanges=[{CidrIp=203.0.113.0/24,Description='RDP
 office'}]'
```

Salida:

```
{
    "Return": true,
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-0397bbcc01e974db3",
            "GroupId": "sg-1234567890abcdef0",
            "GroupOwnerId": "123456789012",
            "IsEgress": false,
            "IpProtocol": "tcp",
            "FromPort": 3389,
            "ToPort": 3389,
            "CidrIpv4": "203.0.113.0/24",
            "Description": "RDP access from NY office"
        }
    ]
}
```

Ejemplo 8: Agregar una regla de entrada que use una lista de prefijos

En el siguiente ejemplo de `authorize-security-group-ingress`, se usa el parámetro `ip-permissions` para agregar una regla de entrada que permita todo el tráfico de los rangos de CIDR de la lista de prefijos especificada.

```
aws ec2 authorize-security-group-ingress \
    --group-id sg-04a351bfe432d4e71 \
    --ip-permissions
 'IpProtocol=all,PrefixListIds=[{PrefixListId=pl-002dc3ec097de1514}]'
```

Salida:

```
{
    "Return": true,
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-09c74b32f677c6c7c",
            "GroupId": "sg-1234567890abcdef0",
            "GroupOwnerId": "123456789012",
            "IsEgress": false,
            "IpProtocol": "-1",
            "FromPort": -1,
            "ToPort": -1,
            "PrefixListId": "pl-0721453c7ac4ec009"
        }
    ]
}
```

Para obtener más información, consulte Grupo de seguridad en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte AuthorizeSecurityGroupIngress en la Referencia de comandos de la AWS CLI.

`bundle-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `bundle-instance`.

AWS CLI

Para agrupar una instancia

En este ejemplo, se agrupa la instancia `i-1234567890abcdef0` con un bucket denominado `bundletasks`. Antes de especificar valores para los ID de las claves de acceso, consulte y siga las instrucciones de las prácticas recomendadas para administrar las claves de acceso de AWS.

Comando:

```
aws ec2 bundle-instance --instance-id i-1234567890abcdef0 --bucket bundletasks --
prefix winami --owner-akid AK12AJEXAMPLE --owner-sak example123example
```

Salida:

```
{
  "BundleTask": {
    "UpdateTime": "2015-09-15T13:30:35.000Z",
    "InstanceId": "i-1234567890abcdef0",
    "Storage": {
      "S3": {
        "Prefix": "winami",
        "Bucket": "bundletasks"
      }
    },
    "State": "pending",
    "StartTime": "2015-09-15T13:30:35.000Z",
    "BundleId": "bun-294e041f"
  }
}
```

- Para obtener información sobre la API, consulte BundleInstance en la Referencia de comandos de la AWS CLI.

`cancel-bundle-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-bundle-task`.

AWS CLI

Para cancelar una tarea agrupada

En este ejemplo, se cancela la tarea agrupada `bun-2a4e041c`.

Comando:

```
aws ec2 cancel-bundle-task --bundle-id bun-2a4e041c
```

Salida:

```
{
  "BundleTask": {
    "UpdateTime": "2015-09-15T13:27:40.000Z",
    "InstanceId": "i-1234567890abcdef0",
    "Storage": {
      "S3": {
        "Prefix": "winami",
        "Bucket": "bundletasks"
      }
    },
    "State": "cancelling",
    "StartTime": "2015-09-15T13:24:35.000Z",
    "BundleId": "bun-2a4e041c"
  }
}
```

- Para obtener información sobre la API, consulte CancelBundleTask en la Referencia de comandos de la AWS CLI.

`cancel-capacity-reservation-fleets`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-capacity-reservation-fleets`.

AWS CLI

Para cancelar una Flota de reservas de capacidad

En el siguiente ejemplo de `cancel-capacity-reservation-fleets`, se cancelan la flota de reservas de capacidad especificada y la capacidad que reserva. Al cancelar una flota, su estado cambia a `cancelled` y ya no puede crear nuevas reservas de capacidad. Además, se cancelan todas las reservas de capacidad individuales de la flota y las instancias que se estaban ejecutando anteriormente en la capacidad reservada siguen funcionando normalmente en capacidad compartida.

```
aws ec2 cancel-capacity-reservation-fleets \
```

```
    --capacity-reservation-fleet-ids crf-abcdef01234567890
```

Salida:

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "cancelling",
            "PreviousFleetState": "active",
            "CapacityReservationFleetId": "crf-abcdef01234567890"
        }
    ],
    "FailedFleetCancellations": []
}
```

Para obtener más información sobre flotas de reserva de capacidad, consulte Flotas de reservas de capacidad en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CancelCapacityReservationFleets en la Referencia de comandos de la AWS CLI.

`cancel-capacity-reservation`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-capacity-reservation`.

AWS CLI

Para cancelar una reserva de capacidad

En el siguiente ejemplo de `cancel-capacity-reservation`, se cancela la reserva de capacidad especificada.

```
aws ec2 cancel-capacity-reservation \
    --capacity-reservation-id cr-1234abcd56EXAMPLE
```

Salida:

```
{
    "Return": true
}
```

Para obtener más información, consulte Cancelar una reserva de capacidad en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CancelCapacityReservation en la Referencia de comandos de la AWS CLI.

`cancel-conversion-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-conversion-task`.

AWS CLI

Para cancelar una conversión activa de una instancia o un volumen

En este ejemplo, se cancela la carga asociada al ID de tarea import-i-fh95npoc. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 cancel-conversion-task --conversion-task-id import-i-fh95npoc
```

- Para obtener información sobre la API, consulte CancelConversionTask en la Referencia de comandos de la AWS CLI.

`cancel-export-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-export-task`.

AWS CLI

Para cancelar una tarea de exportación activa

En este ejemplo, se cancela una tarea de exportación activa con el ID de tarea export-i-fgelt0i7. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 cancel-export-task --export-task-id export-i-fgelt0i7
```

- Para obtener información sobre la API, consulte CancelExportTask en la Referencia de comandos de la AWS CLI.

`cancel-image-launch-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-image-launch-permission`.

AWS CLI

Para cancelar que se comparta una AMI con la cuenta de Amazon Web Services

En el siguiente ejemplo de `cancel-image-launch-permission`, se eliminan de la cuenta los permisos de lanzamiento de la AMI especificada.

```
aws ec2 cancel-image-launch-permission \
    --image-id ami-0123456789example \
    --region us-east-1
```

Salida:

```
{
    "Return": true
}
```

Para obtener más información, consulte Cancelar que se comparta una AMI con su Cuenta de AWS en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CancelImageLaunchPermission en la Referencia de comandos de la AWS CLI.

`cancel-import-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-import-task`.

AWS CLI

Para cancelar una tarea de importación

En el siguiente ejemplo de `cancel-import-task`, se cancela la tarea de importación de imágenes especificada.

```
aws ec2 cancel-import-task \
    --import-task-id import-ami-1234567890abcdef0
```

Salida:

```
{
    "ImportTaskId": "import-ami-1234567890abcdef0",
    "PreviousState": "active",
    "State": "deleting"
}
```

- Para obtener información sobre la API, consulte CancelImportTask en la Referencia de comandos de la AWS CLI.

`cancel-reserved-instances-listing`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-reserved-instances-listing`.

AWS CLI

Para cancelar un listado de instancias reservadas

En el siguiente ejemplo de `cancel-reserved-instances-listing`, se cancela el listado de instancias reservadas especificado.

```
aws ec2 cancel-reserved-instances-listing \
    --reserved-instances-listing-id 5ec28771-05ff-4b9b-aa31-9e57dexample
```

- Para obtener información sobre la API, consulte CancelReservedInstancesListing en la Referencia de comandos de la AWS CLI.

`cancel-spot-fleet-requests`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-spot-fleet-requests`.

AWS CLI

Ejemplo 1: cancelación de una solicitud de flota de spot y terminación de las instancias asociadas

En el siguiente ejemplo de `cancel-spot-fleet-requests`, se cancela una solicitud de flota de spot y se terminan las instancias bajo demanda y las instancias de spot asociadas.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
```

```
    --terminate-instances
```

Salida:

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_terminating",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

Ejemplo 2: cancelación de una solicitud de flota de spot sin terminar las instancias asociadas

En el siguiente ejemplo de `cancel-spot-fleet-requests`, se cancela una solicitud de flota de spot sin terminar las instancias bajo demanda y las instancias de spot asociadas.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Salida:

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_running",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

Para obtener más información, consulte Cancelar una solicitud de flota de spot en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CancelSpotFleetRequests en la Referencia de comandos de la AWS CLI.

`cancel-spot-instance-requests`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-spot-instance-requests`.

AWS CLI

Para cancelar solicitudes de instancias de spot

En este ejemplo de comando, se cancela una solicitud de instancia de spot.

Comando:

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

Salida:

```
{
    "CancelledSpotInstanceRequests": [
        {
            "State": "cancelled",
            "SpotInstanceRequestId": "sir-08b93456"
        }
    ]
}
```

- Para obtener información sobre la API, consulte CancelSpotInstanceRequests en la Referencia de comandos de la AWS CLI.

`confirm-product-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `confirm-product-instance`.

AWS CLI

Para confirmar la instancia de producto

En este ejemplo, se determina si el código de producto especificado está asociado a la instancia especificada.

Comando:

```
aws ec2 confirm-product-instance --product-code 774F4FF8 --instance-
id i-1234567890abcdef0
```

Salida:

```
{
  "OwnerId": "123456789012"
}
```

- Para obtener información sobre la API, consulte ConfirmProductInstance en la Referencia de comandos de la AWS CLI.

copy-fpga-image

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-fpga-image`.

AWS CLI

Para copiar una imagen de Amazon FPGA

En este ejemplo, se copia la AFI especificada de la región `us-east-1` en la región actual (`eu-west-1`).

Comando:

```
aws ec2 copy-fpga-image --name copy-afi --source-fpga-image-id afi-0d123e123bfc85abc
 --source-region us-east-1 --region eu-west-1
```

Salida:

```
{
  "FpgaImageId": "afi-06b12350a123fbabc"
}
```

- Para obtener información sobre la API, consulte CopyFpgaImage en la Referencia de comandos de la AWS CLI.

copy-image

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-image`.

AWS CLI

Ejemplo 1: copia de una AMI a otra región

En el siguiente ejemplo de `copy-image`, se copia la AMI especificada de la región `us-west-2` en la región `us-east-1` y se agrega una breve descripción.

```
aws ec2 copy-image \
    --region us-east-1 \
    --name ami-name \
    --source-region us-west-2 \
    --source-image-id ami-066877671789bd71b \
    --description "This is my copied image."
```

Salida:

```
{
    "ImageId": "ami-0123456789abcdefg"
}
```

Para obtener más información, consulte Copiar una AMI en la Guía del usuario de Amazon EC2.

Ejemplo 2: copia de una AMI en otra región y cifrado de la instantánea respaldada

En el siguiente comando `copy-image`, se copia la AMI especificada de la región `us-west-2` en la región actual y se usa la clave de KMS especificada para cifrar la instantánea respaldada.

```
aws ec2 copy-image \
    --source-region us-west-2 \
    --name ami-name \
    --source-image-id ami-066877671789bd71b \
    --encrypted \
    --kms-key-id alias/my-kms-key
```

Salida:

```
{
    "ImageId": "ami-0123456789abcdefg"
}
```

Para obtener más información, consulte Copiar una AMI en la Guía del usuario de Amazon EC2.

Ejemplo 3: inclusión de las etiquetas de AMI definidas por el usuario al copiar una AMI

En el siguiente comando `copy-image` se usa el parámetro `--copy-image-tags` para copiar las etiquetas de AMI definidas por el usuario al copiar la AMI.

```
aws ec2 copy-image \
    --region us-east-1 \
    --name ami-name \
    --source-region us-west-2 \
    --source-image-id ami-066877671789bd71b \
    --description "This is my copied image."
    --copy-image-tags
```

Salida:

```
{
    "ImageId": "ami-0123456789abcdefg"
}
```

Para obtener más información, consulte Copiar una AMI en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CopyImage en la Referencia de comandos de la AWS CLI.

`copy-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-snapshot`.

AWS CLI

Ejemplo 1: copia de una instantánea en otra región

En el siguiente ejemplo del comando `copy-snapshot` se copia la instantánea especificada de la región `us-west-2` en la región `us-east-1` y se agrega una breve descripción.

```
aws ec2 copy-snapshot \
    --region us-east-1 \
    --source-region us-west-2 \
    --source-snapshot-id snap-066877671789bd71b \
    --description 'This is my copied snapshot.'
```

Salida:

```
{
    "SnapshotId": "snap-066877671789bd71b"
}
```

Ejemplo 2: copia de una instantánea no cifrada y cifrado de la nueva instantánea

En el siguiente comando `copy-snapshot` se copia la instantánea no cifrada especificada de la región `us-west-2` en la región actual y se usa la clave de KMS especificada para cifrar la nueva instantánea.

```
aws ec2 copy-snapshot \
    --source-region us-west-2 \
    --source-snapshot-id snap-066877671789bd71b \
    --encrypted \
    --kms-key-id alias/my-kms-key
```

Salida:

```
{
    "SnapshotId": "snap-066877671789bd71b"
}
```

Para obtener más información, consulte Copia de una instantánea de Amazon EBS en la Guía del usuario de Amazon EBS.

- Para obtener información sobre la API, consulte CopySnapshot en la Referencia de comandos de la AWS CLI.

`create-capacity-reservation-fleet`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-capacity-reservation-fleet`.

AWS CLI

Para crear una flota de reservas de capacidad

En el siguiente ejemplo de `create-capacity-reservation-fleet` se crea una flota de reservas de capacidad para el tipo de instancia especificado en la solicitud, hasta la capacidad de

destino total especificada. El número de instancias para las que reservará capacidad la flota de reservas de capacidad depende de la capacidad de destino total y de las ponderaciones de los tipos de instancias que especifique en la solicitud. Especifique los tipos de instancias que se van a utilizar y una prioridad para cada uno de los tipos de instancias designados.

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity 24 \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy default \
--end-date 2022-12-31T23:59:59.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

Contenido de `instanceTypeSpecification.json`:

```
[
    {
        "InstanceType": "m5.xlarge",
        "InstancePlatform": "Linux/UNIX",
        "Weight": 3.0,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 1
    }
]
```

Salida:

```
{
    "Status": "submitted",
    "TotalFulfilledCapacity": 0.0,
    "CapacityReservationFleetId": "crf-abcdef01234567890",
    "TotalTargetCapacity": 24
}
```

Para obtener más información sobre flotas de reserva de capacidad, consulte Flotas de reservas de capacidad en la Guía del usuario de Amazon EC2.

Para obtener más información sobre las ponderaciones de los tipos de instancias y la capacidad de destino total, consulte Ponderación de tipo de instancias y Capacidad de destino total en la Guía del usuario de Amazon EC2.

Para obtener más información sobre la designación de prioridades para determinados tipos de instancias, consulte Estrategia de asignación y Prioridad de tipo de instancias en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CreateCapacityReservationFleet en la Referencia de comandos de la AWS CLI.

`create-capacity-reservation`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-capacity-reservation`.

AWS CLI

Ejemplo 1: creación de una reserva de capacidad

En el siguiente ejemplo de `create-capacity-reservation`, se crea una reserva de capacidad en la zona de disponibilidad `eu-west-1a`, en la que puede lanzar tres instancias de `t2.medium` que ejecuten un sistema operativo Linux/Unix. De forma predeterminada, la reserva de capacidad se crea con criterios abiertos de asignación de instancias, no admite el almacenamiento efímero y permanece activa hasta que se cancela manualmente.

```
aws ec2 create-capacity-reservation \
    --availability-zone eu-west-1a \
    --instance-type t2.medium \
    --instance-platform Linux/UNIX \
    --instance-count 3
```

Salida:

```
{
    "CapacityReservation": {
        "CapacityReservationId": "cr-1234abcd56EXAMPLE ",
        "EndDateType": "unlimited",
        "AvailabilityZone": "eu-west-1a",
        "InstanceMatchCriteria": "open",
        "EphemeralStorage": false,
        "CreateDate": "2019-08-16T09:27:35.000Z",
        "AvailableInstanceCount": 3,
        "InstancePlatform": "Linux/UNIX",
        "TotalInstanceCount": 3,
        "State": "active",
        "Tenancy": "default",
```

```
        "EbsOptimized": false,
        "InstanceType": "t2.medium"
    }
}
```

Ejemplo 2: creación de una reserva de capacidad que finalice automáticamente en una fecha y hora especificadas

En el siguiente ejemplo de `create-capacity-reservation`, se crea una reserva de capacidad en la zona de disponibilidad `eu-west-1a`, en la que puede lanzar tres instancias de `m5.large` que ejecuten un sistema operativo Linux/Unix. Esta reserva de capacidad finaliza automáticamente el 31 de agosto de 2019 a las 23:59:59.

```
aws ec2 create-capacity-reservation \
    --availability-zone eu-west-1a \
    --instance-type m5.large \
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --end-date-type limited \
    --end-date 2019-08-31T23:59:59Z
```

Salida:

```
{
    "CapacityReservation": {
        "CapacityReservationId": "cr-1234abcd56EXAMPLE ",
        "EndDateType": "limited",
        "AvailabilityZone": "eu-west-1a",
        "EndDate": "2019-08-31T23:59:59.000Z",
        "InstanceMatchCriteria": "open",
        "EphemeralStorage": false,
        "CreateDate": "2019-08-16T10:15:53.000Z",
        "AvailableInstanceCount": 3,
        "InstancePlatform": "Linux/UNIX",
        "TotalInstanceCount": 3,
        "State": "active",
        "Tenancy": "default",
        "EbsOptimized": false,
        "InstanceType": "m5.large"
    }
}
```

Ejemplo 3: creación de una reserva de capacidad que solo acepta lanzamientos de instancias específicas

En el siguiente ejemplo de `create-capacity-reservation`, se crea una reserva de capacidad que solo acepta lanzamientos de instancias específicas.

```
aws ec2 create-capacity-reservation \
    --availability-zone eu-west-1a \
    --instance-type m5.large \
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Salida:

```
{
    "CapacityReservation": {
        "CapacityReservationId": "cr-1234abcd56EXAMPLE ",
        "EndDateType": "unlimited",
        "AvailabilityZone": "eu-west-1a",
        "InstanceMatchCriteria": "targeted",
        "EphemeralStorage": false,
        "CreateDate": "2019-08-16T10:21:57.000Z",
        "AvailableInstanceCount": 3,
        "InstancePlatform": "Linux/UNIX",
        "TotalInstanceCount": 3,
        "State": "active",
        "Tenancy": "default",
        "EbsOptimized": false,
        "InstanceType": "m5.large"
    }
}
```

Para obtener más información, consulte Creación de una reserva de capacidad en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CreateCapacityReservation en la Referencia de comandos de la AWS CLI.

`create-carrier-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-carrier-gateway`.

AWS CLI

Para crear una puerta de enlace de operador

En el siguiente ejemplo de `create-carrier-gateway`, se crea una puerta de enlace de operador para la VPC especificada.

```
aws ec2 create-carrier-gateway \
    --vpc-id vpc-0c529aEXAMPLE1111
```

Salida:

```
{
    "CarrierGateway": {
        "CarrierGatewayId": "cagw-0465cdEXAMPLE1111",
        "VpcId": "vpc-0c529aEXAMPLE1111",
        "State": "pending",
        "OwnerId": "123456789012"
    }
}
```

Para obtener más información, consulte Carrier gateways en la Guía del usuario de AWS Wavelength.

- Para obtener información sobre la API, consulte CreateCarrierGateway en la Referencia de comandos de la AWS CLI.

`create-client-vpn-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-client-vpn-endpoint`.

AWS CLI

Para crear un punto de conexión de Client VPN

En el siguiente ejemplo de `create-client-vpn-endpoint`, se crea un punto de conexión de Client VPN que utiliza la autenticación mutua y especifica un valor para el bloque de CIDR del cliente.

```
aws ec2 create-client-vpn-endpoint \
    --client-cidr-block "172.31.0.0/16" \
```

```
    --server-certificate-arn arn:aws:acm:ap-south-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:ap-
south-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
    --connection-log-options Enabled=false
```

Salida:

```
{
    "ClientVpnEndpointId": "cvpn-endpoint-123456789123abcde",
    "Status": {
        "Code": "pending-associate"
    },
    "DnsName": "cvpn-endpoint-123456789123abcde.prod.clientvpn.ap-
south-1.amazonaws.com"
}
```

Para obtener más información, consulte Client VPN Endpoints en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte CreateClientVpnEndpoint en la Referencia de comandos de la AWS CLI.

`create-client-vpn-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-client-vpn-route`.

AWS CLI

Para crear una ruta para un punto de conexión de Client VPN

En el siguiente ejemplo de `create-client-vpn-route`, se agrega una ruta a internet (`0.0.0.0/0`) para la subred especificada del punto de conexión de Client VPN.

```
aws ec2 create-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde \
    --destination-cidr-block 0.0.0.0/0  \
    --target-vpc-subnet-id subnet-0123456789abcabca
```

Salida:

```
{
    "Status": {
        "Code": "creating"
    }
}
```

Para obtener más información, consulte Routes en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte CreateClientVpnRoute en la Referencia de comandos de la AWS CLI.

`create-coip-cidr`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-coip-cidr`.

AWS CLI

Para crear un rango de direcciones IP propiedad del cliente (CoIP

En el siguiente ejemplo de `create-coip-cidr`, se crea el rango especificado de direcciones de CoIP en el grupo de CoIP especificado.

```
aws ec2 create-coip-cidr \
    --cidr 15.0.0.0/24 \
    --coip-pool-id ipv4pool-coip-1234567890abcdefg
```

Salida:

```
{
    "CoipCidr": {
        "Cidr": "15.0.0.0/24",
        "CoipPoolId": "ipv4pool-coip-1234567890abcdefg",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890"
    }
}
```

Para obtener más información, consulte Direcciones IP propiedad del cliente en la Guía del usuario de AWS.

- Para obtener información sobre la API, consulte CreateCoipCidr en la Referencia de comandos de la AWS CLI.

`create-coip-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-coip-pool`.

AWS CLI

Para crear un grupo de direcciones IP propiedad del cliente (CoIP

En el siguiente ejemplo de `create-coip-pool`, se crea un grupo de CoIP para las direcciones de CoIP en la tabla de enrutamiento de puerta de enlace local especificada.

```
aws ec2 create-coip-pool \
    --local-gateway-route-table-id lgw-rtb-abcdefg1234567890
```

Salida:

```
{
    "CoipPool": {
        "PoolId": "ipv4pool-coip-1234567890abcdefg",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890",
        "PoolArn": "arn:aws:ec2:us-west-2:123456789012:coip-pool/ipv4pool-
coip-1234567890abcdefg"
    }
}
```

Para obtener más información, consulte Direcciones IP propiedad del cliente en la Guía del usuario de AWS.

- Para obtener información sobre la API, consulte CreateCoipPool en la Referencia de comandos de la AWS CLI.

`create-customer-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-customer-gateway`.

AWS CLI

Para crear una puerta de enlace de cliente

En este ejemplo se crea una puerta de enlace de cliente con la dirección IP especificada para su interfaz exterior.

Comando:

```
aws ec2 create-customer-gateway --type ipsec.1 --public-ip 12.1.2.3 --bgp-asn 65534
```

Salida:

```
{
    "CustomerGateway": {
        "CustomerGatewayId": "cgw-0e11f167",
        "IpAddress": "12.1.2.3",
        "State": "available",
        "Type": "ipsec.1",
        "BgpAsn": "65534"
    }
}
```

- Para obtener información sobre la API, consulte CreateCustomerGateway en la Referencia de comandos de la AWS CLI.

`create-default-subnet`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-default-subnet`.

AWS CLI

Para crear una subred predeterminada

En este ejemplo se crea una subred predeterminada en la zona de disponibilidad `us-east-2a`.

Comando:

```
 aws ec2 create-default-subnet --availability-zone us-east-2a

{
   "Subnet": {
       "AvailabilityZone": "us-east-2a",
       "Tags": [],
       "AvailableIpAddressCount": 4091,
       "DefaultForAz": true,
       "Ipv6CidrBlockAssociationSet": [],
       "VpcId": "vpc-1a2b3c4d",
       "State": "available",
```

```
        "MapPublicIpOnLaunch": true,
        "SubnetId": "subnet-1122aabb",
        "CidrBlock": "172.31.32.0/20",
        "AssignIpv6AddressOnCreation": false
    }
}
```

- Para obtener información sobre la API, consulte CreateDefaultSubnet en la Referencia de comandos de la AWS CLI.

`create-default-vpc`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-default-vpc`.

AWS CLI

Para crear una VPC predeterminada

En este ejemplo se crea una VPC predeterminada.

Comando:

```
aws ec2 create-default-vpc
```

Salida:

```
{
    "Vpc": {
        "VpcId": "vpc-8eaae5ea",
        "InstanceTenancy": "default",
        "Tags": [],
        "Ipv6CidrBlockAssociationSet": [],
        "State": "pending",
        "DhcpOptionsId": "dopt-af0c32c6",
        "CidrBlock": "172.31.0.0/16",
        "IsDefault": true
    }
}
```

- Para obtener información sobre la API, consulte CreateDefaultVpc en la Referencia de comandos de la AWS CLI.

`create-dhcp-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-dhcp-options`.

AWS CLI

Para crear un conjunto de opciones de DHCP

En el siguiente ejemplo de `create-dhcp-options`, se crea un conjunto de opciones de DHCP que especifica el nombre de dominio, los servidores de nombres de dominio y el tipo de nodo de NetBIOS.

```
aws ec2 create-dhcp-options \
    --dhcp-configuration \
        "Key=domain-name-servers,Values=10.2.5.1,10.2.5.2" \
        "Key=domain-name,Values=example.com" \
        "Key=netbios-node-type,Values=2"
```

Salida:

```
{
    "DhcpOptions": {
        "DhcpConfigurations": [
            {
                "Key": "domain-name",
                "Values": [
                    {
                        "Value": "example.com"
                    }
                ]
            },
            {
                "Key": "domain-name-servers",
                "Values": [
                    {
                        "Value": "10.2.5.1"
                    },
                    {
                        "Value": "10.2.5.2"
                    }
                ]
            },
            {
```

```
                "Key": "netbios-node-type",
                "Values": [
                    {
                        "Value": "2"
                    }
                ]
            }
        ],
        "DhcpOptionsId": "dopt-06d52773eff4c55f3"
    }
}
```

- Para obtener información sobre la API, consulte CreateDhcpOptions en la Referencia de comandos de la AWS CLI.

`create-egress-only-internet-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-egress-only-internet-gateway`.

AWS CLI

Para crear una puerta de enlace de Internet de solo salida

En este ejemplo, se crea una puerta de enlace de Internet de solo salida para la VPC especificada.

Comando:

```
aws ec2 create-egress-only-internet-gateway --vpc-id vpc-0c62a468
```

Salida:

```
{
  "EgressOnlyInternetGateway": {
      "EgressOnlyInternetGatewayId": "eigw-015e0e244e24dfe8a",
      "Attachments": [
          {
              "State": "attached",
              "VpcId": "vpc-0c62a468"
          }
      ]
```

```
  }
}
```

- Para obtener información sobre la API, consulte CreateEgressOnlyInternetGateway en la Referencia de comandos de la AWS CLI.

`create-fleet`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-fleet`.

AWS CLI

Ejemplo 1: creación de una flota de EC2 que lance instancias de spot como modelo de compra predeterminado

En el siguiente ejemplo de `create-fleet`, se crea una flota de EC2 mediante los parámetros mínimos requeridos para lanzar una flota: una plantilla de lanzamiento, la capacidad de destino y el modelo de compra predeterminado. La plantilla de inicialización se identifica mediante su ID y número de versión. La capacidad de destino de la flota es de dos instancias y el modelo de compra predeterminado es `spot`, lo que da lugar a que la flota lance dos instancias de spot.

Al crear una flota de EC2, use un archivo JSON para especificar la información sobre las instancias que se van a lanzar.

```
aws ec2 create-fleet \
    --cli-input-json file://file_name.json
```

Contenido de file_name.json:

```
{
    "LaunchTemplateConfigs": [
    {
        "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0e8c754449b27161c",
        "Version": "1"
        }
    }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "spot"
```

```
    }
}
```

Salida:

```
{
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

Ejemplo 2: creación de una flota de EC2 que lance instancias bajo demanda como modelo de compra predeterminado

En el siguiente ejemplo de `create-fleet`, se crea una flota de EC2 mediante los parámetros mínimos requeridos para lanzar una flota: una plantilla de lanzamiento, la capacidad de destino y el modelo de compra predeterminado. La plantilla de inicialización se identifica mediante su ID y número de versión. La capacidad de destino de la flota es de dos instancias y la opción de compra predeterminada es `on-demand`, lo que da lugar a que la flota lance dos instancias bajo demanda.

Al crear una flota de EC2, use un archivo JSON para especificar la información sobre las instancias que se van a lanzar.

```
aws ec2 create-fleet \
    --cli-input-json file://file_name.json
```

Contenido de file_name.json:

```
{
    "LaunchTemplateConfigs": [
    {
        "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0e8c754449b27161c",
        "Version": "1"
        }
    }
    ],
    "TargetCapacitySpecification": {
    "TotalTargetCapacity": 2,
    "DefaultTargetCapacityType": "on-demand"
    }
}
```

Salida:

```
{
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

Ejemplo 3: creación de una flota de EC2 que lance instancias bajo demanda como la capacidad principal

En el siguiente ejemplo de `create-fleet`, se crea una flota de EC2 que especifica la capacidad de destino total de 2 instancias para la flota y una capacidad de destino de una instancia bajo demanda. El modelo de compra predeterminado es `spot`. La flota lanza una instancia bajo demanda según lo especificado, pero ha de lanzar otra instancia más para cubrir la capacidad de destino total. El modelo de compra aplicado a la diferencia se calcula de la siguiente manera: `TotalTargetCapacity` – `OnDemandTargetCapacity` = `DefaultTargetCapacityType`, lo que da lugar a que la flota lance una instancia de spot.

Al crear una flota de EC2, use un archivo JSON para especificar la información sobre las instancias que se van a lanzar.

```
aws ec2 create-fleet \
    --cli-input-json file://file_name.json
```

Contenido de file_name.json:

```
{
    "LaunchTemplateConfigs": [
    {
        "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0e8c754449b27161c",
        "Version": "1"
        }
    }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "OnDemandTargetCapacity":1,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Salida:

```
{
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

Ejemplo 4: creación de una flota de EC2 que lance instancias de spot utilizando la estrategia de asignación de precios más bajos

Si la estrategia de asignación de instancias de spot no se especifica, se usa la estrategia predeterminada, que es `lowest-price`. En el siguiente ejemplo de `create-fleet`, se crea una flota de EC2 mediante la estrategia de asignación `lowest-price`. Las tres especificaciones de inicialización, que invalidan la plantilla de inicialización, tienen tipos de instancias diferentes, pero las mismas capacidad ponderada y subred. La capacidad de destino total es de dos instancias y el modelo de compra predeterminado es `spot`. La flota de EC2 inicia 2 instancias de spot empleando el tipo de instancia indicado en la especificación de inicialización que tiene el precio más bajo.

Al crear una flota de EC2, use un archivo JSON para especificar la información sobre las instancias que se van a lanzar.

```
aws ec2 create-fleet \
    --cli-input-json file://file_name.jsonContents of file_name.json::

{
    "LaunchTemplateConfigs": [
    {
        "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0e8c754449b27161c",
        "Version": "1"
        },
        "Overrides": [
            {
                "InstanceType": "c4.large",
                "WeightedCapacity": 1,
                "SubnetId": "subnet-a4f6c5d3"
            },
            {
                "InstanceType": "c3.large",
                "WeightedCapacity": 1,
                "SubnetId": "subnet-a4f6c5d3"
```

```
            },
            {
                "InstanceType": "c5.large",
                "WeightedCapacity": 1,
                "SubnetId": "subnet-a4f6c5d3"
            }
        ]
    }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "spot"

  }
}
```

Salida:

```
{
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

- Para obtener información sobre la API, consulte CreateFleet en la Referencia de comandos de la AWS CLI.

`create-flow-logs`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-flow-logs`.

AWS CLI

Ejemplo 1: creación de un registro de flujo

En el siguiente ejemplo de `create-flow-logs`, se crea un registro de flujo que captura todo el tráfico rechazado para la subred especificada. Los registros de flujo se envían a un grupo de registro de registros de CloudWatch mediante los permisos del rol de IAM especificado.

```
aws ec2 create-flow-logs \
    --resource-type NetworkInterface \
    --resource-ids eni-11223344556677889 \
    --traffic-type REJECT \
```

```
    --log-group-name my-flow-logs \
    --deliver-logs-permission-arn arn:aws:iam::123456789101:role/publishFlowLogs
```

Salida:

```
{
    "ClientToken": "so0eNA2uSHUNlHI0S2cJ305GuIX1CezaRdGtexample",
    "FlowLogIds": [
        "fl-12345678901234567"
    ],
    "Unsuccessful": []
}
```

Para obtener más información, consulte Registros de flujo de VPC en la Guía del usuario de Amazon VPC.

Ejemplo 2: creación de un registro de flujo con un formato personalizado

En el siguiente ejemplo de `create-flow-logs`, se crea un registro de flujo que captura todo el tráfico de la VPC especificada y entrega los registros de flujo a un bucket de Amazon S3. El parámetro `--log-format` especifica un formato personalizado para las entradas de registros de flujo. Para ejecutar este comando en Windows, cambie la comillas simples (') por comillas dobles (").

```
aws ec2 create-flow-logs \
    --resource-type VPC \
    --resource-ids vpc-00112233344556677 \
    --traffic-type ALL \
    --log-destination-type s3 \
    --log-destination arn:aws:s3:::flow-log-bucket/my-custom-flow-logs/ \
    --log-format '${version} ${vpc-id} ${subnet-id} ${instance-id} ${srcaddr}
 ${dstaddr} ${srcport} ${dstport} ${protocol} ${tcp-flags} ${type} ${pkt-srcaddr}
 ${pkt-dstaddr}'
```

Para obtener más información, consulte Registros de flujo de VPC en la Guía del usuario de Amazon VPC.

Ejemplo 3: creación de un registro de flujo con un intervalo de agregación máximo de un minuto

En el siguiente ejemplo de `create-flow-logs`, se crea un registro de flujo que captura todo el tráfico de la VPC especificada y entrega los registros de flujo a un bucket de Amazon S3. El

parámetro `--max-aggregation-interval` especifica un intervalo de agregación máximo de 60 segundos (1 minuto).

```
aws ec2 create-flow-logs \
    --resource-type VPC \
    --resource-ids vpc-00112233344556677 \
    --traffic-type ALL \
    --log-destination-type s3 \
    --log-destination arn:aws:s3:::flow-log-bucket/my-custom-flow-logs/ \
    --max-aggregation-interval 60
```

Para obtener más información, consulte Registros de flujo de VPC en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte CreateFlowLogs en la Referencia de comandos de la AWS CLI.

`create-fpga-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-fpga-image`.

AWS CLI

Para crear una imagen de Amazon FPGA

En este ejemplo, se crea una AFI a partir del tarball especificado en el bucket especificado.

Comando:

```
aws ec2 create-fpga-image --name my-afi --description test-afi --input-storage-
location Bucket=my-fpga-bucket,Key=dcp/17_12_22-103226.Developer_CL.tar --logs-
storage-location Bucket=my-fpga-bucket,Key=logs
```

Salida:

```
{
  "FpgaImageId": "afi-0d123e123bfc85abc",
  "FpgaImageGlobalId": "agfi-123cb27b5e84a0abc"
}
```

- Para obtener información sobre la API, consulte CreateFpgaImage en la Referencia de comandos de la AWS CLI.

`create-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-image`.

AWS CLI

Ejemplo 1: creación de una AMI a partir de una instancia con respaldo de Amazon EBS

En el siguiente ejemplo de `create-image`, se crea una AMI a partir de la instancia especificada.

```
aws ec2 create-image \
    --instance-id i-1234567890abcdef0 \
    --name "My server" \
    --description "An AMI for my server"
```

Salida:

```
{
    "ImageId": "ami-abcdef01234567890"
}
```

Para obtener más información sobre cómo especificar una asignación de dispositivos de bloques para la AMI, consulte Asignaciones de dispositivos de bloques para volúmenes en instancias de Amazon EC2 en la Guía del usuario de Amazon EC2.

Ejemplo 2: creación de una AMI a partir de una instancia con respaldo de Amazon EBS sin reinicio

En el siguiente ejemplo de `create-image`, se crea una AMI y se establece el parámetro --no-reboot para que la instancia no se reinicie antes de crear la imagen.

```
aws ec2 create-image \
    --instance-id i-1234567890abcdef0 \
    --name "My server" \
    --no-reboot
```

Salida:

```
{
    "ImageId": "ami-abcdef01234567890"
}
```

Para obtener más información sobre cómo especificar una asignación de dispositivos de bloques para la AMI, consulte Asignaciones de dispositivos de bloques para volúmenes en instancias de Amazon EC2 en la Guía del usuario de Amazon EC2.

Ejemplo 3: etiquetado de una AMI y de las instantáneas al crearlas

En el siguiente ejemplo de `create-image`, se crea una AMI y se etiquetan la propia AMI y las instantáneas con la misma etiqueta `cost-center=cc123`

```
aws ec2 create-image \
    --instance-id i-1234567890abcdef0 \
    --name "My server" \
    --tag-specifications "ResourceType=image,Tags=[{Key=cost-
center,Value=cc123}]" "ResourceType=snapshot,Tags=[{Key=cost-center,Value=cc123}]"
```

Salida:

```
{
    "ImageId": "ami-abcdef01234567890"
}
```

Para obtener más información sobre cómo etiquetar los recursos al crearlos, consulte Etiquetar los recursos en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CreateImage en la Referencia de comandos de la AWS CLI.

`create-instance-connect-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-instance-connect-endpoint`.

AWS CLI

Para crear un punto de conexión de EC2 Instance Connect

En el siguiente ejemplo de `create-instance-connect-endpoint`, se crea un punto de conexión de EC2 Instance Connect en la subred especificada.

```
aws ec2 create-instance-connect-endpoint \
    --region us-east-1 \
```

```
    --subnet-id subnet-0123456789example
```

Salida:

```
{
    "VpcId": "vpc-0123abcd",
    "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
    "AvailabilityZone": "us-east-1a",
    "NetworkInterfaceIds": [
        "eni-0123abcd"
    ],
    "PreserveClientIp": true,
    "Tags": [],
    "FipsDnsName": "eice-0123456789example.0123abcd.fips.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com",
    "StateMessage": "",
    "State": "create-complete",
    "DnsName": "eice-0123456789example.0123abcd.ec2-instance-connect-endpoint.us-
east-1.amazonaws.com",
    "SubnetId": "subnet-0123abcd",
    "OwnerId": "111111111111",
    "SecurityGroupIds": [
        "sg-0123abcd"
    ],
    "InstanceConnectEndpointId": "eice-0123456789example",
    "CreatedAt": "2023-04-07T15:43:53.000Z"
}
```

Para obtener más información, consulte Creación de un punto de conexión de EC2 Instance Connect en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CreateInstanceConnectEndpoint en la Referencia de comandos de la AWS CLI.

`create-instance-event-window`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-instance-event-window`.

AWS CLI

Ejemplo 1: creación de un período de evento con un intervalo de tiempo

En el siguiente ejemplo de `create-instance-event-window`, se crea un período de evento con un intervalo de tiempo. No puede especificar el parámetro `cron-expression`.

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8 \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Salida:

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Para conocer las restricciones de los períodos de eventos, consulte Consideraciones en la sección sobre eventos programados de la Guía del usuario de Amazon EC2.

Ejemplo 2: creación de un período de evento con una expresión cron

En el siguiente ejemplo de `create-instance-event-window`, se crea un período de evento con una expresión cron. No puede especificar el parámetro `time-range`.

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --cron-expression "* 21-23 * * 2,3" \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Salida:

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Para conocer las restricciones de los períodos de eventos, consulte Consideraciones en la sección sobre eventos programados de la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CreateInstanceEventWindow en la Referencia de comandos de la AWS CLI.

`create-instance-export-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-instance-export-task`.

AWS CLI

Para exportar una instancia

En este ejemplo de comando, se crea una tarea para exportar la instancia i-1234567890abcdef0 al bucket de Amazon S3 myexportbucket.

Comando:

```
aws ec2 create-instance-export-task --description "RHEL5 instance" --
instance-id i-1234567890abcdef0 --target-environment vmware --export-to-s3-
task DiskImageFormat=vmdk,ContainerFormat=ova,S3Bucket=myexportbucket,S3Prefix=RHEL5
```

Salida:

```
{
    "ExportTask": {
        "State": "active",
        "InstanceExportDetails": {
            "InstanceId": "i-1234567890abcdef0",
            "TargetEnvironment": "vmware"
        },
        "ExportToS3Task": {
            "S3Bucket": "myexportbucket",
            "S3Key": "RHEL5export-i-fh8sjjsq.ova",
            "DiskImageFormat": "vmdk",
            "ContainerFormat": "ova"
        },
        "Description": "RHEL5 instance",
        "ExportTaskId": "export-i-fh8sjjsq"
    }
}
```

- Para obtener información sobre la API, consulte CreateInstanceExportTask en la Referencia de comandos de la AWS CLI.

`create-internet-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-internet-gateway`.

AWS CLI

Para crear una puerta de enlace de Internet

En el siguiente ejemplo de `create-internet-gateway`, se crea una puerta de enlace de Internet con la etiqueta `Name=my-igw`.

```
aws ec2 create-internet-gateway \
    --tag-specifications ResourceType=internet-gateway,Tags=[{Key=Name,Value=my-
igw}]
```

Salida:

```
{
    "InternetGateway": {
        "Attachments": [],
        "InternetGatewayId": "igw-0d0fb496b3994d755",
        "OwnerId": "123456789012",
        "Tags": [
            {
                "Key": "Name",
                "Value": "my-igw"
            }
        ]
    }
}
```

Para obtener más información, consulte Puertas de enlace de Internet en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte CreateInternetGateway en la Referencia de comandos de la AWS CLI.

`create-ipam-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-ipam-pool`.

AWS CLI

Para crear un grupo de IPAM

En el siguiente ejemplo de `create-ipam-pool`, se crea un grupo de IPAM.

(Linux):

```
aws ec2 create-ipam-pool \
    --ipam-scope-id ipam-scope-02fc38cd4c48e7d38 \
    --address-family ipv4 \
    --auto-import \
    --allocation-min-netmask-length 16 \
    --allocation-max-netmask-length 26 \
    --allocation-default-netmask-length 24 \
    --allocation-resource-tags "Key=Environment,Value=Preprod" \
```

```
    --tag-specifications 'ResourceType=ipam-pool,Tags=[{Key=Name,Value="Preprod
 pool"}]'
```

(Windows):

```
aws ec2 create-ipam-pool ^
    --ipam-scope-id ipam-scope-02fc38cd4c48e7d38 ^
    --address-family ipv4 ^
    --auto-import ^
    --allocation-min-netmask-length 16 ^
    --allocation-max-netmask-length 26 ^
    --allocation-default-netmask-length 24 ^
    --allocation-resource-tags "Key=Environment,Value=Preprod" ^
    --tag-specifications ResourceType=ipam-pool,Tags=[{Key=Name,Value="Preprod
 pool"}]
```

Salida:

```
{
    "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0533048da7d823723",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0533048da7d823723",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-02fc38cd4c48e7d38",
        "IpamScopeType": "private",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-08440e7a3acde3908",
        "IpamRegion": "us-east-1",
        "Locale": "None",
        "PoolDepth": 1,
        "State": "create-in-progress",
        "AutoImport": true,
        "AddressFamily": "ipv4",
        "AllocationMinNetmaskLength": 16,
        "AllocationMaxNetmaskLength": 26,
        "AllocationDefaultNetmaskLength": 24,
        "AllocationResourceTags": [
            {
                "Key": "Environment",
                "Value": "Preprod"
            }
        ],
```

```
        "Tags": [
            {
                "Key": "Name",
                "Value": "Preprod pool"
            }
        ]
    }
}
```

Para obtener más información, consulte Planificar el aprovisionamiento de direcciones IP en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte CreateIpamPool en la Referencia de comandos de la AWS CLI.

`create-ipam-resource-discovery`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-ipam-resource-discovery`.

AWS CLI

Para crear una detección de recursos

En este ejemplo, usted es un administrador delegado de IPAM y desea crear y compartir una detección de recursos con el administrador de IPAM de otra organización de AWS para que el administrador de esa otra organización pueda administrar y supervisar las direcciones IP de esos recursos de su organización.

Importante

En este ejemplo se incluyen las opciones `--region` y `--operating-regions` porque, si bien son opcionales, deben configurarse de una manera determinada para integrar correctamente una detección de recursos con un IPAM. * `--operating-regions` debe coincidir con las regiones en las que se encuentran los recursos que IPAM deba detectar. Si hay regiones cuyas direcciones IP no desea que IPAM administre (por ejemplo, por motivos de cumplimiento), no las incluya. * `--region` debe coincidir con la región de origen del IPAM al que desee asociarla. Debe crear la detección de recursos en la misma región en la que se ha creado el IPAM. Por ejemplo, si el IPAM al que se va a asociar se ha creado en us-east-1, incluya `--region us-east-1` en la solicitud. Si no se especifican, las opciones `--region` y `--operating-regions` se establecerán de forma predeterminada en la región en la que se ejecuta el comando.

En este ejemplo, las regiones operativas del IPAM con las que se va a realizar la integración son `us-west-1`, `us-west-2` y `ap-south-1`. Al detectar la detección de recursos, es preciso que IPAM detecte las direcciones IP de los recursos en `us-west-1` y `us-west-2`, pero no en `ap-south-1`. Por lo tanto, solo incluimos `--operating-regions RegionName='us-west-1' RegionName='us-west-2'` en la solicitud.

En el siguiente ejemplo de `create-ipam-resource-discovery`, se crea una detección de recursos de IPAM.

```
aws ec2 create-ipam-resource-discovery \
    --description 'Example-resource-discovery' \
    --tag-specifications 'ResourceType=ipam-resource-discovery,Tags=[{Key=cost-center,Value=cc123}]' \
    --operating-regions RegionName='us-west-1' RegionName='us-west-2' \
    --region us-east-1
```

Salida:

```
{
    "IpamResourceDiscovery":{
        "OwnerId": "149977607591",
        "IpamResourceDiscoveryId": "ipam-res-disco-0257046d8aa78b8bc",
        "IpamResourceDiscoveryArn": "arn:aws:ec2::149977607591:ipam-resource-discovery/ipam-res-disco-0257046d8aa78b8bc",
        "IpamResourceDiscoveryRegion": "us-east-1",
        "Description": "'Example-resource-discovery'",
        "OperatingRegions":[
            {"RegionName": "us-west-1"},
            {"RegionName": "us-west-2"},
            {"RegionName": "us-east-1"}
        ],
        "IsDefault": false,
        "State": "create-in-progress",
        "Tags": [
            {
                "Key": "cost-center",
                "Value": "cc123"
            }
        ]
}
```

Una vez que haya creado una detección de recursos, puede ser conveniente compartirla con otro administrador delegado de IPAM. Esto se puede hacer con create-resource-share. Para obtener más información, consulte Integración de IPAM con cuentas ajenas a su organización en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte CreateIpamResourceDiscovery en la Referencia de comandos de la AWS CLI.

`create-ipam-scope`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-ipam-scope`.

AWS CLI

Para crear un ámbito de IPAM

En el siguiente ejemplo de `create-ipam-scope`, se crea un ámbito de IPAM.

(Linux):

```
aws ec2 create-ipam-scope \
    --ipam-id ipam-08440e7a3acde3908 \
    --description "Example description" \
    --tag-specifications 'ResourceType=ipam-scope,Tags=[{Key=Name,Value="Example
 name value"}]'
```

(Windows):

```
aws ec2 create-ipam-scope ^
    --ipam-id ipam-08440e7a3acde3908 ^
    --description "Example description" ^
    --tag-specifications ResourceType=ipam-scope,Tags=[{Key=Name,Value="Example name
 value"}]
```

Salida:

```
{
    "IpamScope": {
        "OwnerId": "123456789012",
        "IpamScopeId": "ipam-scope-01c1ebab2b63bd7e4",
```

```
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-01c1ebab2b63bd7e4",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-08440e7a3acde3908",
        "IpamRegion": "us-east-1",
        "IpamScopeType": "private",
        "IsDefault": false,
        "Description": "Example description",
        "PoolCount": 0,
        "State": "create-in-progress",
        "Tags": [
            {
                "Key": "Name",
                "Value": "Example name value"
            }
        ]
    }
}
```

Para obtener más información, consulte Creación de alcances adicionales en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte CreateIpamScope en la Referencia de comandos de la AWS CLI.

`create-ipam`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-ipam`.

AWS CLI

Para crear un IPAM

En el siguiente ejemplo de `create-ipam`, se crea un IPAM.

(Linux):

```
aws ec2 create-ipam \
    --description "Example description" \
    --operating-regions "RegionName=us-east-2" "RegionName=us-west-1" \
    --tag-specifications 'ResourceType=ipam,Tags=[{Key=Name,Value=ExampleIPAM}]'
```

(Windows):

```
aws ec2 create-ipam ^
    --description "Example description" ^
    --operating-regions "RegionName=us-east-2" "RegionName=us-west-1" ^
    --tag-specifications ResourceType=ipam,Tags=[{Key=Name,Value=ExampleIPAM}]
```

Salida:

```
{
    "Ipam": {
        "OwnerId": "123456789012",
        "IpamId": "ipam-036486dfa6af58ee0",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-036486dfa6af58ee0",
        "IpamRegion": "us-east-1",
        "PublicDefaultScopeId": "ipam-scope-071b8042b0195c183",
        "PrivateDefaultScopeId": "ipam-scope-0807405dece705a30",
        "ScopeCount": 2,
        "OperatingRegions": [
            {
                "RegionName": "us-east-2"
            },
            {
                "RegionName": "us-west-1"
            },
            {
                "RegionName": "us-east-1"
            }
        ],
        "State": "create-in-progress",
        "Tags": [
            {
                "Key": "Name",
                "Value": "ExampleIPAM"
            }
        ]
    }
}
```

Para obtener más información, consulte Creación de un IPAM en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte CreateIpam en la Referencia de comandos de la AWS CLI.

`create-key-pair`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-key-pair`.

AWS CLI

Crear un par de claves

En este ejemplo, se crea un par de claves denominado `MyKeyPair`.

Comando:

```
aws ec2 create-key-pair --key-name MyKeyPair
```

El resultado es una versión ASCII de la clave privada y la huella digital de la clave. Debe guardar la clave en un archivo.

Para obtener más información, consulte Uso del par de claves en la Guía del usuario de la Interfaz de la línea de comandos de AWS.

- Para obtener información sobre la API, consulte CreateKeyPair en la Referencia de comandos de la AWS CLI.

`create-launch-template-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-launch-template-version`.

AWS CLI

Para crear una versión de plantilla de lanzamiento

En este ejemplo se crea una nueva versión de plantilla de lanzamiento basada en la versión 1 de la plantilla de lanzamiento y se especifica un ID de AMI diferente.

Comando:

```
aws ec2 create-launch-template-version --launch-template-id lt-0abcd290751193123
 --version-description WebVersion2 --source-version 1 --launch-template-data
 '{"ImageId":"ami-c998b6b2"}'
```

Salida:

```
{
  "LaunchTemplateVersion": {
      "VersionDescription": "WebVersion2",
      "LaunchTemplateId": "lt-0abcd290751193123",
      "LaunchTemplateName": "WebServers",
      "VersionNumber": 2,
      "CreatedBy": "arn:aws:iam::123456789012:root",
      "LaunchTemplateData": {
          "ImageId": "ami-c998b6b2",
          "InstanceType": "t2.micro",
          "NetworkInterfaces": [
              {
                  "Ipv6Addresses": [
                      {
                          "Ipv6Address": "2001:db8:1234:1a00::123"
                      }
                  ],
                  "DeviceIndex": 0,
                  "SubnetId": "subnet-7b16de0c",
                  "AssociatePublicIpAddress": true
              }
          ]
      },
      "DefaultVersion": false,
      "CreateTime": "2017-12-01T13:35:46.000Z"
  }
}
```

- Para obtener información sobre la API, consulte CreateLaunchTemplateVersion en la Referencia de comandos de la AWS CLI.

`create-launch-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-launch-template`.

AWS CLI

Ejemplo 1: Crear una plantilla de lanzamiento

En el siguiente ejemplo de `create-launch-template`, se crea una plantilla de lanzamiento que especifica la subred en la que se lanza la instancia, se asigna una dirección IP pública y una dirección IPv6 a la instancia y se crea una etiqueta para la instancia.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --version-description WebVersion1 \
    --launch-template-data '{"NetworkInterfaces":
[{"AssociatePublicIpAddress":true,"DeviceIndex":0,"Ipv6AddressCount":1,"SubnetId":"subnet-7b
[{"ResourceType":"instance","Tags":[{"Key":"purpose","Value":"webserver"}]}]}'
```

Salida:

```
{
    "LaunchTemplate": {
        "LatestVersionNumber": 1,
        "LaunchTemplateId": "lt-01238c059e3466abc",
        "LaunchTemplateName": "TemplateForWebServer",
        "DefaultVersionNumber": 1,
        "CreatedBy": "arn:aws:iam::123456789012:user/Bob",
        "CreateTime": "2019-01-27T09:13:24.000Z"
    }
}
```

Para obtener más información, consulte Lanzamiento de una instancia desde una plantilla de lanzamiento en la Guía del usuario de Amazon Elastic Compute Cloud. Para obtener información acerca de cómo citar parámetros con formato JSON, consulte Entrecomillado de cadenas en la Guía del usuario de la Interfaz de la línea de comandos de AWS.

Ejemplo 2: Crear una plantilla de lanzamiento para Amazon EC2 Auto Scaling

En el siguiente ejemplo de `create-launch-template`, se crea una plantilla de lanzamiento con varias etiquetas y una asignación de dispositivos de bloques para especificar un volumen de EBS adicional cuando se lanza una instancia. Especifique un valor para `Groups` que corresponda a los grupos de seguridad de la VPC en la que el grupo de escalado automático lanzará las instancias. Especifique las subredes de la VPC como propiedades del grupo de escalado automático.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForAutoScaling \
    --version-description AutoScalingVersion1 \
    --launch-template-data '{"NetworkInterfaces":
[{"DeviceIndex":0,"AssociatePublicIpAddress":true,"Groups":
["sg-7c227019,sg-903004f8"],"DeleteOnTermination":true}],"ImageId":"ami-
b42209de","InstanceType":"m4.large","TagSpecifications":
```

```
[{"ResourceType":"instance","Tags":[{"Key":"environment","Value":"production"},
{"Key":"purpose","Value":"webserver"}]},{"ResourceType":"volume","Tags":
[{"Key":"environment","Value":"production"},{"Key":"cost-
center","Value":"cc123"}]}],"BlockDeviceMappings":[{"DeviceName":"/dev/sda1","Ebs":
{"VolumeSize":100}}]}' --region us-east-1
```

Salida:

```
{
    "LaunchTemplate": {
        "LatestVersionNumber": 1,
        "LaunchTemplateId": "lt-0123c79c33a54e0abc",
        "LaunchTemplateName": "TemplateForAutoScaling",
        "DefaultVersionNumber": 1,
        "CreatedBy": "arn:aws:iam::123456789012:user/Bob",
        "CreateTime": "2019-04-30T18:16:06.000Z"
    }
}
```

Para obtener más información, consulte Creación de una plantilla de lanzamiento para un grupo de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling. Para obtener información acerca de cómo citar parámetros con formato JSON, consulte Entrecomillado de cadenas en la Guía del usuario de la Interfaz de la línea de comandos de AWS.

Ejemplo 3: crear una plantilla de lanzamiento que especifique el cifrado de los volúmenes de EBS

En el siguiente ejemplo de `create-launch-template`, se crea una plantilla de lanzamiento que incluye volúmenes de EBS cifrados creados a partir de una instantánea no cifrada. También etiqueta los volúmenes durante la creación. Si el cifrado está deshabilitado de forma predeterminada, debe especificar la opción `"Encrypted"` que se muestra en el siguiente ejemplo. Si usa la opción `"KmsKeyId"` para especificar una CMK administrada por el cliente, también debe especificar la opción `"Encrypted"` aunque el cifrado esté habilitado de forma predeterminada.

```
aws ec2 create-launch-template \
  --launch-template-name TemplateForEncryption \
  --launch-template-data file://config.json
```

Contenido de `config.json`:

```
{
```

```
    "BlockDeviceMappings":[
        {
            "DeviceName":"/dev/sda1",
            "Ebs":{
                "VolumeType":"gp2",
                "DeleteOnTermination":true,
                "SnapshotId":"snap-066877671789bd71b",
                "Encrypted":true,
                "KmsKeyId":"arn:aws:kms:us-east-1:012345678910:key/abcd1234-
a123-456a-a12b-a123b4cd56ef"
            }
        }
    ],
    "ImageId":"ami-00068cd7555f543d5",
    "InstanceType":"c5.large",
    "TagSpecifications":[
        {
            "ResourceType":"volume",
            "Tags":[
                {
                    "Key":"encrypted",
                    "Value":"yes"
                }
            ]
        }
    ]
}
```

Salida:

```
{
    "LaunchTemplate": {
        "LatestVersionNumber": 1,
        "LaunchTemplateId": "lt-0d5bd51bcf8530abc",
        "LaunchTemplateName": "TemplateForEncryption",
        "DefaultVersionNumber": 1,
        "CreatedBy": "arn:aws:iam::123456789012:user/Bob",
        "CreateTime": "2020-01-07T19:08:36.000Z"
    }
}
```

Para obtener más información, consulte Restauración de un volumen de Amazon EBS a partir de una instantánea en la Guía del usuario de Amazon Elastic Compute Cloud.

- Para obtener información sobre la API, consulte CreateLaunchTemplate en la Referencia de comandos de la AWS CLI.

`create-local-gateway-route-table-virtual-interface-group-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-local-gateway-route-table-virtual-interface-group-association`.

AWS CLI

Para asociar una tabla de enrutamiento de puerta de enlace local a un grupo de interfaces virtuales (VIF

En el siguiente ejemplo de `create-local-gateway-route-table-virtual-interface-group-association`, se crea una asociación entre la tabla de enrutamiento de puerta de enlace local especificada y el grupo de VIF.

```
aws ec2 create-local-gateway-route-table-virtual-interface-group-association \
    --local-gateway-route-table-id lgw-rtb-exampleidabcd1234 \
    --local-gateway-virtual-interface-group-id lgw-vif-grp-exampleid0123abcd
```

Salida:

```
{
    "LocalGatewayRouteTableVirtualInterfaceGroupAssociation": {
        "LocalGatewayRouteTableVirtualInterfaceGroupAssociationId": "lgw-vif-grp-
assoc-exampleid12345678",
        "LocalGatewayVirtualInterfaceGroupId": "lgw-vif-grp-exampleid0123abcd",
        "LocalGatewayId": "lgw-exampleid11223344",
        "LocalGatewayRouteTableId": "lgw-rtb-exampleidabcd1234",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-exampleidabcd1234",
        "OwnerId": "111122223333",
        "State": "pending",
        "Tags": []
    }
}
```

Para obtener más información, consulte VIF group associations en la Guía del usuario de AWS Outposts.

- Para obtener información sobre la API, consulte CreateLocalGatewayRouteTableVirtualInterfaceGroupAssociation en la Referencia de comandos de la AWS CLI.

`create-local-gateway-route-table-vpc-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-local-gateway-route-table-vpc-association`.

AWS CLI

Para asociar una VPC a una tabla de enrutamiento

En el siguiente ejemplo de `create-local-gateway-route-table-vpc-association`, se asocia la VPC especificada a la tabla de enrutamiento de puerta de enlace local especificada.

```
aws ec2 create-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

Salida:

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

- Para obtener información sobre la API, consulte CreateLocalGatewayRouteTableVpcAssociation en la Referencia de comandos de la AWS CLI.

`create-local-gateway-route-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-local-gateway-route-table`.

AWS CLI

Para crear una tabla de enrutamiento de puerta de enlace local

En el siguiente ejemplo de `create-local-gateway-route-table`, se crea una tabla de enrutamiento de puerta de enlace local con el modo de enrutamiento de VPC directo.

```
aws ec2 create-local-gateway-route-table \
    --local-gateway-id lgw-1a2b3c4d5e6f7g8h9 \
    --mode direct-vpc-routing
```

Salida:

```
{
    "LocalGatewayRouteTable": {
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-abcdefg1234567890",
        "LocalGatewayId": "lgw-1a2b3c4d5e6f7g8h9",
        "OutpostArn": "arn:aws:outposts:us-west-2:111122223333:outpost/
op-021345abcdef67890",
        "OwnerId": "111122223333",
        "State": "pending",
        "Tags": [],
        "Mode": "direct-vpc-routing"
    }
}
```

Para obtener más información, consulte Tablas de enrutamiento de puertas de enlace locales en la Guía del usuario de AWS Outposts.

- Para obtener información sobre la API, consulte CreateLocalGatewayRouteTable en la Referencia de comandos de la AWS CLI.

`create-local-gateway-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-local-gateway-route`.

AWS CLI

Para crear una ruta estática para una tabla de enrutamiento de puerta de enlace local

En el siguiente ejemplo de `create-local-gateway-route`, se crea la ruta especificada en la tabla de enrutamiento de puerta de enlace local especificada.

```
aws ec2 create-local-gateway-route \
    --destination-cidr-block 0.0.0.0/0 \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE
```

Salida:

```
{
    "Route": {
        "DestinationCidrBlock": "0.0.0.0/0",
        "LocalGatewayVirtualInterfaceGroupId": "lgw-vif-grp-07145b276bEXAMPLE",
        "Type": "static",
        "State": "deleted",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE"
    }
}
```

- Para obtener información sobre la API, consulte CreateLocalGatewayRoute en la Referencia de comandos de la AWS CLI.

`create-managed-prefix-list`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-managed-prefix-list`.

AWS CLI

Para crear una lista de prefijos

En el siguiente ejemplo de `create-managed-prefix-list`, se crea una lista de prefijos de IPv4 con un máximo de diez entradas y se crean dos entradas en la lista de prefijos.

```
aws ec2 create-managed-prefix-list \
    --address-family IPv4 \
    --max-entries 10 \
    --entries Cidr=10.0.0.0/16,Description=vpc-a Cidr=10.2.0.0/16,Description=vpc-b
 \
    --prefix-list-name vpc-cidrs
```

Salida:

```
{
    "PrefixList": {
        "PrefixListId": "pl-0123456abcabcabc1",
        "AddressFamily": "IPv4",
        "State": "create-in-progress",
        "PrefixListArn": "arn:aws:ec2:us-west-2:123456789012:prefix-list/
pl-0123456abcabcabc1",
        "PrefixListName": "vpc-cidrs",
        "MaxEntries": 10,
        "Version": 1,
        "Tags": [],
        "OwnerId": "123456789012"
    }
}
```

Para obtener más información, consulte Managed prefix lists en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte CreateManagedPrefixList en la Referencia de comandos de la AWS CLI.

`create-nat-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-nat-gateway`.

AWS CLI

Ejemplo 1: creación de una puerta de enlace de NAT pública

En el siguiente ejemplo de `create-nat-gateway`, se crea una puerta de enlace de NAT pública en la subred especificada y se asocia la dirección IP elástica al ID de asignación especificado. Al crear una puerta de enlace de NAT pública, es preciso asociarle una dirección IP elástica.

```
aws ec2 create-nat-gateway \
    --subnet-id subnet-0250c25a1fEXAMPLE \
    --allocation-id eipalloc-09ad461b0dEXAMPLE
```

Salida:

```
{
    "NatGateway": {
        "CreateTime": "2021-12-01T22:22:38.000Z",
```

```
        "NatGatewayAddresses": [
            {
                "AllocationId": "eipalloc-09ad461b0dEXAMPLE"
            }
        ],
        "NatGatewayId": "nat-0c61bf8a12EXAMPLE",
        "State": "pending",
        "SubnetId": "subnet-0250c25a1fEXAMPLE",
        "VpcId": "vpc-0a60eb65b4EXAMPLE",
        "ConnectivityType": "public"
    }
}
```

Para obtener información, consulte Gateways NAT en la Guía del usuario de Amazon VPC.

Ejemplo 2: creación de una puerta de enlace de NAT privada

En el siguiente ejemplo de `create-nat-gateway`, se crea una puerta de enlace de NAT privada en la subred especificada. Una puerta de enlace de NAT privada no tiene una dirección IP elástica asociada.

```
aws ec2 create-nat-gateway \
    --subnet-id subnet-0250c25a1fEXAMPLE \
    --connectivity-type private
```

Salida:

```
{
    "NatGateway": {
        "CreateTime": "2021-12-01T22:26:00.000Z",
        "NatGatewayAddresses": [
            {}
        ],
        "NatGatewayId": "nat-011b568379EXAMPLE",
        "State": "pending",
        "SubnetId": "subnet-0250c25a1fEXAMPLE",
        "VpcId": "vpc-0a60eb65b4EXAMPLE",
        "ConnectivityType": "private"
    }
}
```

Para obtener información, consulte Gateways NAT en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte CreateNatGateway en la Referencia de comandos de la AWS CLI.

`create-network-acl-entry`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-network-acl-entry`.

AWS CLI

Para crear una entrada para la ACL de red

En este ejemplo, se crea una entrada para la ACL de red especificada. La regla permite la entrada de tráfico desde cualquier dirección IPv4 (0.0.0.0/0) en el puerto 53 de UDP (DNS) a cualquier subred asociada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 create-network-acl-entry --network-acl-id acl-5fb85d36 --ingress --rule-number 100 --protocol udp --port-range From=53,To=53 --cidr-block 0.0.0.0/0 --rule-action allow
```

En este ejemplo, se crea una regla para la ACL de red especificada que permite la entrada de tráfico desde cualquier dirección IPv6 (::/0) en el puerto TCP 80 (HTTP).

Comando:

```
aws ec2 create-network-acl-entry --network-acl-id acl-5fb85d36 --ingress --rule-number 120 --protocol tcp --port-range From=80,To=80 --ipv6-cidr-block ::/0 --rule-action allow
```

- Para obtener información sobre la API, consulte CreateNetworkAclEntry en la Referencia de comandos de la AWS CLI.

`create-network-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-network-acl`.

AWS CLI

Para crear una ACL de red

En este ejemplo, se crea una ACL para la VPC especificada.

Comando:

```
aws ec2 create-network-acl --vpc-id vpc-a01106c2
```

Salida:

```
{
    "NetworkAcl": {
        "Associations": [],
        "NetworkAclId": "acl-5fb85d36",
        "VpcId": "vpc-a01106c2",
        "Tags": [],
        "Entries": [
            {
                "CidrBlock": "0.0.0.0/0",
                "RuleNumber": 32767,
                "Protocol": "-1",
                "Egress": true,
                "RuleAction": "deny"
            },
            {
                "CidrBlock": "0.0.0.0/0",
                "RuleNumber": 32767,
                "Protocol": "-1",
                "Egress": false,
                "RuleAction": "deny"
            }
        ],
        "IsDefault": false
    }
}
```

- Para obtener información sobre la API, consulte CreateNetworkAcl en la Referencia de comandos de la AWS CLI.

`create-network-insights-access-scope`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-network-insights-access-scope`.

AWS CLI

Para crear un ámbito de acceso a la red

En el siguiente ejemplo de `create-network-insights-access-scope`, se crea un ámbito de acceso a la red.

```
aws ec2 create-network-insights-access-scope \
    --cli-input-json file://access-scope-file.json
```

Contenido de `access-scope-file.json`:

```
{
    "MatchPaths": [
        {
            "Source": {
                "ResourceStatement": {
                    "Resources": [
                        "vpc-abcd12e3"
                    ]
                }
            }
         }
    ],
    "ExcludePaths": [
        {
            "Source": {
                "ResourceStatement": {
                    "ResourceTypes": [
                        "AWS::EC2::InternetGateway"
                    ]
                }
            }
        }
    ]
}
```

Salida:

```
{
    "NetworkInsightsAccessScope": {
        "NetworkInsightsAccessScopeId": "nis-123456789abc01234",
```

```
        "NetworkInsightsAccessScopeArn": "arn:aws:ec2:us-
east-1:123456789012:network-insights-access-scope/nis-123456789abc01234",
        "CreatedDate": "2022-01-25T19:20:28.796000+00:00",
        "UpdatedDate": "2022-01-25T19:20:28.797000+00:00"
    },
    "NetworkInsightsAccessScopeContent": {
        "NetworkInsightsAccessScopeId": "nis-123456789abc01234",
        "MatchPaths": [
            {
                "Source": {
                    "ResourceStatement": {
                        "Resources": [
                            "vpc-abcd12e3"
                        ]
                    }
                }
            }
        ],
        "ExcludePaths": [
            {
                "Source": {
                    "ResourceStatement": {
                        "ResourceTypes": [
                            "AWS::EC2::InternetGateway"
                        ]
                    }
                }
            }
        ]
    }
}
```

Para obtener más información, consulte Getting started with Network Access Analyzer using the AWS CLI en la Guía del analizador de acceso a la red.

- Para obtener información sobre la API, consulte CreateNetworkInsightsAccessScope en la Referencia de comandos de la AWS CLI.

`create-network-insights-path`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-network-insights-path`.

AWS CLI

Para crear una ruta

En el siguiente ejemplo de `create-network-insights-path`, se crea una ruta. El origen es la puerta de enlace de Internet especificada y el destino es la instancia de EC2 especificada. Para determinar si se puede acceder al destino mediante el protocolo y el puerto especificados, analice la ruta mediante el comando `start-network-insights-analysis`.

```
aws ec2 create-network-insights-path \
    --source igw-0797cccdc9d73b0e5 \
    --destination i-0495d385ad28331c7 \
    --destination-port 22 \
    --protocol TCP
```

Salida:

```
{
    "NetworkInsightsPaths": {
        "NetworkInsightsPathId": "nip-0b26f224f1d131fa8",
        "NetworkInsightsPathArn": "arn:aws:ec2:us-east-1:123456789012:network-
insights-path/nip-0b26f224f1d131fa8",
        "CreatedDate": "2021-01-20T22:43:46.933Z",
        "Source": "igw-0797cccdc9d73b0e5",
        "Destination": "i-0495d385ad28331c7",
        "Protocol": "tcp"
    }
}
```

Para obtener más información, consulte Getting started using the AWS CLI en la Guía del analizador de accesibilidad.

- Para obtener información sobre la API, consulte CreateNetworkInsightsPath en la Referencia de comandos de la AWS CLI.

`create-network-interface-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-network-interface-permission`.

AWS CLI

Para crear un permiso de interfaz de red

En este ejemplo, se concede permiso a la cuenta `123456789012` para asociar la interfaz de red `eni-1a2b3c4d` a una instancia.

Comando:

```
aws ec2 create-network-interface-permission --network-interface-id eni-1a2b3c4d --
aws-account-id 123456789012 --permission INSTANCE-ATTACH
```

Salida:

```
{
  "InterfacePermission": {
      "PermissionState": {
          "State": "GRANTED"
      },
      "NetworkInterfacePermissionId": "eni-perm-06fd19020ede149ea",
      "NetworkInterfaceId": "eni-1a2b3c4d",
      "Permission": "INSTANCE-ATTACH",
      "AwsAccountId": "123456789012"
  }
}
```

- Para obtener información sobre la API, consulte CreateNetworkInterfacePermission en la Referencia de comandos de la AWS CLI.

`create-network-interface`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-network-interface`.

AWS CLI

Ejemplo 1: especificación de una dirección IPv4 para una interfaz de red

En el siguiente ejemplo de `create-network-interface`, se crea una interfaz de red para la subred especificada con la dirección IPv4 principal especificada.

```
aws ec2 create-network-interface \
```

```
    --subnet-id subnet-00a24d0d67acf6333 \
    --description "my network interface" \
    --groups sg-09dfba7ed20cda78b \
    --private-ip-address 10.0.8.17
```

Salida:

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "my network interface",
        "Groups": [
            {
                "GroupName": "my-security-group",
                "GroupId": "sg-09dfba7ed20cda78b"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "06:6a:0f:9a:49:37",
        "NetworkInterfaceId": "eni-0492b355f0cf3b3f8",
        "OwnerId": "123456789012",
        "PrivateDnsName": "ip-10-0-8-18.us-west-2.compute.internal",
        "PrivateIpAddress": "10.0.8.17",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateDnsName": "ip-10-0-8-17.us-west-2.compute.internal",
                "PrivateIpAddress": "10.0.8.17"
            }
        ],
        "RequesterId": "AIDA4Z3Y7GSXTMEXAMPLE",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-00a24d0d67acf6333",
        "TagSet": [],
        "VpcId": "vpc-02723a0feeeb9d57b"
    }
}
```

Ejemplo 2: creación de una interfaz de red con una dirección IPv4 y una dirección IPv

En el siguiente ejemplo de `create-network-interface`, se crea una interfaz de red para la subred especificada con una dirección IPv4 y una dirección IPv6 seleccionadas por Amazon EC2.

```
aws ec2 create-network-interface \
    --subnet-id subnet-00a24d0d67acf6333 \
    --description "my dual stack network interface" \
    --ipv6-address-count 1 \
    --groups sg-09dfba7ed20cda78b
```

Salida:

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "my dual stack network interface",
        "Groups": [
            {
                "GroupName": "my-security-group",
                "GroupId": "sg-09dfba7ed20cda78b"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [
            {
                "Ipv6Address": "2600:1f13:cfe:3650:a1dc:237c:393a:4ba7",
                "IsPrimaryIpv6": false
            }
        ],
        "MacAddress": "06:b8:68:d2:b2:2d",
        "NetworkInterfaceId": "eni-05da417453f9a84bf",
        "OwnerId": "123456789012",
        "PrivateDnsName": "ip-10-0-8-18.us-west-2.compute.internal",
        "PrivateIpAddress": "10.0.8.18",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateDnsName": "ip-10-0-8-18.us-west-2.compute.internal",
                "PrivateIpAddress": "10.0.8.18"
            }
        ],
        "RequesterId": "AIDA4Z3Y7GSXTMEXAMPLE",
        "RequesterManaged": false,
        "SourceDestCheck": true,
```

```
        "Status": "pending",
        "SubnetId": "subnet-00a24d0d67acf6333",
        "TagSet": [],
        "VpcId": "vpc-02723a0feeeb9d57b",
        "Ipv6Address": "2600:1f13:cfe:3650:a1dc:237c:393a:4ba7"
    }
}
```

Ejemplo 3: creación de una interfaz de red con opciones de configuración de seguimiento de conexiones

En el siguiente ejemplo de `create-network-interface`, se crea una interfaz de red y se configuran los tiempos de espera de seguimiento de las conexiones inactivas.

```
aws ec2 create-network-interface \
    --subnet-id subnet-00a24d0d67acf6333 \
    --groups sg-02e57dbcfe0331c1b \
    --connection-tracking-specification TcpEstablishedTimeout=86400,UdpTimeout=60
```

Salida:

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "ConnectionTrackingConfiguration": {
            "TcpEstablishedTimeout": 86400,
            "UdpTimeout": 60
        },
        "Description": "",
        "Groups": [
            {
                "GroupName": "my-security-group",
                "GroupId": "sg-02e57dbcfe0331c1b"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "06:4c:53:de:6d:91",
        "NetworkInterfaceId": "eni-0c133586e08903d0b",
        "OwnerId": "123456789012",
        "PrivateDnsName": "ip-10-0-8-94.us-west-2.compute.internal",
        "PrivateIpAddress": "10.0.8.94",
        "PrivateIpAddresses": [
```

```
            {
                "Primary": true,
                "PrivateDnsName": "ip-10-0-8-94.us-west-2.compute.internal",
                "PrivateIpAddress": "10.0.8.94"
            }
        ],
        "RequesterId": "AIDA4Z3Y7GSXTMEXAMPLE",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-00a24d0d67acf6333",
        "TagSet": [],
        "VpcId": "vpc-02723a0feeeb9d57b"
    }
}
```

Ejemplo 4: creación de un Elastic Fabric Adapter

En el siguiente ejemplo de `create-network-interface`, se crea un EFA.

```
aws ec2 create-network-interface \
    --interface-type efa \
    --subnet-id subnet-00a24d0d67acf6333 \
    --description "my efa" \
    --groups sg-02e57dbcfe0331c1b
```

Salida:

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "my efa",
        "Groups": [
            {
                "GroupName": "my-efa-sg",
                "GroupId": "sg-02e57dbcfe0331c1b"
            }
        ],
        "InterfaceType": "efa",
        "Ipv6Addresses": [],
        "MacAddress": "06:d7:a4:f7:4d:57",
        "NetworkInterfaceId": "eni-034acc2885e862b65",
        "OwnerId": "123456789012",
```

```
        "PrivateDnsName": "ip-10-0-8-180.us-west-2.compute.internal",
        "PrivateIpAddress": "10.0.8.180",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateDnsName": "ip-10-0-8-180.us-west-2.compute.internal",
                "PrivateIpAddress": "10.0.8.180"
            }
        ],
        "RequesterId": "AIDA4Z3Y7GSXTMEXAMPLE",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-00a24d0d67acf6333",
        "TagSet": [],
        "VpcId": "vpc-02723a0feeeb9d57b"
    }
}
```

Para obtener más información, consulte Interfaces de red elásticas en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CreateNetworkInterface en la Referencia de comandos de la AWS CLI.

`create-placement-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-placement-group`.

AWS CLI

Para crear un grupo de ubicación

En este ejemplo de comando, se crea un grupo de ubicación con el nombre especificado.

Comando:

```
aws ec2 create-placement-group --group-name my-cluster --strategy cluster
```

Para crear un grupo con ubicación en particiones

En este ejemplo de comando, se crea un grupo con ubicación en particiones denominado `HDFS-Group-A` con cinco particiones.

Comando:

```
aws ec2 create-placement-group --group-name HDFS-Group-A --strategy partition --
partition-count 5
```

- Para obtener información sobre la API, consulte CreatePlacementGroup en la Referencia de comandos de la AWS CLI.

`create-replace-root-volume-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-replace-root-volume-task`.

AWS CLI

Ejemplo 1: restauración de un volumen raíz a su estado de lanzamiento inicial

En el siguiente ejemplo de `create-replace-root-volume-task`, se restaura el volumen raíz de la instancia i-0123456789abcdefa a su estado de lanzamiento inicial.

```
aws ec2 create-replace-root-volume-task \
    --instance-id i-0123456789abcdefa
```

Salida:

```
{
    "ReplaceRootVolumeTask":
    {
        "InstanceId": "i-0123456789abcdefa",
            "ReplaceRootVolumeTaskId": "replacevol-0111122223333abcd",
            "TaskState": "pending",
            "StartTime": "2022-03-14T15:06:38Z",
            "Tags": []
    }
}
```

Ejemplo 2: restauración de un volumen raíz a una instantánea específica

En el siguiente ejemplo de `create-replace-root-volume-task`, se restaura el volumen raíz de la instancia i-0123456789abcdefa a la instantánea snap-0abcdef1234567890.

```
aws ec2 create-replace-root-volume-task \
    --instance-id i-0123456789abcdefa \
    --snapshot-id  snap-0abcdef1234567890
```

Salida:

```
{
    "ReplaceRootVolumeTask":
    {
        "InstanceId": "i-0123456789abcdefa",
        "ReplaceRootVolumeTaskId": "replacevol-0555566667777abcd",
        "TaskState": "pending",
        "StartTime": "2022-03-14T15:16:28Z",
        "Tags": []
    }
}
```

Para obtener más información, consulte Sustituir un volumen raíz en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CreateReplaceRootVolumeTask en la Referencia de comandos de la AWS CLI.

`create-reserved-instances-listing`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-reserved-instances-listing`.

AWS CLI

Para publicar una instancia reservada en el Marketplace de instancias reservadas

En el siguiente ejemplo de `create-reserved-instances-listing`, se crea una lista para la instancia reservada especificada en el Marketplace de instancias reservadas.

```
aws ec2 create-reserved-instances-listing \
    --reserved-instances-id 5ec28771-05ff-4b9b-aa31-9e57dexample \
    --instance-count 3 \
    --price-schedules CurrencyCode=USD,Price=25.50 \
    --client-token 550e8400-e29b-41d4-a716-446655440000
```

- Para obtener información sobre la API, consulte CreateReservedInstancesListing en la Referencia de comandos de la AWS CLI.

`create-restore-image-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-restore-image-task`.

AWS CLI

Para restaurar una AMI desde un bucket de S

En el siguiente ejemplo de `create-restore-image-task`, se restaura una AMI a partir de un bucket de S3. Utilice los valores de `S3ObjectKey `` and ``Bucket` de la salida de `describe-store-image-tasks`, especifique la clave de objeto de la AMI y el nombre del bucket de S3 en el que se copió la AMI y especifique el nombre de la AMI restaurada. El nombre debe ser único para las AMI de la región de esta cuenta. La AMI restaurada recibirá un nuevo ID de AMI.

```
aws ec2 create-restore-image-task \
    --object-key ami-1234567890abcdef0.bin \
    --bucket my-ami-bucket \
    --name 'New AMI Name'
```

Salida:

```
{
    "ImageId": "ami-0eab20fe36f83e1a8"
}
```

Para obtener más información, consulte Almacenar y restaurar una AMI mediante S3 en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CreateRestoreImageTask en la Referencia de comandos de la AWS CLI.

`create-route-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-route-table`.

AWS CLI

Crear una tabla de enrutamiento

En este ejemplo, se crea una tabla de enrutamiento para la VPC especificada.

Comando:

```
aws ec2 create-route-table --vpc-id vpc-a01106c2
```

Salida:

```
{
    "RouteTable": {
        "Associations": [],
        "RouteTableId": "rtb-22574640",
        "VpcId": "vpc-a01106c2",
        "PropagatingVgws": [],
        "Tags": [],
        "Routes": [
            {
                "GatewayId": "local",
                "DestinationCidrBlock": "10.0.0.0/16",
                "State": "active"
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte CreateRouteTable en la Referencia de comandos de la AWS CLI.

`create-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-route`.

AWS CLI

Para crear una ruta

En este ejemplo, se crea una ruta para la tabla de enrutamiento especificada. La ruta coincide con todo el tráfico IPv4 (`0.0.0.0/0`) y lo dirige a la puerta de enlace de Internet especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 create-route --route-table-id rtb-22574640 --destination-cidr-
block 0.0.0.0/0 --gateway-id igw-c0a643a9
```

En este ejemplo de comando, se crea una ruta en la tabla de enrutamiento rtb-g8ff4ea2. La ruta coincide con el tráfico del bloque de CIDR de IPv4 10.0.0.0/16 y lo enruta a la conexión de emparejamiento de VPC, pcx-111aaa22. Esta ruta permite dirigir el tráfico a la VPC emparejada en la conexión de emparejamiento de VPC. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 create-route --route-table-id rtb-g8ff4ea2 --destination-cidr-
block 10.0.0.0/16 --vpc-peering-connection-id pcx-1a2b3c4d
```

En este ejemplo, se crea una ruta en la tabla de enrutamiento especificada que coincide con todo el tráfico IPv6 (`::/0`) y lo enruta a la puerta de enlace de Internet de solo salida especificada.

Comando:

```
aws ec2 create-route --route-table-id rtb-dce620b8 --destination-ipv6-cidr-
block ::/0 --egress-only-internet-gateway-id eigw-01eadbd45ecd7943f
```

- Para obtener información sobre la API, consulte CreateRoute en la Referencia de comandos de la AWS CLI.

`create-security-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-security-group`.

AWS CLI

Crear un grupo de seguridad para EC2-Classic

En este ejemplo, se crea un grupo de seguridad denominado `MySecurityGroup`.

Comando:

```
aws ec2 create-security-group --group-name MySecurityGroup --description "My
 security group"
```

Salida:

```
{
    "GroupId": "sg-903004f8"
}
```

Crear un grupo de seguridad para EC2-VPC

En este ejemplo, se crea un grupo de seguridad para la VPC especificada denominado `MySecurityGroup`.

Comando:

```
aws ec2 create-security-group --group-name MySecurityGroup --description "My
 security group" --vpc-id vpc-1a2b3c4d
```

Salida:

```
{
    "GroupId": "sg-903004f8"
}
```

Para obtener más información, consulte Uso de los grupos de seguridad en la Guía del usuario de la Interfaz de la línea de comandos de AWS.

- Para obtener información sobre la API, consulte CreateSecurityGroup en la Referencia de comandos de la AWS CLI.

`create-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-snapshot`.

AWS CLI

Para crear una instantánea

En este ejemplo de comando, se crea una instantánea del volumen con el ID de volumen `vol-1234567890abcdef0` y una breve descripción para identificar la instantánea.

Comando:

```
aws ec2 create-snapshot --volume-id vol-1234567890abcdef0 --description "This is my
 root volume snapshot"
```

Salida:

```
{
    "Description": "This is my root volume snapshot",
    "Tags": [],
    "Encrypted": false,
    "VolumeId": "vol-1234567890abcdef0",
    "State": "pending",
    "VolumeSize": 8,
    "StartTime": "2018-02-28T21:06:01.000Z",
    "Progress": "",
    "OwnerId": "012345678910",
    "SnapshotId": "snap-066877671789bd71b"
}
```

Para crear una instantánea con etiquetas

En este ejemplo de comando, se crea una instantánea y se aplican dos etiquetas: purpose=prod y costcenter=123.

Comando:

```
aws ec2 create-snapshot --volume-id vol-1234567890abcdef0 --description 'Prod
 backup' --tag-specifications 'ResourceType=snapshot,Tags=[{Key=purpose,Value=prod},
{Key=costcenter,Value=123}]'
```

Salida:

```
{
    "Description": "Prod backup",
    "Tags": [
        {
            "Value": "prod",
```

```
            "Key": "purpose"
        },
        {
            "Value": "123",
            "Key": "costcenter"
        }
    ],
    "Encrypted": false,
    "VolumeId": "vol-1234567890abcdef0",
    "State": "pending",
    "VolumeSize": 8,
    "StartTime": "2018-02-28T21:06:06.000Z",
    "Progress": "",
    "OwnerId": "012345678910",
    "SnapshotId": "snap-09ed24a70bc19bbe4"
}
```

- Para obtener información sobre la API, consulte CreateSnapshot en la Referencia de comandos de la AWS CLI.

`create-snapshots`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-snapshots`.

AWS CLI

Ejemplo 1: creación de una instantánea de varios volúmenes

En el siguiente ejemplo de `create-snapshots`, se crean instantáneas de todos los volúmenes asociados a la instancia especificada.

```
aws ec2 create-snapshots \
    --instance-specification InstanceId=i-1234567890abcdef0 \
    --description "This is snapshot of a volume from my-instance"
```

Salida:

```
{
    "Snapshots": [
        {
            "Description": "This is a snapshot of a volume from my-instance",
```

```
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0a01d2d5a34697479",
            "State": "pending",
            "VolumeSize": 16,
            "StartTime": "2019-08-05T16:58:19.000Z",
            "Progress": "",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-07f30e3909aa0045e"
        },
        {
            "Description": "This is a snapshot of a volume from my-instance",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-02d0d4947008cb1a2",
            "State": "pending",
            "VolumeSize": 20,
            "StartTime": "2019-08-05T16:58:19.000Z",
            "Progress": "",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-0ec20b602264aad48"
        },
        ...
    ]
}
```

Ejemplo 2: creación de una instantánea de varios volúmenes con etiquetas del volumen de origen

En el siguiente ejemplo de `create-snapshots`, se crean instantáneas de todos los volúmenes asociados a la instancia especificada y se copian las etiquetas de cada volumen en la instantánea correspondiente.

```
aws ec2 create-snapshots \
    --instance-specification InstanceId=i-1234567890abcdef0 \
    --copy-tags-from-source volume \
    --description "This is snapshot of a volume from my-instance"
```

Salida:

```
{
    "Snapshots": [
        {
```

```
            "Description": "This is a snapshot of a volume from my-instance",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "my-volume"
                }
            ],
            "Encrypted": false,
            "VolumeId": "vol-02d0d4947008cb1a2",
            "State": "pending",
            "VolumeSize": 20,
            "StartTime": "2019-08-05T16:53:04.000Z",
            "Progress": "",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-053bfaeb821a458dd"
        }
        ...
    ]
}
```

Ejemplo 3: creación de una instantánea de varios volúmenes que no incluye el volumen raíz

En el siguiente ejemplo de `create-snapshots`, se crea una instantánea de todos los volúmenes asociados a la instancia especificada, excepto el volumen raíz.

```
aws ec2 create-snapshots \
    --instance-specification InstanceId=i-1234567890abcdef0,ExcludeBootVolume=true
```

Consulte el ejemplo 1 para ver una salida de muestra.

Ejemplo 4: creación de una instantánea de varios volúmenes y adición de etiquetas

En el siguiente ejemplo de `create-snapshots`, se crean instantáneas de todos los volúmenes asociados a la instancia especificada y se agregan dos etiquetas a cada instantánea.

```
aws ec2 create-snapshots \
    --instance-specification InstanceId=i-1234567890abcdef0 \
    --tag-specifications 'ResourceType=snapshot,Tags=[{Key=Name,Value=backup},
{Key=costcenter,Value=123}]'
```

Consulte el ejemplo 1 para ver una salida de muestra.

- Para obtener información sobre la API, consulte CreateSnapshots en la Referencia de comandos de la AWS CLI.

`create-spot-datafeed-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-spot-datafeed-subscription`.

AWS CLI

Para crear una fuente de datos de instancia de spot

En el siguiente ejemplo de `create-spot-datafeed-subscription`, se crea una fuente de datos de instancia de spot.

```
aws ec2 create-spot-datafeed-subscription \
    --bucket amzn-s3-demo-bucket \
    --prefix spot-data-feed
```

Salida:

```
{
    "SpotDatafeedSubscription": {
        "Bucket": "amzn-s3-demo-bucket",
        "OwnerId": "123456789012",
        "Prefix": "spot-data-feed",
        "State": "Active"
    }
}
```

La fuente de datos se almacena en el bucket de Amazon S3 que se especifica. Los nombres de archivo de esta fuente de datos tienen el siguiente formato.

```
amzn-s3-demo-bucket.s3.amazonaws.com/spot-data-feed/123456789012.YYYY-MM-DD-
HH.n.abcd1234.gz
```

Para obtener más información, consulte Fuente de datos de instancias de spot en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CreateSpotDatafeedSubscription en la Referencia de comandos de la AWS CLI.

`create-store-image-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-store-image-task`.

AWS CLI

Para almacenar una AMI en un bucket de S

En el siguiente ejemplo de `create-store-image-task`, se almacena una AMI en un bucket de S3. Especifique el ID de la AMI y el nombre del bucket de S3 en el que desea almacenar la AMI.

```
aws ec2 create-store-image-task \
  --image-id ami-1234567890abcdef0 \
  --bucket my-ami-bucket
```

Salida:

```
{
    "ObjectKey": "ami-1234567890abcdef0.bin"
}
```

Para obtener más información, consulte Almacenar y restaurar una AMI mediante S3 en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CreateStoreImageTask en la Referencia de comandos de la AWS CLI.

`create-subnet-cidr-reservation`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-subnet-cidr-reservation`.

AWS CLI

Para crear una reserva de CIDR de subred

En el siguiente ejemplo de `create-subnet-cidr-reservation`, se crea una reserva de CIDR de subred para la subred y el rango de CIDR especificados.

```
aws ec2 create-subnet-cidr-reservation \
    --subnet-id subnet-03c51e2eEXAMPLE \
```

```
    --reservation-type prefix \
    --cidr 10.1.0.20/26
```

Salida:

```
{
    "SubnetCidrReservation": {
        "SubnetCidrReservationId": "scr-044f977c4eEXAMPLE",
        "SubnetId": "subnet-03c51e2e6cEXAMPLE",
        "Cidr": "10.1.0.16/28",
        "ReservationType": "prefix",
        "OwnerId": "123456789012"
    }
}
```

Para obtener más información, consulte Reservas de la subred de CIDR en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte CreateSubnetCidrReservation en la Referencia de comandos de la AWS CLI.

`create-subnet`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-subnet`.

AWS CLI

Ejemplo 1: Crear una subred solo con un bloque de CIDR IPv

En el siguiente ejemplo de `create-subnet`, se crea una subred en la VPC especificada con el bloque de CIDR IPv4 especificado.

```
aws ec2 create-subnet \
    --vpc-id vpc-081ec835f3EXAMPLE \
    --cidr-block 10.0.0.0/24 \
    --tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-
subnet}]
```

Salida:

```
{
```

```
    "Subnet": {
        "AvailabilityZone": "us-west-2a",
        "AvailabilityZoneId": "usw2-az2",
        "AvailableIpAddressCount": 251,
        "CidrBlock": "10.0.0.0/24",
        "DefaultForAz": false,
        "MapPublicIpOnLaunch": false,
        "State": "available",
        "SubnetId": "subnet-0e99b93155EXAMPLE",
        "VpcId": "vpc-081ec835f3EXAMPLE",
        "OwnerId": "123456789012",
        "AssignIpv6AddressOnCreation": false,
        "Ipv6CidrBlockAssociationSet": [],
        "Tags": [
            {
                "Key": "Name",
                "Value": "my-ipv4-only-subnet"
            }
        ],
        "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/
subnet-0e99b93155EXAMPLE"
    }
}
```

Ejemplo 2: Crear una subred con bloques de CIDR IPv4 e IPv

En el siguiente ejemplo de `create-subnet`, se crea una subred en la VPC especificada con los bloques de CIDR IPv4 e IPv6 especificados.

```
aws ec2 create-subnet \
    --vpc-id vpc-081ec835f3EXAMPLE \
    --cidr-block 10.0.0.0/24 \
    --ipv6-cidr-block 2600:1f16:cfe:3660::/64 \
    --tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-ipv6-
subnet}]
```

Salida:

```
{
    "Subnet": {
        "AvailabilityZone": "us-west-2a",
        "AvailabilityZoneId": "usw2-az2",
        "AvailableIpAddressCount": 251,
```

```
        "CidrBlock": "10.0.0.0/24",
        "DefaultForAz": false,
        "MapPublicIpOnLaunch": false,
        "State": "available",
        "SubnetId": "subnet-0736441d38EXAMPLE",
        "VpcId": "vpc-081ec835f3EXAMPLE",
        "OwnerId": "123456789012",
        "AssignIpv6AddressOnCreation": false,
        "Ipv6CidrBlockAssociationSet": [
            {
                "AssociationId": "subnet-cidr-assoc-06c5f904499fcc623",
                "Ipv6CidrBlock": "2600:1f13:cfe:3660::/64",
                "Ipv6CidrBlockState": {
                    "State": "associating"
                }
            }
        ],
        "Tags": [
            {
                "Key": "Name",
                "Value": "my-ipv4-ipv6-subnet"
            }
        ],
        "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/
subnet-0736441d38EXAMPLE"
    }
}
```

Ejemplo 3: crear una subred solo con un bloque de CIDR IPv

En el siguiente ejemplo de `create-subnet`, se crea una subred en la VPC especificada con el bloque de CIDR IPv6 especificado.

```
aws ec2 create-subnet \
    --vpc-id vpc-081ec835f3EXAMPLE \
    --ipv6-native \
    --ipv6-cidr-block 2600:1f16:115:200::/64 \
    --tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv6-only-
subnet}]
```

Salida:

```
{
```

```
    "Subnet": {
        "AvailabilityZone": "us-west-2a",
        "AvailabilityZoneId": "usw2-az2",
        "AvailableIpAddressCount": 0,
        "DefaultForAz": false,
        "MapPublicIpOnLaunch": false,
        "State": "available",
        "SubnetId": "subnet-03f720e7deEXAMPLE",
        "VpcId": "vpc-081ec835f3EXAMPLE",
        "OwnerId": "123456789012",
        "AssignIpv6AddressOnCreation": true,
        "Ipv6CidrBlockAssociationSet": [
            {
                "AssociationId": "subnet-cidr-assoc-01ef639edde556709",
                "Ipv6CidrBlock": "2600:1f13:cfe:3660::/64",
                "Ipv6CidrBlockState": {
                    "State": "associating"
                }
            }
        ],
        "Tags": [
            {
                "Key": "Name",
                "Value": "my-ipv6-only-subnet"
            }
        ],
        "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/
subnet-03f720e7deEXAMPLE"
    }
}
```

Para obtener más información, consulte VPC y subredes en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte CreateSubnet en la Referencia de comandos de la AWS CLI.

`create-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-tags`.

AWS CLI

Ejemplo 1: adición de una etiqueta a un recurso

En el siguiente ejemplo de `create-tags`, se agrega la etiqueta `Stack=production` a la imagen especificada o se sobrescribe una etiqueta existente para la AMI en la que la clave de etiqueta es `Stack`.

```
aws ec2 create-tags \
    --resources ami-1234567890abcdef0 \
    --tags Key=Stack,Value=production
```

Este comando no genera ninguna salida.

Ejemplo 2: adición de etiquetas a varios recursos

En el siguiente ejemplo de `create-tags`, se agregan (o sobrescriben) dos etiquetas para una AMI y una instancia. Una de las etiquetas tiene una clave (`webserver`), pero no tiene valor (el valor se establece en una cadena vacía). La otra etiqueta tiene una clave (`stack`) y un valor (`Production`).

```
aws ec2 create-tags \
    --resources ami-1a2b3c4d i-1234567890abcdef0 \
    --tags Key=webserver,Value=   Key=stack,Value=Production
```

Este comando no genera ninguna salida.

Ejemplo 3: adición de etiquetas que contengan caracteres especiales

En los siguientes ejemplos de `create-tags`, se agrega la etiqueta `[Group]=test` a una instancia. Los corchetes ([y]) son caracteres especiales y deben incluirse en el carácter de escape. En los siguientes ejemplos también se usa el carácter de continuación de línea adecuado para cada entorno.

Si usa Windows, encierre el elemento que tiene caracteres especiales entre comillas dobles (“”) y, a continuación, preceda cada carácter de comillas dobles con una barra invertida (\) de la siguiente manera.

```
aws ec2 create-tags ^
    --resources i-1234567890abcdef0 ^
    --tags Key=\"[Group]\",Value=test
```

Si usa Windows PowerShell, encierre el valor que tiene caracteres especiales entre comillas dobles (“”), preceda cada carácter de comillas dobles con una barra invertida (\) y, a continuación, encierre toda la estructura de clave y valor entre comillas simples (‘’) de la siguiente manera.

```
aws ec2 create-tags `
    --resources i-1234567890abcdef0 `
    --tags 'Key=\"[Group]\",Value=test'
```

Si usa Linux u OS X, encierre el elemento con caracteres especiales entre comillas dobles (“”) y, a continuación, encierre toda la estructura de clave y valor entre comillas simples (‘’) de la siguiente manera.

```
aws ec2 create-tags \
    --resources i-1234567890abcdef0 \
    --tags 'Key="[Group]",Value=test'
```

Para obtener más información, consulte Etiquetado de los recursos de Amazon EC2 en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte CreateTags en la Referencia de comandos de la AWS CLI.

`create-traffic-mirror-filter-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-traffic-mirror-filter-rule`.

AWS CLI

Para crear una regla de filtro para el tráfico de TCP entrante

En el siguiente ejemplo de `create-traffic-mirror-filter-rule`, se crea una regla que se puede utilizar para reflejar todo el tráfico de TCP entrante. Antes de ejecutar este comando, utilice `create-traffic-mirror-filter` para crear el filtro de reflejo de tráfico.

```
aws ec2 create-traffic-mirror-filter-rule \
    --description 'TCP Rule' \
    --destination-cidr-block 0.0.0.0/0  \
    --protocol 6 \
    --rule-action accept \
    --rule-number 1 \
    --source-cidr-block 0.0.0.0/0 \
    --traffic-direction ingress \
    --traffic-mirror-filter-id tmf-04812ff784b25ae67
```

Salida:

```
{
    "TrafficMirrorFilterRule": {
        "DestinationCidrBlock": "0.0.0.0/0",
        "TrafficMirrorFilterId": "tmf-04812ff784b25ae67",
        "TrafficMirrorFilterRuleId": "tmfr-02d20d996673f3732",
        "SourceCidrBlock": "0.0.0.0/0",
        "TrafficDirection": "ingress",
        "Description": "TCP Rule",
        "RuleNumber": 1,
        "RuleAction": "accept",
        "Protocol": 6
    },
    "ClientToken": "4752b573-40a6-4eac-a8a4-a72058761219"
}
```

Para obtener más información, consulte Crear un filtro de reflejo de tráfico en la Guía de reflejo de tráfico.

- Para obtener información sobre la API, consulte CreateTrafficMirrorFilterRule en la Referencia de comandos de la AWS CLI.

`create-traffic-mirror-filter`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-traffic-mirror-filter`.

AWS CLI

Creación de un filtro de reflejo de tráfico

En el siguiente ejemplo de `create-traffic-mirror-filter`, se crea un filtro de reflejo de tráfico. Tras crear el filtro, utilice `create-traffic-mirror-filter-rule` para agregar reglas.

```
aws ec2 create-traffic-mirror-filter \
    --description 'TCP Filter'
```

Salida:

```
{
```

```
    "ClientToken": "28908518-100b-4987-8233-8c744EXAMPLE",
    "TrafficMirrorFilter": {
        "TrafficMirrorFilterId": "tmf-04812ff784EXAMPLE",
        "Description": "TCP Filter",
        "EgressFilterRules": [],
        "IngressFilterRules": [],
        "Tags": [],
        "NetworkServices": []
    }
}
```

Para obtener más información, consulte Crear un filtro de reflejo de tráfico en la Guía de reflejo de tráfico.

- Para obtener información sobre la API, consulte CreateTrafficMirrorFilter en la Referencia de comandos de la AWS CLI.

`create-traffic-mirror-session`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-traffic-mirror-session`.

AWS CLI

Creación de una sesión de reflejo de tráfico

El comando `create-traffic-mirror-session` siguiente crea una sesión de reflejo de tráfico para el origen y el destino especificados para 25 bytes del paquete.

```
aws ec2 create-traffic-mirror-session \
    --description 'example session' \
    --traffic-mirror-target-id tmt-07f75d8feeEXAMPLE \
    --network-interface-id eni-070203f901EXAMPLE \
    --session-number 1  \
    --packet-length 25 \
    --traffic-mirror-filter-id tmf-04812ff784EXAMPLE
```

Salida:

```
{
    "TrafficMirrorSession": {
        "TrafficMirrorSessionId": "tms-08a33b1214EXAMPLE",
```

```
        "TrafficMirrorTargetId": "tmt-07f75d8feeEXAMPLE",
        "TrafficMirrorFilterId": "tmf-04812ff784EXAMPLE",
        "NetworkInterfaceId": "eni-070203f901EXAMPLE",
        "OwnerId": "111122223333",
        "PacketLength": 25,
        "SessionNumber": 1,
        "VirtualNetworkId": 7159709,
        "Description": "example session",
        "Tags": []
    },
    "ClientToken": "5236cffc-ee13-4a32-bb5b-388d9da09d96"
}
```

Para obtener más información, consulte Crear una sesión de reflejo de tráfico en la Guía de reflejo de tráfico.

- Para obtener información sobre la API, consulte CreateTrafficMirrorSession en la Referencia de comandos de la AWS CLI.

`create-traffic-mirror-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-traffic-mirror-target`.

AWS CLI

Creación de un destino de reflejo de tráfico de un equilibrador de carga de red

En el siguiente ejemplo de `create-traffic-mirror-target`, se crea un objetivo de reflejo de tráfico de equilibrador de carga de red.

```
aws ec2 create-traffic-mirror-target \
    --description 'Example Network Load Balancer Target' \
    --network-load-balancer-arn arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/net/NLB/7cdec873EXAMPLE
```

Salida:

```
{
    "TrafficMirrorTarget": {
        "Type": "network-load-balancer",
        "Tags": [],
        "Description": "Example Network Load Balancer Target",
```

```
        "OwnerId": "111122223333",
        "NetworkLoadBalancerArn": "arn:aws:elasticloadbalancing:us-
east-1:724145273726:loadbalancer/net/NLB/7cdec873EXAMPLE",
        "TrafficMirrorTargetId": "tmt-0dabe9b0a6EXAMPLE"
    },
    "ClientToken": "d5c090f5-8a0f-49c7-8281-72c796a21f72"
}
```

Creación de un destino de reflejo de tráfico de red

En el siguiente ejemplo de `create-traffic-mirror-target`, se crea un objetivo de reflejo de tráfico de interfaz de red.

```
aws ec2 create-traffic-mirror-target \
    --description 'Network interface target' \
    --network-interface-id eni-eni-01f6f631eEXAMPLE
```

Salida:

```
{
    "ClientToken": "5289a345-0358-4e62-93d5-47ef3061d65e",
    "TrafficMirrorTarget": {
        "Description": "Network interface target",
        "NetworkInterfaceId": "eni-01f6f631eEXAMPLE",
        "TrafficMirrorTargetId": "tmt-02dcdbe2abEXAMPLE",
        "OwnerId": "111122223333",
        "Type": "network-interface",
        "Tags": []
    }
}
```

Para obtener más información, consulte Crear un destino de reflejo de tráfico en la Guía de reflejo de tráfico.

- Para obtener información sobre la API, consulte CreateTrafficMirrorTarget en la Referencia de comandos de la AWS CLI.

`create-transit-gateway-connect-peer`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-transit-gateway-connect-peer`.

AWS CLI

Para crear un emparejamiento de Transit Gateway Connect

En el siguiente ejemplo de `create-transit-gateway-connect-peer`, se crea un emparejamiento de Connect.

```
aws ec2 create-transit-gateway-connect-peer \
    --transit-gateway-attachment-id tgw-attach-0f0927767cEXAMPLE \
    --peer-address 172.31.1.11 \
    --inside-cidr-blocks 169.254.6.0/29
```

Salida:

```
{
    "TransitGatewayConnectPeer": {
        "TransitGatewayAttachmentId": "tgw-attach-0f0927767cEXAMPLE",
        "TransitGatewayConnectPeerId": "tgw-connect-peer-0666adbac4EXAMPLE",
        "State": "pending",
        "CreationTime": "2021-10-13T03:35:17.000Z",
        "ConnectPeerConfiguration": {
            "TransitGatewayAddress": "10.0.0.234",
            "PeerAddress": "172.31.1.11",
            "InsideCidrBlocks": [
                "169.254.6.0/29"
            ],
            "Protocol": "gre",
            "BgpConfigurations": [
                {
                    "TransitGatewayAsn": 64512,
                    "PeerAsn": 64512,
                    "TransitGatewayAddress": "169.254.6.2",
                    "PeerAddress": "169.254.6.1",
                    "BgpStatus": "down"
                },
                {
                    "TransitGatewayAsn": 64512,
                    "PeerAsn": 64512,
                    "TransitGatewayAddress": "169.254.6.3",
                    "PeerAddress": "169.254.6.1",
                    "BgpStatus": "down"
                }
            ]
```

```
        }
    }
}
```

Para obtener más información, consulte Transit gateway Connect attachments and Transit Gateway Connect peers en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte CreateTransitGatewayConnectPeer en la Referencia de comandos de la AWS CLI.

`create-transit-gateway-connect`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-transit-gateway-connect`.

AWS CLI

Para crear una conexión de Transit Gateway Connect

En el siguiente ejemplo de `create-transit-gateway-connect`, se crea una conexión de Connect con el protocolo gre para la conexión especificada.

```
aws ec2 create-transit-gateway-connect \
    --transport-transit-gateway-attachment-id tgw-attach-0a89069f57EXAMPLE \
    --options "Protocol=gre"
```

Salida:

```
{
    "TransitGatewayConnect": {
        "TransitGatewayAttachmentId": "tgw-attach-037012e5dcEXAMPLE",
        "TransportTransitGatewayAttachmentId": "tgw-attach-0a89069f57EXAMPLE",
        "TransitGatewayId": "tgw-02f776b1a7EXAMPLE",
        "State": "pending",
        "CreationTime": "2021-03-09T19:59:17+00:00",
        "Options": {
            "Protocol": "gre"
        }
    }
}
```

Para obtener más información, consulte Transit gateway Connect attachments and Transit Gateway Connect peers en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte CreateTransitGatewayConnect en la Referencia de comandos de la AWS CLI.

`create-transit-gateway-multicast-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-transit-gateway-multicast-domain`.

AWS CLI

Ejemplo 1: creación de un dominio de multidifusión de IGMP

En el siguiente ejemplo de `create-transit-gateway-multicast-domain`, se crea un dominio de multidifusión para la puerta de enlace de tránsito especificada. Con los orígenes estáticos deshabilitados, cualquier instancia de las subredes asociadas con el dominio de multidifusión puede enviar tráfico de multidifusión. Si al menos un miembro utiliza el protocolo IGMP, debe habilitar la compatibilidad con IGMPv2.

```
aws ec2 create-transit-gateway-multicast-domain \
    --transit-gateway-id tgw-0bf0bffefaEXAMPLE \
    --options StaticSourcesSupport=disable,Igmpv2Support=enable
```

Salida:

```
{
    "TransitGatewayMulticastDomain": {
        "TransitGatewayMulticastDomainId": "tgw-mcast-domain-0c9e29e2a7EXAMPLE",
        "TransitGatewayId": "tgw-0bf0bffefaEXAMPLE",
        "TransitGatewayMulticastDomainArn": "arn:aws:ec2:us-
west-2:123456789012:transit-gateway-multicast-domain/tgw-mcast-
domain-0c9e29e2a7EXAMPLE",
        "OwnerId": "123456789012",
        "Options": {
            "Igmpv2Support": "enable",
            "StaticSourcesSupport": "disable",
            "AutoAcceptSharedAssociations": "disable"
        },
        "State": "pending",
        "CreationTime": "2021-09-29T22:17:13.000Z"
    }
}
```

Ejemplo 2: creación de un dominio de multidifusión estático

En el siguiente ejemplo de `create-transit-gateway-multicast-domain`, se crea un dominio de multidifusión para la puerta de enlace de tránsito especificada. Con los orígenes estáticos habilitados, debe agregar orígenes de forma estática.

```
aws ec2 create-transit-gateway-multicast-domain \
    --transit-gateway-id tgw-0bf0bffefaEXAMPLE \
    --options StaticSourcesSupport=enable,Igmpv2Support=disable
```

Salida:

```
{
    "TransitGatewayMulticastDomain": {
        "TransitGatewayMulticastDomainId": "tgw-mcast-domain-000fb24d04EXAMPLE",
        "TransitGatewayId": "tgw-0bf0bffefaEXAMPLE",
        "TransitGatewayMulticastDomainArn": "arn:aws:ec2:us-
west-2:123456789012:transit-gateway-multicast-domain/tgw-mcast-
domain-000fb24d04EXAMPLE",
        "OwnerId": "123456789012",
        "Options": {
            "Igmpv2Support": "disable",
            "StaticSourcesSupport": "enable",
            "AutoAcceptSharedAssociations": "disable"
        },
        "State": "pending",
        "CreationTime": "2021-09-29T22:20:19.000Z"
    }
}
```

Para obtener más información, consulte Managing multicast domains en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte CreateTransitGatewayMulticastDomain en la Referencia de comandos de la AWS CLI.

`create-transit-gateway-peering-attachment`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-transit-gateway-peering-attachment`.

AWS CLI

Para crear una conexión de emparejamiento de puerta de enlace de tránsito

En el siguiente ejemplo de `create-transit-gateway-peering-attachment`, se crea una solicitud de conexión de emparejamiento entre las dos puertas de enlace de tránsito especificadas.

```
aws ec2 create-transit-gateway-peering-attachment \
    --transit-gateway-id tgw-123abc05e04123abc \
    --peer-transit-gateway-id tgw-11223344aabbcc112 \
    --peer-account-id 123456789012 \
    --peer-region us-east-2
```

Salida:

```
{
    "TransitGatewayPeeringAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-4455667788aabbccd",
        "RequesterTgwInfo": {
            "TransitGatewayId": "tgw-123abc05e04123abc",
            "OwnerId": "123456789012",
            "Region": "us-west-2"
        },
        "AccepterTgwInfo": {
            "TransitGatewayId": "tgw-11223344aabbcc112",
            "OwnerId": "123456789012",
            "Region": "us-east-2"
        },
        "State": "initiatingRequest",
        "CreationTime": "2019-12-09T11:38:05.000Z"
    }
}
```

Para obtener más información, consulte Transit Gateway Peering Attachments en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte CreateTransitGatewayPeeringAttachment en la Referencia de comandos de la AWS CLI.

`create-transit-gateway-policy-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-transit-gateway-policy-table`.

AWS CLI

Para crear una tabla de políticas de puerta de enlace de tránsito

En el siguiente ejemplo de `create-transit-gateway-policy-table`, se crea una tabla de políticas de puerta de enlace de tránsito para la puerta de enlace de tránsito especificada.

```
aws ec2 create-transit-gateway-policy-table \
    --transit-gateway-id tgw-067f8505c18f0bd6e
```

Salida:

```
{
    "TransitGatewayPolicyTable": {
        "TransitGatewayPolicyTableId": "tgw-ptb-0a16f134b78668a81",
        "TransitGatewayId": "tgw-067f8505c18f0bd6e",
        "State": "pending",
        "CreationTime": "2023-11-28T16:36:43+00:00"
    }
}
```

Para obtener más información, consulte Transit gateway policy tables en la Guía del usuario de Transit Gateway.

- Para obtener información sobre la API, consulte CreateTransitGatewayPolicyTable en la Referencia de comandos de la AWS CLI.

`create-transit-gateway-prefix-list-reference`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-transit-gateway-prefix-list-reference`.

AWS CLI

Para crear una referencia a una lista de prefijos

En el siguiente ejemplo de `create-transit-gateway-prefix-list-reference`, se crea una referencia a la lista de prefijos especificada en la tabla de enrutamiento de puerta de enlace de tránsito especificada.

```
aws ec2 create-transit-gateway-prefix-list-reference \
    --transit-gateway-route-table-id tgw-rtb-0123456789abcd123 \
    --prefix-list-id pl-1111112222222333 \
    --transit-gateway-attachment-id tgw-attach-aaaaaabbbbbb11111
```

Salida:

```
{
    "TransitGatewayPrefixListReference": {
        "TransitGatewayRouteTableId": "tgw-rtb-0123456789abcd123",
        "PrefixListId": "pl-1111112222222333",
        "PrefixListOwnerId": "123456789012",
        "State": "pending",
        "Blackhole": false,
        "TransitGatewayAttachment": {
            "TransitGatewayAttachmentId": "tgw-attach-aaaaaabbbbbb11111",
            "ResourceType": "vpc",
            "ResourceId": "vpc-112233445566aabbc"
        }
    }
}
```

Para obtener más información, consulte Crear una referencia de lista de prefijos en la Guía de puertas de enlace de tránsito.

- Para obtener información sobre la API, consulte CreateTransitGatewayPrefixListReference en la Referencia de comandos de la AWS CLI.

`create-transit-gateway-route-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-transit-gateway-route-table`.

AWS CLI

Para crear una tabla de enrutamiento de puerta de enlace de tránsito

En el siguiente ejemplo de `create-transit-gateway-route-table`, se crea una tabla de enrutamiento para la puerta de enlace de tránsito especificada.

```
aws ec2 create-transit-gateway-route-table \
    --transit-gateway-id tgw-0262a0e521EXAMPLE
```

Salida:

```
{
    "TransitGatewayRouteTable": {
        "TransitGatewayRouteTableId": "tgw-rtb-0960981be7EXAMPLE",
        "TransitGatewayId": "tgw-0262a0e521EXAMPLE",
        "State": "pending",
        "DefaultAssociationRouteTable": false,
        "DefaultPropagationRouteTable": false,
        "CreationTime": "2019-07-10T19:01:46.000Z"
    }
}
```

Para obtener más información, consulte Create a transit gateway route table en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte CreateTransitGatewayRouteTable en la Referencia de comandos de la AWS CLI.

`create-transit-gateway-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-transit-gateway-route`.

AWS CLI

Para crear una ruta de puertas de enlace de tránsito

En el siguiente ejemplo de `create-transit-gateway-route`, se crea una ruta con el destino especificado para la tabla de enrutamiento especificada.

```
aws ec2 create-transit-gateway-route \
    --destination-cidr-block 10.0.2.0/24 \
    --transit-gateway-route-table-id tgw-rtb-0b6f6aaa01EXAMPLE \
    --transit-gateway-attachment-id tgw-attach-0b5968d3b6EXAMPLE
```

Salida:

```
{
    "Route": {
        "DestinationCidrBlock": "10.0.2.0/24",
        "TransitGatewayAttachments": [
            {
                "ResourceId": "vpc-0065acced4EXAMPLE",
                "TransitGatewayAttachmentId": "tgw-attach-0b5968d3b6EXAMPLE",
                "ResourceType": "vpc"
            }
        ],
        "Type": "static",
        "State": "active"
    }
}
```

Para obtener más información, consulte Transit gateway route tables en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte CreateTransitGatewayRoute en la Referencia de comandos de la AWS CLI.

`create-transit-gateway-vpc-attachment`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-transit-gateway-vpc-attachment`.

AWS CLI

Ejemplo 1: asociación de una puerta de enlace de tránsito a una VPC

En el siguiente ejemplo de `create-transit-gateway-vpc-attachment`, se crea una conexión de puerta de enlace de tránsito a la VPC especificada.

```
aws ec2 create-transit-gateway-vpc-attachment \
    --transit-gateway-id tgw-0262a0e521EXAMPLE \
    --vpc-id vpc-07e8ffd50f49335df \
    --subnet-id subnet-0752213d59EXAMPLE
```

Salida:

```
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-0a34fe6b4fEXAMPLE",
        "TransitGatewayId": "tgw-0262a0e521EXAMPLE",
        "VpcId": "vpc-07e8ffd50fEXAMPLE",
        "VpcOwnerId": "111122223333",
        "State": "pending",
        "SubnetIds": [
            "subnet-0752213d59EXAMPLE"
        ],
        "CreationTime": "2019-07-10T17:33:46.000Z",
        "Options": {
            "DnsSupport": "enable",
            "Ipv6Support": "disable"
        }
    }
}
```

Para obtener más información, consulte Create a transit gateway attachment to a VPC en la Guía de Transit Gateway.

Ejemplo 2: asociación de una puerta de enlace de tránsito con varias subredes en una VPC

En el siguiente ejemplo de `create-transit-gateway-vpc-attachment`, se crea una conexión de puerta de enlace de tránsito a la VPC y las subredes especificadas.

```
aws ec2 create-transit-gateway-vpc-attachment \
    --transit-gateway-id tgw-02f776b1a7EXAMPLE  \
    --vpc-id vpc-3EXAMPLE \
    --subnet-ids "subnet-dEXAMPLE" "subnet-6EXAMPLE"
```

Salida:

```
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-0e141e0bebEXAMPLE",
        "TransitGatewayId": "tgw-02f776b1a7EXAMPLE",
        "VpcId": "vpc-3EXAMPLE",
        "VpcOwnerId": "111122223333",
        "State": "pending",
        "SubnetIds": [
            "subnet-6EXAMPLE",
```

```
            "subnet-dEXAMPLE"
        ],
        "CreationTime": "2019-12-17T20:07:52.000Z",
        "Options": {
            "DnsSupport": "enable",
            "Ipv6Support": "disable"
        }
    }
}
```

Para obtener más información, consulte Create a transit gateway attachment to a VPC en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte CreateTransitGatewayVpcAttachment en la Referencia de comandos de la AWS CLI.

`create-transit-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-transit-gateway`.

AWS CLI

Para crear una puerta de enlace de tránsito

En el siguiente ejemplo de `create-transit-gateway`, se crea una puerta de enlace de tránsito.

```
aws ec2 create-transit-gateway \
    --description MyTGW \
    --
options AmazonSideAsn=64516,AutoAcceptSharedAttachments=enable,DefaultRouteTableAssociation=
```

Salida:

```
{
    "TransitGateway": {
        "TransitGatewayId": "tgw-0262a0e521EXAMPLE",
        "TransitGatewayArn": "arn:aws:ec2:us-east-2:111122223333:transit-gateway/
tgw-0262a0e521EXAMPLE",
        "State": "pending",
        "OwnerId": "111122223333",
        "Description": "MyTGW",
```

```
        "CreationTime": "2019-07-10T14:02:12.000Z",
        "Options": {
            "AmazonSideAsn": 64516,
            "AutoAcceptSharedAttachments": "enable",
            "DefaultRouteTableAssociation": "enable",
            "AssociationDefaultRouteTableId": "tgw-rtb-018774adf3EXAMPLE",
            "DefaultRouteTablePropagation": "enable",
            "PropagationDefaultRouteTableId": "tgw-rtb-018774adf3EXAMPLE",
            "VpnEcmpSupport": "enable",
            "DnsSupport": "enable"
        }
    }
}
```

Para obtener más información, consulte Create a transit gateway en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte CreateTransitGateway en la Referencia de comandos de la AWS CLI.

`create-verified-access-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-verified-access-endpoint`.

AWS CLI

Para crear un punto de conexión de Acceso verificado

En el siguiente ejemplo de `create-verified-access-endpoint`, se crea un punto de conexión de acceso verificado para el grupo de acceso verificado especificado. El grupo de seguridad y la interfaz de red deben pertenecer a la misma VPC.

```
aws ec2 create-verified-access-endpoint \
    --verified-access-group-id vagr-0dbe967baf14b7235 \
    --endpoint-type network-interface \
    --attachment-type vpc \
    --domain-certificate-arn arn:aws:acm:us-east-2:123456789012:certificate/
eb065ea0-26f9-4e75-a6ce-0a1a7EXAMPLE \
    --application-domain example.com \
    --endpoint-domain-prefix my-ava-app \
    --security-group-ids sg-004915970c4c8f13a \
    --network-interface-
options NetworkInterfaceId=eni-0aec70418c8d87a0f,Protocol=https,Port=443 \
```

```
    --tag-specifications ResourceType=verified-access-
endpoint,Tags=[{Key=Name,Value=my-va-endpoint}]
```

Salida:

```
{
    "VerifiedAccessEndpoint": {
        "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
        "VerifiedAccessGroupId": "vagr-0dbe967baf14b7235",
        "VerifiedAccessEndpointId": "vae-066fac616d4d546f2",
        "ApplicationDomain": "example.com",
        "EndpointType": "network-interface",
        "AttachmentType": "vpc",
        "DomainCertificateArn": "arn:aws:acm:us-east-2:123456789012:certificate/
eb065ea0-26f9-4e75-a6ce-0a1a7EXAMPLE",
        "EndpointDomain": "my-ava-
app.edge-00c3372d53b1540bb.vai-0ce000c0b7643abea.prod.verified-access.us-
east-2.amazonaws.com",
        "SecurityGroupIds": [
            "sg-004915970c4c8f13a"
        ],
        "NetworkInterfaceOptions": {
            "NetworkInterfaceId": "eni-0aec70418c8d87a0f",
            "Protocol": "https",
            "Port": 443
        },
        "Status": {
            "Code": "pending"
        },
        "Description": "",
        "CreationTime": "2023-08-25T20:54:43",
        "LastUpdatedTime": "2023-08-25T20:54:43",
        "Tags": [
            {
                "Key": "Name",
                "Value": "my-va-endpoint"
            }
        ]
    }
}
```

Para obtener más información, consulte Verified Access endpoints en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte CreateVerifiedAccessEndpoint en la Referencia de comandos de la AWS CLI.

`create-verified-access-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-verified-access-group`.

AWS CLI

Para crear un grupo de Acceso verificado

En el siguiente ejemplo de `create-verified-access-group`, se crea un grupo de acceso verificado para la instancia de acceso verificado especificada.

```
aws ec2 create-verified-access-group \
    --verified-access-instance-id vai-0ce000c0b7643abea \
    --tag-specifications ResourceType=verified-access-
group,Tags=[{Key=Name,Value=my-va-group}]
```

Salida:

```
{
    "VerifiedAccessGroup": {
        "VerifiedAccessGroupId": "vagr-0dbe967baf14b7235",
        "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
        "Description": "",
        "Owner": "123456789012",
        "VerifiedAccessGroupArn": "arn:aws:ec2:us-east-2:123456789012:verified-
access-group/vagr-0dbe967baf14b7235",
        "CreationTime": "2023-08-25T19:55:19",
        "LastUpdatedTime": "2023-08-25T19:55:19",
        "Tags": [
            {
                "Key": "Name",
                "Value": "my-va-group"
            }
        ]
    }
}
```

Para obtener más información, consulte Verified Access groups en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte CreateVerifiedAccessGroup en la Referencia de comandos de la AWS CLI.

`create-verified-access-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-verified-access-instance`.

AWS CLI

Para crear una instancia de Acceso verificado

En el siguiente ejemplo de `create-verified-access-instance`, se crea una instancia de acceso verificado con una etiqueta de nombre.

```
aws ec2 create-verified-access-instance \
    --tag-specifications ResourceType=verified-access-
instance,Tags=[{Key=Name,Value=my-va-instance}]
```

Salida:

```
{
    "VerifiedAccessInstance": {
        "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
        "Description": "",
        "VerifiedAccessTrustProviders": [],
        "CreationTime": "2023-08-25T18:27:56",
        "LastUpdatedTime": "2023-08-25T18:27:56",
        "Tags": [
            {
                "Key": "Name",
                "Value": "my-va-instance"
            }
        ]
    }
}
```

Para obtener más información, consulte Verified Access instances en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte CreateVerifiedAccessInstance en la Referencia de comandos de la AWS CLI.

`create-verified-access-trust-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-verified-access-trust-provider`.

AWS CLI

Para crear un proveedor de confianza de Acceso verificado

En el siguiente ejemplo de `create-verified-access-trust-provider`, se configura un proveedor de confianza de acceso verificado mediante AWS Identity Center.

```
aws ec2 create-verified-access-trust-provider \
    --trust-provider-type user \
    --user-trust-provider-type iam-identity-center \
    --policy-reference-name idc \
    --tag-specifications ResourceType=verified-access-trust-
provider,Tags=[{Key=Name,Value=my-va-trust-provider}]
```

Salida:

```
{
    "VerifiedAccessTrustProvider": {
        "VerifiedAccessTrustProviderId": "vatp-0bb32de759a3e19e7",
        "Description": "",
        "TrustProviderType": "user",
        "UserTrustProviderType": "iam-identity-center",
        "PolicyReferenceName": "idc",
        "CreationTime": "2023-08-25T18:40:36",
        "LastUpdatedTime": "2023-08-25T18:40:36",
        "Tags": [
            {
                "Key": "Name",
                "Value": "my-va-trust-provider"
            }
        ]
    }
}
```

Para obtener más información, consulte Trust providers for Verified Access en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte CreateVerifiedAccessTrustProvider en la Referencia de comandos de la AWS CLI.

`create-volume`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-volume`.

AWS CLI

Para crear un volumen de SSD de uso general (gp2) vacío

En el siguiente ejemplo de `create-volume`, se crea un volumen de SSD de uso general (gp2) de 80 GiB en la zona de disponibilidad especificada. Tenga en cuenta que la región actual debe ser `us-east-1`. También puede agregar el parámetro `--region` para especificarla en el comando.

```
aws ec2 create-volume \
    --volume-type gp2 \
    --size 80 \
    --availability-zone us-east-1a
```

Salida:

```
{
    "AvailabilityZone": "us-east-1a",
    "Tags": [],
    "Encrypted": false,
    "VolumeType": "gp2",
    "VolumeId": "vol-1234567890abcdef0",
    "State": "creating",
    "Iops": 240,
    "SnapshotId": "",
    "CreateTime": "YYYY-MM-DDTHH:MM:SS.000Z",
    "Size": 80
}
```

Si no especifica un tipo de volumen, el predeterminado es gp2.

```
aws ec2 create-volume \
    --size 80 \
    --availability-zone us-east-1a
```

Ejemplo 2: creación de un volumen de SSD de IOPS aprovisionadas (io1) a partir de una instantánea

En el siguiente ejemplo de `create-volume`, se crea un volumen SSD de IOPS aprovisionadas (io1) con 1000 IOPS aprovisionadas en la zona de disponibilidad especificada mediante la instantánea especificada.

```
aws ec2 create-volume \
    --volume-type io1 \
    --iops 1000 \
    --snapshot-id snap-066877671789bd71b \
    --availability-zone us-east-1a
```

Salida:

```
{
    "AvailabilityZone": "us-east-1a",
    "Tags": [],
    "Encrypted": false,
    "VolumeType": "io1",
    "VolumeId": "vol-1234567890abcdef0",
    "State": "creating",
    "Iops": 1000,
    "SnapshotId": "snap-066877671789bd71b",
    "CreateTime": "YYYY-MM-DDTHH:MM:SS.000Z",
    "Size": 500
}
```

Ejemplo 3: creación de un volumen cifrado

En el siguiente ejemplo de `create-volume`, se crea un volumen cifrado con la CMK predeterminada para el cifrado de EBS. Si el cifrado se encuentra deshabilitado de forma predeterminada, debe especificar el parámetro `--encrypted` de la siguiente manera.

```
aws ec2 create-volume \
    --size 80 \
    --encrypted \
    --availability-zone us-east-1a
```

Salida:

```
{
    "AvailabilityZone": "us-east-1a",
    "Tags": [],
    "Encrypted": true,
    "VolumeType": "gp2",
    "VolumeId": "vol-1234567890abcdef0",
    "State": "creating",
    "Iops": 240,
    "SnapshotId": "",
    "CreateTime": "YYYY-MM-DDTHH:MM:SS.000Z",
    "Size": 80
}
```

Si el cifrado está habilitado de forma predeterminada, en el ejemplo de comando siguiente se crea un volumen cifrado, incluso sin el parámetro `--encrypted`.

```
aws ec2 create-volume \
    --size 80 \
    --availability-zone us-east-1a
```

Si se usa la opción `--kms-key-id` para especificar una CMK administrada por el cliente, también debe especificar la opción `--encrypted` aunque el cifrado esté habilitado de forma predeterminada.

```
aws ec2 create-volume \
    --volume-type gp2 \
    --size 80 \
    --encrypted \
    --kms-key-id 0ea3fef3-80a7-4778-9d8c-1c0c6EXAMPLE \
    --availability-zone us-east-1a
```

Ejemplo 4: creación de un volumen con etiquetas

En el siguiente ejemplo de `create-volume`, se crea un volumen y se agregan dos etiquetas.

```
aws ec2 create-volume \
    --availability-zone us-east-1a \
    --volume-type gp2 \
    --size 80 \
    --tag-specifications 'ResourceType=volume,Tags=[{Key=purpose,Value=production},
{Key=cost-center,Value=cc123}]'
```

- Para obtener información sobre la API, consulte CreateVolume en la Referencia de comandos de la AWS CLI.

`create-vpc-endpoint-connection-notification`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-vpc-endpoint-connection-notification`.

AWS CLI

Para crear una notificación de conexión de punto de conexión

En este ejemplo se crea una notificación para un servicio de punto de conexión específico que le avisa cuando los puntos de conexión de interfaz se han conectado a su servicio y cuando los puntos de conexión se han aceptado para su servicio.

Comando:

```
aws ec2 create-vpc-endpoint-connection-notification --connection-notification-
arn arn:aws:sns:us-east-2:123456789012:VpceNotification --connection-
events Connect Accept --service-id vpce-svc-1237881c0d25a3abc
```

Salida:

```
{
   "ConnectionNotification": {
       "ConnectionNotificationState": "Enabled",
       "ConnectionNotificationType": "Topic",
       "ServiceId": "vpce-svc-1237881c0d25a3abc",
       "ConnectionEvents": [
           "Accept",
           "Connect"
       ],
       "ConnectionNotificationId": "vpce-nfn-008776de7e03f5abc",
       "ConnectionNotificationArn": "arn:aws:sns:us-
east-2:123456789012:VpceNotification"
   }
 }
```

- Para obtener información sobre la API, consulte CreateVpcEndpointConnectionNotification en la Referencia de comandos de la AWS CLI.

`create-vpc-endpoint-service-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-vpc-endpoint-service-configuration`.

AWS CLI

Ejemplo 1: creación de una configuración de servicio de punto de conexión para un punto de conexión de interfaz

En el siguiente ejemplo de `create-vpc-endpoint-service-configuration`, se crea una configuración de servicio de punto de conexión de VPC mediante el equilibrador de carga de red `nlb-vpce`. En este ejemplo también se especifica que se deben aceptar las solicitudes de conexión al servicio a través de un punto de conexión de interfaz.

```
aws ec2 create-vpc-endpoint-service-configuration \
    --network-load-balancer-arns arn:aws:elasticloadbalancing:us-
east-1:123456789012:loadbalancer/net/nlb-vpce/e94221227f1ba532 \
    --acceptance-required
```

Salida:

```
{
   "ServiceConfiguration": {
       "ServiceType": [
           {
               "ServiceType": "Interface"
           }
       ],
       "NetworkLoadBalancerArns": [
           "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/
nlb-vpce/e94221227f1ba532"
       ],
       "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-03d5ebb7d9579a2b3",
       "ServiceState": "Available",
       "ServiceId": "vpce-svc-03d5ebb7d9579a2b3",
       "AcceptanceRequired": true,
       "AvailabilityZones": [
           "us-east-1d"
       ],
       "BaseEndpointDnsNames": [
           "vpce-svc-03d5ebb7d9579a2b3.us-east-1.vpce.amazonaws.com"
```

```
        ]
    }
}
```

Para obtener más información, consulte Crear un servicio de punto de conexión en la Guía del usuario de AWS PrivateLink.

Ejemplo 2: creación de una configuración de servicio de punto de conexión para un punto de conexión de equilibrador de carga de puerta de enlace

En el siguiente ejemplo de `create-vpc-endpoint-service-configuration`, se crea una configuración de servicio de punto de conexión de VPC mediante el equilibrador de carga de puerta de enlace `GWLBService`. Las solicitudes de conexión al servicio a través de un punto de conexión de equilibrador de carga de puerta de enlace se aceptan automáticamente.

```
aws ec2 create-vpc-endpoint-service-configuration \
    --gateway-load-balancer-arns arn:aws:elasticloadbalancing:us-
east-1:123456789012:loadbalancer/gwy/GWLBService/123123123123abcc \
    --no-acceptance-required
```

Salida:

```
{
    "ServiceConfiguration": {
        "ServiceType": [
            {
                "ServiceType": "GatewayLoadBalancer"
            }
        ],
        "ServiceId": "vpce-svc-123123a1c43abc123",
        "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-123123a1c43abc123",
        "ServiceState": "Available",
        "AvailabilityZones": [
            "us-east-1d"
        ],
        "AcceptanceRequired": false,
        "ManagesVpcEndpoints": false,
        "GatewayLoadBalancerArns": [
            "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/gwy/
GWLBService/123123123123abcc"
        ]
    }
```

```
}
```

Para obtener más información, consulte Crear un servicio de punto de conexión de equilibrador de carga de puerta de enlace en la Guía del usuario de AWS PrivateLink.

- Para obtener información sobre la API, consulte CreateVpcEndpointServiceConfiguration en la Referencia de comandos de la AWS CLI.

`create-vpc-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-vpc-endpoint`.

AWS CLI

Ejemplo 1: creación de un punto de conexión de puerta de enlace

En el siguiente ejemplo de `create-vpc-endpoint`, se crea un punto de conexión de VPC de puerta de enlace entre la VPC `vpc-1a2b3c4d` y Amazon S3 en la región `us-east-1` y se asocia la tabla de enrutamiento `rtb-11aa22bb` al punto de conexión.

```
aws ec2 create-vpc-endpoint \
    --vpc-id vpc-1a2b3c4d \
    --service-name com.amazonaws.us-east-1.s3 \
    --route-table-ids rtb-11aa22bb
```

Salida:

```
{
    "VpcEndpoint": {
        "PolicyDocument": "{\"Version\":\"2008-10-17\",\"Statement\":[{\"Sid\":\"\",
\"Effect\":\"Allow\",\"Principal\":\"\*\",\"Action\":\"\*\",\"Resource\":\"\*\"}]}",
        "VpcId": "vpc-1a2b3c4d",
        "State": "available",
        "ServiceName": "com.amazonaws.us-east-1.s3",
        "RouteTableIds": [
            "rtb-11aa22bb"
        ],
        "VpcEndpointId": "vpc-1a2b3c4d",
        "CreationTimestamp": "2015-05-15T09:40:50Z"
    }
}
```

Para obtener más información, consulte Crear un punto de conexión de puerta de enlace en la Guía del usuario de AWS PrivateLink.

Ejemplo 2: creación de un punto de conexión de interfaz

En el siguiente ejemplo de `create-vpc-endpoint`, se crea un punto de conexión de VPC de interfaz entre la VPC `vpc-1a2b3c4d` y Amazon S3 en la región `us-east-1`. En el comando se crea el punto de conexión en la subred `subnet-1a2b3c4d`, se asocia al grupo de seguridad `sg-1a2b3c4d` y se agrega una etiqueta con la clave Service y el valor S3.

```
aws ec2 create-vpc-endpoint \
    --vpc-id vpc-1a2b3c4d \
    --vpc-endpoint-type Interface \
    --service-name com.amazonaws.us-east-1.s3 \
    --subnet-ids subnet-7b16de0c \
    --security-group-id sg-1a2b3c4d \
    --tag-specifications ResourceType=vpc-endpoint,Tags=[{Key=service,Value=S3}]
```

Salida:

```
{
    "VpcEndpoint": {
        "VpcEndpointId": "vpce-1a2b3c4d5e6f1a2b3",
        "VpcEndpointType": "Interface",
        "VpcId": "vpc-1a2b3c4d",
        "ServiceName": "com.amazonaws.us-east-1.s3",
        "State": "pending",
        "RouteTableIds": [],
        "SubnetIds": [
            "subnet-1a2b3c4d"
        ],
        "Groups": [
            {
                "GroupId": "sg-1a2b3c4d",
                "GroupName": "default"
            }
        ],
        "PrivateDnsEnabled": false,
        "RequesterManaged": false,
        "NetworkInterfaceIds": [
            "eni-0b16f0581c8ac6877"
        ],
```

```
        "DnsEntries": [
            {
                "DnsName": "*.vpce-1a2b3c4d5e6f1a2b3-9hnenorg.s3.us-
east-1.vpce.amazonaws.com",
                "HostedZoneId": "Z7HUB22UULQXV"
            },
            {
                "DnsName": "*.vpce-1a2b3c4d5e6f1a2b3-9hnenorg-us-east-1c.s3.us-
east-1.vpce.amazonaws.com",
                "HostedZoneId": "Z7HUB22UULQXV"
            }
        ],
        "CreationTimestamp": "2021-03-05T14:46:16.030000+00:00",
        "Tags": [
            {
                "Key": "service",
                "Value": "S3"
            }
        ],
        "OwnerId": "123456789012"
    }
}
```

Para obtener más información, consulte Crear un punto de conexión de VPC de interfaz en la Guía del usuario de AWS PrivateLink.

Ejemplo 3: creación de un punto de conexión de equilibrador de carga de puerta de enlace

En el siguiente ejemplo de `create-vpc-endpoint`, se crea un punto de conexión de equilibrador de carga de puerta de enlace entre la VPC `vpc-111122223333aabbc` y un servicio que se configura mediante un equilibrador de carga de puerta de enlace.

```
aws ec2 create-vpc-endpoint \
    --service-name com.amazonaws.vpce.us-east-1.vpce-svc-123123a1c43abc123 \
    --vpc-endpoint-type GatewayLoadBalancer \
    --vpc-id vpc-111122223333aabbc \
    --subnet-ids subnet-0011aabbcc2233445
```

Salida:

```
{
    "VpcEndpoint": {
```

```
        "VpcEndpointId": "vpce-aabbaabbaabbaabba",
        "VpcEndpointType": "GatewayLoadBalancer",
        "VpcId": "vpc-111122223333aabbc",
        "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-123123a1c43abc123",
        "State": "pending",
        "SubnetIds": [
            "subnet-0011aabbcc2233445"
        ],
        "RequesterManaged": false,
        "NetworkInterfaceIds": [
            "eni-01010120203030405"
        ],
        "CreationTimestamp": "2020-11-11T08:06:03.522Z",
        "OwnerId": "123456789012"
    }
}
```

Para obtener más información, consulte Puntos de conexión del equilibrador de carga de la puerta de enlace en la Guía del usuario de AWS PrivateLink.

Ejemplo 4: creación de un punto de conexión de recurso

En el siguiente ejemplo de `create-vpc-endpoint`, se crea un punto de conexión de recurso.

```
aws ec2 create-vpc-endpoint \
    --vpc-endpoint-type Resource \
    --vpc-id vpc-111122223333aabbc \
    --subnet-ids subnet-0011aabbcc2233445 \
    --resource-configuration-arn arn:aws:vpc-lattice-us-
east-1:123456789012:resourceconfiguration/rcfg-0123abcde98765432
```

Salida:

```
{
    "VpcEndpoint": {
        "VpcEndpointId": "vpce-00939a7ed9EXAMPLE",
        "VpcEndpointType": "Resource",
        "VpcId": "vpc-111122223333aabbc",
        "State": "Pending",
        "SubnetIds": [
            "subnet-0011aabbcc2233445"
        ],
        "Groups": [
```

```
            {
                "GroupId": "sg-03e2f15fbfc09b000",
                "GroupName": "default"
            }
        ],
        "IpAddressType": "IPV4",
        "PrivateDnsEnabled": false,
        "CreationTimestamp": "2025-02-06T23:38:49.525000+00:00",
        "Tags": [],
        "OwnerId": "123456789012",
        "ResourceConfigurationArn": "arn:aws:vpc-lattice:us-
east-1:123456789012:resourceconfiguration/rcfg-0123abcde98765432"
    }
}
```

Para obtener más información, consulte Puntos de conexión de recurso en la Guía del usuario de AWS PrivateLink.

Ejemplo 5: creación de un punto de conexión de red de servicios

En el siguiente ejemplo de `create-vpc-endpoint`, se crea un punto de conexión de red de servicios.

```
aws ec2 create-vpc-endpoint \
    --vpc-endpoint-type ServiceNetwork \
    --vpc-id vpc-111122223333aabbc \
    --subnet-ids subnet-0011aabbcc2233445 \
    --service-network-arn arn:aws:vpc-lattice:us-east-1:123456789012:servicenetwork/
sn-0101abcd5432abcd0 \
    --security-group-ids sg-0123456789012abcd
```

Salida:

```
{
    "VpcEndpoint": {
        "VpcEndpointId": "vpce-0f00567fa8EXAMPLE",
        "VpcEndpointType": "ServiceNetwork",
        "VpcId": "vpc-111122223333aabbc",
        "State": "Pending",
        "SubnetIds": [
            "subnet-0011aabbcc2233445"
        ],
```

```
        "Groups": [
            {
                "GroupId": "sg-0123456789012abcd",
                "GroupName": "my-security-group"
            }
        ],
        "IpAddressType": "IPV4",
        "PrivateDnsEnabled": false,
        "CreationTimestamp": "2025-02-06T23:44:20.449000+00:00",
        "Tags": [],
        "OwnerId": "123456789012",
        "ServiceNetworkArn": "arn:aws:vpc-lattice:us-
east-1:123456789012:servicenetwork/sn-0101abcd5432abcd0"
    }
}
```

Para obtener más información, consulte Puntos de conexión de red de servicios en la Guía del usuario de AWS PrivateLink.

- Para obtener información sobre la API, consulte CreateVpcEndpoint en la Referencia de comandos de la AWS CLI.

`create-vpc-peering-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-vpc-peering-connection`.

AWS CLI

Para crear una conexión de emparejamiento de VPC entre las VPC

En este ejemplo se solicita una conexión de emparejamiento entre las VPC vpc-1a2b3c4d y vpc-11122233.

Comando:

```
aws ec2 create-vpc-peering-connection --vpc-id vpc-1a2b3c4d --peer-vpc-
id vpc-11122233
```

Salida:

```
{
    "VpcPeeringConnection": {
```

```
        "Status": {
            "Message": "Initiating Request to 444455556666",
            "Code": "initiating-request"
        },
        "Tags": [],
        "RequesterVpcInfo": {
            "OwnerId": "444455556666",
            "VpcId": "vpc-1a2b3c4d",
            "CidrBlock": "10.0.0.0/28"
        },
        "VpcPeeringConnectionId": "pcx-111aaa111",
        "ExpirationTime": "2014-04-02T16:13:36.000Z",
        "AccepterVpcInfo": {
            "OwnerId": "444455556666",
            "VpcId": "vpc-11122233"
        }
    }
}
```

Para crear una conexión de emparejamiento de VPC con una VPC de otra cuenta

En este ejemplo se solicita una conexión de emparejamiento entre su VPC (vpc-1a2b3c4d) y una VPC (vpc-11122233) que pertenece a la cuenta de AWS 123456789012.

Comando:

```
aws ec2 create-vpc-peering-connection --vpc-id vpc-1a2b3c4d --peer-vpc-
id vpc-11122233 --peer-owner-id 123456789012
```

Para crear una conexión de emparejamiento de VPC con una VPC de otra región

En este ejemplo se solicita una conexión de emparejamiento entre su VPC de la región actual (vpc-1a2b3c4d) y una VPC (vpc-11122233) que pertenece a su cuenta en la región `us-west-2`.

Comando:

```
aws ec2 create-vpc-peering-connection --vpc-id vpc-1a2b3c4d --peer-vpc-
id vpc-11122233 --peer-region us-west-2
```

En este ejemplo se solicita una conexión de emparejamiento entre su VPC de la región actual (vpc-1a2b3c4d) y una VPC (vpc-11122233) que pertenece a su cuenta de AWS 123456789012 que se encuentra en la región `us-west-2`.

Comando:

```
aws ec2 create-vpc-peering-connection --vpc-id vpc-1a2b3c4d --peer-vpc-
id vpc-11122233 --peer-owner-id 123456789012 --peer-region us-west-2
```

- Para obtener información sobre la API, consulte CreateVpcPeeringConnection en la Referencia de comandos de la AWS CLI.

`create-vpc`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-vpc`.

AWS CLI

Ejemplo 1: Crear una VPC

En el siguiente ejemplo de `create-vpc`, se crea una VPC con el bloque de CIDR IPv4 especificado y una etiqueta de nombre.

```
aws ec2 create-vpc \
    --cidr-block 10.0.0.0/16 \
    --tag-specifications ResourceType=vpc,Tags=[{Key=Name,Value=MyVpc}]
```

Salida:

```
{
    "Vpc": {
        "CidrBlock": "10.0.0.0/16",
        "DhcpOptionsId": "dopt-5EXAMPLE",
        "State": "pending",
        "VpcId": "vpc-0a60eb65b4EXAMPLE",
        "OwnerId": "123456789012",
        "InstanceTenancy": "default",
        "Ipv6CidrBlockAssociationSet": [],
        "CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-07501b79ecEXAMPLE",
                "CidrBlock": "10.0.0.0/16",
                "CidrBlockState": {
                    "State": "associated"
                }
```

```
            }
        ],
        "IsDefault": false,
        "Tags": [
            {
                "Key": "Name",
                "Value": MyVpc"
            }
        ]
    }
}
```

Ejemplo 2: Crear una VPC con un tenencia dedicada

En el siguiente ejemplo de `create-vpc`, se crea una VPC con el bloque de CIDR IPv4 especificado y una tenencia dedicada.

```
aws ec2 create-vpc \
    --cidr-block 10.0.0.0/16 \
    --instance-tenancy dedicated
```

Salida:

```
{
    "Vpc": {
        "CidrBlock": "10.0.0.0/16",
        "DhcpOptionsId": "dopt-19edf471",
        "State": "pending",
        "VpcId": "vpc-0a53287fa4EXAMPLE",
        "OwnerId": "111122223333",
        "InstanceTenancy": "dedicated",
        "Ipv6CidrBlockAssociationSet": [],
        "CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-00b24cc1c2EXAMPLE",
                "CidrBlock": "10.0.0.0/16",
                "CidrBlockState": {
                    "State": "associated"
                }
            }
        ],
        "IsDefault": false
    }
```

```
}
```

Ejemplo 3: crear una VPC con un bloque de CIDR IPv

En el siguiente ejemplo de `create-vpc`, se crea una VPC con un bloque de CIDR IPv6 proporcionado por Amazon.

```
aws ec2 create-vpc \
    --cidr-block 10.0.0.0/16 \
    --amazon-provided-ipv6-cidr-block
```

Salida:

```
{
    "Vpc": {
        "CidrBlock": "10.0.0.0/16",
        "DhcpOptionsId": "dopt-dEXAMPLE",
        "State": "pending",
        "VpcId": "vpc-0fc5e3406bEXAMPLE",
        "OwnerId": "123456789012",
        "InstanceTenancy": "default",
        "Ipv6CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-068432c60bEXAMPLE",
                "Ipv6CidrBlock": "",
                "Ipv6CidrBlockState": {
                    "State": "associating"
                },
                "Ipv6Pool": "Amazon",
                "NetworkBorderGroup": "us-west-2"
            }
        ],
        "CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-0669f8f9f5EXAMPLE",
                "CidrBlock": "10.0.0.0/16",
                "CidrBlockState": {
                    "State": "associated"
                }
            }
        ],
        "IsDefault": false
    }
```

```
}
```

Ejemplo 4: crear una VPC con un CIDR desde un grupo de IPAM

En el siguiente ejemplo de `create-vpc`, se crea una VPC con un CIDR desde un grupo del Administrador de direcciones IP (IPAM) de Amazon VPC.

Linux y macOS:

```
aws ec2 create-vpc \
    --ipv4-ipam-pool-id ipam-pool-0533048da7d823723 \
    --tag-specifications ResourceType=vpc,Tags='[{Key=Environment,Value="Preprod"},
{Key=Owner,Value="Build Team"}]'
```

Windows:

```
aws ec2 create-vpc ^
    --ipv4-ipam-pool-id ipam-pool-0533048da7d823723 ^
    --tag-specifications ResourceType=vpc,Tags=[{Key=Environment,Value="Preprod"},
{Key=Owner,Value="Build Team"}]
```

Salida:

```
{
    "Vpc": {
        "CidrBlock": "10.0.1.0/24",
        "DhcpOptionsId": "dopt-2afccf50",
        "State": "pending",
        "VpcId": "vpc-010e1791024eb0af9",
        "OwnerId": "123456789012",
        "InstanceTenancy": "default",
        "Ipv6CidrBlockAssociationSet": [],
        "CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-0a77de1d803226d4b",
                "CidrBlock": "10.0.1.0/24",
                "CidrBlockState": {
                    "State": "associated"
                }
            }
        ],
        "IsDefault": false,
```

```
        "Tags": [
            {
                "Key": "Environment",
                "Value": "Preprod"
            },
            {
                "Key": "Owner",
                "Value": "Build Team"
            }
        ]
    }
}
```

Para obtener más información, consulte Crear una VPC que use un CIDR de un grupo de IPAM en la Guía del usuario de IPAM de Amazon VPC.

- Para obtener información sobre la API, consulte CreateVpc en la Referencia de comandos de la AWS CLI.

`create-vpn-connection-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-vpn-connection-route`.

AWS CLI

Para crear una ruta estática para una conexión de VPN

En este ejemplo se crea una ruta estática para la conexión de VPN especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 create-vpn-connection-route --vpn-connection-id vpn-40f41529 --destination-cidr-block 11.12.0.0/16
```

- Para obtener información sobre la API, consulte CreateVpnConnectionRoute en la Referencia de comandos de la AWS CLI.

`create-vpn-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-vpn-connection`.

AWS CLI

Ejemplo 1: creación de una conexión de VPN con enrutamiento dinámico

En el siguiente ejemplo de `create-vpn-connection`, se crea una conexión de VPN entre la puerta de enlace privada virtual especificada y la puerta de enlace de cliente especificada, y se aplican etiquetas a la conexión de VPN. La salida incluye la información de configuración del dispositivo de puerta de enlace de cliente en formato XML.

```
aws ec2 create-vpn-connection \
    --type ipsec.1 \
    --customer-gateway-id cgw-001122334455aabbc \
    --vpn-gateway-id vgw-1a1a1a1a1a1a2b2b2 \
    --tag-specification 'ResourceType=vpn-connection,Tags=[{Key=Name,Value=BGP-
VPN}]'
```

Salida:

```
{
    "VpnConnection": {
        "CustomerGatewayConfiguration": "...configuration information...",
        "CustomerGatewayId": "cgw-001122334455aabbc",
        "Category": "VPN",
        "State": "pending",
        "VpnConnectionId": "vpn-123123123123abcab",
        "VpnGatewayId": "vgw-1a1a1a1a1a1a2b2b2",
        "Options": {
            "EnableAcceleration": false,
            "StaticRoutesOnly": false,
            "LocalIpv4NetworkCidr": "0.0.0.0/0",
            "RemoteIpv4NetworkCidr": "0.0.0.0/0",
            "TunnelInsideIpVersion": "ipv4",
            "TunnelOptions": [
                {},
                {}
            ]
        },
        "Routes": [],
        "Tags": [
             {
                "Key": "Name",
                "Value": "BGP-VPN"
            }
```

```
        ]
    }
}
```

Para obtener más información, consulte How AWS Site-to-Site VPN works en la Guía del usuario de AWS Site-to-Site VPN.

Ejemplo 2: creación de una conexión de VPN con enrutamiento estático

En el siguiente ejemplo de `create-vpn-connection`, se crea una conexión de VPN entre la puerta de enlace privada virtual especificada y la puerta de enlace de cliente especificada. Las opciones especifican el enrutamiento estático. La salida incluye la información de configuración del dispositivo de puerta de enlace de cliente en formato XML.

```
aws ec2 create-vpn-connection \
    --type ipsec.1 \
    --customer-gateway-id cgw-001122334455aabbc \
    --vpn-gateway-id vgw-1a1a1a1a1a1a2b2b2 \
    --options "{\"StaticRoutesOnly\":true}"
```

Salida:

```
{
    "VpnConnection": {
        "CustomerGatewayConfiguration": "..configuration information...",
        "CustomerGatewayId": "cgw-001122334455aabbc",
        "Category": "VPN",
        "State": "pending",
        "VpnConnectionId": "vpn-123123123123abcab",
        "VpnGatewayId": "vgw-1a1a1a1a1a1a2b2b2",
        "Options": {
            "EnableAcceleration": false,
            "StaticRoutesOnly": true,
            "LocalIpv4NetworkCidr": "0.0.0.0/0",
            "RemoteIpv4NetworkCidr": "0.0.0.0/0",
            "TunnelInsideIpVersion": "ipv4",
            "TunnelOptions": [
                {},
                {}
            ]
        },
        "Routes": [],
```

```
        "Tags": []
    }
}
```

Para obtener más información, consulte How AWS Site-to-Site VPN works en la Guía del usuario de AWS Site-to-Site VPN.

Ejemplo 3: creación de una conexión de VPN y especificación de la suya propia dentro del CIDR y de la clave compartida previamente

En el siguiente ejemplo de `create-vpn-connection`, se crea una conexión de VPN y se especifican el bloque de CIDR de direcciones IP interno y una clave previamente compartida y personalizada para cada túnel. Los valores especificados se devuelven en la información de `CustomerGatewayConfiguration`.

```
aws ec2 create-vpn-connection \
    --type ipsec.1 \
    --customer-gateway-id cgw-001122334455aabbc \
    --vpn-gateway-id vgw-1a1a1a1a1a1a2b2b2 \
    --options
 TunnelOptions='[{TunnelInsideCidr=169.254.12.0/30,PreSharedKey=ExamplePreSharedKey1},
{TunnelInsideCidr=169.254.13.0/30,PreSharedKey=ExamplePreSharedKey2}]'
```

Salida:

```
{
    "VpnConnection": {
        "CustomerGatewayConfiguration": "..configuration information...",
        "CustomerGatewayId": "cgw-001122334455aabbc",
        "Category": "VPN",
        "State": "pending",
        "VpnConnectionId": "vpn-123123123123abcab",
        "VpnGatewayId": "vgw-1a1a1a1a1a1a2b2b2",
        "Options": {
            "EnableAcceleration": false,
            "StaticRoutesOnly": false,
            "LocalIpv4NetworkCidr": "0.0.0.0/0",
            "RemoteIpv4NetworkCidr": "0.0.0.0/0",
            "TunnelInsideIpVersion": "ipv4",
            "TunnelOptions": [
                {
                    "OutsideIpAddress": "203.0.113.3",
```

```
                    "TunnelInsideCidr": "169.254.12.0/30",
                    "PreSharedKey": "ExamplePreSharedKey1"
                },
                {
                    "OutsideIpAddress": "203.0.113.5",
                    "TunnelInsideCidr": "169.254.13.0/30",
                    "PreSharedKey": "ExamplePreSharedKey2"
                }
            ]
        },
        "Routes": [],
        "Tags": []
    }
}
```

Para obtener más información, consulte How AWS Site-to-Site VPN works en la Guía del usuario de AWS Site-to-Site VPN.

Ejemplo 4: creación de una conexión de VPN que admita el tráfico de IPv

En el siguiente ejemplo de `create-vpn-connection`, se crea una conexión de VPN que admite el tráfico de IPv6 entre la puerta de enlace de tránsito especificada y la puerta de enlace de cliente especificada. Las opciones de túnel para ambos túneles especifican que AWS debe iniciar la negociación de IKE.

```
aws ec2 create-vpn-connection \
    --type ipsec.1 \
    --transit-gateway-id tgw-12312312312312312 \
    --customer-gateway-id cgw-001122334455aabbc \
    --options TunnelInsideIpVersion=ipv6,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

Salida:

```
{
    "VpnConnection": {
        "CustomerGatewayConfiguration": "..configuration information...",
        "CustomerGatewayId": "cgw-001122334455aabbc",
        "Category": "VPN",
        "State": "pending",
        "VpnConnectionId": "vpn-11111111122222222",
        "TransitGatewayId": "tgw-12312312312312312",
```

```
        "Options": {
            "EnableAcceleration": false,
            "StaticRoutesOnly": false,
            "LocalIpv6NetworkCidr": "::/0",
            "RemoteIpv6NetworkCidr": "::/0",
            "TunnelInsideIpVersion": "ipv6",
            "TunnelOptions": [
                {
                    "OutsideIpAddress": "203.0.113.3",
                    "StartupAction": "start"
                },
                {
                    "OutsideIpAddress": "203.0.113.5",
                    "StartupAction": "start"
                }
            ]
        },
        "Routes": [],
        "Tags": []
    }
}
```

Para obtener más información, consulte How AWS Site-to-Site VPN works en la Guía del usuario de AWS Site-to-Site VPN.

- Para obtener información sobre la API, consulte CreateVpnConnection en la Referencia de comandos de la AWS CLI.

`create-vpn-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-vpn-gateway`.

AWS CLI

Para crear una puerta de enlace privada virtual

En este ejemplo se crea una puerta de enlace privada virtual.

Comando:

```
aws ec2 create-vpn-gateway --type ipsec.1
```

Salida:

```
{
    "VpnGateway": {
        "AmazonSideAsn": 64512,
        "State": "available",
        "Type": "ipsec.1",
        "VpnGatewayId": "vgw-9a4cacf3",
        "VpcAttachments": []
    }
}
```

Para crear una puerta de enlace privada virtual con un ASN específico de Amazon

En este ejemplo se crea una puerta de enlace privada virtual y se especifica el número de sistema autónomo (ASN) de Amazon de la sesión de BGP.

Comando:

```
aws ec2 create-vpn-gateway --type ipsec.1 --amazon-side-asn 65001
```

Salida:

```
{
    "VpnGateway": {
        "AmazonSideAsn": 65001,
        "State": "available",
        "Type": "ipsec.1",
        "VpnGatewayId": "vgw-9a4cacf3",
        "VpcAttachments": []
    }
}
```

- Para obtener información sobre la API, consulte CreateVpnGateway en la Referencia de comandos de la AWS CLI.

`delete-carrier-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-carrier-gateway`.

AWS CLI

Para eliminar una puerta de enlace de operador

En el siguiente ejemplo de `delete-carrier-gateway`, se elimina la puerta de enlace de operador especificada.

```
aws ec2 delete-carrier-gateway \
    --carrier-gateway-id cagw-0465cdEXAMPLE1111
```

Salida:

```
{
    "CarrierGateway": {
        "CarrierGatewayId": "cagw-0465cdEXAMPLE1111",
        "VpcId": "vpc-0c529aEXAMPLE1111",
        "State": "deleting",
        "OwnerId": "123456789012"
    }
}
```

Para obtener más información, consulte Carrier gateways en la Guía del usuario de Amazon Virtual Private Cloud.

- Para obtener información sobre la API, consulte DeleteCarrierGateway en la Referencia de comandos de la AWS CLI.

`delete-client-vpn-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-client-vpn-endpoint`.

AWS CLI

Para eliminar un punto de conexión de Client VPN

En el siguiente ejemplo de `delete-client-vpn-endpoint`, se elimina el punto de conexión de Client VPN especificado.

```
aws ec2 delete-client-vpn-endpoint \
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde
```

Salida:

```
{
    "Status": {
```

```
        "Code": "deleting"
    }
}
```

Para obtener más información, consulte Client VPN Endpoints en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte DeleteClientVpnEndpoint en la Referencia de comandos de la AWS CLI.

`delete-client-vpn-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-client-vpn-route`.

AWS CLI

Para eliminar una ruta de un punto de conexión de Client VPN

En el siguiente ejemplo de `delete-client-vpn-route`, se elimina la ruta `0.0.0.0/0` para la subred especificada de un punto de conexión de Client VPN.

```
aws ec2 delete-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde \
    --destination-cidr-block 0.0.0.0/0 \
    --target-vpc-subnet-id subnet-0123456789abcabca
```

Salida:

```
{
    "Status": {
        "Code": "deleting"
    }
}
```

Para obtener más información, consulte Routes en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte DeleteClientVpnRoute en la Referencia de comandos de la AWS CLI.

`delete-coip-cidr`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-coip-cidr`.

AWS CLI

Para eliminar un rango de direcciones IP propiedad del cliente (CoIP

En el siguiente ejemplo de `delete-coip-cidr`, se elimina el rango especificado de direcciones de CoIP en el grupo de CoIP especificado.

```
aws ec2 delete-coip-cidr \
    --cidr 14.0.0.0/24 \
    --coip-pool-id ipv4pool-coip-1234567890abcdefg
```

Salida:

```
{
    "CoipCidr": {
        "Cidr": "14.0.0.0/24",
        "CoipPoolId": "ipv4pool-coip-1234567890abcdefg",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890"
    }
}
```

Para obtener más información, consulte Direcciones IP propiedad del cliente en la Guía del usuario de AWS.

- Para obtener información sobre la API, consulte DeleteCoipCidr en la Referencia de comandos de la AWS CLI.

`delete-coip-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-coip-pool`.

AWS CLI

Para eliminar un grupo de direcciones IP propiedad del cliente (CoIP

En el siguiente ejemplo de `delete-coip-pool`, se elimina un grupo de CoIP de direcciones de CoIP.

```
aws ec2 delete-coip-pool \
    --coip-pool-id ipv4pool-coip-1234567890abcdefg
```

Salida:

```
{
    "CoipPool": {
        "PoolId": "ipv4pool-coip-1234567890abcdefg",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890",
        "PoolArn": "arn:aws:ec2:us-west-2:123456789012:coip-pool/ipv4pool-
coip-1234567890abcdefg"
    }
}
```

Para obtener más información, consulte Direcciones IP propiedad del cliente en la Guía del usuario de AWS.

- Para obtener información sobre la API, consulte DeleteCoipPool en la Referencia de comandos de la AWS CLI.

`delete-customer-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-customer-gateway`.

AWS CLI

Para eliminar una puerta de enlace de cliente

En este ejemplo se elimina la puerta de enlace de cliente especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-customer-gateway --customer-gateway-id cgw-0e11f167
```

- Para obtener información sobre la API, consulte DeleteCustomerGateway en la Referencia de comandos de la AWS CLI.

`delete-dhcp-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-dhcp-options`.

AWS CLI

Para eliminar un conjunto de opciones de DHCP

En este ejemplo se elimina el conjunto de opciones de DHCP especificado. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-dhcp-options --dhcp-options-id dopt-d9070ebb
```

- Para obtener información sobre la API, consulte DeleteDhcpOptions en la Referencia de comandos de la AWS CLI.

`delete-egress-only-internet-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-egress-only-internet-gateway`.

AWS CLI

Para eliminar una puerta de enlace de Internet de solo salida

En este ejemplo se elimina la puerta de enlace de Internet de solo salida especificada.

Comando:

```
aws ec2 delete-egress-only-internet-gateway --egress-only-internet-gateway-
id eigw-01eadbd45ecd7943f
```

Salida:

```
{
  "ReturnCode": true
}
```

- Para obtener información sobre la API, consulte DeleteEgressOnlyInternetGateway en la Referencia de comandos de la AWS CLI.

`delete-fleets`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-fleets`.

AWS CLI

Ejemplo 1: eliminación de una flota de EC2 y terminación de las instancias asociadas

En el siguiente ejemplo de `delete-fleets`, se elimina la flota de EC2 especificada y se terminan las instancias bajo demanda y las instancias de spot asociadas.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE \
    --terminate-instances
```

Salida:

```
{
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_terminating",
            "PreviousFleetState": "active",
            "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
        }
    ],
    "UnsuccessfulFleetDeletions": []
}
```

Para obtener más información, consulte Delete an EC2 Fleet en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

Ejemplo 2: eliminación de una flota de EC2 sin terminar las instancias asociadas

En el siguiente ejemplo de `delete-fleets`, se elimina la flota de EC2 especificada sin terminar las instancias bajo demanda y las instancias de spot asociadas.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE \
    --no-terminate-instances
```

Salida:

```
{
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_running",
```

```
            "PreviousFleetState": "active",
            "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
        }
    ],
    "UnsuccessfulFleetDeletions": []
}
```

Para obtener más información, consulte Delete an EC2 Fleet en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

- Para obtener información sobre la API, consulte DeleteFleets en la Referencia de comandos de la AWS CLI.

`delete-flow-logs`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-flow-logs`.

AWS CLI

Para eliminar un registro de flujo

En el siguiente ejemplo de `delete-flow-logs`, se elimina el registro de flujo especificado.

```
aws ec2 delete-flow-logs --flow-log-id fl-11223344556677889
```

Salida:

```
{
    "Unsuccessful": []
}
```

- Para obtener información sobre la API, consulte DeleteFlowLogs en la Referencia de comandos de la AWS CLI.

`delete-fpga-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-fpga-image`.

AWS CLI

Para eliminar una imagen de Amazon FPGA

En este ejemplo se elimina la AFI especificada.

Comando:

```
aws ec2 delete-fpga-image --fpga-image-id afi-06b12350a123fbabc
```

Salida:

```
{
  "Return": true
}
```

- Para obtener información sobre la API, consulte DeleteFpgaImage en la Referencia de comandos de la AWS CLI.

`delete-instance-connect-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-instance-connect-endpoint`.

AWS CLI

Para eliminar un punto de conexión de EC2 Instance Connect

En el siguiente ejemplo de `delete-instance-connect-endpoint`, se elimina el punto de conexión de EC2 Instance Connect especificado.

```
aws ec2 delete-instance-connect-endpoint \
    --instance-connect-endpoint-id eice-03f5e49b83924bbc7
```

Salida:

```
{
    "InstanceConnectEndpoint": {
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "delete-in-progress",
        "StateMessage": "",
        "NetworkInterfaceIds": [],
```

```
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1d",
        "CreatedAt": "2023-02-07T12:05:37+00:00",
        "SubnetId": "subnet-0123abcd"
    }
}
```

Para obtener más información, consulte Eliminar un punto de conexión de EC2 Instance Connect en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DeleteInstanceConnectEndpoint en la Referencia de comandos de la AWS CLI.

`delete-instance-event-window`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-instance-event-window`.

AWS CLI

Ejemplo 1: eliminación de un período de evento

En el siguiente ejemplo de `delete-instance-event-window`, se elimina un período de evento.

```
aws ec2 delete-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890
```

Salida:

```
{
    "InstanceEventWindowState": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "State": "deleting"
    }
}
```

Para conocer las restricciones de los períodos de eventos, consulte Consideraciones en la sección sobre eventos programados de la Guía del usuario de Amazon EC2.

Ejemplo 2: eliminación forzada de un período de evento

En el siguiente ejemplo de `delete-instance-event-window`, se fuerza la eliminación de un período de evento si dicho período de evento tiene destinos asociados en ese momento.

```
aws ec2 delete-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --force-delete
```

Salida:

```
{
    "InstanceEventWindowState": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "State": "deleting"
    }
}
```

Para conocer las restricciones de los períodos de eventos, consulte Consideraciones en la sección sobre eventos programados de la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DeleteInstanceEventWindow en la Referencia de comandos de la AWS CLI.

`delete-internet-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-internet-gateway`.

AWS CLI

Para eliminar una puerta de enlace de Internet

En el siguiente ejemplo de `delete-internet-gateway`, se elimina la puerta de enlace de Internet especificada.

```
aws ec2 delete-internet-gateway \
    --internet-gateway-id igw-0d0fb496b3EXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Puertas de enlace de Internet en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte DeleteInternetGateway en la Referencia de comandos de la AWS CLI.

`delete-ipam-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-ipam-pool`.

AWS CLI

Para eliminar un grupo de IPAM

En este ejemplo, usted es un administrador delegado de IPAM que quiere eliminar un grupo de IPAM que ya no necesita, pero el grupo tiene aprovisionado un CIDR. No se puede eliminar un grupo si tiene CIDR aprovisionados, a menos que se utilice la opción `--cascade`, de modo que se utiliza `--cascade`.

Para llevar a cabo esta solicitud:

Necesitará el ID de grupo de IPAM, que puede obtener mediante describe-ipam-pools. El valor de `--region` debe ser la región de origen del IPAM.

En el siguiente ejemplo de `delete-ipam-pool`, se elimina un grupo de IPAM de su cuenta de AWS.

```
aws ec2 delete-ipam-pool \
    --ipam-pool-id ipam-pool-050c886a3ca41cd5b \
    --cascade \
    --region us-east-1
```

Salida:

```
{
    "IpamPool": {
        "OwnerId": "320805250157",
        "IpamPoolId": "ipam-pool-050c886a3ca41cd5b",
        "IpamPoolArn": "arn:aws:ec2::320805250157:ipam-pool/ipam-
pool-050c886a3ca41cd5b",
        "IpamScopeArn": "arn:aws:ec2::320805250157:ipam-scope/ipam-
scope-0a158dde35c51107b",
        "IpamScopeType": "private",
        "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-005f921c17ebd5107",
        "IpamRegion": "us-east-1",
```

```
        "Locale": "None",
        "PoolDepth": 1,
        "State": "delete-in-progress",
        "Description": "example",
        "AutoImport": false,
        "AddressFamily": "ipv4",
        "AllocationMinNetmaskLength": 0,
        "AllocationMaxNetmaskLength": 32
    }
}
```

Para obtener más información, consulte Eliminar un grupo en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte DeleteIpamPool en la Referencia de comandos de la AWS CLI.

`delete-ipam-resource-discovery`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-ipam-resource-discovery`.

AWS CLI

Para eliminar una detección de recursos

En este ejemplo, usted es un administrador delegado de IPAM y desea eliminar una detección de recursos no predeterminada que ha creado para compartirla con otro administrador de IPAM durante el proceso de integración de IPAM con cuentas ajenas a su organización.

Para llevar a cabo esta solicitud:

El valor de `--region` debe ser la región en la que se creó la detección de recursos. No se puede eliminar una detección de recursos predeterminada si `"IsDefault": true`. Una detección de recursos predeterminada es aquella que se crea automáticamente al crear un IPAM. Para eliminar una detección de recursos predeterminada, debe eliminar el IPAM.

En el siguiente ejemplo de `delete-ipam-resource-discovery`, se elimina una detección de recursos.

```
aws ec2 delete-ipam-resource-discovery \
    --ipam-resource-discovery-id ipam-res-disco-0e39761475298ee0f \
    --region us-east-1
```

Salida:

```
{
    "IpamResourceDiscovery": {
        "OwnerId": "149977607591",
        "IpamResourceDiscoveryId": "ipam-res-disco-0e39761475298ee0f",
        "IpamResourceDiscoveryArn": "arn:aws:ec2::149977607591:ipam-resource-
discovery/ipam-res-disco-0e39761475298ee0f",
        "IpamResourceDiscoveryRegion": "us-east-1",
        "OperatingRegions": [
            {
                "RegionName": "us-east-1"
            }
        ],
        "IsDefault": false,
        "State": "delete-in-progress"
    }
}
```

Para obtener más información sobre detecciones de recursos, consulte Trabajo con las detecciones de recursos en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte DeleteIpamResourceDiscovery en la Referencia de comandos de la AWS CLI.

`delete-ipam-scope`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-ipam-scope`.

AWS CLI

Para eliminar un ámbito de IPAM

En el siguiente ejemplo de `delete-ipam-scope`, se elimina un IPAM.

```
aws ec2 delete-ipam-scope \
    --ipam-scope-id ipam-scope-01c1ebab2b63bd7e4
```

Salida:

```
{
    "IpamScope": {
```

```
        "OwnerId": "123456789012",
        "IpamScopeId": "ipam-scope-01c1ebab2b63bd7e4",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-01c1ebab2b63bd7e4",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-08440e7a3acde3908",
        "IpamRegion": "us-east-1",
        "IpamScopeType": "private",
        "IsDefault": false,
        "Description": "Example description",
        "PoolCount": 0,
        "State": "delete-in-progress"
    }
}
```

Para obtener más información, consulte Eliminar un alcance en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte DeleteIpamScope en la Referencia de comandos de la AWS CLI.

`delete-ipam`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-ipam`.

AWS CLI

Para eliminar un IPAM

En el siguiente ejemplo de `delete-ipam`, se elimina un IPAM.

```
aws ec2 delete-ipam \
    --ipam-id ipam-036486dfa6af58ee0
```

Salida:

```
{
    "Ipam": {
        "OwnerId": "123456789012",
        "IpamId": "ipam-036486dfa6af58ee0",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-036486dfa6af58ee0",
        "IpamRegion": "us-east-1",
        "PublicDefaultScopeId": "ipam-scope-071b8042b0195c183",
```

```
        "PrivateDefaultScopeId": "ipam-scope-0807405dece705a30",
        "ScopeCount": 2,
        "OperatingRegions": [
            {
                "RegionName": "us-east-1"
            },
            {
                "RegionName": "us-east-2"
            },
            {
                "RegionName": "us-west-1"
            }
        ],
        "State": "delete-in-progress"
    }
}
```

Para obtener más información, consulte Eliminar un IPAM en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte DeleteIpam en la Referencia de comandos de la AWS CLI.

`delete-key-pair`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-key-pair`.

AWS CLI

Eliminar un par de claves

En el siguiente ejemplo de `delete-key-pair`, se elimina el par de claves especificado.

```
aws ec2 delete-key-pair \
    --key-name my-key-pair
```

Salida:

```
{
    "Return": true,
    "KeyPairId": "key-03c8d3aceb53b507"
}
```

Para obtener más información, consulte Create and delete key pairs en la Guía del usuario de la interfaz de la línea de comandos de AWS.

- Para obtener información sobre la API, consulte DeleteKeyPair en la Referencia de comandos de la AWS CLI.

`delete-launch-template-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-launch-template-versions`.

AWS CLI

Para eliminar una versión de plantilla de lanzamiento

En este ejemplo, se elimina la versión de plantilla de lanzamiento especificada.

Comando:

```
aws ec2 delete-launch-template-versions --launch-template-id lt-0abcd290751193123 --versions 1
```

Salida:

```
{
  "UnsuccessfullyDeletedLaunchTemplateVersions": [],
  "SuccessfullyDeletedLaunchTemplateVersions": [
      {
          "LaunchTemplateName": "TestVersion",
          "VersionNumber": 1,
          "LaunchTemplateId": "lt-0abcd290751193123"
      }
  ]
}
```

- Para obtener información sobre la API, consulte DeleteLaunchTemplateVersions en la Referencia de comandos de la AWS CLI.

`delete-launch-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-launch-template`.

AWS CLI

Eliminar una plantilla de lanzamiento

En este ejemplo, se elimina la plantilla de lanzamiento especificada.

Comando:

```
aws ec2 delete-launch-template --launch-template-id lt-0abcd290751193123
```

Salida:

```
{
  "LaunchTemplate": {
      "LatestVersionNumber": 2,
      "LaunchTemplateId": "lt-0abcd290751193123",
      "LaunchTemplateName": "TestTemplate",
      "DefaultVersionNumber": 2,
      "CreatedBy": "arn:aws:iam::123456789012:root",
      "CreateTime": "2017-11-23T16:46:25.000Z"
  }
}
```

- Para obtener información sobre la API, consulte DeleteLaunchTemplate en la Referencia de comandos de la AWS CLI.

`delete-local-gateway-route-table-virtual-interface-group-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-local-gateway-route-table-virtual-interface-group-association`.

AWS CLI

Para desasociar una tabla de enrutamiento de puerta de enlace local de un grupo de interfaces virtuales (VIF

En el siguiente ejemplo de `delete-local-gateway-route-table-virtual-interface-group-association`, se elimina una asociación entre la tabla de enrutamiento de puerta de enlace local especificada y el grupo de VIF.

```
aws ec2 delete-local-gateway-route-table-virtual-interface-group-association \
```

```
    --local-gateway-route-table-virtual-interface-group-association-id lgw-vif-grp-assoc-exampleid12345678
```

Salida:

```
{
    "LocalGatewayRouteTableVirtualInterfaceGroupAssociation": {
        "LocalGatewayRouteTableVirtualInterfaceGroupAssociationId": "lgw-vif-grp-assoc-exampleid12345678",
        "LocalGatewayVirtualInterfaceGroupId": "lgw-vif-grp-exampleid0123abcd",
        "LocalGatewayId": "lgw-exampleid11223344",
        "LocalGatewayRouteTableId": "lgw-rtb-exampleidabcd1234",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-gateway-route-table/lgw-rtb-exampleidabcd1234",
        "OwnerId": "111122223333",
        "State": "disassociating",
        "Tags": []
    }
}
```

Para obtener más información, consulte VIF group associations en la Guía del usuario de AWS Outposts.

- Para obtener información sobre la API, consulte DeleteLocalGatewayRouteTableVirtualInterfaceGroupAssociation en la Referencia de comandos de la AWS CLI.

`delete-local-gateway-route-table-vpc-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-local-gateway-route-table-vpc-association`.

AWS CLI

Para desasociar de una VPC una tabla de enrutamiento de una puerta de enlace

En el siguiente ejemplo de `delete-local-gateway-route-table-vpc-association`, se elimina la asociación entre la tablas de enrutamiento de puerta de enlace local y la VPC.

```
aws ec2 delete-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-vpc-association-id vpc-example0123456789
```

Salida:

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-abcd1234wxyz56789",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:555555555555:local-
gateway-route-table/lgw-rtb-abcdefg1234567890",
        "LocalGatewayId": "lgw-exampleid01234567",
        "VpcId": "vpc-example0123456789",
        "OwnerId": "555555555555",
        "State": "disassociating"
    }
}
```

Para obtener más información, consulte VPC associations en la Guía del usuario de AWS Outposts.

- Para obtener información sobre la API, consulte DeleteLocalGatewayRouteTableVpcAssociation en la Referencia de comandos de la AWS CLI.

`delete-local-gateway-route-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-local-gateway-route-table`.

AWS CLI

Para eliminar una tabla de enrutamiento de puerta de enlace local

En el siguiente ejemplo de `delete-local-gateway-route-table`, se crea una tabla de enrutamiento de puerta de enlace local con el modo de enrutamiento de VPC directo.

```
aws ec2 delete-local-gateway-route-table \
    --local-gateway-route-table-id lgw-rtb-abcdefg1234567890
```

Salida:

```
{
    "LocalGatewayRouteTable": {
```

```
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-abcdefg1234567890",
        "LocalGatewayId": "lgw-1a2b3c4d5e6f7g8h9",
        "OutpostArn": "arn:aws:outposts:us-west-2:111122223333:outpost/
op-021345abcdef67890",
        "OwnerId": "111122223333",
        "State": "deleting",
        "Tags": [],
        "Mode": "direct-vpc-routing"
    }
}
```

Para obtener más información, consulte Tablas de enrutamiento de puertas de enlace locales en la Guía del usuario de AWS Outposts.

- Para obtener información sobre la API, consulte DeleteLocalGatewayRouteTable en la Referencia de comandos de la AWS CLI.

`delete-local-gateway-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-local-gateway-route`.

AWS CLI

Para eliminar una ruta de una tabla de enrutamiento de puerta de enlace local

En el siguiente ejemplo de `delete-local-gateway-route`, se elimina la ruta especificada de la tabla de enrutamiento de puerta de enlace local especificada.

```
aws ec2 delete-local-gateway-route \
    --destination-cidr-block 0.0.0.0/0 \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE
```

Salida:

```
{
    "Route": {
        "DestinationCidrBlock": "0.0.0.0/0",
        "LocalGatewayVirtualInterfaceGroupId": "lgw-vif-grp-07145b276bEXAMPLE",
        "Type": "static",
```

```
        "State": "deleted",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7EXAMPLE"
    }
}
```

- Para obtener información sobre la API, consulte DeleteLocalGatewayRoute en la Referencia de comandos de la AWS CLI.

`delete-managed-prefix-list`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-managed-prefix-list`.

AWS CLI

Para eliminar una lista de prefijos

En el siguiente ejemplo de `delete-managed-prefix-list`, se elimina la lista de prefijos especificada.

```
aws ec2 delete-managed-prefix-list \
    --prefix-list-id pl-0123456abcabcabc1
```

Salida:

```
{
    "PrefixList": {
        "PrefixListId": "pl-0123456abcabcabc1",
        "AddressFamily": "IPv4",
        "State": "delete-in-progress",
        "PrefixListArn": "arn:aws:ec2:us-west-2:123456789012:prefix-list/
pl-0123456abcabcabc1",
        "PrefixListName": "test",
        "MaxEntries": 10,
        "Version": 1,
        "OwnerId": "123456789012"
    }
}
```

Para obtener más información, consulte Managed prefix lists en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte DeleteManagedPrefixList en la Referencia de comandos de la AWS CLI.

`delete-nat-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-nat-gateway`.

AWS CLI

Para eliminar una puerta de enlace de NAT

En este ejemplo se elimina la puerta de enlace de NAT `nat-04ae55e711cec5680`.

Comando:

```
aws ec2 delete-nat-gateway --nat-gateway-id nat-04ae55e711cec5680
```

Salida:

```
{
   "NatGatewayId": "nat-04ae55e711cec5680"
}
```

- Para obtener información sobre la API, consulte DeleteNatGateway en la Referencia de comandos de la AWS CLI.

`delete-network-acl-entry`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-network-acl-entry`.

AWS CLI

Para eliminar una entrada de ACL de red

En este ejemplo se elimina la regla de entrada número 100 de la ACL de red especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-network-acl-entry --network-acl-id acl-5fb85d36 --ingress --rule-
number 100
```

- Para obtener información sobre la API, consulte DeleteNetworkAclEntry en la Referencia de comandos de la AWS CLI.

`delete-network-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-network-acl`.

AWS CLI

Para eliminar una ACL de red

En este ejemplo, se elimina la ACL de red especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-network-acl --network-acl-id acl-5fb85d36
```

- Para obtener información sobre la API, consulte DeleteNetworkAcl en la Referencia de comandos de la AWS CLI.

`delete-network-insights-access-scope-analysis`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-network-insights-access-scope-analysis`.

AWS CLI

Para eliminar un análisis de ámbito de acceso a la red

En el siguiente ejemplo de `delete-network-insights-access-scope-analysis`, se elimina el análisis del ámbito de acceso a la red especificado.

```
aws ec2 delete-network-insights-access-scope-analysis \
    --network-insights-access-scope-analysis-id nisa-01234567891abcdef
```

Salida:

```
{
```

```
    "NetworkInsightsAccessScopeAnalysisId": "nisa-01234567891abcdef
}
```

Para obtener más información, consulte Getting started with Network Access Analyzer using the AWS CLI en la Guía del analizador de acceso a la red.

- Para obtener información sobre la API, consulte DeleteNetworkInsightsAccessScopeAnalysis en la Referencia de comandos de la AWS CLI.

`delete-network-insights-access-scope`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-network-insights-access-scope`.

AWS CLI

Para eliminar un ámbito de acceso a la red

En el siguiente ejemplo de `delete-network-insights-access-scope`, se elimina el ámbito de acceso a la red especificado.

```
aws ec2 delete-network-insights-access-scope \
    --network-insights-access-scope-id nis-123456789abc01234
```

Salida:

```
{
    "NetworkInsightsAccessScopeId": "nis-123456789abc01234"
}
```

Para obtener más información, consulte Getting started with Network Access Analyzer using the AWS CLI en la Guía del analizador de acceso a la red.

- Para obtener información sobre la API, consulte DeleteNetworkInsightsAccessScope en la Referencia de comandos de la AWS CLI.

`delete-network-insights-analysis`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-network-insights-analysis`.

AWS CLI

Para eliminar un análisis de ruta

En el siguiente ejemplo de `delete-network-insights-analysis`, se elimina el análisis especificado.

```
aws ec2 delete-network-insights-analysis \
    --network-insights-analysis-id nia-02207aa13eb480c7a
```

Salida:

```
{
    "NetworkInsightsAnalysisId": "nia-02207aa13eb480c7a"
}
```

Para obtener más información, consulte Getting started using the AWS CLI en la Guía del analizador de accesibilidad.

- Para obtener información sobre la API, consulte DeleteNetworkInsightsAnalysis en la Referencia de comandos de la AWS CLI.

`delete-network-insights-path`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-network-insights-path`.

AWS CLI

Para eliminar una ruta

En el siguiente ejemplo de `delete-network-insights-path`, se elimina la ruta especificada. Para poder eliminar una ruta, primero debe eliminar todos sus análisis mediante el comando `delete-network-insights-analysis`.

```
aws ec2 delete-network-insights-path \
    --network-insights-path-id nip-0b26f224f1d131fa8
```

Salida:

```
{
```

```
    "NetworkInsightsPathId": "nip-0b26f224f1d131fa8"
}
```

Para obtener más información, consulte Getting started using the AWS CLI en la Guía del analizador de accesibilidad.

- Para obtener información sobre la API, consulte DeleteNetworkInsightsPath en la Referencia de comandos de la AWS CLI.

`delete-network-interface-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-network-interface-permission`.

AWS CLI

Para eliminar un permiso de interfaz de red

En este ejemplo se elimina el permiso de interfaz de red especificado.

Comando:

```
aws ec2 delete-network-interface-permission --network-interface-permission-id eni-perm-06fd19020ede149ea
```

Salida:

```
{
  "Return": true
}
```

- Para obtener información sobre la API, consulte DeleteNetworkInterfacePermission en la Referencia de comandos de la AWS CLI.

`delete-network-interface`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-network-interface`.

AWS CLI

Para eliminar una interfaz de red

En este ejemplo se elimina la interfaz de red especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-network-interface --network-interface-id eni-e5aa89a3
```

- Para obtener información sobre la API, consulte DeleteNetworkInterface en la Referencia de comandos de la AWS CLI.

`delete-placement-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-placement-group`.

AWS CLI

Para eliminar un grupo de ubicación

En este ejemplo de comando se elimina el grupo de ubicación especificado.

Comando:

```
aws ec2 delete-placement-group --group-name my-cluster
```

- Para obtener información sobre la API, consulte DeletePlacementGroup en la Referencia de comandos de la AWS CLI.

`delete-queued-reserved-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-queued-reserved-instances`.

AWS CLI

Para eliminar una compra en cola

En el siguiente ejemplo de `delete-queued-reserved-instances`, se elimina la instancia reservada especificada que estaba en cola para su compra.

```
aws ec2 delete-queued-reserved-instances \
```

```
    --reserved-instances-ids af9f760e-6f91-4559-85f7-4980eexample
```

Salida:

```
{
    "SuccessfulQueuedPurchaseDeletions": [
        {
            "ReservedInstancesId": "af9f760e-6f91-4559-85f7-4980eexample"
        }
    ],
    "FailedQueuedPurchaseDeletions": []
}
```

- Para obtener información sobre la API, consulte DeleteQueuedReservedInstances en la Referencia de comandos de la AWS CLI.

`delete-route-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-route-table`.

AWS CLI

Para eliminar una tabla de enrutamiento

En este ejemplo, se elimina la tabla de enrutamiento especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-route-table --route-table-id rtb-22574640
```

- Para obtener información sobre la API, consulte DeleteRouteTable en la Referencia de comandos de la AWS CLI.

`delete-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-route`.

AWS CLI

Para eliminar una ruta

En este ejemplo, se elimina la ruta especificada de la tabla de enrutamiento especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-route --route-table-id rtb-22574640 --destination-cidr-
block 0.0.0.0/0
```

- Para obtener información sobre la API, consulte DeleteRoute en la Referencia de comandos de la AWS CLI.

`delete-security-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-security-group`.

AWS CLI

[EC2-Classic] Eliminar un grupo de seguridad

En este ejemplo, se elimina el grupo de seguridad denominado `MySecurityGroup`. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-security-group --group-name MySecurityGroup
```

[EC2-VPC] Eliminar un grupo de seguridad

En este ejemplo, se elimina el grupo de seguridad con el ID `sg-903004f8`. Tenga en cuenta que no puede hacer referencia a un grupo de seguridad de EC2-VPC por nombre. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-security-group --group-id sg-903004f8
```

Para obtener más información, consulte Uso de los grupos de seguridad en la Guía del usuario de la Interfaz de la línea de comandos de AWS.

- Para obtener información sobre la API, consulte DeleteSecurityGroup en la Referencia de comandos de la AWS CLI.

`delete-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-snapshot`.

AWS CLI

Eliminar una instantánea

Este comando de ejemplo elimina la instantánea con el ID de instantánea de `snap-1234567890abcdef0`. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-snapshot --snapshot-id snap-1234567890abcdef0
```

- Para obtener información sobre la API, consulte DeleteSnapshot en la Referencia de comandos de la AWS CLI.

`delete-spot-datafeed-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-spot-datafeed-subscription`.

AWS CLI

Para cancelar una suscripción a una fuente de datos de instancia de spot

En este ejemplo de comando, se elimina una suscripción a una fuente de datos de spot de la cuenta. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-spot-datafeed-subscription
```

- Para obtener información sobre la API, consulte DeleteSpotDatafeedSubscription en la Referencia de comandos de la AWS CLI.

`delete-subnet-cidr-reservation`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-subnet-cidr-reservation`.

AWS CLI

Para eliminar una reserva de CIDR de subred

En el siguiente ejemplo de `delete-subnet-cidr-reservation`, se elimina la reserva de CIDR de subred especificada.

```
aws ec2 delete-subnet-cidr-reservation \
    --subnet-cidr-reservation-id scr-044f977c4eEXAMPLE
```

Salida:

```
{
    "DeletedSubnetCidrReservation": {
        "SubnetCidrReservationId": "scr-044f977c4eEXAMPLE",
        "SubnetId": "subnet-03c51e2e6cEXAMPLE",
        "Cidr": "10.1.0.16/28",
        "ReservationType": "prefix",
        "OwnerId": "123456789012"
    }
}
```

Para obtener más información, consulte Reservas de la subred de CIDR en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte DeleteSubnetCidrReservation en la Referencia de comandos de la AWS CLI.

`delete-subnet`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-subnet`.

AWS CLI

Para eliminar una subred

En este ejemplo se elimina la subred especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-subnet --subnet-id subnet-9d4a7b6c
```

- Para obtener información sobre la API, consulte DeleteSubnet en la Referencia de comandos de AWS CLI.

`delete-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-tags`.

AWS CLI

Ejemplo 1: eliminación de una etiqueta de un recurso

En el siguiente ejemplo de `delete-tags`, se elimina de la imagen especificada la etiqueta `Stack=Test`. Cuando se especifican tanto un valor como un nombre de clave, la etiqueta se elimina únicamente si su valor coincide con el valor especificado.

```
aws ec2 delete-tags \
    --resources ami-1234567890abcdef0 \
    --tags Key=Stack,Value=Test
```

Especificar el valor de una etiqueta es opcional. En el siguiente ejemplo de `delete-tags`, se elimina de la instancia especificada la etiqueta con el nombre de clave `purpose`, independientemente del valor de la etiqueta.

```
aws ec2 delete-tags \
    --resources i-1234567890abcdef0 \
    --tags Key=purpose
```

Si el valor de etiqueta especificado es la cadena vacía, la etiqueta se eliminará únicamente si su valor es la cadena vacía. En el siguiente ejemplo de `delete-tags`, se especifica la cadena vacía como valor de etiqueta de la etiqueta que se va a eliminar.

```
aws ec2 delete-tags \
    --resources i-1234567890abcdef0 \
    --tags Key=Name,Value=
```

Ejemplo 2: eliminación de una etiqueta de varios recursos

En el siguiente ejemplo de `delete-tags`, se elimina la etiqueta Purpose=Test tanto de una instancia como de una AMI. Como se muestra en el ejemplo anterior, se puede omitir el valor de la etiqueta en el comando.

```
aws ec2 delete-tags \
    --resources i-1234567890abcdef0 ami-1234567890abcdef0 \
    --tags Key=Purpose
```

- Para obtener información sobre la API, consulte DeleteTags en la Referencia de comandos de la AWS CLI.

`delete-traffic-mirror-filter-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-traffic-mirror-filter-rule`.

AWS CLI

Para eliminar una regla de filtro de reflejo de tráfico

En el siguiente ejemplo de `delete-traffic-mirror-filter-rule`, se elimina la regla de filtro de reflejo de tráfico especificada.

```
aws ec2 delete-traffic-mirror-filter-rule \
    --traffic-mirror-filter-rule-id tmfr-081f71283bEXAMPLE
```

Salida:

```
{
    "TrafficMirrorFilterRuleId": "tmfr-081f71283bEXAMPLE"
}
```

Para obtener más información, consulte Modify Your Traffic Mirror Filter Rules en la Guía de creación de reflejo de tráfico de AWS.

- Para obtener información sobre la API, consulte DeleteTrafficMirrorFilterRule en la Referencia de comandos de la AWS CLI.

`delete-traffic-mirror-filter`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-traffic-mirror-filter`.

AWS CLI

Para eliminar un filtro de reflejo de tráfico

En el siguiente ejemplo de `delete-traffic-mirror-filter`, se elimina el filtro de reflejo de tráfico especificado.

```
aws ec2 delete-traffic-mirror-filter \
    --traffic-mirror-filter-id tmf-0be0b25fcdEXAMPLE
```

Salida:

```
{
    "TrafficMirrorFilterId": "tmf-0be0b25fcdEXAMPLE"
}
```

Para obtener más información, consulte Delete a Traffic Mirror Filter en la Guía de creación de reflejo de tráfico de AWS.

- Para obtener información sobre la API, consulte DeleteTrafficMirrorFilter en la Referencia de comandos de la AWS CLI.

`delete-traffic-mirror-session`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-traffic-mirror-session`.

AWS CLI

Para eliminar una sesión de reflejo de tráfico

En el siguiente ejemplo de `delete-traffic-mirror-session`, se elimina la sesión de reflejo de tráfico especificada.

```
aws ec2 delete-traffic-mirror-session \
    --traffic-mirror-session-id tms-0af3141ce5EXAMPLE
```

Salida:

```
{
    "TrafficMirrorSessionId": "tms-0af3141ce5EXAMPLE"
}
```

Para obtener más información, consulte Delete a Traffic Mirror Session en la Guía de creación de reflejo de tráfico de AWS.

- Para obtener información sobre la API, consulte DeleteTrafficMirrorSession en la Referencia de comandos de la AWS CLI.

`delete-traffic-mirror-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-traffic-mirror-target`.

AWS CLI

Para eliminar un destino de reflejo de tráfico

En el siguiente ejemplo de `delete-traffic-mirror-target`, se elimina el destino de reflejo de tráfico especificado.

```
aws ec2 delete-traffic-mirror-target \
    --traffic-mirror-target-id tmt-060f48ce9EXAMPLE
```

Salida:

```
{
    "TrafficMirrorTargetId": "tmt-060f48ce9EXAMPLE"
}
```

Para obtener más información, consulte Delete a Traffic Mirror Target en la Guía de creación de reflejo de tráfico de AWS.

- Para obtener información sobre la API, consulte DeleteTrafficMirrorTarget en la Referencia de comandos de la AWS CLI.

`delete-transit-gateway-connect-peer`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-transit-gateway-connect-peer`.

AWS CLI

Para eliminar un emparejamiento de Transit Gateway Connect

En el siguiente ejemplo de `delete-transit-gateway-connect-peer`, se elimina el emparejamiento de Connect especificado.

```
aws ec2 delete-transit-gateway-connect-peer \
    --transit-gateway-connect-peer-id tgw-connect-peer-0666adbac4EXAMPLE
```

Salida:

```
{
    "TransitGatewayConnectPeer": {
        "TransitGatewayAttachmentId": "tgw-attach-0f0927767cEXAMPLE",
        "TransitGatewayConnectPeerId": "tgw-connect-peer-0666adbac4EXAMPLE",
        "State": "deleting",
        "CreationTime": "2021-10-13T03:35:17.000Z",
        "ConnectPeerConfiguration": {
            "TransitGatewayAddress": "10.0.0.234",
            "PeerAddress": "172.31.1.11",
            "InsideCidrBlocks": [
                "169.254.6.0/29"
            ],
            "Protocol": "gre",
            "BgpConfigurations": [
                {
                    "TransitGatewayAsn": 64512,
                    "PeerAsn": 64512,
                    "TransitGatewayAddress": "169.254.6.2",
                    "PeerAddress": "169.254.6.1",
                    "BgpStatus": "down"
                },
                {
                    "TransitGatewayAsn": 64512,
                    "PeerAsn": 64512,
                    "TransitGatewayAddress": "169.254.6.3",
                    "PeerAddress": "169.254.6.1",
                    "BgpStatus": "down"
                }
            ]
        }
    }
```

```
}
```

Para obtener más información, consulte Transit gateway Connect attachments and Transit Gateway Connect peers en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DeleteTransitGatewayConnectPeer en la Referencia de comandos de la AWS CLI.

`delete-transit-gateway-connect`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-transit-gateway-connect`.

AWS CLI

Para eliminar una conexión de Transit Gateway Connect

En el siguiente ejemplo de `delete-transit-gateway-connect`, se elimina la conexión de Connect especificada.

```
aws ec2 delete-transit-gateway-connect \
    --transit-gateway-attachment-id tgw-attach-037012e5dcEXAMPLE
```

Salida:

```
{
    "TransitGatewayConnect": {
        "TransitGatewayAttachmentId": "tgw-attach-037012e5dcEXAMPLE",
        "TransportTransitGatewayAttachmentId": "tgw-attach-0a89069f57EXAMPLE",
        "TransitGatewayId": "tgw-02f776b1a7EXAMPLE",
        "State": "deleting",
        "CreationTime": "2021-03-09T19:59:17+00:00",
        "Options": {
            "Protocol": "gre"
        }
    }
}
```

Para obtener más información, consulte Transit gateway Connect attachments and Transit Gateway Connect peers en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DeleteTransitGatewayConnect en la Referencia de comandos de la AWS CLI.

`delete-transit-gateway-multicast-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-transit-gateway-multicast-domain`.

AWS CLI

Para eliminar un dominio de multidifusión de puerta de enlace de tránsito

En el siguiente ejemplo de `delete-transit-gateway-multicast-domain`, se elimina el dominio de multidifusión especificado.

```
aws ec2 delete-transit-gateway-multicast-domain \
    --transit-gateway-multicast-domain-id tgw-mcast-domain-0c4905cef7EXAMPLE
```

Salida:

```
{
    "TransitGatewayMulticastDomain": {
        "TransitGatewayMulticastDomainId": "tgw-mcast-domain-02bb79002bEXAMPLE",
        "TransitGatewayId": "tgw-0d88d2d0d5EXAMPLE",
        "State": "deleting",
        "CreationTime": "2019-11-20T22:02:03.000Z"
    }
}
```

Para obtener más información, consulte Managing multicast domains en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DeleteTransitGatewayMulticastDomain en la Referencia de comandos de la AWS CLI.

`delete-transit-gateway-peering-attachment`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-transit-gateway-peering-attachment`.

AWS CLI

Para eliminar una conexión de emparejamiento de puerta de enlace de tránsito

En el siguiente ejemplo de `delete-transit-gateway-peering-attachment`, se elimina la conexión de emparejamiento de puerta de enlace de tránsito especificada.

```
aws ec2 delete-transit-gateway-peering-attachment \
    --transit-gateway-attachment-id tgw-attach-4455667788aabbccd
```

Salida:

```
{
    "TransitGatewayPeeringAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-4455667788aabbccd",
        "RequesterTgwInfo": {
            "TransitGatewayId": "tgw-123abc05e04123abc",
            "OwnerId": "123456789012",
            "Region": "us-west-2"
        },
        "AccepterTgwInfo": {
            "TransitGatewayId": "tgw-11223344aabbcc112",
            "OwnerId": "123456789012",
            "Region": "us-east-2"
        },
        "State": "deleting",
        "CreationTime": "2019-12-09T11:38:31.000Z"
    }
}
```

Para obtener más información, consulte Transit Gateway Peering Attachments en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DeleteTransitGatewayPeeringAttachment en la Referencia de comandos de la AWS CLI.

`delete-transit-gateway-policy-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-transit-gateway-policy-table`.

AWS CLI

Para eliminar una tabla de políticas de puerta de enlace de tránsito

En el siguiente ejemplo de `delete-transit-gateway-policy-table`, se elimina la tabla de políticas de puerta de enlace de tránsito especificada.

```
aws ec2 delete-transit-gateway-policy-table \
    --transit-gateway-policy-table-id tgw-ptb-0a16f134b78668a81
```

Salida:

```
{
    "TransitGatewayPolicyTables": [
        {
            "TransitGatewayPolicyTableId": "tgw-ptb-0a16f134b78668a81",
            "TransitGatewayId": "tgw-067f8505c18f0bd6e",
            "State": "deleting",
            "CreationTime": "2023-11-28T16:36:43+00:00",
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Transit gateway policy tables en la Guía del usuario de Transit Gateway.

- Para obtener información sobre la API, consulte DeleteTransitGatewayPolicyTable en la Referencia de comandos de la AWS CLI.

`delete-transit-gateway-prefix-list-reference`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-transit-gateway-prefix-list-reference`.

AWS CLI

Para eliminar una referencia de lista de prefijos

En el siguiente ejemplo de `delete-transit-gateway-prefix-list-reference`, se elimina la referencia de lista de prefijos especificada.

```
aws ec2 delete-transit-gateway-prefix-list-reference \
    --transit-gateway-route-table-id tgw-rtb-0123456789abcd123 \
    --prefix-list-id pl-11111122222222333
```

Salida:

```
{
    "TransitGatewayPrefixListReference": {
        "TransitGatewayRouteTableId": "tgw-rtb-0123456789abcd123",
        "PrefixListId": "pl-11111122222222333",
        "PrefixListOwnerId": "123456789012",
        "State": "deleting",
        "Blackhole": false,
        "TransitGatewayAttachment": {
            "TransitGatewayAttachmentId": "tgw-attach-aabbccddaabbccaab",
            "ResourceType": "vpc",
            "ResourceId": "vpc-112233445566aabbc"
        }
    }
}
```

Para obtener más información, consulte Prefix list references en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DeleteTransitGatewayPrefixListReference en la Referencia de comandos de la AWS CLI.

`delete-transit-gateway-route-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-transit-gateway-route-table`.

AWS CLI

Para eliminar una tabla de enrutamiento de puerta de enlace de tránsito

En el siguiente ejemplo de `delete-transit-gateway-route-table`, se elimina una tabla de enrutamiento de puerta de enlace de tránsito especificada.

```
aws ec2  delete-transit-gateway-route-table \
    --transit-gateway-route-table-id tgw-rtb-0b6f6aaa01EXAMPLE
```

Salida:

```
{
    "TransitGatewayRouteTable": {
        "TransitGatewayRouteTableId": "tgw-rtb-0b6f6aaa01EXAMPLE",
```

```
        "TransitGatewayId": "tgw-02f776b1a7EXAMPLE",
        "State": "deleting",
        "DefaultAssociationRouteTable": false,
        "DefaultPropagationRouteTable": false,
        "CreationTime": "2019-07-17T20:27:26.000Z"
    }
}
```

Para obtener más información, consulte Delete a transit gateway route table en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DeleteTransitGatewayRouteTable en la Referencia de comandos de la AWS CLI.

`delete-transit-gateway-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-transit-gateway-route`.

AWS CLI

Para eliminar un bloque de CIDR de una tabla de enrutamiento

En el siguiente ejemplo de `delete-transit-gateway-route`, se elimina un bloque de CIDR de la tabla de enrutamiento de puerta de enlace de tránsito especificada.

```
aws ec2 delete-transit-gateway-route \
    --transit-gateway-route-table-id tgw-rtb-0b6f6aaa01EXAMPLE \
    --destination-cidr-block 10.0.2.0/24
```

Salida:

```
{
    "Route": {
        "DestinationCidrBlock": "10.0.2.0/24",
        "TransitGatewayAttachments": [
            {
                "ResourceId": "vpc-0065acced4EXAMPLE",
                "TransitGatewayAttachmentId": "tgw-attach-0b5968d3b6EXAMPLE",
                "ResourceType": "vpc"
            }
        ],
        "Type": "static",
        "State": "deleted"
```

```
    }
}
```

Para obtener más información, consulte Delete a static route en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DeleteTransitGatewayRoute en la Referencia de comandos de la AWS CLI.

`delete-transit-gateway-vpc-attachment`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-transit-gateway-vpc-attachment`.

AWS CLI

Para eliminar una conexión de VPC de puerta de enlace de tránsito

En el siguiente ejemplo de `delete-transit-gateway-vpc-attachment`, se elimina la conexión de VPC especificada.

```
aws ec2 delete-transit-gateway-vpc-attachment \
    --transit-gateway-attachment-id tgw-attach-0d2c54bdbEXAMPLE
```

Salida:

```
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-0d2c54bdb3EXAMPLE",
        "TransitGatewayId": "tgw-02f776b1a7EXAMPLE",
        "VpcId": "vpc-0065acced4f61c651",
        "VpcOwnerId": "111122223333",
        "State": "deleting",
        "CreationTime": "2019-07-17T16:04:27.000Z"
    }
}
```

Para obtener más información, consulte Delete a VPC attachment en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DeleteTransitGatewayVpcAttachment en la Referencia de comandos de la AWS CLI.

`delete-transit-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-transit-gateway`.

AWS CLI

Para eliminar una puerta de enlace de tránsito

En el siguiente ejemplo de `delete-transit-gateway`, se elimina la puerta de enlace de tránsito especificada.

```
aws ec2  delete-transit-gateway \
    --transit-gateway-id tgw-01f04542b2EXAMPLE
```

Salida:

```
{
    "TransitGateway": {
        "TransitGatewayId": "tgw-01f04542b2EXAMPLE",
        "State": "deleting",
        "OwnerId": "123456789012",
        "Description": "Example Transit Gateway",
        "CreationTime": "2019-08-27T15:04:35.000Z",
        "Options": {
            "AmazonSideAsn": 64515,
            "AutoAcceptSharedAttachments": "disable",
            "DefaultRouteTableAssociation": "enable",
            "AssociationDefaultRouteTableId": "tgw-rtb-0ce7a6948fEXAMPLE",
            "DefaultRouteTablePropagation": "enable",
            "PropagationDefaultRouteTableId": "tgw-rtb-0ce7a6948fEXAMPLE",
            "VpnEcmpSupport": "enable",
            "DnsSupport": "enable"
        }
    }
}
```

Para obtener más información, consulte Delete a transit gateway en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DeleteTransitGateway en la Referencia de comandos de la AWS CLI.

`delete-verified-access-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-verified-access-endpoint`.

AWS CLI

Para eliminar un punto de conexión de Acceso verificado

En el siguiente ejemplo de `delete-verified-access-endpoint`, se elimina el punto de conexión de acceso verificado especificado.

```
aws ec2 delete-verified-access-endpoint \
    --verified-access-endpoint-id vae-066fac616d4d546f2
```

Salida:

```
{
    "VerifiedAccessEndpoint": {
        "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
        "VerifiedAccessGroupId": "vagr-0dbe967baf14b7235",
        "VerifiedAccessEndpointId": "vae-066fac616d4d546f2",
        "ApplicationDomain": "example.com",
        "EndpointType": "network-interface",
        "AttachmentType": "vpc",
        "DomainCertificateArn": "arn:aws:acm:us-east-2:123456789012:certificate/
eb065ea0-26f9-4e75-a6ce-0a1a7EXAMPLE",
        "EndpointDomain": "my-ava-
app.edge-00c3372d53b1540bb.vai-0ce000c0b7643abea.prod.verified-access.us-
east-2.amazonaws.com",
        "SecurityGroupIds": [
            "sg-004915970c4c8f13a"
        ],
        "NetworkInterfaceOptions": {
            "NetworkInterfaceId": "eni-0aec70418c8d87a0f",
            "Protocol": "https",
            "Port": 443
        },
        "Status": {
            "Code": "deleting"
        },
        "Description": "Testing Verified Access",
        "CreationTime": "2023-08-25T20:54:43",
```

```
        "LastUpdatedTime": "2023-08-25T22:46:32"
    }
}
```

Para obtener más información, consulte Verified Access endpoints en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte DeleteVerifiedAccessEndpoint en la Referencia de comandos de la AWS CLI.

`delete-verified-access-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-verified-access-group`.

AWS CLI

Para eliminar un grupo de Acceso verificado

En el siguiente ejemplo de `delete-verified-access-group`, se elimina el grupo de acceso verificado especificado.

```
aws ec2 delete-verified-access-group \
    --verified-access-group-id vagr-0dbe967baf14b7235
```

Salida:

```
{
    "VerifiedAccessGroup": {
        "VerifiedAccessGroupId": "vagr-0dbe967baf14b7235",
        "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
        "Description": "Testing Verified Access",
        "Owner": "123456789012",
        "VerifiedAccessGroupArn": "arn:aws:ec2:us-east-2:123456789012:verified-
access-group/vagr-0dbe967baf14b7235",
        "CreationTime": "2023-08-25T19:55:19",
        "LastUpdatedTime": "2023-08-25T22:49:03",
        "DeletionTime": "2023-08-26T00:58:31"
    }
}
```

Para obtener más información, consulte Verified Access groups en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte DeleteVerifiedAccessGroup en la Referencia de comandos de AWS CLI.

`delete-verified-access-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-verified-access-instance`.

AWS CLI

Para eliminar una instancia de Acceso verificado

En el siguiente ejemplo de `delete-verified-access-instance`, se elimina la instancia de acceso verificado especificada.

```
aws ec2 delete-verified-access-instance \
    --verified-access-instance-id vai-0ce000c0b7643abea
```

Salida:

```
{
    "VerifiedAccessInstance": {
        "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
        "Description": "Testing Verified Access",
        "VerifiedAccessTrustProviders": [],
        "CreationTime": "2023-08-25T18:27:56",
        "LastUpdatedTime": "2023-08-26T01:00:18"
    }
}
```

Para obtener más información, consulte Verified Access instances en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte DeleteVerifiedAccessInstance en la Referencia de comandos de la AWS CLI.

`delete-verified-access-trust-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-verified-access-trust-provider`.

AWS CLI

Para eliminar un proveedor de confianza de Acceso verificado

En el siguiente ejemplo de `delete-verified-access-trust-provider`, se elimina el proveedor de confianza de acceso verificado especificado.

```
aws ec2 delete-verified-access-trust-provider \
    --verified-access-trust-provider-id vatp-0bb32de759a3e19e7
```

Salida:

```
{
    "VerifiedAccessTrustProvider": {
        "VerifiedAccessTrustProviderId": "vatp-0bb32de759a3e19e7",
        "Description": "Testing Verified Access",
        "TrustProviderType": "user",
        "UserTrustProviderType": "iam-identity-center",
        "PolicyReferenceName": "idc",
        "CreationTime": "2023-08-25T18:40:36",
        "LastUpdatedTime": "2023-08-25T18:40:36"
    }
}
```

Para obtener más información, consulte Trust providers for Verified Access en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte DeleteVerifiedAccessTrustProvider en la Referencia de comandos de la AWS CLI.

`delete-volume`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-volume`.

AWS CLI

Para eliminar un volumen

En este ejemplo de comando, se elimina un volumen disponible con el ID de volumen `vol-049df61146c4d7901`. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-volume --volume-id vol-049df61146c4d7901
```

- Para obtener información sobre la API, consulte DeleteVolume en la Referencia de comandos de la AWS CLI.

`delete-vpc-endpoint-connection-notifications`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-vpc-endpoint-connection-notifications`.

AWS CLI

Para eliminar una notificación de conexión de punto de conexión

En este ejemplo, se elimina la notificación de conexión de punto de conexión especificada.

Comando:

```
aws ec2 delete-vpc-endpoint-connection-notifications --connection-notification-ids vpce-nfn-008776de7e03f5abc
```

Salida:

```
{
  "Unsuccessful": []
}
```

- Para obtener información sobre la API, consulte DeleteVpcEndpointConnectionNotifications en la Referencia de comandos de la AWS CLI.

`delete-vpc-endpoint-service-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-vpc-endpoint-service-configurations`.

AWS CLI

Para eliminar una configuración de servicio de punto de conexión

En este ejemplo, se elimina la configuración de servicio de punto de conexión especificada.

Comando:

```
aws ec2 delete-vpc-endpoint-service-configurations --service-ids vpce-svc-03d5ebb7d9579a2b3
```

Salida:

```
{
   "Unsuccessful": []
}
```

- Para obtener información sobre la API, consulte DeleteVpcEndpointServiceConfigurations en la Referencia de comandos de la AWS CLI.

`delete-vpc-endpoints`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-vpc-endpoints`.

AWS CLI

Para eliminar un punto de conexión

En este ejemplo se eliminan los puntos de conexión vpce-aa22bb33 y vpce-1a2b3c4d. Si el comando se ejecuta parcial o incorrectamente, se devuelve una lista de los elementos incorrectos. Si el comando se ejecuta correctamente, la lista devuelta está vacía.

Comando:

```
aws ec2 delete-vpc-endpoints --vpc-endpoint-ids vpce-aa22bb33 vpce-1a2b3c4d
```

Salida:

```
{
  "Unsuccessful": []
}
```

- Para obtener información sobre la API, consulte DeleteVpcEndpoints en la Referencia de comandos de la AWS CLI.

`delete-vpc-peering-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-vpc-peering-connection`.

AWS CLI

Para eliminar una conexión de emparejamiento de VPC

En este ejemplo, se elimina la solicitud de conexión de emparejamiento de VPC especificada.

Comando:

```
aws ec2 delete-vpc-peering-connection --vpc-peering-connection-id pcx-1a2b3c4d
```

Salida:

```
{
    "Return": true
}
```

- Para obtener información sobre la API, consulte DeleteVpcPeeringConnection en la Referencia de comandos de la AWS CLI.

`delete-vpc`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-vpc`.

AWS CLI

Para eliminar una VPC

En este ejemplo, se elimina la VPC especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-vpc --vpc-id vpc-a01106c2
```

- Para obtener información sobre la API, consulte DeleteVpc en la Referencia de comandos de la AWS CLI.

`delete-vpn-connection-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-vpn-connection-route`.

AWS CLI

Para eliminar una ruta estática de una conexión de VPN

En este ejemplo, se elimina la ruta estática especificada de la conexión de VPN especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-vpn-connection-route --vpn-connection-id vpn-40f41529 --destination-cidr-block 11.12.0.0/16
```

- Para obtener información sobre la API, consulte DeleteVpnConnectionRoute en la Referencia de comandos de la AWS CLI.

`delete-vpn-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-vpn-connection`.

AWS CLI

Para eliminar una conexión de VPN

En este ejemplo, se elimina la configuración de VPN especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-vpn-connection --vpn-connection-id vpn-40f41529
```

- Para obtener información sobre la API, consulte DeleteVpnConnection en la Referencia de comandos de la AWS CLI.

`delete-vpn-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-vpn-gateway`.

AWS CLI

Para eliminar una puerta de enlace privada virtual

En este ejemplo, se elimina la puerta de enlace privada virtual especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 delete-vpn-gateway --vpn-gateway-id vgw-9a4cacf3
```

- Para obtener información sobre la API, consulte DeleteVpnGateway en la Referencia de comandos de la AWS CLI.

`deprovision-byoip-cidr`

En el siguiente ejemplo de código, se muestra cómo utilizar `deprovision-byoip-cidr`.

AWS CLI

Para eliminar un rango de direcciones IP a fin de dejar de usarlas

En el siguiente ejemplo, se elimina el rango de direcciones especificado para dejar de usarlo con AWS.

```
aws ec2 deprovision-byoip-cidr \
    --cidr 203.0.113.25/24
```

Salida:

```
{
    "ByoipCidr": {
        "Cidr": "203.0.113.25/24",
        "State": "pending-deprovision"
    }
}
```

- Para obtener información sobre la API, consulte DeprovisionByoipCidr en la Referencia de comandos de la AWS CLI.

`deprovision-ipam-pool-cidr`

En el siguiente ejemplo de código, se muestra cómo utilizar `deprovision-ipam-pool-cidr`.

AWS CLI

Para anular el aprovisionamiento de CIDR de un grupo de IPAM

En el siguiente ejemplo de `deprovision-ipam-pool-cidr`, se anula el aprovisionamiento de un CIDR aprovisionado en un grupo de IPAM.

(Linux):

```
aws ec2 deprovision-ipam-pool-cidr \
    --ipam-pool-id ipam-pool-02ec043a19bbe5d08 \
    --cidr 11.0.0.0/16
```

(Windows):

```
aws ec2 deprovision-ipam-pool-cidr ^
    --ipam-pool-id ipam-pool-02ec043a19bbe5d08 ^
    --cidr 11.0.0.0/16
```

Salida:

```
{
    "IpamPoolCidr": {
        "Cidr": "11.0.0.0/16",
        "State": "pending-deprovision"
    }
}
```

Para obtener más información, consulte Anular el aprovisionamiento del CIDR de un grupo en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte DeprovisionIpamPoolCidr en la Referencia de comandos de la AWS CLI.

`deregister-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-image`.

AWS CLI

Para anular el registro de una AMI

En este ejemplo, se anula el registro de la AMI especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 deregister-image --image-id ami-4fa54026
```

- Para obtener información sobre la API, consulte DeregisterImage en la Referencia de comandos de la AWS CLI.

`deregister-instance-event-notification-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-instance-event-notification-attributes`.

AWS CLI

Ejemplo 1: eliminación de todas las etiquetas de las notificaciones de eventos

En el siguiente ejemplo de `deregister-instance-event-notification-attributes`, se elimina `IncludeAllTagsOfInstance=true`, lo que tiene el efecto de establecer `IncludeAllTagsOfInstance` en `false`.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute IncludeAllTagsOfInstance=true
```

Salida:

```
{
    "InstanceTagAttribute": {
        "InstanceTagKeys": [],
        "IncludeAllTagsOfInstance": true
    }
}
```

Para obtener más información, consulte Eventos programados para las instancias en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

Ejemplo 2: eliminación de etiquetas específicas de las notificaciones de eventos

En el siguiente ejemplo de `deregister-instance-event-notification-attributes`, se elimina la etiqueta especificada de las etiquetas incluidas en las notificaciones de eventos. Para describir el resto de etiquetas incluidas en las notificaciones de eventos, utilice `describe-instance-event-notification-attributes`.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute InstanceTagKeys="tag-key2"
```

Salida:

```
{
    "InstanceTagAttribute": {
        "InstanceTagKeys": [
            "tag-key2"
        ],
        "IncludeAllTagsOfInstance": false
    }
}
```

Para obtener más información, consulte Eventos programados para las instancias en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

- Para obtener información sobre la API, consulte DeregisterInstanceEventNotificationAttributes en la Referencia de comandos de la AWS CLI.

`deregister-transit-gateway-multicast-group-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-transit-gateway-multicast-group-members`.

AWS CLI

Para anular el registro de los miembros de un grupo de multidifusión

En este ejemplo, se anula el registro del miembro del grupo de interfaz de red especificado del grupo de multidifusión de puerta de enlace de tránsito.

```
aws ec2 deregister-transit-gateway-multicast-group-members \
    --transit-gateway-multicast-domain-id tgw-mcast-domain-0c4905cef7EXAMPLE \
    --group-ip-address 224.0.1.0 \
```

```
    --network-interface-ids eni-0e246d3269EXAMPLE
```

Salida:

```
{
    "DeregisteredMulticastGroupMembers": {
        "TransitGatewayMulticastDomainId": "tgw-mcast-domain-0c4905cef7EXAMPLE",
        "RegisteredNetworkInterfaceIds": [
            "eni-0e246d3269EXAMPLE"
        ],
        "GroupIpAddress": "224.0.1.0"
    }
}
```

Para obtener más información, consulte Deregister Members from a Multicast Group en la Guía del usuario de AWS Transit Gateway.

- Para obtener información sobre la API, consulte DeregisterTransitGatewayMulticastGroupMembers en la Referencia de comandos de la AWS CLI.

`deregister-transit-gateway-multicast-group-source`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-transit-gateway-multicast-group-source`.

AWS CLI

Para anular el registro de un origen del grupo de multidifusión de puerta de enlace de tránsito

En este ejemplo, se anula el registro del origen del grupo de interfaz de red especificado del grupo de multidifusión.

```
aws ec2 register-transit-gateway-multicast-group-sources \
    --transit-gateway-multicast-domain-id tgw-mcast-domain-0c4905cef79d6e597 \
    --group-ip-address 224.0.1.0 \
    --network-interface-ids eni-07f290fc3c090cbae
```

Salida:

```
{
    "DeregisteredMulticastGroupSources": {
```

```
        "TransitGatewayMulticastDomainId": "tgw-mcast-domain-0c4905cef79d6e597",
        "DeregisteredNetworkInterfaceIds": [
            "eni-07f290fc3c090cbae"
        ],
        "GroupIpAddress": "224.0.1.0"
    }
}
```

Para obtener más información, consulte Deregister Sources from a Multicast Group en la Guía del usuario de AWS Transit Gateway.

- Para obtener información sobre la API, consulte DeregisterTransitGatewayMulticastGroupSource en la Referencia de comandos de la AWS CLI.

`describe-account-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-account-attributes`.

AWS CLI

Para describir todos los atributos de su cuenta de AWS

En este ejemplo, se describen los atributos de su cuenta de AWS.

Comando:

```
aws ec2 describe-account-attributes
```

Salida:

```
{
    "AccountAttributes": [
        {
            "AttributeName": "vpc-max-security-groups-per-interface",
            "AttributeValues": [
                {
                    "AttributeValue": "5"
                }
            ]
        },
        {
            "AttributeName": "max-instances",
            "AttributeValues": [
```

```
                {
                    "AttributeValue": "20"
                }
            ]
        },
        {
            "AttributeName": "supported-platforms",
            "AttributeValues": [
                {
                    "AttributeValue": "EC2"
                },
                {
                    "AttributeValue": "VPC"
                }
            ]
        },
        {
            "AttributeName": "default-vpc",
            "AttributeValues": [
                {
                    "AttributeValue": "none"
                }
            ]
        },
        {
            "AttributeName": "max-elastic-ips",
            "AttributeValues": [
                {
                    "AttributeValue": "5"
                }
            ]
        },
        {
            "AttributeName": "vpc-max-elastic-ips",
            "AttributeValues": [
                {
                    "AttributeValue": "5"
                }
            ]
        }
    ]
}
```

Para describir un solo atributo de su cuenta de AWS

En este ejemplo, se describe el atributo `supported-platforms` de su cuenta de AWS.

Comando:

```
aws ec2 describe-account-attributes --attribute-names supported-platforms
```

Salida:

```
{
    "AccountAttributes": [
        {
            "AttributeName": "supported-platforms",
            "AttributeValues": [
                {
                    "AttributeValue": "EC2"
                },
                {
                    "AttributeValue": "VPC"
                }
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeAccountAttributes en la Referencia de comandos de la AWS CLI.

`describe-address-transfers`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-address-transfers`.

AWS CLI

Para describir una transferencia de una dirección IP elástica

En el siguiente ejemplo de `describe-address-transfers`, se describe la transferencia de dirección IP elástica para la dirección IP elástica especificada.

```
aws ec2 describe-address-transfers \
```

```
    --allocation-ids eipalloc-09ad461b0d03f6aaf
```

Salida:

```
{
    "AddressTransfers": [
        {
            "PublicIp": "100.21.184.216",
            "AllocationId": "eipalloc-09ad461b0d03f6aaf",
            "TransferAccountId": "123456789012",
            "TransferOfferExpirationTimestamp": "2023-02-22T22:51:01.000Z",
            "AddressTransferStatus": "pending"
        }
    ]
}
```

Para obtener más información, consulte Transfer Elastic IP addresses en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte DescribeAddressTransfers en la Referencia de comandos de la AWS CLI.

`describe-addresses-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-addresses-attribute`.

AWS CLI

Para ver los atributos del nombre de dominio asociado a una dirección IP elástica

En los siguientes ejemplos de `describe-addresses-attribute`, se devuelven los atributos del nombre de dominio asociado a la dirección IP elástica.

Linux:

```
aws ec2 describe-addresses-attribute \
    --allocation-ids eipalloc-abcdef01234567890 \
    --attribute domain-name
```

Windows:

```
aws ec2 describe-addresses-attribute ^
```

```
    --allocation-ids eipalloc-abcdef01234567890 ^
    --attribute domain-name
```

Salida:

```
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.com."
        }
    ]
}
```

Para ver los atributos de una dirección IP elástica, antes debe haber asociado un nombre de dominio asociado a la dirección IP elástica. Para obtener más información, consulte Use reverse DNS for email applications en la Guía del usuario de Amazon EC2 o modify-address-attribute en la Referencia de comandos de la AWS CLI.

- Para obtener información sobre la API, consulte DescribeAddressesAttribute en la Referencia de comandos de la AWS CLI.

`describe-addresses`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-addresses`.

AWS CLI

Ejemplo 1: Recuperar detalles sobre todas las direcciones IP elásticas

En el siguiente ejemplo de `describe addresses`, se muestran los detalles de las direcciones IP elásticas.

```
aws ec2 describe-addresses
```

Salida:

```
{
    "Addresses": [
```

```
        {
            "InstanceId": "i-1234567890abcdef0",
            "PublicIp": "198.51.100.0",
            "PublicIpv4Pool": "amazon",
            "Domain": "standard"
        },
        {
            "Domain": "vpc",
            "PublicIpv4Pool": "amazon",
            "InstanceId": "i-1234567890abcdef0",
            "NetworkInterfaceId": "eni-12345678",
            "AssociationId": "eipassoc-12345678",
            "NetworkInterfaceOwnerId": "123456789012",
            "PublicIp": "203.0.113.0",
            "AllocationId": "eipalloc-12345678",
            "PrivateIpAddress": "10.0.1.241"
        }
    ]
}
```

Ejemplo 2: Recuperar detalles sobre las direcciones IP elásticas de EC2-VPC

En el siguiente ejemplo de `describe-addresses`, se muestran detalles sobre las direcciones IP elásticas para usarlas con las instancias de una VPC.

```
aws ec2 describe-addresses \
    --filters "Name=domain,Values=vpc"
```

Salida:

```
{
    "Addresses": [
        {
            "Domain": "vpc",
            "PublicIpv4Pool": "amazon",
            "InstanceId": "i-1234567890abcdef0",
            "NetworkInterfaceId": "eni-12345678",
            "AssociationId": "eipassoc-12345678",
            "NetworkInterfaceOwnerId": "123456789012",
            "PublicIp": "203.0.113.0",
            "AllocationId": "eipalloc-12345678",
            "PrivateIpAddress": "10.0.1.241"
```

```
        }
    ]
}
```

Ejemplo 3: recuperar detalles sobre una dirección IP elástica especificada por el ID de asignación

En el siguiente ejemplo de `describe-addresses`, se muestran los detalles sobre la dirección IP elástica con el ID de asignación especificado, el cual está asociado a una instancia en EC2-VPC.

```
aws ec2 describe-addresses \
    --allocation-ids eipalloc-282d9641
```

Salida:

```
{
    "Addresses": [
        {
            "Domain": "vpc",
            "PublicIpv4Pool": "amazon",
            "InstanceId": "i-1234567890abcdef0",
            "NetworkInterfaceId": "eni-1a2b3c4d",
            "AssociationId": "eipassoc-123abc12",
            "NetworkInterfaceOwnerId": "1234567891012",
            "PublicIp": "203.0.113.25",
            "AllocationId": "eipalloc-282d9641",
            "PrivateIpAddress": "10.251.50.12"
        }
    ]
}
```

Ejemplo 4: recuperar detalles sobre una dirección IP elástica especificada por la dirección IP privada de su VPC

En el siguiente ejemplo de `describe-addresses`, se muestran los detalles sobre la dirección IP elástica asociada a una dirección IP privada en particular en EC2-VPC.

```
aws ec2 describe-addresses \
    --filters "Name=private-ip-address,Values=10.251.50.12"
```

Ejemplo 5: recuperar detalles sobre las direcciones IP elásticas en EC2-Classic

En el siguiente ejemplo de `describe-addresses`, se muestran los detalles de una dirección IP elástica para su uso en EC2-Classic.

```
aws ec2 describe-addresses \
    --filters "Name=domain,Values=standard"
```

Salida:

```
{
    "Addresses": [
        {
            "InstanceId": "i-1234567890abcdef0",
            "PublicIp": "203.0.110.25",
            "PublicIpv4Pool": "amazon",
            "Domain": "standard"
        }
    ]
}
```

Ejemplo 6: recuperar detalles sobre una dirección IP elástica especificada por la dirección IP pública

En el siguiente ejemplo de `describe-addresses`, se muestran detalles sobre la dirección IP elástica con el valor `203.0.110.25`, el cual está asociado a una instancia en EC2-Classic.

```
aws ec2 describe-addresses \
    --public-ips 203.0.110.25
```

Salida:

```
{
    "Addresses": [
        {
            "InstanceId": "i-1234567890abcdef0",
            "PublicIp": "203.0.110.25",
            "PublicIpv4Pool": "amazon",
            "Domain": "standard"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeAddresses en la Referencia de comandos de la AWS CLI.

`describe-aggregate-id-format`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-aggregate-id-format`.

AWS CLI

Para describir la configuración de formato de ID más largo de todos los tipos de recursos de una región

En el siguiente ejemplo de `describe-aggregate-id-format`, se describe el estado general del formato de ID largo de la región actual. El valor `Deadline` indica que han expirado los plazos para que estos recursos cambien permanentemente del formato de ID corto al formato de ID largo. El valor `UseLongIdsAggregated` indica que todos los usuarios y roles de IAM están configurados para utilizar un formato de ID largo en todos los tipos de recursos.

```
aws ec2 describe-aggregate-id-format
```

Salida:

```
{
    "UseLongIdsAggregated": true,
    "Statuses": [
        {
            "Deadline": "2018-08-13T02:00:00.000Z",
            "Resource": "network-interface-attachment",
            "UseLongIds": true
        },
        {
            "Deadline": "2016-12-13T02:00:00.000Z",
            "Resource": "instance",
            "UseLongIds": true
        },
        {
            "Deadline": "2018-08-13T02:00:00.000Z",
            "Resource": "elastic-ip-association",
            "UseLongIds": true
        },
        ...
```

```
    ]
}
```

- Para obtener información sobre la API, consulte DescribeAggregateIdFormat en la Referencia de comandos de la AWS CLI.

`describe-availability-zones`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-availability-zones`.

AWS CLI

Describir las zonas de disponibilidad

En el siguiente ejemplo de `describe-availability-zones`, se muestran los detalles de las zonas de disponibilidad que están disponibles para usted. La respuesta incluye las zonas de disponibilidad solo para la región actual. En este ejemplo, se usa la región predeterminada del perfil `us-west-2` (Oregón).

```
aws ec2 describe-availability-zones
```

Salida:

```
{
    "AvailabilityZones": [
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2a",
            "ZoneId": "usw2-az1",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2b",
            "ZoneId": "usw2-az2",
```

```
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2c",
            "ZoneId": "usw2-az3",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2d",
            "ZoneId": "usw2-az4",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2"
        },
        {
            "State": "available",
            "OptInStatus": "opted-in",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2-lax-1a",
            "ZoneId": "usw2-lax1-az1",
            "GroupName": "us-west-2-lax-1",
            "NetworkBorderGroup": "us-west-2-lax-1"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeAvailabilityZones en la Referencia de comandos de la AWS CLI.

`describe-aws-network-performance-metric-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-aws-network-performance-metric-subscription`.

AWS CLI

Para describir sus suscripciones a métricas

En el siguiente ejemplo de `describe-aws-network-performance-metric-subscriptions`, se describen sus suscripciones a métricas.

```
aws ec2 describe-aws-network-performance-metric-subscriptions
```

Salida:

```
{
    "Subscriptions": [
        {
            "Source": "us-east-1",
            "Destination": "eu-west-1",
            "Metric": "aggregate-latency",
            "Statistic": "p50",
            "Period": "five-minutes"
        }
    ]
}
```

Para obtener más información, consulte Manage subscriptions en la Guía del usuario de rendimiento de la infraestructura.

- Para obtener información sobre la API, consulte DescribeAwsNetworkPerformanceMetricSubscription en la Referencia de comandos de la AWS CLI.

`describe-aws-network-performance-metric-subscriptions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-aws-network-performance-metric-subscriptions`.

AWS CLI

Para describir sus suscripciones a métricas

En el siguiente ejemplo de `describe-aws-network-performance-metric-subscriptions`, se describen sus suscripciones a métricas.

```
aws ec2 describe-aws-network-performance-metric-subscriptions
```

Salida:

```
{
    "Subscriptions": [
        {
            "Source": "us-east-1",
            "Destination": "eu-west-1",
            "Metric": "aggregate-latency",
            "Statistic": "p50",
            "Period": "five-minutes"
        }
    ]
}
```

Para obtener más información, consulte Manage subscriptions en la Guía del usuario de rendimiento de la infraestructura.

- Para obtener información sobre la API, consulte DescribeAwsNetworkPerformanceMetricSubscriptions en la Referencia de comandos de la AWS CLI.

`describe-bundle-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-bundle-tasks`.

AWS CLI

Para describir sus tareas agrupadas

En este ejemplo, se describen todas sus tareas agrupadas.

Comando:

```
aws ec2 describe-bundle-tasks
```

Salida:

```
{
  "BundleTasks": [
```

```
    {
      "UpdateTime": "2015-09-15T13:26:54.000Z",
      "InstanceId": "i-1234567890abcdef0",
      "Storage": {
        "S3": {
            "Prefix": "winami",
            "Bucket": "bundletasks"
        }
      },
      "State": "bundling",
      "StartTime": "2015-09-15T13:24:35.000Z",
      "Progress": "3%",
      "BundleId": "bun-2a4e041c"
    }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeBundleTasks en la Referencia de comandos de la AWS CLI.

`describe-byoip-cidrs`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-byoip-cidrs`.

AWS CLI

Para describir los rangos de direcciones aprovisionadas

En el siguiente ejemplo de `describe-byoip-cidrs`, se muestra la información sobre los rangos de direcciones IPv4 públicas que ha aprovisionado para su uso por parte de AWS.

```
aws ec2 describe-byoip-cidrs
```

Salida:

```
{
    "ByoipCidrs": [
        {
            "Cidr": "203.0.113.25/24",
            "StatusMessage": "ipv4pool-ec2-1234567890abcdef0",
            "State": "provisioned"
        }
```

```
    ]
}
```

- Para obtener información sobre la API, consulte DescribeByoipCidrs en la Referencia de comandos de la AWS CLI.

`describe-capacity-reservation-fleets`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-capacity-reservation-fleets`.

AWS CLI

Para ver una flota de reservas de capacidad

En el siguiente ejemplo de `describe-capacity-reservation-fleets`, se enumera la información de configuración y capacidad de la flota de reservas de capacidad especificada. También se muestran los detalles sobre las reservas de capacidad individuales contenidas en la flota.

```
aws ec2 describe-capacity-reservation-fleets \
    --capacity-reservation-fleet-ids crf-abcdef01234567890
```

Salida:

```
{
    "CapacityReservationFleets": [
        {
            "State": "active",
            "EndDate": "2022-12-31T23:59:59.000Z",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "CapacityReservationFleetId": "crf-abcdef01234567890",
            "Tenancy": "default",
            "InstanceTypeSpecifications": [
                {
                    "CapacityReservationId": "cr-1234567890abcdef0",
                    "AvailabilityZone": "us-east-1a",
                    "FulfilledCapacity": 5.0,
                    "Weight": 1.0,
                    "CreateDate": "2022-07-02T08:34:33.398Z",
                    "InstancePlatform": "Linux/UNIX",
```

```
                    "TotalInstanceCount": 5,
                    "Priority": 1,
                    "EbsOptimized": true,
                    "InstanceType": "m5.xlarge"
                }
            ],
            "TotalTargetCapacity": 5,
            "TotalFulfilledCapacity": 5.0,
            "CreateTime": "2022-07-02T08:34:33.397Z",
            "AllocationStrategy": "prioritized"
        }
    ]
}
```

Para obtener más información sobre flotas de reserva de capacidad, consulte Flotas de reservas de capacidad en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeCapacityReservationFleets en la Referencia de comandos de la AWS CLI.

`describe-capacity-reservations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-capacity-reservations`.

AWS CLI

Ejemplo 1: descripción de una o varias de sus reservas de capacidad

En el siguiente ejemplo de `describe-capacity-reservations`, se muestra la información sobre todas sus reservas de capacidad en la región de AWS actual.

```
aws ec2 describe-capacity-reservations
```

Salida:

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1234abcd56EXAMPLE ",
            "OwnerId": "123456789111",
            "CapacityReservationArn": "arn:aws:ec2:us-east-1:123456789111:capacity-
reservation/cr-1234abcd56EXAMPLE",
```

```
            "AvailabilityZoneId": "use1-az2",
            "InstanceType": "c5.large",
            "InstancePlatform": "Linux/UNIX",
            "AvailabilityZone": "us-east-1a",
            "Tenancy": "default",
            "TotalInstanceCount": 1,
            "AvailableInstanceCount": 1,
            "EbsOptimized": true,
            "EphemeralStorage": false,
            "State": "active",
            "StartDate": "2024-10-23T15:00:24+00:00",
            "EndDateType": "unlimited",
            "InstanceMatchCriteria": "open",
            "CreateDate": "2024-10-23T15:00:24+00:00",
            "Tags": [],
            "CapacityAllocations": []
        },
        {
            "CapacityReservationId": "cr-abcdEXAMPLE9876ef ",
            "OwnerId": "123456789111",
            "CapacityReservationArn": "arn:aws:ec2:us-east-1:123456789111:capacity-
reservation/cr-abcdEXAMPLE9876ef",
            "AvailabilityZoneId": "use1-az2",
            "InstanceType": "c4.large",
            "InstancePlatform": "Linux/UNIX",
            "AvailabilityZone": "us-east-1a",
            "Tenancy": "default",
            "TotalInstanceCount": 1,
            "AvailableInstanceCount": 1,
            "EbsOptimized": true,
            "EphemeralStorage": false,
            "State": "cancelled",
            "StartDate": "2024-10-23T15:01:03+00:00",
            "EndDateType": "unlimited",
            "InstanceMatchCriteria": "open",
            "CreateDate": "2024-10-23T15:01:02+00:00",
            "Tags": [],
            "CapacityAllocations": []
        }
    ]
}
```

Ejemplo 2: descripción de una o varias de sus reservas de capacidad

En el siguiente ejemplo de `describe-capacity-reservations`, se muestra la información sobre la reserva de capacidad especificada.

```
aws ec2 describe-capacity-reservations \
    --capacity-reservation-ids cr-1234abcd56EXAMPLE
```

Salida:

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-abcdEXAMPLE9876ef ",
            "OwnerId": "123456789111",
            "CapacityReservationArn": "arn:aws:ec2:us-east-1:123456789111:capacity-
reservation/cr-abcdEXAMPLE9876ef",
            "AvailabilityZoneId": "use1-az2",
            "InstanceType": "c4.large",
            "InstancePlatform": "Linux/UNIX",
            "AvailabilityZone": "us-east-1a",
            "Tenancy": "default",
            "TotalInstanceCount": 1,
            "AvailableInstanceCount": 1,
            "EbsOptimized": true,
            "EphemeralStorage": false,
            "State": "active",
            "StartDate": "2024-10-23T15:01:03+00:00",
            "EndDateType": "unlimited",
            "InstanceMatchCriteria": "open",
            "CreateDate": "2024-10-23T15:01:02+00:00",
            "Tags": [],
            "CapacityAllocations": []
        }
    ]
}
```

Para obtener más información, consulte Viewing a Capacity Reservation en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

- Para obtener información sobre la API, consulte DescribeCapacityReservations en la Referencia de comandos de la AWS CLI.

`describe-carrier-gateways`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-carrier-gateways`.

AWS CLI

Para describir todas las puertas de enlace de operador

En el siguiente ejemplo de `describe-carrier-gateways`, se muestran todas las puertas de enlace de operador.

```
aws ec2 describe-carrier-gateways
```

Salida:

```
{
    "CarrierGateways": [
        {
            "CarrierGatewayId": "cagw-0465cdEXAMPLE1111",
            "VpcId": "vpc-0c529aEXAMPLE",
            "State": "available",
            "OwnerId": "123456789012",
            "Tags": [
                {

                    "Key": "example",
                    "Value": "tag"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Carrier gateways<https://docs.aws.amazon.com/vpc/latest/userguide/Carrier_Gateway.html> en la Guía del usuario de Amazon Virtual Private Cloud.

- Para obtener información sobre la API, consulte DescribeCarrierGateways en la Referencia de comandos de la AWS CLI.

describe-classic-link-instances

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-classic-link-instances`.

AWS CLI

Para describir instancias EC2-Classic vinculadas

En este ejemplo se muestran todas las instancias de EC2-Classic vinculadas.

Comando:

```
aws ec2 describe-classic-link-instances
```

Salida:

```
{
        "Instances": [
                {
                        "InstanceId": "i-1234567890abcdef0",
                        "VpcId": "vpc-88888888",
                        "Groups": [
                                {
                                        "GroupId": "sg-11122233"
                                }
                        ],
                        "Tags": [
                                {
                                        "Value": "ClassicInstance",
                                        "Key": "Name"
                                }
                        ]
                },
                {
                        "InstanceId": "i-0598c7d356eba48d7",
                        "VpcId": "vpc-12312312",
                        "Groups": [
                                {
                                        "GroupId": "sg-aabbccdd"
                                }
                        ],
```

```
                        "Tags": [
                                {
                                        "Value": "ClassicInstance2",
                                        "Key": "Name"
                                }
                        ]
                }
        ]
}
```

En este ejemplo, se enumeran todas las instancias de EC2-Classic vinculadas y se filtra la respuesta para incluir solo las instancias que están vinculadas a la VPC vpc-88888888.

Comando:

```
aws ec2 describe-classic-link-instances --filter "Name=vpc-id,Values=vpc-88888888"
```

Salida:

```
{
        "Instances": [
                {
                        "InstanceId": "i-1234567890abcdef0",
                        "VpcId": "vpc-88888888",
                        "Groups": [
                                {
                                        "GroupId": "sg-11122233"
                                }
                        ],
                        "Tags": [
                                {
                                        "Value": "ClassicInstance",
                                        "Key": "Name"
                                }
                        ]
                }
        ]
}
```

- Para obtener información sobre la API, consulte DescribeClassicLinkInstances en la Referencia de comandos de la AWS CLI.

`describe-client-vpn-authorization-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-client-vpn-authorization-rules`.

AWS CLI

Para describir las reglas de autorización para un punto de conexión de Client VPN

En el siguiente ejemplo de `describe-client-vpn-authorization-rules`, se muestra la información sobre las reglas de autorización para el punto de conexión de Client VPN especificado.

```
aws ec2 describe-client-vpn-authorization-rules \
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde
```

Salida:

```
{
    "AuthorizationRules": [
        {
            "ClientVpnEndpointId": "cvpn-endpoint-123456789123abcde",
            "GroupId": "",
            "AccessAll": true,
            "DestinationCidr": "0.0.0.0/0",
            "Status": {
                "Code": "active"
            }
        }
    ]
}
```

Para obtener más información, consulte Authorization Rules en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte DescribeClientVpnAuthorizationRules en la Referencia de comandos de la AWS CLI.

`describe-client-vpn-connections`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-client-vpn-connections`.

AWS CLI

Para describir las conexiones a un punto de conexión de Client VPN

En el siguiente ejemplo de `describe-client-vpn-connections`, se muestra la información sobre las conexiones de cliente al punto de conexión de Client VPN especificado.

```
aws ec2 describe-client-vpn-connections \
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde
```

Salida:

```
{
    "Connections": [
        {
            "ClientVpnEndpointId": "cvpn-endpoint-123456789123abcde",
            "Timestamp": "2019-08-12 07:58:34",
            "ConnectionId": "cvpn-connection-0e03eb24267165acd",
            "ConnectionEstablishedTime": "2019-08-12 07:57:14",
            "IngressBytes": "32302",
            "EgressBytes": "5696",
            "IngressPackets": "332",
            "EgressPackets": "67",
            "ClientIp": "172.31.0.225",
            "CommonName": "client1.domain.tld",
            "Status": {
                "Code": "terminated"
            },
            "ConnectionEndTime": "2019-08-12 07:58:34"
        },
        {
            "ClientVpnEndpointId": "cvpn-endpoint-123456789123abcde",
            "Timestamp": "2019-08-12 08:02:54",
            "ConnectionId": "cvpn-connection-00668867a40f18253",
            "ConnectionEstablishedTime": "2019-08-12 08:02:53",
            "IngressBytes": "2951",
            "EgressBytes": "2611",
            "IngressPackets": "9",
            "EgressPackets": "6",
            "ClientIp": "172.31.0.226",
            "CommonName": "client1.domain.tld",
            "Status": {
                "Code": "active"
```

```
            },
            "ConnectionEndTime": "-"
        }
    ]
}
```

Para obtener más información, consulte Client Connections en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte DescribeClientVpnConnections en la Referencia de comandos de la AWS CLI.

`describe-client-vpn-endpoints`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-client-vpn-endpoints`.

AWS CLI

Para describir los puntos de conexión de Client VPN

En el siguiente ejemplo de `describe-client-vpn-endpoints`, se muestra la información sobre todos los puntos de conexión de Client VPN.

```
aws ec2 describe-client-vpn-endpoints
```

Salida:

```
{
    "ClientVpnEndpoints": [
        {
            "ClientVpnEndpointId": "cvpn-endpoint-123456789123abcde",
            "Description": "Endpoint for Admin access",
            "Status": {
                "Code": "available"
            },
            "CreationTime": "2020-11-13T11:37:27",
            "DnsName": "*.cvpn-endpoint-123456789123abcde.prod.clientvpn.ap-
south-1.amazonaws.com",
            "ClientCidrBlock": "172.31.0.0/16",
            "DnsServers": [
                "8.8.8.8"
            ],
            "SplitTunnel": false,
```

```
            "VpnProtocol": "openvpn",
            "TransportProtocol": "udp",
            "VpnPort": 443,
            "ServerCertificateArn": "arn:aws:acm:ap-
south-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "AuthenticationOptions": [
                {
                    "Type": "certificate-authentication",
                    "MutualAuthentication": {
                        "ClientRootCertificateChain": "arn:aws:acm:ap-
south-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE"
                    }
                }
            ],
            "ConnectionLogOptions": {
                "Enabled": true,
                "CloudwatchLogGroup": "Client-vpn-connection-logs",
                "CloudwatchLogStream": "cvpn-endpoint-123456789123abcde-ap-
south-1-2020/11/13-FCD8HEMVaCcw"
            },
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Client VPN"
                }
            ],
            "SecurityGroupIds": [
                "sg-aabbcc11223344567"
            ],
            "VpcId": "vpc-a87f92c1",
            "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/
endpoints/cvpn-endpoint-123456789123abcde",
            "ClientConnectOptions": {
                 "Enabled": false
            }
        }
    ]
}
```

Para obtener más información, consulte Client VPN Endpoints en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte DescribeClientVpnEndpoints en la Referencia de comandos de la AWS CLI.

`describe-client-vpn-routes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-client-vpn-routes`.

AWS CLI

Para describir las rutas de un punto de conexión de Client VPN

En el siguiente ejemplo de `describe-client-vpn-routes`, se muestra la información sobre las rutas para el punto de conexión de Client VPN especificado.

```
aws ec2 describe-client-vpn-routes \
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde
```

Salida:

```
{
    "Routes": [
        {
            "ClientVpnEndpointId": "cvpn-endpoint-123456789123abcde",
            "DestinationCidr": "10.0.0.0/16",
            "TargetSubnet": "subnet-0123456789abcabca",
            "Type": "Nat",
            "Origin": "associate",
            "Status": {
                "Code": "active"
            },
            "Description": "Default Route"
        },
        {
            "ClientVpnEndpointId": "cvpn-endpoint-123456789123abcde",
            "DestinationCidr": "0.0.0.0/0",
            "TargetSubnet": "subnet-0123456789abcabca",
            "Type": "Nat",
            "Origin": "add-route",
            "Status": {
                "Code": "active"
            }
        }
    ]
}
```

Para obtener más información, consulte Routes en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte DescribeClientVpnRoutes en la Referencia de comandos de la AWS CLI.

`describe-client-vpn-target-networks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-client-vpn-target-networks`.

AWS CLI

Para describir las redes de destino de un punto de conexión de Client VPN

En el siguiente ejemplo de `describe-client-vpn-target-networks`, se muestra la información sobre las redes de destino para el punto de conexión de Client VPN especificado.

```
aws ec2 describe-client-vpn-target-networks \
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde
```

Salida:

```
{
    "ClientVpnTargetNetworks": [
        {
            "AssociationId": "cvpn-assoc-012e837060753dc3d",
            "VpcId": "vpc-11111222222333333",
            "TargetNetworkId": "subnet-0123456789abcabca",
            "ClientVpnEndpointId": "cvpn-endpoint-123456789123abcde",
            "Status": {
                "Code": "associating"
            },
            "SecurityGroups": [
                "sg-012345678910abcab"
            ]
        }
    ]
}
```

Para obtener más información, consulte Target Networks en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte DescribeClientVpnTargetNetworks en la Referencia de comandos de la AWS CLI.

`describe-coip-pools`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-coip-pools`.

AWS CLI

Para describir los grupos de direcciones IP propiedad del cliente

En el siguiente ejemplo de `describe-coip-pools`, se describen los grupos de direcciones IP propiedad del cliente de su cuenta de AWS.

```
aws ec2 describe-coip-pools
```

Salida:

```
{
    "CoipPools": [
        {
            "PoolId": "ipv4pool-coip-123a45678bEXAMPLE",
            "PoolCidrs": [
                "0.0.0.0/0"
            ],
            "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
            "PoolArn": "arn:aws:ec2:us-west-2:123456789012:coip-pool/ipv4pool-
coip-123a45678bEXAMPLE"
        }
    ]
}
```

Para obtener más información, consulte Direcciones IP propiedad del cliente en la Guía del usuario de AWS.

- Para obtener información sobre la API, consulte DescribeCoipPools en la Referencia de comandos de la AWS CLI.

`describe-conversion-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-conversion-tasks`.

AWS CLI

Para ver el estado de una tarea de conversión

En este ejemplo, se devuelve el estado de una tarea de conversión con el ID import-i-ffvko9js.

Comando:

```
aws ec2 describe-conversion-tasks --conversion-task-ids import-i-ffvko9js
```

Salida:

```
{
    "ConversionTasks": [
        {
            "ConversionTaskId": "import-i-ffvko9js",
            "ImportInstance": {
                "InstanceId": "i-1234567890abcdef0",
                "Volumes": [
                    {
                        "Volume": {
                            "Id": "vol-049df61146c4d7901",
                            "Size": 16
                        },
                        "Status": "completed",
                        "Image": {
                            "Size": 1300687360,
                            "ImportManifestUrl": "https://s3.amazonaws.com/
myimportbucket/411443cd-d620-4f1c-9d66-13144EXAMPLE/RHEL5.vmdkmanifest.xml?
AWSAccessKeyId=AKIAIOSFODNN7EXAMPLE&Expires=140EXAMPLE&Signature=XYNhznHNgCqsjDxL9wRL
%2FJvEXAMPLE",
                            "Format": "VMDK"
                        },
                        "BytesConverted": 1300682960,
                        "AvailabilityZone": "us-east-1d"
                    }
                ]
            },
            "ExpirationTime": "2014-05-14T22:06:23Z",
            "State": "completed"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeConversionTasks en la Referencia de comandos de la AWS CLI.

`describe-customer-gateways`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-customer-gateways`.

AWS CLI

Para describir sus puertas de enlace de cliente

En este ejemplo, se describen sus puertas de enlace de cliente.

Comando:

```
aws ec2 describe-customer-gateways
```

Salida:

```
{
    "CustomerGateways": [
        {
            "CustomerGatewayId": "cgw-b4dc3961",
            "IpAddress": "203.0.113.12",
            "State": "available",
            "Type": "ipsec.1",
            "BgpAsn": "65000"
        },
        {
            "CustomerGatewayId": "cgw-0e11f167",
            "IpAddress": "12.1.2.3",
            "State": "available",
            "Type": "ipsec.1",
            "BgpAsn": "65534"
        }
    ]
}
```

Para describir una puerta de enlace de cliente específica

En este ejemplo, se describe la puerta de enlace de cliente especificada.

Comando:

```
aws ec2 describe-customer-gateways --customer-gateway-ids cgw-0e11f167
```

Salida:

```
{
    "CustomerGateways": [
        {
            "CustomerGatewayId": "cgw-0e11f167",
            "IpAddress": "12.1.2.3",
            "State": "available",
            "Type": "ipsec.1",
            "BgpAsn": "65534"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeCustomerGateways en la Referencia de comandos de la AWS CLI.

`describe-dhcp-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-dhcp-options`.

AWS CLI

Ejemplo 1: descripción de sus opciones de DHCP

En el siguiente ejemplo de `describe-dhcp-options`, se recuperan los detalles de todas sus opciones de DHCP.

```
aws ec2 describe-dhcp-options
```

Salida:

```
{
    "DhcpOptions": [
        {
            "DhcpConfigurations": [
                {
                    "Key": "domain-name",
                    "Values": [
                        {
                            "Value": "us-east-2.compute.internal"
                        }
```

```
                    ]
                },
                {
                    "Key": "domain-name-servers",
                    "Values": [
                        {
                            "Value": "AmazonProvidedDNS"
                        }
                    ]
                }
            ],
            "DhcpOptionsId": "dopt-19edf471",
            "OwnerId": "111122223333"
        },
        {
            "DhcpConfigurations": [
                {
                    "Key": "domain-name",
                    "Values": [
                        {
                            "Value": "us-east-2.compute.internal"
                        }
                    ]
                },
                {
                    "Key": "domain-name-servers",
                    "Values": [
                        {
                            "Value": "AmazonProvidedDNS"
                        }
                    ]
                }
            ],
            "DhcpOptionsId": "dopt-fEXAMPLE",
            "OwnerId": "111122223333"
        }
    ]
}
```

Para obtener más información, consulte Working with DHCP Option Sets en la Guía del usuario de AWS VPC.

Ejemplo 2: descripción de las opciones de DHCP y filtrado de la salida

En el siguiente ejemplo de `describe-dhcp-options`, se describen las opciones de DHCP y se utiliza un filtro para devolver únicamente las opciones de DHCP disponibles cuyo nombre de servidor de dominio es `example.com`. En el ejemplo se usa el parámetro `--query` para mostrar únicamente la información de configuración y el ID en la salida.

```
aws ec2 describe-dhcp-options \
    --filters Name=key,Values=domain-name-servers Name=value,Values=example.com \
    --query "DhcpOptions[*].[DhcpConfigurations,DhcpOptionsId]"
```

Salida:

```
[
    [
        [
            {
                "Key": "domain-name",
                "Values": [
                    {
                        "Value": "example.com"
                    }
                ]
            },
            {
                "Key": "domain-name-servers",
                "Values": [
                    {
                        "Value": "172.16.16.16"
                    }
                ]
            }
        ],
        "dopt-001122334455667ab"
    ]
]
```

Para obtener más información, consulte Working with DHCP Option Sets en la Guía del usuario de AWS VPC.

- Para obtener información sobre la API, consulte DescribeDhcpOptions en la Referencia de comandos de la AWS CLI.

`describe-egress-only-internet-gateways`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-egress-only-internet-gateways`.

AWS CLI

Para describir una puerta de enlace de Internet de solo salida

En este ejemplo, se describen sus puertas de enlace de Internet de solo salida.

Comando:

```
aws ec2 describe-egress-only-internet-gateways
```

Salida:

```
{
  "EgressOnlyInternetGateways": [
      {
          "EgressOnlyInternetGatewayId": "eigw-015e0e244e24dfe8a",
          "Attachments": [
              {
                  "State": "attached",
                  "VpcId": "vpc-0c62a468"
              }
          ]
      }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeEgressOnlyInternetGateways en la Referencia de comandos de la AWS CLI.

`describe-elastic-gpus`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-elastic-gpus`.

AWS CLI

Para describir una GPU elástica

Comando:

```
aws ec2 describe-elastic-gpus --elastic-gpu-
ids egpu-12345678901234567890abcdefghijkl
```

- Para obtener información sobre la API, consulte DescribeElasticGpus en la Referencia de comandos de la AWS CLI.

`describe-export-image-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-export-image-tasks`.

AWS CLI

Para supervisar una tarea de exportación de imágenes

En el siguiente ejemplo de `describe-export-image-tasks`, se comprueba el estado de la tarea de exportación de imágenes especificada. El archivo de imagen resultante en Amazon S3 es `my-export-bucket/exports/export-ami-1234567890abcdef0.vmdk`.

```
aws ec2 describe-export-image-tasks \
    --export-image-task-ids export-ami-1234567890abcdef0
```

Salida de una tarea de exportación de imágenes que está en curso.

```
{
    "ExportImageTasks": [
        {
            "ExportImageTaskId": "export-ami-1234567890abcdef0"
            "Progress": "21",
            "S3ExportLocation": {
                "S3Bucket": "my-export-bucket",
                "S3Prefix": "exports/"
            },
            "Status": "active",
            "StatusMessage": "updating"
        }
    ]
}
```

Salida de una tarea de exportación de imágenes que ha finalizado.

```
{
    "ExportImageTasks": [
        {
            "ExportImageTaskId": "export-ami-1234567890abcdef0"
            "S3ExportLocation": {
                "S3Bucket": "my-export-bucket",
                "S3Prefix": "exports/"
            },
            "Status": "completed"
        }
    ]
}
```

Para obtener más información, consulte Export a VM from an AMI en la Guía del usuario de VM Import/Export.

- Para obtener información sobre la API, consulte DescribeExportImageTasks en la Referencia de comandos de la AWS CLI.

`describe-export-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-export-tasks`.

AWS CLI

Para enumerar los detalles de una tarea de exportación de instancias

En este ejemplo, se describe la tarea de exportación con el ID export-i-fh8sjjsq.

Comando:

```
aws ec2 describe-export-tasks --export-task-ids export-i-fh8sjjsq
```

Salida:

```
{
    "ExportTasks": [
        {
            "State": "active",
            "InstanceExportDetails": {
                "InstanceId": "i-1234567890abcdef0",
```

```
                "TargetEnvironment": "vmware"
            },
            "ExportToS3Task": {
                "S3Bucket": "myexportbucket",
                "S3Key": "RHEL5export-i-fh8sjjsq.ova",
                "DiskImageFormat": "vmdk",
                "ContainerFormat": "ova"
            },
            "Description": "RHEL5 instance",
            "ExportTaskId": "export-i-fh8sjjsq"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeExportTasks en la Referencia de comandos de la AWS CLI.

`describe-fast-launch-images`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fast-launch-images`.

AWS CLI

Para describir los detalles de las AMI de Windows configuradas para un lanzamiento más rápido

En el siguiente ejemplo de `describe-fast-launch-images`, se describen los detalles de cada una de las AMI de su cuenta que están configuradas para un lanzamiento más rápido, incluidos el tipo de recurso, la configuración de las instantáneas, los detalles de la plantilla de lanzamiento, el número máximo de lanzamientos paralelos, el ID del propietario de la AMI, el estado de la configuración de lanzamiento rápido, el motivo por el que se cambió el estado y la hora en que se produjo el cambio de estado.

```
aws ec2 describe-fast-launch-images
```

Salida:

```
{
    "FastLaunchImages": [
        {
            "ImageId": "ami-01234567890abcedf",
            "ResourceType": "snapshot",
```

```
            "SnapshotConfiguration": {},
            "LaunchTemplate": {
                "LaunchTemplateId": "lt-01234567890abcedf",
                "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
                "Version": "1"
            },
            "MaxParallelLaunches": 6,
            "OwnerId": "0123456789123",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated",
            "StateTransitionTime": "2022-01-27T22:20:06.552000+00:00"
        }
    ]
}
```

Para obtener más información sobre la configuración de una AMI de Windows para un lanzamiento más rápido, consulte Configure your AMI for faster launching en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeFastLaunchImages en la Referencia de comandos de la AWS CLI.

`describe-fast-snapshot-restores`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fast-snapshot-restores`.

AWS CLI

Para describir las restauraciones rápidas de instantáneas

En el siguiente ejemplo de `describe-fast-snapshot-restores`, se muestra la información de todas las restauraciones rápidas de instantáneas con el estado `disabled`.

```
aws ec2 describe-fast-snapshot-restores \
    --filters Name=state,Values=disabled
```

Salida:

```
{
```

```
    "FastSnapshotRestores": [
        {
            "SnapshotId": "snap-1234567890abcdef0",
            "AvailabilityZone": "us-west-2c",
            "State": "disabled",
            "StateTransitionReason": "Client.UserInitiated - Lifecycle state
 transition",
            "OwnerId": "123456789012",
            "EnablingTime": "2020-01-25T23:57:49.596Z",
            "OptimizingTime": "2020-01-25T23:58:25.573Z",
            "EnabledTime": "2020-01-25T23:59:29.852Z",
            "DisablingTime": "2020-01-26T00:40:56.069Z",
            "DisabledTime": "2020-01-26T00:41:27.390Z"
        }
    ]
}
```

En el siguiente ejemplo de `describe-fast-snapshot-restores`, se describen todas las restauraciones rápidas de instantáneas.

```
aws ec2 describe-fast-snapshot-restores
```

- Para obtener información sobre la API, consulte DescribeFastSnapshotRestores en la Referencia de comandos de la AWS CLI.

`describe-fleet-history`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fleet-history`.

AWS CLI

Para describir el historial de la flota de EC

En el siguiente ejemplo de `describe-fleet-history`, se devuelve el historial de la flota de EC2 especificada a partir de la hora especificada. El resultado es para una flota de EC2 con dos instancias en ejecución.

```
aws ec2 describe-fleet-history \
    --fleet-id fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE \
    --start-time 2020-09-01T00:00:00Z
```

Salida:

```
{
    "HistoryRecords": [
        {
            "EventInformation": {
                "EventSubType": "submitted"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:05.000Z"
        },
        {
            "EventInformation": {
                "EventSubType": "active"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:15.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "t2.small, ami-07c8bc5c1ce9598c3, ...",
                "EventSubType": "progress"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-083a1c446e66085d2"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-090db02406cc3c2d6"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        }
```

```
    ],
    "LastEvaluatedTime": "2020-09-01T19:10:19.000Z",
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
    "StartTime": "2020-08-31T23:53:20.000Z"
}
```

Para obtener más información, consulte Trabajar con la flota de EC2 en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

- Para obtener información sobre la API, consulte DescribeFleetHistory en la Referencia de comandos de la AWS CLI.

`describe-fleet-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fleet-instances`.

AWS CLI

Para describir las instancias en ejecución de una flota de EC

En el siguiente ejemplo de `describe-fleet-instances`, se describen las instancias en ejecución de la flota de EC2 especificada.

```
aws ec2 describe-fleet-instances \
    --fleet-id 12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE
```

Salida:

```
{
    "ActiveInstances": [
        {
            "InstanceId": "i-090db02406cc3c2d6",
            "InstanceType": "t2.small",
            "SpotInstanceRequestId": "sir-a43gtpfk",
            "InstanceHealth": "healthy"
        },
        {
            "InstanceId": "i-083a1c446e66085d2",
            "InstanceType": "t2.small",
            "SpotInstanceRequestId": "sir-iwcit2nj",
            "InstanceHealth": "healthy"
        }
```

```
    ],
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

Para obtener más información, consulte Trabajar con la flota de EC2 en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

- Para obtener información sobre la API, consulte DescribeFleetInstances en la Referencia de comandos de la AWS CLI.

`describe-fleets`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fleets`.

AWS CLI

Para describir una flota de EC

En el siguiente ejemplo de `describe-fleets`, se describe la flota de EC2 especificada.

```
aws ec2 describe-fleets \
    --fleet-ids fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE
```

Salida:

```
{
    "Fleets": [
        {
            "ActivityStatus": "pending_fulfillment",
            "CreateTime": "2020-09-01T18:26:05.000Z",
            "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
            "FleetState": "active",
            "ExcessCapacityTerminationPolicy": "termination",
            "FulfilledCapacity": 0.0,
            "FulfilledOnDemandCapacity": 0.0,
            "LaunchTemplateConfigs": [
                {
                    "LaunchTemplateSpecification": {
                        "LaunchTemplateId": "lt-0e632f2855a979cd5",
                        "Version": "1"
                    }
                }
            ],
```

```
            "TargetCapacitySpecification": {
                "TotalTargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "SpotTargetCapacity": 2,
                "DefaultTargetCapacityType": "spot"
            },
            "TerminateInstancesWithExpiration": false,
            "Type": "maintain",
            "ReplaceUnhealthyInstances": false,
            "SpotOptions": {
                "AllocationStrategy": "lowestPrice",
                "InstanceInterruptionBehavior": "terminate",
                "InstancePoolsToUseCount": 1
            },
            "OnDemandOptions": {
                "AllocationStrategy": "lowestPrice"
            }
        }
    ]
}
```

Para obtener más información, consulte Trabajar con la flota de EC2 en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

- Para obtener información sobre la API, consulte DescribeFleets en la Referencia de comandos de la AWS CLI.

`describe-flow-logs`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-flow-logs`.

AWS CLI

Ejemplo 1: descripción de todos sus registros de flujo

En el siguiente ejemplo de `describe-flow-logs`, se muestra la información de todos sus registros de flujo.

```
aws ec2 describe-flow-logs
```

Salida:

```
{
```

```
    "FlowLogs": [
        {
            "CreationTime": "2018-02-21T13:22:12.644Z",
            "DeliverLogsPermissionArn": "arn:aws:iam::123456789012:role/flow-logs-
role",
            "DeliverLogsStatus": "SUCCESS",
            "FlowLogId": "fl-aabbccdd112233445",
            "MaxAggregationInterval": 600,
            "FlowLogStatus": "ACTIVE",
            "LogGroupName": "FlowLogGroup",
            "ResourceId": "subnet-12345678901234567",
            "TrafficType": "ALL",
            "LogDestinationType": "cloud-watch-logs",
            "LogFormat": "${version} ${account-id} ${interface-id} ${srcaddr}
 ${dstaddr} ${srcport} ${dstport} ${protocol} ${packets} ${bytes} ${start} ${end}
 ${action} ${log-status}"
        },
        {
            "CreationTime": "2020-02-04T15:22:29.986Z",
            "DeliverLogsStatus": "SUCCESS",
            "FlowLogId": "fl-01234567890123456",
            "MaxAggregationInterval": 60,
            "FlowLogStatus": "ACTIVE",
            "ResourceId": "vpc-00112233445566778",
            "TrafficType": "ACCEPT",
            "LogDestinationType": "s3",
            "LogDestination": "arn:aws:s3:::my-flow-log-bucket/custom",
            "LogFormat": "${version} ${vpc-id} ${subnet-id} ${instance-id}
 ${interface-id} ${account-id} ${type} ${srcaddr} ${dstaddr} ${srcport} ${dstport}
 ${pkt-srcaddr} ${pkt-dstaddr} ${protocol} ${bytes} ${packets} ${start} ${end}
 ${action} ${tcp-flags} ${log-status}"
        }
    ]
}
```

Ejemplo 2: descripción de un subconjunto de sus registros de flujo

En el siguiente ejemplo de `describe-flow-logs`, se utiliza un filtro para mostrar la información únicamente de los registros de flujo que se encuentran en el grupo de registros especificado en registros de Amazon CloudWatch.

```
aws ec2 describe-flow-logs \
    --filter "Name=log-group-name,Values=MyFlowLogs"
```

- Para obtener información sobre la API, consulte DescribeFlowLogs en la Referencia de comandos de la AWS CLI.

`describe-fpga-image-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fpga-image-attribute`.

AWS CLI

Para describir los atributos de una imagen de Amazon FPGA

En este ejemplo, se describen los permisos de carga de la AFI especificada.

Comando:

```
aws ec2 describe-fpga-image-attribute --fpga-image-id afi-0d123e123bfc85abc --
attribute loadPermission
```

Salida:

```
{
  "FpgaImageAttribute": {
      "FpgaImageId": "afi-0d123e123bfc85abc",
      "LoadPermissions": [
          {
              "UserId": "123456789012"
          }
      ]
  }
}
```

- Para obtener información sobre la API, consulte DescribeFpgaImageAttribute en la Referencia de comandos de la AWS CLI.

`describe-fpga-images`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fpga-images`.

AWS CLI

Para describir las imágenes de Amazon FPGA

En este ejemplo, se describen las AFI que son propiedad de la cuenta 123456789012.

Comando:

```
aws ec2 describe-fpga-images --filters Name=owner-id,Values=123456789012
```

Salida:

```
{
  "FpgaImages": [
      {
          "UpdateTime": "2017-12-22T12:09:14.000Z",
          "Name": "my-afi",
          "PciId": {
              "SubsystemVendorId": "0xfedd",
              "VendorId": "0x1d0f",
              "DeviceId": "0xf000",
              "SubsystemId": "0x1d51"
          },
          "FpgaImageGlobalId": "agfi-123cb27b5e84a0abc",
          "Public": false,
          "State": {
              "Code": "available"
          },
          "ShellVersion": "0x071417d3",
          "OwnerId": "123456789012",
          "FpgaImageId": "afi-0d123e123bfc85abc",
          "CreateTime": "2017-12-22T11:43:33.000Z",
          "Description": "my-afi"
      }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeFpgaImages en la Referencia de comandos de la AWS CLI.

`describe-host-reservation-offerings`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-host-reservation-offerings`.

AWS CLI

Para describir las ofertas de reservas de hosts dedicados

En este ejemplo, se describen las reservas de hosts dedicados de la familia de instancias M4 que están disponibles para compra.

Comando:

```
aws ec2 describe-host-reservation-offerings --filter Name=instance-family,Values=m4
```

Salida:


```
{
  "OfferingSet": [
      {
          "HourlyPrice": "1.499",
          "OfferingId": "hro-03f707bf363b6b324",
          "InstanceFamily": "m4",
          "PaymentOption": "NoUpfront",
          "UpfrontPrice": "0.000",
          "Duration": 31536000
      },
      {
          "HourlyPrice": "1.045",
          "OfferingId": "hro-0ef9181cabdef7a02",
          "InstanceFamily": "m4",
          "PaymentOption": "NoUpfront",
          "UpfrontPrice": "0.000",
          "Duration": 94608000
      },
      {
          "HourlyPrice": "0.714",
          "OfferingId": "hro-04567a15500b92a51",
          "InstanceFamily": "m4",
          "PaymentOption": "PartialUpfront",
          "UpfrontPrice": "6254.000",
          "Duration": 31536000
      },
      {
          "HourlyPrice": "0.484",
          "OfferingId": "hro-0d5d7a9d23ed7fbfe",
          "InstanceFamily": "m4",
```

```
            "PaymentOption": "PartialUpfront",
            "UpfrontPrice": "12720.000",
            "Duration": 94608000
        },
        {
            "HourlyPrice": "0.000",
            "OfferingId": "hro-05da4108ca998c2e5",
            "InstanceFamily": "m4",
            "PaymentOption": "AllUpfront",
            "UpfrontPrice": "23913.000",
            "Duration": 94608000
        },
        {
            "HourlyPrice": "0.000",
            "OfferingId": "hro-0a9f9be3b95a3dc8f",
            "InstanceFamily": "m4",
            "PaymentOption": "AllUpfront",
            "UpfrontPrice": "12257.000",
            "Duration": 31536000
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeHostReservationOfferings en la Referencia de comandos de la AWS CLI.

`describe-host-reservations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-host-reservations`.

AWS CLI

Para describir las reservas de hosts dedicados de su cuenta

En este ejemplo, se describen las reservas de hosts dedicados de su cuenta.

Comando:

```
aws ec2 describe-host-reservations
```

Salida:

```
{
```

```
  "HostReservationSet": [
      {
          "Count": 1,
          "End": "2019-01-10T12:14:09Z",
          "HourlyPrice": "1.499",
          "InstanceFamily": "m4",
          "OfferingId": "hro-03f707bf363b6b324",
          "PaymentOption": "NoUpfront",
          "State": "active",
          "HostIdSet": [
              "h-013abcd2a00cbd123"
          ],
          "Start": "2018-01-10T12:14:09Z",
          "HostReservationId": "hr-0d418a3a4ffc669ae",
          "UpfrontPrice": "0.000",
          "Duration": 31536000
      }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeHostReservations en la Referencia de comandos de la AWS CLI.

`describe-hosts`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-hosts`.

AWS CLI

Para ver los detalles de los hosts dedicados

En el siguiente ejemplo de `describe-hosts`, se muestra la información de los hosts dedicados de `available` de su cuenta de AWS.

```
aws ec2 describe-hosts --filter "Name=state,Values=available"
```

Salida:

```
{
    "Hosts": [
        {
```

```
            "HostId": "h-07879acf49EXAMPLE",
            "Tags": [
                {
                    "Value": "production",
                    "Key": "purpose"
                }
            ],
            "HostProperties": {
                "Cores": 48,
                "TotalVCpus": 96,
                "InstanceType": "m5.large",
                "Sockets": 2
            },
            "Instances": [],
            "State": "available",
            "AvailabilityZone": "eu-west-1a",
            "AvailableCapacity": {
                "AvailableInstanceCapacity": [
                    {
                        "AvailableCapacity": 48,
                        "InstanceType": "m5.large",
                        "TotalCapacity": 48
                    }
                ],
                "AvailableVCpus": 96
            },
            "HostRecovery": "on",
            "AllocationTime": "2019-08-19T08:57:44.000Z",
            "AutoPlacement": "off"
        }
    ]
}
```

Para obtener más información, consulte Viewing Dedicated Hosts en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

- Para obtener información sobre la API, consulte DescribeHosts en la Referencia de comandos de la AWS CLI.

`describe-iam-instance-profile-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-iam-instance-profile-associations`.

AWS CLI

Describir las asociaciones de perfiles de instancias de IAM

En este ejemplo, se describen todas las asociaciones de perfiles de instancias de IAM.

Comando:

```
aws ec2 describe-iam-instance-profile-associations
```

Salida:

```
{
  "IamInstanceProfileAssociations": [
      {
          "InstanceId": "i-09eb09efa73ec1dee",
          "State": "associated",
          "AssociationId": "iip-assoc-0db249b1f25fa24b8",
          "IamInstanceProfile": {
              "Id": "AIPAJVQN4F5WVLGCJDRGM",
              "Arn": "arn:aws:iam::123456789012:instance-profile/admin-role"
          }
      },
      {
          "InstanceId": "i-0402909a2f4dffd14",
          "State": "associating",
          "AssociationId": "iip-assoc-0d1ec06278d29f44a",
          "IamInstanceProfile": {
              "Id": "AGJAJVQN4F5WVLGCJABCM",
              "Arn": "arn:aws:iam::123456789012:instance-profile/user1-role"
          }
      }
   ]
}
```

- Para obtener información sobre la API, consulte DescribeIamInstanceProfileAssociations en la Referencia de comandos de la AWS CLI.

`describe-id-format`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-id-format`.

AWS CLI

Ejemplo 1: descripción del formato de ID de un recurso

En el siguiente ejemplo de `describe-id-format`, se describe el formato de ID de los grupos de seguridad.

```
aws ec2 describe-id-format \
    --resource security-group
```

En la salida del ejemplo siguiente, el valor `Deadline` indica que la fecha límite para que este tipo de recurso cambie permanentemente del formato de ID corto al formato de ID largo que expiró a las 00:00 UTC del 15 de agosto de 2018.

```
{
    "Statuses": [
        {
            "Deadline": "2018-08-15T00:00:00.000Z",
            "Resource": "security-group",
            "UseLongIds": true
        }
    ]
}
```

Ejemplo 2: descripción del formato de ID de todos los recursos

En el siguiente ejemplo de `describe-id-format`, se describe el formato de ID de todos los tipos de recursos. Todos los tipos de recursos que admitían el formato de ID corto se cambiaron para usar el formato de ID largo.

```
aws ec2 describe-id-format
```

- Para obtener información sobre la API, consulte DescribeIdFormat en la Referencia de comandos de la AWS CLI.

`describe-identity-id-format`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-identity-id-format`.

AWS CLI

Para describir el formato de ID de un rol de IAM

En el siguiente ejemplo de `describe-identity-id-format`, se describe el formato de ID que reciben las instancias creadas por el rol de IAM `EC2Role` de su cuenta de AWS.

```
aws ec2 describe-identity-id-format \
    --principal-arn arn:aws:iam::123456789012:role/my-iam-role \
    --resource instance
```

En la salida siguiente se indica que las instancias creadas por este rol reciben los ID en formato de ID largo.

```
{
    "Statuses": [
        {
            "Deadline": "2016-12-15T00:00:00Z",
            "Resource": "instance",
            "UseLongIds": true
        }
    ]
}
```

Para describir el formato de ID de un usuario de IAM

En el siguiente ejemplo de `describe-identity-id-format`, se describe el formato de ID que reciben las instantáneas por el usuario de IAM `AdminUser` de su cuenta de AWS.

```
aws ec2 describe-identity-id-format \
    --principal-arn arn:aws:iam::123456789012:user/AdminUser \
    --resource snapshot
```

En la salida se indica que las instantáneas creadas por este usuario reciben los ID en formato de ID largo.

```
{
    "Statuses": [
        {
            "Deadline": "2016-12-15T00:00:00Z",
```

```
            "Resource": "snapshot",
            "UseLongIds": true
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeIdentityIdFormat en la Referencia de comandos de la AWS CLI.

`describe-image-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-image-attribute`.

AWS CLI

Para describir los permisos de lanzamiento de una AMI

En este ejemplo, se describen los permisos de lanzamiento de la AMI especificada.

Comando:

```
aws ec2 describe-image-attribute --image-id ami-5731123e --
attribute launchPermission
```

Salida:

```
{
    "LaunchPermissions": [
        {
            "UserId": "123456789012"
        }
    ],
    "ImageId": "ami-5731123e",
}
```

Para describir los códigos de producto de una AMI

En este ejemplo, se describen los códigos de producto de la AMI especificada. Tenga en cuenta que esta AMI no tiene códigos de producto.

Comando:

```
aws ec2 describe-image-attribute --image-id ami-5731123e --attribute productCodes
```

Salida:

```
{
    "ProductCodes": [],
    "ImageId": "ami-5731123e",
}
```

- Para obtener información sobre la API, consulte DescribeImageAttribute en la Referencia de comandos de la AWS CLI.

`describe-images`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-images`.

AWS CLI

Ejemplo 1: Describir una AMI

En el siguiente ejemplo de `describe-images`, se describe una AMI especificada en la región especificada.

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-ids ami-1234567890EXAMPLE
```

Salida:

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "EnaSupport": true,
            "Hypervisor": "xen",
            "State": "available",
            "SriovNetSupport": "simple",
            "ImageId": "ami-1234567890EXAMPLE",
            "UsageOperation": "RunInstances:0010",
```

```
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-1112223334444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": true,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```

Para obtener más información, consulte Imágenes de máquina de Amazon (AMI) en la Guía del usuario de Amazon EC2.

Ejemplo 2: Describir las AMI con base en filtros

En el siguiente ejemplo de `describe-images`, se describen las AMI de Windows proporcionadas por Amazon y respaldadas por Amazon EBS.

```
aws ec2 describe-images \
    --owners amazon \
    --filters "Name=platform,Values=windows" "Name=root-device-type,Values=ebs"
```

Para ver un ejemplo del resultado de `describe-images`, consulte el ejemplo 1.

Para ver ejemplos adicionales de uso de filtros, consulte Enumerar y filtrar los recursos en la Guía del usuario de Amazon EC2.

Ejemplo 3: describir las AMI con base en etiquetas

En el siguiente ejemplo de `describe-images`, se describen todas las AMI que tienen la etiqueta `Type=Custom`. En el ejemplo se usa el parámetro `--query` para mostrar solo los ID de las AMI.

```
aws ec2 describe-images \
    --filters "Name=tag:Type,Values=Custom" \
    --query 'Images[*].[ImageId]' \
    --output text
```

Salida:

```
ami-1234567890EXAMPLE
ami-0abcdef1234567890
```

Para ver ejemplos adicionales de uso de filtros de etiquetas, consulte Trabajo con etiquetas en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeImages en la Referencia de comandos de la AWS CLI.

`describe-import-image-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-import-image-tasks`.

AWS CLI

Para supervisar una tarea de importación de imágenes

En el siguiente ejemplo de `describe-import-image-tasks`, se comprueba el estado de la tarea de importación de imágenes especificada.

```
aws ec2 describe-import-image-tasks \
    --import-task-ids import-ami-1234567890abcdef0
```

Salida de una tarea de importación de imágenes que está en curso.

```
{
    "ImportImageTasks": [
        {
```

```
            "ImportTaskId": "import-ami-1234567890abcdef0",
            "Progress": "28",
            "SnapshotDetails": [
                {
                    "DiskImageSize": 705638400.0,
                    "Format": "ova",
                    "Status": "completed",
                    "UserBucket": {
                        "S3Bucket": "my-import-bucket",
                        "S3Key": "vms/my-server-vm.ova"
                    }
                }
            ],
            "Status": "active",
            "StatusMessage": "converting"
        }
    ]
}
```

Salida de una tarea de importación de imágenes que ha finalizado. `ImageId` proporciona el ID de la AMI resultante.

```
{
    "ImportImageTasks": [
        {
            "ImportTaskId": "import-ami-1234567890abcdef0",
            "ImageId": "ami-1234567890abcdef0",
            "SnapshotDetails": [
                {
                    "DiskImageSize": 705638400.0,
                    "Format": "ova",
                    "SnapshotId": "snap-1234567890abcdef0"
                    "Status": "completed",
                    "UserBucket": {
                        "S3Bucket": "my-import-bucket",
                        "S3Key": "vms/my-server-vm.ova"
                    }
                }
            ],
            "Status": "completed"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeImportImageTasks en la Referencia de comandos de la AWS CLI.

`describe-import-snapshot-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-import-snapshot-tasks`.

AWS CLI

Para supervisar una tarea de importación de instantáneas

En el siguiente ejemplo de `describe-import-snapshot-tasks` se comprueba el estado de la tarea de importación de instantáneas especificada.

```
aws ec2 describe-import-snapshot-tasks \
    --import-task-ids import-snap-1234567890abcdef0
```

Salida de una tarea de importación de instantáneas que está en curso:

```
{
    "ImportSnapshotTasks": [
        {
            "Description": "My server VMDK",
            "ImportTaskId": "import-snap-1234567890abcdef0",
            "SnapshotTaskDetail": {
                "Description": "My server VMDK",
                "DiskImageSize": "705638400.0",
                "Format": "VMDK",
                "Progress": "42",
                "Status": "active",
                "StatusMessage": "downloading/converting",
                "UserBucket": {
                    "S3Bucket": "my-import-bucket",
                    "S3Key": "vms/my-server-vm.vmdk"
                }
            }
        }
    ]
}
```

Salida de una tarea de importación de instantáneas que ha finalizado. `SnapshotId` proporciona el ID de la instantánea resultante.

```
{
    "ImportSnapshotTasks": [
        {
            "Description": "My server VMDK",
            "ImportTaskId": "import-snap-1234567890abcdef0",
            "SnapshotTaskDetail": {
                "Description": "My server VMDK",
                "DiskImageSize": "705638400.0",
                "Format": "VMDK",
                "SnapshotId": "snap-1234567890abcdef0"
                "Status": "completed",
                "UserBucket": {
                    "S3Bucket": "my-import-bucket",
                    "S3Key": "vms/my-server-vm.vmdk"
                }
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeImportSnapshotTasks en la Referencia de comandos de la AWS CLI.

`describe-instance-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-attribute`.

AWS CLI

Para describir el tipo de instancia

En este ejemplo, se describe el tipo de instancia de la instancia especificada.

Comando:

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --
attribute instanceType
```

Salida:

```
{
```

```
    "InstanceId": "i-1234567890abcdef0"
    "InstanceType": {
        "Value": "t1.micro"
    }
}
```

Para describir el atributo disableApiTermination

En este ejemplo, se describe el atributo `disableApiTermination` de la instancia especificada.

Comando:

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --
attribute disableApiTermination
```

Salida:

```
{
"InstanceId": "i-1234567890abcdef0"
    "DisableApiTermination": {
        "Value": "false"
    }
}
```

Para describir la asignación de dispositivos de bloques de una instancia

En este ejemplo, se describe el atributo `blockDeviceMapping` de la instancia especificada.

Comando:

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --
attribute blockDeviceMapping
```

Salida:

```
{
    "InstanceId": "i-1234567890abcdef0"
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/sda1",
            "Ebs": {
```

```
                "Status": "attached",
                "DeleteOnTermination": true,
                "VolumeId": "vol-049df61146c4d7901",
                "AttachTime": "2013-05-17T22:42:34.000Z"
            }
        },
        {
            "DeviceName": "/dev/sdf",
            "Ebs": {
                "Status": "attached",
                "DeleteOnTermination": false,
                "VolumeId": "vol-049df61146c4d7901",
                "AttachTime": "2013-09-10T23:07:00.000Z"
            }
        }
    ],
}
```

- Para obtener información sobre la API, consulte DescribeInstanceAttribute en la Referencia de comandos de la AWS CLI.

`describe-instance-connect-endpoints`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-connect-endpoints`.

AWS CLI

Para describir un punto de conexión de EC2 Instance Connect

En el siguiente ejemplo de `describe-instance-connect-endpoints`, se describe el punto de conexión de EC2 Instance Connect especificado.

```
aws ec2 describe-instance-connect-endpoints \
    --region us-east-1 \
    --instance-connect-endpoint-ids eice-0123456789example
```

Salida:

```
{
    "InstanceConnectEndpoints": [
        {
```

```
            "OwnerId": "111111111111",
            "InstanceConnectEndpointId": "eice-0123456789example",
            "InstanceConnectEndpointArn": "arn:aws:ec2:us-
east-1:111111111111:instance-connect-endpoint/eice-0123456789example",
            "State": "create-complete",
            "StateMessage": "",
            "DnsName": "eice-0123456789example.b67b86ba.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com",
            "NetworkInterfaceIds": [
                "eni-0123456789example"
            ],
            "VpcId": "vpc-0123abcd",
            "AvailabilityZone": "us-east-1d",
            "CreatedAt": "2023-02-07T12:05:37+00:00",
            "SubnetId": "subnet-0123abcd",
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Creación de un punto de conexión de EC2 Instance Connect en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeInstanceConnectEndpoints en la Referencia de comandos de la AWS CLI.

`describe-instance-credit-specifications`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-credit-specifications`.

AWS CLI

Para describir la opción de crédito para la utilización de la CPU de una o varias de instancias

En el siguiente ejemplo de `describe-instance-credit-specifications`, se describe la opción de crédito de CPU de la instancia especificada.

```
aws ec2 describe-instance-credit-specifications \
    --instance-ids i-1234567890abcdef0
```

Salida:

```
{
    "InstanceCreditSpecifications": [
        {
            "InstanceId": "i-1234567890abcdef0",
            "CpuCredits": "unlimited"
        }
    ]
}
```

Para obtener más información, consulte Trabajo con instancias de rendimiento ampliables en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeInstanceCreditSpecifications en la Referencia de comandos de la AWS CLI.

`describe-instance-event-notification-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-event-notification-attributes`.

AWS CLI

Para describir las etiquetas de las notificaciones de eventos programados

En el siguiente ejemplo de `describe-instance-event-notification-attributes`, se describen las etiquetas que deben aparecer en las notificaciones de eventos programados.

```
aws ec2 describe-instance-event-notification-attributes
```

Salida:

```
{
    "InstanceTagAttribute": {
        "InstanceTagKeys": [],
        "IncludeAllTagsOfInstance": true
    }
}
```

Para obtener más información, consulte Eventos programados para las instancias en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

- Para obtener información sobre la API, consulte DescribeInstanceEventNotificationAttributes en la Referencia de comandos de la AWS CLI.

`describe-instance-event-windows`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-event-windows`.

AWS CLI

Ejemplo 1: descripción de todos los períodos de eventos

En el siguiente ejemplo de `describe-instance-event-windows`, se describen todos los períodos de eventos de la región especificada.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1
```

Salida:

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0abcdef1234567890",
            "Name": "myEventWindowName",
            "CronExpression": "* 21-23 * * 2,3",
            "AssociationTarget": {
                "InstanceIds": [
                    "i-1234567890abcdef0",
                    "i-0598c7d356eba48d7"
                ],
                "Tags": [],
                "DedicatedHostIds": []
            },
            "State": "active",
            "Tags": []
        }

        ...

    ],
```

```
    "NextToken": "9d624e0c-388b-4862-a31e-a85c64fc1d4a"
}
```

Ejemplo 2: descripción de un período de evento específico

En el siguiente ejemplo de `describe-instance-event-windows`, se describe un evento específico mediante el uso del parámetro `instance-event-window` para describir un período de eventos específico.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1 \
    --instance-event-window-ids iew-0abcdef1234567890
```

Salida:

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0abcdef1234567890",
            "Name": "myEventWindowName",
            "CronExpression": "* 21-23 * * 2,3",
            "AssociationTarget": {
                "InstanceIds": [
                    "i-1234567890abcdef0",
                    "i-0598c7d356eba48d7"
                ],
                "Tags": [],
                "DedicatedHostIds": []
            },
            "State": "active",
            "Tags": []
        }
}
```

Ejemplo 3: descripción de los períodos de eventos que coinciden con uno o varios filtros

En el siguiente ejemplo de `describe-instance-event-windows`, se describen los períodos de eventos que coinciden con uno o varios filtros mediante el parámetro `filter`. El filtro `instance-id` se utiliza para describir todos los períodos de eventos asociados con la instancia especificada. Cuando se utiliza un filtro, este realiza una coincidencia directa. Sin embargo, el filtro `instance-id` es diferente. Si no hay una coincidencia directa con el ID de instancia, se

recurre a asociaciones indirectas con el período de evento, como las etiquetas de la instancia o el ID de host dedicado (si la instancia se encuentra en un host dedicado).

```
aws ec2 describe-instance-event-windows \
    --region us-east-1 \
    --filters Name=instance-id,Values=i-1234567890abcdef0 \
    --max-results 100 \
    --next-token <next-token-value>
```

Salida:

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0dbc0adb66f235982",
            "TimeRanges": [
                {
                    "StartWeekDay": "sunday",
                    "StartHour": 2,
                    "EndWeekDay": "sunday",
                    "EndHour": 8
                }
            ],
            "Name": "myEventWindowName",
            "AssociationTarget": {
                "InstanceIds": [],
                "Tags": [],
                "DedicatedHostIds": [
                    "h-0140d9a7ecbd102dd"
                ]
            },
            "State": "active",
            "Tags": []
        }
    ]
}
```

En la salida del ejemplo, la instancia se encuentra en un host dedicado, que está asociado con el período de evento.

Para conocer las restricciones de los períodos de eventos, consulte Consideraciones en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeInstanceEventWindows en la Referencia de comandos de la AWS CLI.

`describe-instance-image-metadata`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-image-metadata`.

AWS CLI

Ejemplo 1: descripción de los metadatos de AMI de todas las instancias

En el siguiente ejemplo de `describe-instance-image-metadata`, se describen los metadatos de AMI de todas las instancias de la cuenta de AWS en la región especificada.

```
aws ec2 describe-instance-image-metadata \
    --region us-east-1
```

Salida:

```
{
    "InstanceImageMetadata": [
        {
            "InstanceId": "i-1234567890EXAMPLE",
            "InstanceType": "t2.micro",
            "LaunchTime": "2024-08-28T11:25:45+00:00",
            "AvailabilityZone": "us-east-1a",
            "State": {
                "Code": 16,
                "Name": "running"
            },
            "OwnerId": "123412341234",
            "Tags": [
                {
                    "Key": "MyTagName",
                    "Value": "my-tag-value"
                }
            ],
            "ImageMetadata": {
                "ImageId": "ami-0b752bf1df193a6c4",
                "Name": "al2023-ami-2023.5.20240819.0-kernel-6.1-x86_64",
                "OwnerId": "137112412989",
```

```
                "State": "available",
                "ImageOwnerAlias": "amazon",
                "CreationDate": "2023-01-25T17:20:40Z",
                "DeprecationTime": "2025-01-25T17:20:40Z",
                "IsPublic": true
            }
        }
    ],
    "NextToken": "...EXAMPLEwIAABAA2JHaFxLnEXAMPLE..."
}
```

Para obtener más información, consulte Imágenes de máquina de Amazon en Amazon EC2 en la Guía del usuario de Amazon EC2.

Ejemplo 2: descripción de los metadatos de AMI de las instancias especificadas

En el siguiente ejemplo de `describe-instance-image-metadata`, se describen los metadatos de AMI para las instancias especificadas.

```
aws ec2 describe-instance-image-metadata \
    --region us-east-1 \
    --instance-ids i-1234567890EXAMPLE i-0987654321EXAMPLE
```

Salida:

```
{
    "InstanceImageMetadata": [
        {
            "InstanceId": "i-1234567890EXAMPLE",
            "InstanceType": "t2.micro",
            "LaunchTime": "2024-08-28T11:25:45+00:00",
            "AvailabilityZone": "us-east-1a",
            "State": {
                "Code": 16,
                "Name": "running"
            },
            "OwnerId": "123412341234",
            "Tags": [
                {
                    "Key": "MyTagName",
                    "Value": "my-tag-value"
                }
            ],
```

```
            "ImageMetadata": {
                "ImageId": "ami-0b752bf1df193a6c4",
                "Name": "al2023-ami-2023.5.20240819.0-kernel-6.1-x86_64",
                "OwnerId": "137112412989",
                "State": "available",
                "ImageOwnerAlias": "amazon",
                "CreationDate": "2023-01-25T17:20:40Z",
                "DeprecationTime": "2025-01-25T17:20:40Z",
                "IsPublic": true
            }
        },
        {
            "InstanceId": "i-0987654321EXAMPLE",
            "InstanceType": "t2.micro",
            "LaunchTime": "2024-08-28T11:25:45+00:00",
            "AvailabilityZone": "us-east-1a",
            "State": {
                "Code": 16,
                "Name": "running"
            },
            "OwnerId": "123412341234",
            "Tags": [
                {
                    "Key": "MyTagName",
                    "Value": "my-tag-value"
                }
            ],
            "ImageMetadata": {
                "ImageId": "ami-0b752bf1df193a6c4",
                "Name": "al2023-ami-2023.5.20240819.0-kernel-6.1-x86_64",
                "OwnerId": "137112412989",
                "State": "available",
                "ImageOwnerAlias": "amazon",
                "CreationDate": "2023-01-25T17:20:40Z",
                "DeprecationTime": "2025-01-25T17:20:40Z",
                "IsPublic": true
            }
        }
    ]
}
```


Para obtener más información, consulte Imágenes de máquina de Amazon en Amazon EC2 en la Guía del usuario de Amazon EC2.

Ejemplo 3: descripción de los metadatos de AMI de las instancias basadas en filtros

En el siguiente ejemplo de `describe-instance-image-metadata`, se describen los metadatos de la AMI para instancias `t2.nano` y `t2.micro` en la zona de disponibilidad `us-east-1a`.

```
aws ec2 describe-instance-image-metadata \
    --region us-east-1 \
    --filters Name=availability-zone,Values=us-east-1a Name=instance-
type,Values=t2.nano,t2.micro
```

Salida:

```
{
    "InstanceImageMetadata": [
        {
            "InstanceId": "i-1234567890EXAMPLE",
            "InstanceType": "t2.micro",
            "LaunchTime": "2024-08-28T11:25:45+00:00",
            "AvailabilityZone": "us-east-1a",
            "State": {
                "Code": 16,
                "Name": "running"
            },
            "OwnerId": "123412341234",
            "Tags": [
                {
                    "Key": "MyTagName",
                    "Value": "my-tag-value"
                }
            ],
            "ImageMetadata": {
                "ImageId": "ami-0b752bf1df193a6c4",
                "Name": "al2023-ami-2023.5.20240819.0-kernel-6.1-x86_64",
                "OwnerId": "137112412989",
                "State": "available",
                "ImageOwnerAlias": "amazon",
                "CreationDate": "2023-01-25T17:20:40Z",
                "DeprecationTime": "2025-01-25T17:20:40Z",
                "IsPublic": true
            }
        },
        {
```

```
            "InstanceId": "i-0987654321EXAMPLE",
            "InstanceType": "t2.micro",
            "LaunchTime": "2024-08-28T11:25:45+00:00",
            "AvailabilityZone": "us-east-1a",
            "State": {
                "Code": 16,
                "Name": "running"
            },
            "OwnerId": "123412341234",
            "Tags": [
                {
                    "Key": "MyTagName",
                    "Value": "my-tag-value"
                }
            ],
            "ImageMetadata": {
                "ImageId": "ami-0b752bf1df193a6c4",
                "Name": "al2023-ami-2023.5.20240819.0-kernel-6.1-x86_64",
                "OwnerId": "137112412989",
                "State": "available",
                "ImageOwnerAlias": "amazon",
                "CreationDate": "2023-01-25T17:20:40Z",
                "DeprecationTime": "2025-01-25T17:20:40Z",
                "IsPublic": true
            }
        }
    ],
    "NextToken": "...EXAMPLEV7ixRYHwIAABAA2JHaFxLnDAzpatfEXAMPLE..."
}
```

Para obtener más información, consulte Imágenes de máquina de Amazon en Amazon EC2 en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeInstanceImageMetadata en la Referencia de comandos de la AWS CLI.

`describe-instance-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-status`.

AWS CLI

Describir el estado de las instancias

En el siguiente ejemplo de `describe-instance-status`, se muestran los detalles de la instancia especificada.

```
aws ec2 describe-instance-status \
    --instance-ids i-1234567890abcdef0
```

Salida:

```
{
    "InstanceStatuses": [
        {
            "InstanceId": "i-1234567890abcdef0",
            "InstanceState": {
                "Code": 16,
                "Name": "running"
            },
            "AvailabilityZone": "us-east-1d",
            "SystemStatus": {
                "Status": "ok",
                "Details": [
                    {
                        "Status": "passed",
                        "Name": "reachability"
                    }
                ]
            },
            "InstanceStatus": {
                "Status": "ok",
                "Details": [
                    {
                        "Status": "passed",
                        "Name": "reachability"
                    }
                ]
            }
        }
    ]
}
```

Para obtener más información, consulte Monitorear el estado de las instancias en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeInstanceStatus en la Referencia de comandos de la AWS CLI.

`describe-instance-topology`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-topology`.

AWS CLI

Para describir la topología de todas sus instancias

En el siguiente ejemplo de `describe-instance-topology`, se describe la topología de todas las instancias que coinciden con los tipos de instancias compatibles con este comando.

```
aws ec2 describe-instance-topology \
    --region us-west-2
```

Salida:

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "my-ml-cpg",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
```

```
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1212121212example",
                "nn-1211122211example",
                "nn-1311133311example"
            ],
            "ZoneId": "usw2-az4",
            "AvailabilityZone": "us-west-2d"
        },
        {
            "InstanceId": "i-444444444example",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-5434334334example",
                "nn-1235301234example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Para obtener más información, así como más ejemplos, consulte Topología de instancias de Amazon EC2 en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeInstanceTopology en la Referencia de comandos de la AWS CLI.

`describe-instance-type-offerings`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-type-offerings`.

AWS CLI

Ejemplo 1: enumeración de los tipos de instancias que se ofrecen en una región

En el siguiente ejemplo de `describe-instance-type-offerings`, se enumeran los tipos de instancias que se ofrecen en la región configurada como región predeterminada para la AWS CLI.

```
aws ec2 describe-instance-type-offerings
```

Para enumerar los tipos de instancias que se ofrecen en otra región, especifique la región mediante el parámetro `--region`.

```
aws ec2 describe-instance-type-offerings \
    --region us-east-2
```

Salida:

```
{
  "InstanceTypeOfferings": [
      {
          "InstanceType": "m5.2xlarge",
          "LocationType": "region",
          "Location": "us-east-2"
      },
      {
          "InstanceType": "t3.micro",
          "LocationType": "region",
          "Location": "us-east-2"
      },
      ...
  ]
}
```

Ejemplo 2: enumeración de los tipos de instancias que se ofrecen en una zona de disponibilidad

En el siguiente ejemplo de `describe-instance-type-offerings`, se enumeran los tipos de instancias ofrecidos en la zona de disponibilidad especificada. La zona de disponibilidad debe estar en la región especificada.

```
aws ec2 describe-instance-type-offerings \
    --location-type availability-zone \
    --filters Name=location,Values=us-east-2a \
    --region us-east-2
```

Ejemplo 3: comprobación de si se admite un tipo de instancia

En el siguiente comando de `describe-instance-type-offerings`, se indica si el tipo de instancia `c5.xlarge` se admite en la región especificada.

```
aws ec2 describe-instance-type-offerings \
    --filters Name=instance-type,Values=c5.xlarge \
    --region us-east-2
```

En el siguiente ejemplo de `describe-instance-type-offerings`, se enumeran todos los tipos de instancias C5 que se admiten en la región especificada.

```
aws ec2 describe-instance-type-offerings \
    --filters Name=instance-type,Values=c5* \
    --query "InstanceTypeOfferings[].InstanceType" \
    --region us-east-2
```

Salida:

```
[
    "c5d.12xlarge",
    "c5d.9xlarge",
    "c5n.xlarge",
    "c5.xlarge",
    "c5d.metal",
    "c5n.metal",
    "c5.large",
    "c5d.2xlarge",
    "c5n.4xlarge",
    "c5.2xlarge",
    "c5n.large",
    "c5n.9xlarge",
    "c5d.large",
    "c5.18xlarge",
    "c5d.18xlarge",
    "c5.12xlarge",
    "c5n.18xlarge",
    "c5.metal",
    "c5d.4xlarge",
    "c5.24xlarge",
    "c5d.xlarge",
    "c5n.2xlarge",
    "c5d.24xlarge",
    "c5.9xlarge",
```

```
    "c5.4xlarge"
]
```

- Para obtener información sobre la API, consulte DescribeInstanceTypeOfferings en la Referencia de comandos de la AWS CLI.

`describe-instance-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-types`.

AWS CLI

Ejemplo 1: Describir un tipo de instancia

En el ejemplo siguiente de `describe-instance-types`, se muestran los detalles del tipo de instancia especificado.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro
```

Salida:

```
{
    "InstanceTypes": [
        {
            "InstanceType": "t2.micro",
            "CurrentGeneration": true,
            "FreeTierEligible": true,
            "SupportedUsageClasses": [
                "on-demand",
                "spot"
            ],
            "SupportedRootDeviceTypes": [
                "ebs"
            ],
            "BareMetal": false,
            "Hypervisor": "xen",
            "ProcessorInfo": {
                "SupportedArchitectures": [
                    "i386",
                    "x86_64"
                ],
```

```
                "SustainedClockSpeedInGhz": 2.5
            },
            "VCpuInfo": {
                "DefaultVCpus": 1,
                "DefaultCores": 1,
                "DefaultThreadsPerCore": 1,
                "ValidCores": [
                    1
                ],
                "ValidThreadsPerCore": [
                    1
                ]
            },
            "MemoryInfo": {
                "SizeInMiB": 1024
            },
            "InstanceStorageSupported": false,
            "EbsInfo": {
                "EbsOptimizedSupport": "unsupported",
                "EncryptionSupport": "supported"
            },
            "NetworkInfo": {
                "NetworkPerformance": "Low to Moderate",
                "MaximumNetworkInterfaces": 2,
                "Ipv4AddressesPerInterface": 2,
                "Ipv6AddressesPerInterface": 2,
                "Ipv6Supported": true,
                "EnaSupport": "unsupported"
            },
            "PlacementGroupInfo": {
                "SupportedStrategies": [
                    "partition",
                    "spread"
                ]
            },
            "HibernationSupported": false,
            "BurstablePerformanceSupported": true,
            "DedicatedHostsSupported": false,
            "AutoRecoverySupported": true
        }
    ]
}
```

Para obtener más información, consulte Tipos de instancias en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

Ejemplo 2: Filtrar los tipos de instancias disponibles

Puede especificar un filtro para limitar los resultados a los tipos de instancias que tienen una característica específica. En el siguiente ejemplo de `describe-instance-types`, se enumeran los tipos de instancias que admiten la hibernación.

```
aws ec2 describe-instance-types \
    --filters Name=hibernation-supported,Values=true --query
 'InstanceTypes[*].InstanceType'
```

Salida:

```
[
    "m5.8xlarge",
    "r3.large",
    "c3.8xlarge",
    "r5.large",
    "m4.4xlarge",
    "c4.large",
    "m5.xlarge",
    "m4.xlarge",
    "c3.large",
    "c4.8xlarge",
    "c4.4xlarge",
    "c5.xlarge",
    "c5.12xlarge",
    "r5.4xlarge",
    "c5.4xlarge"
]
```

Para obtener más información, consulte Tipos de instancias en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

- Para obtener información sobre la API, consulte DescribeInstanceTypes en la Referencia de comandos de la AWS CLI.

`describe-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instances`.

AWS CLI

Ejemplo 1: Describir una instancia

En el siguiente ejemplo de `describe-instances`, se describe la instancia especificada.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0
```

Salida:

```
{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-0abcdef1234567890",
                    "InstanceId": "i-1234567890abcdef0",
                    "InstanceType": "t3.nano",
                    "KeyName": "my-key-pair",
                    "LaunchTime": "2022-11-15T10:48:59+00:00",
                    "Monitoring": {
                        "State": "disabled"
                    },
                    "Placement": {
                        "AvailabilityZone": "us-east-2a",
                        "GroupName": "",
                        "Tenancy": "default"
                    },
                    "PrivateDnsName": "ip-10-0-0-157.us-east-2.compute.internal",
                    "PrivateIpAddress": "10-0-0-157",
                    "ProductCodes": [],
                    "PublicDnsName": "ec2-34-253-223-13.us-
east-2.compute.amazonaws.com",
                    "PublicIpAddress": "34.253.223.13",
                    "State": {
                        "Code": 16,
                        "Name": "running"
                    },
                    "StateTransitionReason": "",
                    "SubnetId": "subnet-04a636d18e83cfacb",
```

```
                    "VpcId": "vpc-1234567890abcdef0",
                    "Architecture": "x86_64",
                    "BlockDeviceMappings": [
                        {
                            "DeviceName": "/dev/xvda",
                            "Ebs": {
                                "AttachTime": "2022-11-15T10:49:00+00:00",
                                "DeleteOnTermination": true,
                                "Status": "attached",
                                "VolumeId": "vol-02e6ccdca7de29cf2"
                            }
                        }
                    ],
                    "ClientToken": "1234abcd-1234-abcd-1234-d46a8903e9bc",
                    "EbsOptimized": true,
                    "EnaSupport": true,
                    "Hypervisor": "xen",
                    "IamInstanceProfile": {
                        "Arn": "arn:aws:iam::111111111111:instance-profile/
AmazonSSMRoleForInstancesQuickSetup",
                        "Id": "11111111111111111111"
                    },
                    "NetworkInterfaces": [
                        {
                            "Association": {
                                "IpOwnerId": "amazon",
                                "PublicDnsName": "ec2-34-253-223-13.us-
east-2.compute.amazonaws.com",
                                "PublicIp": "34.253.223.13"
                            },
                            "Attachment": {
                                "AttachTime": "2022-11-15T10:48:59+00:00",
                                "AttachmentId": "eni-attach-1234567890abcdefg",
                                "DeleteOnTermination": true,
                                "DeviceIndex": 0,
                                "Status": "attached",
                                "NetworkCardIndex": 0
                            },
                            "Description": "",
                            "Groups": [
                                {
                                    "GroupName": "launch-wizard-146",
                                    "GroupId": "sg-1234567890abcdefg"
                                }
```

```
                            ],
                            "Ipv6Addresses": [],
                            "MacAddress": "00:11:22:33:44:55",
                            "NetworkInterfaceId": "eni-1234567890abcdefg",
                            "OwnerId": "104024344472",
                            "PrivateDnsName": "ip-10-0-0-157.us-
east-2.compute.internal",
                            "PrivateIpAddress": "10-0-0-157",
                            "PrivateIpAddresses": [
                                {
                                    "Association": {
                                        "IpOwnerId": "amazon",
                                        "PublicDnsName": "ec2-34-253-223-13.us-
east-2.compute.amazonaws.com",
                                        "PublicIp": "34.253.223.13"
                                    },
                                    "Primary": true,
                                    "PrivateDnsName": "ip-10-0-0-157.us-
east-2.compute.internal",
                                    "PrivateIpAddress": "10-0-0-157"
                                }
                            ],
                            "SourceDestCheck": true,
                            "Status": "in-use",
                            "SubnetId": "subnet-1234567890abcdefg",
                            "VpcId": "vpc-1234567890abcdefg",
                            "InterfaceType": "interface"
                        }
                    ],
                    "RootDeviceName": "/dev/xvda",
                    "RootDeviceType": "ebs",
                    "SecurityGroups": [
                        {
                            "GroupName": "launch-wizard-146",
                            "GroupId": "sg-1234567890abcdefg"
                        }
                    ],
                    "SourceDestCheck": true,
                    "Tags": [
                        {
                            "Key": "Name",
                            "Value": "my-instance"
                        }
                    ],
```

```
                    "VirtualizationType": "hvm",
                    "CpuOptions": {
                        "CoreCount": 1,
                        "ThreadsPerCore": 2
                    },
                    "CapacityReservationSpecification": {
                        "CapacityReservationPreference": "open"
                    },
                    "HibernationOptions": {
                        "Configured": false
                    },
                    "MetadataOptions": {
                        "State": "applied",
                        "HttpTokens": "optional",
                        "HttpPutResponseHopLimit": 1,
                        "HttpEndpoint": "enabled",
                        "HttpProtocolIpv6": "disabled",
                        "InstanceMetadataTags": "enabled"
                    },
                    "EnclaveOptions": {
                        "Enabled": false
                    },
                    "PlatformDetails": "Linux/UNIX",
                    "UsageOperation": "RunInstances",
                    "UsageOperationUpdateTime": "2022-11-15T10:48:59+00:00",
                    "PrivateDnsNameOptions": {
                        "HostnameType": "ip-name",
                        "EnableResourceNameDnsARecord": true,
                        "EnableResourceNameDnsAAAARecord": false
                    },
                    "MaintenanceOptions": {
                        "AutoRecovery": "default"
                    }
                }
            ],
            "OwnerId": "111111111111",
            "ReservationId": "r-1234567890abcdefg"
        }
    ]
}
```

Ejemplo 2: Filtrar instancias con el tipo especificado

En el siguiente ejemplo de `describe-instances`, se usan filtros para limitar los resultados a las instancias del tipo especificado.

```
aws ec2 describe-instances \
    --filters Name=instance-type,Values=m5.large
```

Para ver un ejemplo del resultado, consulte el ejemplo 1.

Para obtener más información, consulte Enumerar y filtrar mediante la CLI en la Guía del usuario de Amazon EC2.

Ejemplo 3: filtrar instancias con el tipo y la zona de disponibilidad especificados

En el siguiente ejemplo de `describe-instances`, se usan varios filtros para limitar los resultados a las instancias del tipo especificado que también se encuentran en la zona de disponibilidad especificada.

```
aws ec2 describe-instances \
    --filters Name=instance-type,Values=t2.micro,t3.micro Name=availability-
zone,Values=us-east-2c
```

Para ver un ejemplo del resultado, consulte el ejemplo 1.

Ejemplo 4: filtrar instancias con el tipo y la zona de disponibilidad especificados mediante un archivo JSON

En el siguiente ejemplo de `describe-instances`, se usa un archivo de entrada JSON para realizar el mismo filtrado que en el ejemplo anterior. Cuando los filtros se vuelven más complicados, es más fácil especificarlos en un archivo JSON.

```
aws ec2 describe-instances \
    --filters file://filters.json
```

Contenido de `filters.json`:

```
[
    {
        "Name": "instance-type",
        "Values": ["t2.micro", "t3.micro"]
    },
```

```
    {
        "Name": "availability-zone",
        "Values": ["us-east-2c"]
    }
]
```

Para ver un ejemplo del resultado, consulte el ejemplo 1.

Ejemplo 5: filtrar instancias con la etiqueta de propietario especificada

En el siguiente ejemplo de `describe-instances`, se usan filtros de etiquetas para limitar los resultados a las instancias que tienen una etiqueta con la clave de etiqueta especificada (propietario), independientemente del valor de la etiqueta.

```
aws ec2 describe-instances \
    --filters "Name=tag-key,Values=Owner"
```

Para ver un ejemplo del resultado, consulte el ejemplo 1.

Ejemplo 6: filtrar las instancias con el valor de etiqueta de mi equipo especificado

En el siguiente ejemplo de `describe-instances`, se usan filtros de etiquetas para limitar los resultados a las instancias que tienen una etiqueta con el valor de etiqueta especificado (mi equipo), independientemente de la clave de la etiqueta.

```
aws ec2 describe-instances \
    --filters "Name=tag-value,Values=my-team"
```

Para ver un ejemplo del resultado, consulte el ejemplo 1.

Ejemplo 7: filtrar las instancias con la etiqueta de propietario y el valor de mi equipo especificados

En el siguiente ejemplo de `describe-instances`, se usan filtros de etiquetas para limitar los resultados a las instancias que tienen la etiqueta especificada (propietario = mi equipo).

```
aws ec2 describe-instances \
    --filters "Name=tag:Owner,Values=my-team"
```

Para ver un ejemplo del resultado, consulte el ejemplo 1.

Ejemplo 8: mostrar solo los ID de instancia y subred de todas las instancias

En los siguientes ejemplos de `describe-instances`, se usa el parámetro `--query` para mostrar solo los ID de instancia y subred de todas las instancias, en formato JSON.

Linux y macOS:

```
aws ec2 describe-instances \
    --query 'Reservations[*].Instances[*].{Instance:InstanceId,Subnet:SubnetId}' \
    --output json
```

Windows:

```
aws ec2 describe-instances ^
    --query "Reservations[*].Instances[*].{Instance:InstanceId,Subnet:SubnetId}" ^
    --output json
```

Salida:

```
[
    {
        "Instance": "i-057750d42936e468a",
        "Subnet": "subnet-069beee9b12030077"
    },
    {
        "Instance": "i-001efd250faaa6ffa",
        "Subnet": "subnet-0b715c6b7db68927a"
    },
    {
        "Instance": "i-027552a73f021f3bd",
        "Subnet": "subnet-0250c25a1f4e15235"
    }
    ...
]
```

Ejemplo 9: filtrar instancias del tipo especificado y mostrar solo sus ID de instancia

En el siguiente ejemplo de `describe-instances`, se usan filtros para limitar los resultados a las instancias del tipo especificado y el parámetro `--query` para mostrar solo los ID de las instancias.

```
aws ec2 describe-instances \
    --filters "Name=instance-type,Values=t2.micro" \
```

```
    --query "Reservations[*].Instances[*].[InstanceId]" \
    --output text
```

Salida:

```
i-031c0dc19de2fb70c
i-00d8bff789a736b75
i-0b715c6b7db68927a
i-0626d4edd54f1286d
i-00b8ae04f9f99908e
i-0fc71c25d2374130c
```

Ejemplo 10: filtrar instancias del tipo especificado y mostrar solo sus ID de instancia, la zona de disponibilidad y el valor de etiqueta especificado

En los siguientes ejemplos de `describe-instances`, se muestran el ID de la instancia, la zona de disponibilidad y el valor de la etiqueta Name para las instancias que tienen una etiqueta con el nombre `tag-key`, en formato de tabla.

Linux y macOS:

```
aws ec2 describe-instances \
    --filters Name=tag-key,Values=Name \
    --query 'Reservations[*].Instances[*].
{Instance:InstanceId,AZ:Placement.AvailabilityZone,Name:Tags[?Key==`Name`]|
[0].Value}' \
    --output table
```

Windows:

```
aws ec2 describe-instances ^
    --filters Name=tag-key,Values=Name ^
    --query "Reservations[*].Instances[*].
{Instance:InstanceId,AZ:Placement.AvailabilityZone,Name:Tags[?Key=='Name']|
[0].Value}" ^
    --output table
```

Salida:

```
-------------------------------------------------------------
|                    DescribeInstances                      |
```

```
+--------------+-----------------------+--------------------+
|      AZ      |       Instance        |        Name        |
+--------------+-----------------------+--------------------+
|  us-east-2b  |  i-057750d42936e468a  |  my-prod-server    |
|  us-east-2a  |  i-001efd250faaa6ffa  |  test-server-1     |
|  us-east-2a  |  i-027552a73f021f3bd  |  test-server-2     |
+--------------+-----------------------+--------------------+
```

Ejemplo 11: describir las instancias de un grupo con ubicación en particiones

En el siguiente ejemplo de `describe-instances`, se describe la instancia especificada. El resultado incluye la información de ubicación de la instancia, la cual contiene el nombre del grupo de ubicación y el número de partición de la instancia.

```
aws ec2 describe-instances \
    --instance-ids i-0123a456700123456 \
    --query "Reservations[*].Instances[*].Placement"
```

Salida:

```
[
    [
        {
            "AvailabilityZone": "us-east-1c",
            "GroupName": "HDFS-Group-A",
            "PartitionNumber": 3,
            "Tenancy": "default"
        }

    ]
]
```

Para obtener más información, consulte Descripción de instancias en un grupo con ubicación en la Guía del usuario de Amazon EC2.

Ejemplo 12: filtrar las instancias con el grupo con ubicación y el número de partición especificados

En el siguiente ejemplo de `describe-instances` se filtran los resultados solo para las instancias con el grupo de ubicación y el número de partición especificados.

```
aws ec2 describe-instances \
```

```
    --filters "Name=placement-group-name,Values=HDFS-Group-A" "Name=placement-
partition-number,Values=7"
```

A continuación, se muestra solo la información relevante de la salida.

```
"Instances": [
    {
        "InstanceId": "i-0123a456700123456",
        "InstanceType": "r4.large",
        "Placement": {
            "AvailabilityZone": "us-east-1c",
            "GroupName": "HDFS-Group-A",
            "PartitionNumber": 7,
            "Tenancy": "default"
        }
    },
    {
        "InstanceId": "i-9876a543210987654",
        "InstanceType": "r4.large",
        "Placement": {
            "AvailabilityZone": "us-east-1c",
            "GroupName": "HDFS-Group-A",
            "PartitionNumber": 7,
            "Tenancy": "default"
        }
    ],
```

Para obtener más información, consulte Describing instances in a placement group en la Guía del usuario de Amazon EC2.

Ejemplo 13: filtrar las instancias que están configuradas para permitir el acceso a las etiquetas desde los metadatos de la instancia

En el siguiente ejemplo de `describe-instances`, se filtran los resultados solo para las instancias que están configuradas para permitir el acceso a las etiquetas de la instancia desde los metadatos de la instancia.

```
aws ec2 describe-instances \
    --filters "Name=metadata-options.instance-metadata-tags,Values=enabled" \
    --query "Reservations[*].Instances[*].InstanceId" \
    --output text
```

El resultado esperado es el siguiente.

```
i-1234567890abcdefg
i-abcdefg1234567890
i-11111111aaaaaaaaa
i-aaaaaaaa111111111
```

Para obtener más información, consulte Trabajo con etiquetas de instancia en los metadatos de la instancia en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeInstances en la Referencia de comandos de la AWS CLI.

`describe-internet-gateways`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-internet-gateways`.

AWS CLI

Para describir una puerta de enlace de Internet

En el siguiente ejemplo de `describe-internet-gateways`, se describe la puerta de enlace de Internet especificada.

```
aws ec2 describe-internet-gateways \
    --internet-gateway-ids igw-0d0fb496b3EXAMPLE
```

Salida:

```
{
    "InternetGateways": [
        {
            "Attachments": [
                {
                    "State": "available",
                    "VpcId": "vpc-0a60eb65b4EXAMPLE"
                }
            ],
            "InternetGatewayId": "igw-0d0fb496b3EXAMPLE",
            "OwnerId": "123456789012",
            "Tags": [
                {
```

```
                    "Key": "Name",
                    "Value": "my-igw"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Puertas de enlace de Internet en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte DescribeInternetGateways en la Referencia de comandos de la AWS CLI.

`describe-ipam-pools`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-ipam-pools`.

AWS CLI

Para ver los detalles de un grupo de IPAM

En el siguiente ejemplo de `describe-ipam-pools` se muestra la información de los grupos.

(Linux):

```
aws ec2 describe-ipam-pools \
    --filters Name=owner-id,Values=123456789012 Name=ipam-scope-id,Values=ipam-scope-02fc38cd4c48e7d38
```

(Windows):

```
aws ec2 describe-ipam-pools ^
    --filters Name=owner-id,Values=123456789012 Name=ipam-scope-id,Values=ipam-scope-02fc38cd4c48e7d38
```

Salida:

```
{
    "IpamPools": [
        {
            "OwnerId": "123456789012",
```

```
            "IpamPoolId": "ipam-pool-02ec043a19bbe5d08",
            "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-02ec043a19bbe5d08",
            "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-02fc38cd4c48e7d38",
            "IpamScopeType": "private",
            "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-08440e7a3acde3908",
            "IpamRegion": "us-east-1",
            "Locale": "None",
            "PoolDepth": 1,
            "State": "create-complete",
            "AutoImport": true,
            "AddressFamily": "ipv4",
            "AllocationMinNetmaskLength": 16,
            "AllocationMaxNetmaskLength": 26,
            "AllocationDefaultNetmaskLength": 24,
            "AllocationResourceTags": [
                {
                    "Key": "Environment",
                    "Value": "Preprod"
                }
            ],
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Preprod pool"
                }
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeIpamPools en la Referencia de comandos de la AWS CLI.

`describe-ipam-resource-discoveries`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-ipam-resource-discoveries`.

AWS CLI

Ejemplo 1: visualización de los detalles completos de las detecciones de recursos

En este ejemplo, usted es un administrador delegado de IPAM y desea crear y compartir una detección de recursos con el administrador de IPAM de otra organización de AWS para que el otro administrador pueda administrar y supervisar las direcciones IP de esos recursos de su organización.

Este ejemplo puede resultar útil si:

Ha intentado crear una detección de recursos, pero aparece un error que indica que ha alcanzado el límite de 1. Se ha dado cuenta de que es posible que ya haya creado una detección de recursos y desea verla en su cuenta. Tiene recursos en una región en la que el IPAM no los detecta. Desea ver las `--operating-regions` definidas para el recurso y asegurarse de haber agregado la región correcta como región operativa para poder detectar los recursos que contiene.

En el siguiente ejemplo de `describe-ipam-resource-discoveries` se enumeran los detalles de la detección de recursos de su cuenta de AWS. Puede realizar una detección de recursos por región de AWS.

```
aws ec2 describe-ipam-resource-discoveries \
    --region us-east-1
```

Salida:

```
{
    "IpamResourceDiscoveries": [
        {
            "OwnerId": "149977607591",
            "IpamResourceDiscoveryId": "ipam-res-disco-0f8bdee9067137c0d",
            "IpamResourceDiscoveryArn": "arn:aws:ec2::149977607591:ipam-resource-
discovery/ipam-res-disco-0f8bdee9067137c0d",
            "IpamResourceDiscoveryRegion": "us-east-1",
            "OperatingRegions": [
                {
                    "RegionName": "us-east-1"
                }
            ],
            "IsDefault": false,
            "State": "create-complete",
            "Tags": []
    }
]
}
```

Para obtener más información, consulte Integración de IPAM con cuentas ajenas a su organización en la Guía del usuario de Amazon VPC IPAM.

Ejemplo 2: visualización de los ID de las detecciones de recursos únicamente

En el siguiente ejemplo de `describe-ipam-resource-discoveries` se enumera el ID de la detección de recursos de su cuenta de AWS. Puede realizar una detección de recursos por región de AWS.

```
aws ec2 describe-ipam-resource-discoveries \
    --query "IpamResourceDiscoveries[*].IpamResourceDiscoveryId" \
    --output text
```

Salida:

```
ipam-res-disco-0481e39b242860333
```

Para obtener más información, consulte Integración de IPAM con cuentas ajenas a su organización en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte DescribeIpamResourceDiscoveries en la Referencia de comandos de la AWS CLI.

`describe-ipam-resource-discovery-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-ipam-resource-discovery-associations`.

AWS CLI

Para ver todas las asociaciones de detecciones de recursos con su IPAM

En este ejemplo, usted es un administrador delegado de IPAM que ha asociado detecciones de recursos a su IPAM para integrar otras cuentas con su IPAM. Se ha dado cuenta de que su IPAM no detecta según lo previsto recursos en las regiones operativas de la detección de recursos. Desea comprobar el estado y la situación de la detección de recursos para asegurarse de que la cuenta que la creó sigue activa y de que la detección de recursos se sigue compartiendo.

El valor de `--region` debe ser la región de origen de su IPAM.

En el siguiente ejemplo de `describe-ipam-resource-discovery-associations` se enumeran las asociaciones de la detección de recursos de su cuenta de AWS.

```
aws ec2 describe-ipam-resource-discovery-associations \
    --region us-east-1
```

Salida:

```
{
    "IpamResourceDiscoveryAssociations": [
        {
            "OwnerId": "320805250157",
            "IpamResourceDiscoveryAssociationId": "ipam-res-disco-
assoc-05e6b45eca5bf5cf7",
            "IpamResourceDiscoveryAssociationArn": "arn:aws:ec2::320805250157:ipam-
resource-discovery-association/ipam-res-disco-assoc-05e6b45eca5bf5cf7",
            "IpamResourceDiscoveryId": "ipam-res-disco-0f4ef577a9f37a162",
            "IpamId": "ipam-005f921c17ebd5107",
            "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-005f921c17ebd5107",
            "IpamRegion": "us-east-1",
            "IsDefault": true,
            "ResourceDiscoveryStatus": "active",
            "State": "associate-complete",
            "Tags": []
        },
        {
            "OwnerId": "149977607591",
            "IpamResourceDiscoveryAssociationId": "ipam-res-disco-
assoc-0dfd21ae189ab5f62",
            "IpamResourceDiscoveryAssociationArn": "arn:aws:ec2::149977607591:ipam-
resource-discovery-association/ipam-res-disco-assoc-0dfd21ae189ab5f62",
            "IpamResourceDiscoveryId": "ipam-res-disco-0365d2977fc1672fe",
            "IpamId": "ipam-005f921c17ebd5107",
            "IpamArn": "arn:aws:ec2::149977607591:ipam/ipam-005f921c17ebd5107",
            "IpamRegion": "us-east-1",
            "IsDefault": false,
            "ResourceDiscoveryStatus": "active",
            "State": "create-complete",
            "Tags": []
        }
    ]
}
```

En este ejemplo, después de ejecutar este comando, se observa que hay una detección de recursos no predeterminada (`"IsDefault": false ``) that is ``"ResourceDiscoveryStatus": "not-found"` y `"State": "create-complete"`). Se ha cerrado la cuenta del propietario de la detección de recursos. Si, en otro caso, observa que es `"ResourceDiscoveryStatus": "not-found"` y `"State": "associate-complete"`, esto indica que ha ocurrido una de las siguientes situaciones:

El propietario de la detección de recursos ha eliminado la detección de recursos. El propietario de la detección de recursos ha dejado de compartir la detección de recursos.

Para obtener más información, consulte Integración de IPAM con cuentas ajenas a su organización en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte DescribeIpamResourceDiscoveryAssociations en la Referencia de comandos de la AWS CLI.

`describe-ipam-scopes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-ipam-scopes`.

AWS CLI

Para ver los detalles de un ámbito de IPAM

En el siguiente ejemplo de `describe-ipam-scopes` se muestra la información de los ámbitos.

```
aws ec2 describe-ipam-scopes \
    --filters Name=owner-id,Values=123456789012 Name=ipam-
id,Values=ipam-08440e7a3acde3908
```

Salida:

```
{
    "IpamScopes": [
        {
            "OwnerId": "123456789012",
            "IpamScopeId": "ipam-scope-02fc38cd4c48e7d38",
            "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-02fc38cd4c48e7d38",
            "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-08440e7a3acde3908",
            "IpamRegion": "us-east-1",
```

```
            "IpamScopeType": "private",
            "IsDefault": true,
            "PoolCount": 2,
            "State": "create-complete",
            "Tags": []
        },
        {
            "OwnerId": "123456789012",
            "IpamScopeId": "ipam-scope-0b9eed026396dbc16",
            "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0b9eed026396dbc16",
            "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-08440e7a3acde3908",
            "IpamRegion": "us-east-1",
            "IpamScopeType": "public",
            "IsDefault": true,
            "PoolCount": 0,
            "State": "create-complete",
            "Tags": []
        },
        {
            "OwnerId": "123456789012",
            "IpamScopeId": "ipam-scope-0f1aff29486355c22",
            "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0f1aff29486355c22",
            "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-08440e7a3acde3908",
            "IpamRegion": "us-east-1",
            "IpamScopeType": "private",
            "IsDefault": false,
            "Description": "Example description",
            "PoolCount": 0,
            "State": "create-complete",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Example name value"
                }
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeIpamScopes en la Referencia de comandos de la AWS CLI.

`describe-ipams`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-ipams`.

AWS CLI

Para ver los detalles de un IPAM

En el siguiente ejemplo de `describe-ipams`, se muestra la información de un IPAM.

```
aws ec2 describe-ipams \
    --filters Name=owner-id,Values=123456789012
```

Salida:

```
{
    "Ipams": [
        {
            "OwnerId": "123456789012",
            "IpamId": "ipam-08440e7a3acde3908",
            "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-08440e7a3acde3908",
            "IpamRegion": "us-east-1",
            "PublicDefaultScopeId": "ipam-scope-0b9eed026396dbc16",
            "PrivateDefaultScopeId": "ipam-scope-02fc38cd4c48e7d38",
            "ScopeCount": 3,
            "OperatingRegions": [
                {
                    "RegionName": "us-east-1"
                },
                {
                    "RegionName": "us-east-2"
                },
                {
                    "RegionName": "us-west-1"
                }
            ],
            "State": "create-complete",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "ExampleIPAM"
                }
            ]
        }
```

```
    ]
}
```

- Para obtener información sobre la API, consulte DescribeIpams en la Referencia de comandos de la AWS CLI.

`describe-ipv6-pools`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-ipv6-pools`.

AWS CLI

Para describir sus grupos de direcciones IPv

En el siguiente ejemplo de `describe-ipv6-pools`, se muestra la información de todos los grupos de direcciones IPv6.

```
aws ec2 describe-ipv6-pools
```

Salida:

```
{
    "Ipv6Pools": [
        {
            "PoolId": "ipv6pool-ec2-012345abc12345abc",
            "PoolCidrBlocks": [
                {
                    "Cidr": "2001:db8:123::/48"
                }
            ],
            "Tags": [
                {
                    "Key": "pool-1",
                    "Value": "public"
                }
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeIpv6Pools en la Referencia de comandos de la AWS CLI.

describe-key-pairs

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-key-pairs`.

AWS CLI

Mostrar un par de claves

En el siguiente ejemplo de `describe-key-pairs`, se muestra información sobre el par de claves especificado.

```
aws ec2 describe-key-pairs \
    --key-names my-key-pair
```

Salida:

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0b94643da6EXAMPLE",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "my-key-pair",
            "KeyType": "rsa",
            "Tags": [],
            "CreateTime": "2022-05-27T21:51:16.000Z"
        }
    ]
}
```

Para obtener más información, consulte Describir las claves públicas en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeKeyPairs en la Referencia de comandos de la AWS CLI.

describe-launch-template-versions

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-launch-template-versions`.

AWS CLI

Para describir las versiones de la plantilla de lanzamiento

En este ejemplo, se describen las versiones de la plantilla de lanzamiento especificada.

Comando:

```
aws ec2 describe-launch-template-versions --launch-template-id lt-068f72b72934aff71
```

Salida:

```
{
  "LaunchTemplateVersions": [
      {
          "LaunchTemplateId": "lt-068f72b72934aff71",
          "LaunchTemplateName": "Webservers",
          "VersionNumber": 3,
          "CreatedBy": "arn:aws:iam::123456789102:root",
          "LaunchTemplateData": {
              "KeyName": "kp-us-east",
              "ImageId": "ami-6057e21a",
              "InstanceType": "t2.small",
              "NetworkInterfaces": [
                  {
                      "SubnetId": "subnet-7b16de0c",
                      "DeviceIndex": 0,
                      "Groups": [
                          "sg-7c227019"
                      ]
                  }
              ]
          },
          "DefaultVersion": false,
          "CreateTime": "2017-11-20T13:19:54.000Z"
      },
      {
          "LaunchTemplateId": "lt-068f72b72934aff71",
          "LaunchTemplateName": "Webservers",
          "VersionNumber": 2,
          "CreatedBy": "arn:aws:iam::123456789102:root",
          "LaunchTemplateData": {
              "KeyName": "kp-us-east",
              "ImageId": "ami-6057e21a",
```

```
            "InstanceType": "t2.medium",
            "NetworkInterfaces": [
                {
                    "SubnetId": "subnet-1a2b3c4d",
                    "DeviceIndex": 0,
                    "Groups": [
                        "sg-7c227019"
                    ]
                }
            ]
        },
        "DefaultVersion": false,
        "CreateTime": "2017-11-20T13:12:32.000Z"
    },
    {
        "LaunchTemplateId": "lt-068f72b72934aff71",
        "LaunchTemplateName": "Webservers",
        "VersionNumber": 1,
        "CreatedBy": "arn:aws:iam::123456789102:root",
        "LaunchTemplateData": {
            "UserData": "",
            "KeyName": "kp-us-east",
            "ImageId": "ami-aabbcc11",
            "InstanceType": "t2.medium",
            "NetworkInterfaces": [
                {
                    "SubnetId": "subnet-7b16de0c",
                    "DeviceIndex": 0,
                    "DeleteOnTermination": false,
                    "Groups": [
                        "sg-7c227019"
                    ],
                    "AssociatePublicIpAddress": true
                }
            ]
        },
        "DefaultVersion": true,
        "CreateTime": "2017-11-20T12:52:33.000Z"
    }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeLaunchTemplateVersions en la Referencia de comandos de la AWS CLI.

`describe-launch-templates`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-launch-templates`.

AWS CLI

Para describir las plantillas de lanzamiento

En este ejemplo, se describen las plantillas de lanzamiento.

Comando:

```
aws ec2 describe-launch-templates
```

Salida:

```
{
  "LaunchTemplates": [
      {
          "LatestVersionNumber": 2,
          "LaunchTemplateId": "lt-0e06d290751193123",
          "LaunchTemplateName": "TemplateForWebServer",
          "DefaultVersionNumber": 2,
          "CreatedBy": "arn:aws:iam::123456789012:root",
          "CreateTime": "2017-11-27T09:30:23.000Z"
      },
      {
          "LatestVersionNumber": 6,
          "LaunchTemplateId": "lt-0c45b5e061ec98456",
          "LaunchTemplateName": "DBServersTemplate",
          "DefaultVersionNumber": 1,
          "CreatedBy": "arn:aws:iam::123456789012:root",
          "CreateTime": "2017-11-20T09:25:22.000Z"
      },
      {
          "LatestVersionNumber": 1,
          "LaunchTemplateId": "lt-0d47d774e8e52dabc",
          "LaunchTemplateName": "MyLaunchTemplate2",
          "DefaultVersionNumber": 1,
```

```
            "CreatedBy": "arn:aws:iam::123456789012:root",
            "CreateTime": "2017-11-02T12:06:21.000Z"
        },
        {
            "LatestVersionNumber": 3,
            "LaunchTemplateId": "lt-01e5f948eb4f589d6",
            "LaunchTemplateName": "testingtemplate2",
            "DefaultVersionNumber": 1,
            "CreatedBy": "arn:aws:sts::123456789012:assumed-role/AdminRole/
i-03ee35176e2e5aabc",
            "CreateTime": "2017-12-01T08:19:48.000Z"
        },
    ]
}
```

- Para obtener información sobre la API, consulte DescribeLaunchTemplates en la Referencia de comandos de la AWS CLI.

`describe-local-gateway-route-table-virtual-interface-group-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-local-gateway-route-table-virtual-interface-group-associations`.

AWS CLI

Para describir las asociaciones entre grupos de interfaces virtuales y tablas de enrutamiento de puerta de enlace local

En el siguiente ejemplo de `describe-local-gateway-route-table-virtual-interface-group-associations`, se describen las asociaciones entre los grupos de interfaces virtuales y las tablas de enrutamiento de las puertas de enlace locales de su cuenta de AWS.

```
aws ec2 describe-local-gateway-route-table-virtual-interface-group-associations
```

Salida:

```
{
    "LocalGatewayRouteTableVirtualInterfaceGroupAssociations": [
        {
```

```
            "LocalGatewayRouteTableVirtualInterfaceGroupAssociationId": "lgw-vif-
grp-assoc-07145b276bEXAMPLE",
            "LocalGatewayVirtualInterfaceGroupId": "lgw-vif-grp-07145b276bEXAMPLE",
            "LocalGatewayId": "lgw-0ab1c23d4eEXAMPLE",
            "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
            "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:123456789012:local-
gateway-route-table/lgw-rtb-059615ef7dEXAMPLE",
            "OwnerId": "123456789012",
            "State": "associated",
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Working with local gateways en la Guía del usuario de AWS Outposts.

- Para obtener información sobre la API, consulte DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations en la Referencia de comandos de la AWS CLI.

`describe-local-gateway-route-table-vpc-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-local-gateway-route-table-vpc-associations`.

AWS CLI

Para describir las asociaciones entre las VPC y las tablas de enrutamiento de puerta de enlace local

En el siguiente ejemplo de `describe-local-gateway-route-table-vpc-associations` se muestra información sobre la asociación especificada entre las VPC y las tablas de enrutamiento de puerta de enlace local.

```
aws ec2 describe-local-gateway-route-table-vpc-associations \
    --local-gateway-route-table-vpc-association-ids lgw-vpc-assoc-0e0f27af15EXAMPLE
```

Salida:

```
{
```

```
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0e0f27af1EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-0efe9bde08EXAMPLE",
        "State": "associated"
    }
}
```

Para obtener más información, consulte Tablas de enrutamiento de puertas de enlace locales en la Guía del usuario de Outposts.

- Para obtener información sobre la API, consulte DescribeLocalGatewayRouteTableVpcAssociations en la Referencia de comandos de la AWS CLI.

`describe-local-gateway-route-tables`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-local-gateway-route-tables`.

AWS CLI

Para describir las tablas de enrutamiento de puerta de enlace local

En el siguiente ejemplo de `describe-local-gateway-route-tables` se muestra la información sobre las tablas de enrutamiento de puerta de enlace local.

```
aws ec2 describe-local-gateway-route-tables
```

Salida:

```
{
    "LocalGatewayRouteTables": [
        {
            "LocalGatewayRouteTableId": "lgw-rtb-059615ef7deEXAMPLE",
            "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
            "OutpostArn": "arn:aws:outposts:us-west-2:111122223333:outpost/
op-0dc11b66edEXAMPLE",
            "State": "available"
        }
    ]
```

```
}
```

- Para obtener información sobre la API, consulte DescribeLocalGatewayRouteTables en la Referencia de comandos de la AWS CLI.

`describe-local-gateway-virtual-interface-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-local-gateway-virtual-interface-groups`.

AWS CLI

Para describir grupos de interfaces virtuales de puerta de enlace local

En el siguiente ejemplo de `describe-local-gateway-virtual-interface-groups` se describen los grupos de interfaces virtuales de puerta de enlace local de su cuenta de AWS.

```
aws ec2 describe-local-gateway-virtual-interface-groups
```

Salida:

```
{
    "LocalGatewayVirtualInterfaceGroups": [
        {
            "LocalGatewayVirtualInterfaceGroupId": "lgw-vif-grp-07145b276bEXAMPLE",
            "LocalGatewayVirtualInterfaceIds": [
                "lgw-vif-01a23bc4d5EXAMPLE",
                "lgw-vif-543ab21012EXAMPLE"
            ],
            "LocalGatewayId": "lgw-0ab1c23d4eEXAMPLE",
            "OwnerId": "123456789012",
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Working with local gateways en la Guía del usuario de AWS Outposts.

- Para obtener información sobre la API, consulte DescribeLocalGatewayVirtualInterfaceGroups en la Referencia de comandos de la AWS CLI.

describe-local-gateway-virtual-interfaces

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-local-gateway-virtual-interfaces`.

AWS CLI

Para describir interfaces virtuales de puerta de enlace local

En el siguiente ejemplo de `describe-local-gateway-virtual-interfaces` se describen las interfaces virtuales de puerta de enlace local de su cuenta de AWS.

```
aws ec2 describe-local-gateway-virtual-interfaces
```

Salida:

```
{
    "LocalGatewayVirtualInterfaces": [
        {
            "LocalGatewayVirtualInterfaceId": "lgw-vif-01a23bc4d5EXAMPLE",
            "LocalGatewayId": "lgw-0ab1c23d4eEXAMPLE",
            "Vlan": 2410,
            "LocalAddress": "0.0.0.0/0",
            "PeerAddress": "0.0.0.0/0",
            "LocalBgpAsn": 65010,
            "PeerBgpAsn": 65000,
            "OwnerId": "123456789012",
            "Tags": []
        },
        {
            "LocalGatewayVirtualInterfaceId": "lgw-vif-543ab21012EXAMPLE",
            "LocalGatewayId": "lgw-0ab1c23d4eEXAMPLE",
            "Vlan": 2410,
            "LocalAddress": "0.0.0.0/0",
            "PeerAddress": "0.0.0.0/0",
            "LocalBgpAsn": 65010,
            "PeerBgpAsn": 65000,
            "OwnerId": "123456789012",
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Working with local gateways en la Guía del usuario de AWS Outposts.

- Para obtener información sobre la API, consulte DescribeLocalGatewayVirtualInterfaces en la Referencia de comandos de la AWS CLI.

`describe-local-gateways`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-local-gateways`.

AWS CLI

Para describir sus puertas de enlace locales

En el siguiente ejemplo de `describe-local-gateways` se muestra la información de las puertas de enlace locales que están disponibles para usted.

```
aws ec2 describe-local-gateways
```

Salida:

```
{
    "LocalGateways": [
        {
            "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
            "OutpostArn": "arn:aws:outposts:us-west-2:123456789012:outpost/
op-0dc11b66ed59f995a",
            "OwnerId": "123456789012",
            "State": "available"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeLocalGateways en la Referencia de comandos de la AWS CLI.

`describe-locked-snapshots`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-locked-snapshots`.

AWS CLI

Para describir el estado de bloqueo de una instantánea

En el siguiente ejemplo de `describe-locked-snapshots` se describe el estado de bloqueo de la instantánea especificada.

```
aws ec2 describe-locked-snapshots \
    --snapshot-ids snap-0b5e733b4a8df6e0d
```

Salida:

```
{
    "Snapshots": [
        {
            "OwnerId": "123456789012",
            "SnapshotId": "snap-0b5e733b4a8df6e0d",
            "LockState": "governance",
            "LockDuration": 365,
            "LockCreatedOn": "2024-05-05T00:56:06.208000+00:00",
            "LockDurationStartTime": "2024-05-05T00:56:06.208000+00:00",
            "LockExpiresOn": "2025-05-05T00:56:06.208000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Snapshot lock en la Guía del usuario de Amazon EBS.

- Para obtener información sobre la API, consulte DescribeLockedSnapshots en la Referencia de comandos de la AWS CLI.

`describe-managed-prefix-lists`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-managed-prefix-lists`.

AWS CLI

Para describir listas de prefijos administrados

En el siguiente ejemplo de `describe-managed-prefix-lists` se describen las listas de prefijos propiedad de la cuenta de AWS `123456789012`.

```
aws ec2 describe-managed-prefix-lists \
```

```
    --filters Name=owner-id,Values=123456789012
```

Salida:

```
{
    "PrefixLists": [
        {
            "PrefixListId": "pl-11223344556677aab",
            "AddressFamily": "IPv6",
            "State": "create-complete",
            "PrefixListArn": "arn:aws:ec2:us-west-2:123456789012:prefix-list/
pl-11223344556677aab",
            "PrefixListName": "vpc-ipv6-cidrs",
            "MaxEntries": 25,
            "Version": 1,
            "Tags": [],
            "OwnerId": "123456789012"
        },
        {
            "PrefixListId": "pl-0123456abcabcabc1",
            "AddressFamily": "IPv4",
            "State": "active",
            "PrefixListArn": "arn:aws:ec2:us-west-2:123456789012:prefix-list/
pl-0123456abcabcabc1",
            "PrefixListName": "vpc-cidrs",
            "MaxEntries": 10,
            "Version": 1,
            "Tags": [],
            "OwnerId": "123456789012"
      }
  ]
}
```

Para obtener más información, consulte Managed prefix lists en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte DescribeManagedPrefixLists en la Referencia de comandos de la AWS CLI.

`describe-moving-addresses`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-moving-addresses`.

AWS CLI

Para describir sus direcciones en movimiento

En este ejemplo, se describen todas sus direcciones IP elásticas en movimiento.

Comando:

```
aws ec2 describe-moving-addresses
```

Salida:

```
{
  "MovingAddressStatuses": [
    {
      "PublicIp": "198.51.100.0",
      "MoveStatus": "MovingToVpc"
    }
  ]
}
```

En este ejemplo, se describen todas las direcciones que se están moviendo a la plataforma EC2-VPC.

Comando:

```
aws ec2 describe-moving-addresses --filters Name=moving-status,Values=MovingToVpc
```

- Para obtener información sobre la API, consulte DescribeMovingAddresses en la Referencia de comandos de la AWS CLI.

`describe-nat-gateways`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-nat-gateways`.

AWS CLI

Ejemplo 1: descripción de una puerta de enlace de NAT pública

En el siguiente ejemplo de `describe-nat-gateways` se describe la puerta de enlace de NAT pública especificada.

```
aws ec2 describe-nat-gateways \
    --nat-gateway-id nat-01234567890abcdef
```

Salida:


```
{
    "NatGateways": [
        {
            "CreateTime": "2023-08-25T01:56:51.000Z",
            "NatGatewayAddresses": [
                {
                    "AllocationId": "eipalloc-0790180cd2EXAMPLE",
                    "NetworkInterfaceId": "eni-09cc4b2558794f7f9",
                    "PrivateIp": "10.0.0.211",
                    "PublicIp": "54.85.121.213",
                    "AssociationId": "eipassoc-04d295cc9b8815b24",
                    "IsPrimary": true,
                    "Status": "succeeded"
                },
                {
                    "AllocationId": "eipalloc-0be6ecac95EXAMPLE",
                    "NetworkInterfaceId": "eni-09cc4b2558794f7f9",
                    "PrivateIp": "10.0.0.74",
                    "PublicIp": "3.211.231.218",
                    "AssociationId": "eipassoc-0f96bdca17EXAMPLE",
                    "IsPrimary": false,
                    "Status": "succeeded"
                }
            ],
            "NatGatewayId": "nat-01234567890abcdef",
            "State": "available",
            "SubnetId": "subnet-655eab5f08EXAMPLE",
            "VpcId": "vpc-098eb5ef58EXAMPLE",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "public-nat"
                }
            ],
            "ConnectivityType": "public"
        }
    ]
```

```
}
```

Ejemplo 2: descripción de una puerta de enlace de NAT privada

En el siguiente ejemplo de `describe-nat-gateways` se describe la puerta de enlace de NAT privada especificada.

```
aws ec2 describe-nat-gateways \
    --nat-gateway-id nat-1234567890abcdef0
```

Salida:

```
{
    "NatGateways": [
        {
            "CreateTime": "2023-08-25T00:50:05.000Z",
            "NatGatewayAddresses": [
                {
                    "NetworkInterfaceId": "eni-0065a61b324d1897a",
                    "PrivateIp": "10.0.20.240",
                    "IsPrimary": true,
                    "Status": "succeeded"
                },
                {
                    "NetworkInterfaceId": "eni-0065a61b324d1897a",
                    "PrivateIp": "10.0.20.33",
                    "IsPrimary": false,
                    "Status": "succeeded"
                },
                {
                    "NetworkInterfaceId": "eni-0065a61b324d1897a",
                    "PrivateIp": "10.0.20.197",
                    "IsPrimary": false,
                    "Status": "succeeded"
                }
            ],
            "NatGatewayId": "nat-1234567890abcdef0",
            "State": "available",
            "SubnetId": "subnet-08fc749671EXAMPLE",
            "VpcId": "vpc-098eb5ef58EXAMPLE",
            "Tags": [
                {
                    "Key": "Name",
```

```
                    "Value": "private-nat"
                }
            ],
            "ConnectivityType": "private"
        }
    ]
}
```

Para obtener información, consulte Gateways NAT en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte DescribeNatGateways en la Referencia de comandos de la AWS CLI.

`describe-network-acls`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-network-acls`.

AWS CLI

Para describir las ACL de su red

En el siguiente ejemplo de `describe-network-acls` se recuperan los detalles de todas las ACL de red.

```
aws ec2 describe-network-acls
```

Salida:

```
{
    "NetworkAcls": [
        {
            "Associations": [
                {
                    "NetworkAclAssociationId": "aclassoc-0c1679dc41EXAMPLE",
                    "NetworkAclId": "acl-0ea1f54ca7EXAMPLE",
                    "SubnetId": "subnet-0931fc2fa5EXAMPLE"
                }
            ],
            "Entries": [
                {
                    "CidrBlock": "0.0.0.0/0",
                    "Egress": true,
                    "Protocol": "-1",
```

```
                    "RuleAction": "allow",
                    "RuleNumber": 100
                },
                {
                    "CidrBlock": "0.0.0.0/0",
                    "Egress": true,
                    "Protocol": "-1",
                    "RuleAction": "deny",
                    "RuleNumber": 32767
                },
                {
                    "CidrBlock": "0.0.0.0/0",
                    "Egress": false,
                    "Protocol": "-1",
                    "RuleAction": "allow",
                    "RuleNumber": 100
                },
                {
                    "CidrBlock": "0.0.0.0/0",
                    "Egress": false,
                    "Protocol": "-1",
                    "RuleAction": "deny",
                    "RuleNumber": 32767
                }
            ],
            "IsDefault": true,
            "NetworkAclId": "acl-0ea1f54ca7EXAMPLE",
            "Tags": [],
            "VpcId": "vpc-06e4ab6c6cEXAMPLE",
            "OwnerId": "111122223333"
        },
        {
            "Associations": [],
            "Entries": [
                {
                    "CidrBlock": "0.0.0.0/0",
                    "Egress": true,
                    "Protocol": "-1",
                    "RuleAction": "allow",
                    "RuleNumber": 100
                },
                {
                    "Egress": true,
                    "Ipv6CidrBlock": "::/0",
```

```
            "Protocol": "-1",
            "RuleAction": "allow",
            "RuleNumber": 101
        },
        {
            "CidrBlock": "0.0.0.0/0",
            "Egress": true,
            "Protocol": "-1",
            "RuleAction": "deny",
            "RuleNumber": 32767
        },
        {
            "Egress": true,
            "Ipv6CidrBlock": "::/0",
            "Protocol": "-1",
            "RuleAction": "deny",
            "RuleNumber": 32768
        },
        {
            "CidrBlock": "0.0.0.0/0",
            "Egress": false,
            "Protocol": "-1",
            "RuleAction": "allow",
            "RuleNumber": 100
        },
        {
            "Egress": false,
            "Ipv6CidrBlock": "::/0",
            "Protocol": "-1",
            "RuleAction": "allow",
            "RuleNumber": 101
        },
        {
            "CidrBlock": "0.0.0.0/0",
            "Egress": false,
            "Protocol": "-1",
            "RuleAction": "deny",
            "RuleNumber": 32767
        },
        {
            "Egress": false,
            "Ipv6CidrBlock": "::/0",
            "Protocol": "-1",
            "RuleAction": "deny",
```

```
                    "RuleNumber": 32768
                }
            ],
            "IsDefault": true,
            "NetworkAclId": "acl-0e2a78e4e2EXAMPLE",
            "Tags": [],
            "VpcId": "vpc-03914afb3eEXAMPLE",
            "OwnerId": "111122223333"
        }
    ]
}
```

Para obtener más información, consulte ACL de red en la Guía del usuario de AWS VPC.

- Para obtener información sobre la API, consulte DescribeNetworkAcls en la Referencia de comandos de la AWS CLI.

`describe-network-insights-access-scope-analyses`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-network-insights-access-scope-analyses`.

AWS CLI

Para describir los análisis del ámbito de acceso a la información de red

En el siguiente ejemplo de `describe-network-insights-access-scope-analyses` se describe el análisis del ámbito de acceso en su cuenta de AWS.

```
aws ec2 describe-network-insights-access-scope-analyses \
    --region us-east-1
```

Salida:

```
{
    "NetworkInsightsAccessScopeAnalyses": [
        {
            "NetworkInsightsAccessScopeAnalysisId": "nisa-123456789111",
            "NetworkInsightsAccessScopeAnalysisArn": "arn:aws:ec2:us-
east-1:123456789012:network-insights-access-scope-analysis/nisa-123456789111",
            "NetworkInsightsAccessScopeId": "nis-123456789222",
            "Status": "succeeded",
```

```
            "StartDate": "2022-01-25T19:45:36.842000+00:00",
            "FindingsFound": "true",
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Getting started with Network Access Analyzer using the AWS CLI en la Guía del analizador de acceso a la red.

- Para obtener información sobre la API, consulte DescribeNetworkInsightsAccessScopeAnalyses en la Referencia de comandos de la AWS CLI.

`describe-network-insights-access-scopes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-network-insights-access-scopes`.

AWS CLI

Para describir los ámbitos de acceso a la información de red

En el siguiente ejemplo de `describe-network-insights-access-scopes` se describen los análisis del ámbito de acceso en su cuenta de AWS.

```
aws ec2 describe-network-insights-access-scopes \
    --region us-east-1
```

Salida:

```
{
    "NetworkInsightsAccessScopes": [
        {
            "NetworkInsightsAccessScopeId": "nis-123456789111",
            "NetworkInsightsAccessScopeArn": "arn:aws:ec2:us-
east-1:123456789012:network-insights-access-scope/nis-123456789111",
            "CreatedDate": "2021-11-29T21:12:41.416000+00:00",
            "UpdatedDate": "2021-11-29T21:12:41.416000+00:00",
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Getting started with Network Access Analyzer using the AWS CLI en la Guía del analizador de acceso a la red.

- Para obtener información sobre la API, consulte DescribeNetworkInsightsAccessScopes en la Referencia de comandos de la AWS CLI.

`describe-network-insights-analyses`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-network-insights-analyses`.

AWS CLI

Para ver los resultados de un análisis de rutas

En el siguiente ejemplo de `describe-network-insights-analyses` se describe el análisis especificado. En este ejemplo, el origen es una puerta de enlace de Internet, el destino es una instancia de EC2 y el protocolo es TCP. El análisis se ha llevado a cabo correctamente (`Status` es `succeeded`) y no se puede acceder a la ruta (`NetworkPathFound` y `false`). El código de explicación `ENI_SG_RULES_MISMATCH` indica que el grupo de seguridad de la instancia no contiene una regla que permita el tráfico en el puerto de destino.

```
aws ec2 describe-network-insights-analyses \
    --network-insights-analysis-ids nia-02207aa13eb480c7a
```

Salida:

```
{
    "NetworkInsightsAnalyses": [
        {
            "NetworkInsightsAnalysisId": "nia-02207aa13eb480c7a",
            "NetworkInsightsAnalysisArn": "arn:aws:ec2:us-
east-1:123456789012:network-insights-analysis/nia-02207aa13eb480c7a",
            "NetworkInsightsPathId": "nip-0b26f224f1d131fa8",
            "StartDate": "2021-01-20T22:58:37.495Z",
            "Status": "succeeded",
            "NetworkPathFound": false,
            "Explanations": [
                {
                    "Direction": "ingress",
                    "ExplanationCode": "ENI_SG_RULES_MISMATCH",
```

```
                    "NetworkInterface": {
                        "Id": "eni-0a25edef15a6cc08c",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:network-
interface/eni-0a25edef15a6cc08c"
                    },
                    "SecurityGroups": [
                        {
                            "Id": "sg-02f0d35a850ba727f",
                            "Arn": "arn:aws:ec2:us-east-1:123456789012:security-
group/sg-02f0d35a850ba727f"
                        }
                    ],
                    "Subnet": {
                        "Id": "subnet-004ff41eccb4d1194",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-004ff41eccb4d1194"
                    },
                    "Vpc": {
                        "Id": "vpc-f1663d98ad28331c7",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-
f1663d98ad28331c7"
                    }
                }
            ],
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Getting started using the AWS CLI en la Guía del analizador de accesibilidad.

- Para obtener información sobre la API, consulte DescribeNetworkInsightsAnalyses en la Referencia de comandos de la AWS CLI.

`describe-network-insights-paths`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-network-insights-paths`.

AWS CLI

Para describir una ruta

En el siguiente ejemplo de `describe-network-insights-paths` se describe la ruta especificada.

```
aws ec2 describe-network-insights-paths \
    --network-insights-path-ids nip-0b26f224f1d131fa8
```

Salida:

```
{
    "NetworkInsightsPaths": [
        {
            "NetworkInsightsPathId": "nip-0b26f224f1d131fa8",
            "NetworkInsightsPathArn": "arn:aws:ec2:us-east-1:123456789012:network-
insights-path/nip-0b26f224f1d131fa8",
            "CreatedDate": "2021-01-20T22:43:46.933Z",
            "Source": "igw-0797cccdc9d73b0e5",
            "Destination": "i-0495d385ad28331c7",
            "Protocol": "tcp"
        }
    ]
}
```

Para obtener más información, consulte Getting started using the AWS CLI en la Guía del analizador de accesibilidad.

- Para obtener información sobre la API, consulte DescribeNetworkInsightsPaths en la Referencia de comandos de la AWS CLI.

`describe-network-interface-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-network-interface-attribute`.

AWS CLI

Para describir el atributo de conexión de una interfaz de red

En este ejemplo de comando, se describe el atributo `attachment` de la interfaz de red especificada.

Comando:

```
aws ec2 describe-network-interface-attribute --network-interface-id eni-686ea200 --
attribute attachment
```

Salida:

```
{
  "NetworkInterfaceId": "eni-686ea200",
  "Attachment": {
      "Status": "attached",
      "DeviceIndex": 0,
      "AttachTime": "2015-05-21T20:02:20.000Z",
      "InstanceId": "i-1234567890abcdef0",
      "DeleteOnTermination": true,
      "AttachmentId": "eni-attach-43348162",
      "InstanceOwnerId": "123456789012"
  }
}
```

Para describir el atributo de conexión de una interfaz de red

En este ejemplo de comando, se describe el atributo `description` de la interfaz de red especificada.

Comando:

```
aws ec2 describe-network-interface-attribute --network-interface-id eni-686ea200 --
attribute description
```

Salida:

```
{
  "NetworkInterfaceId": "eni-686ea200",
  "Description": {
      "Value": "My description"
  }
}
```

Para describir el atributo groupSet de una interfaz de red

En este ejemplo de comando, se describe el atributo `groupSet` de la interfaz de red especificada.

Comando:

```
aws ec2 describe-network-interface-attribute --network-interface-id eni-686ea200 --
attribute groupSet
```

Salida:

```
{
  "NetworkInterfaceId": "eni-686ea200",
  "Groups": [
      {
          "GroupName": "my-security-group",
          "GroupId": "sg-903004f8"
      }
  ]
}
```

Para describir el atributo sourceDestCheck de una interfaz de red

En este ejemplo de comando, se describe el atributo `sourceDestCheck` de la interfaz de red especificada.

Comando:

```
aws ec2 describe-network-interface-attribute --network-interface-id eni-686ea200 --
attribute sourceDestCheck
```

Salida:

```
{
  "NetworkInterfaceId": "eni-686ea200",
  "SourceDestCheck": {
      "Value": true
  }
}
```

- Para obtener información sobre la API, consulte DescribeNetworkInterfaceAttribute en la Referencia de comandos de la AWS CLI.

`describe-network-interface-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-network-interface-permissions`.

AWS CLI

Para describir los permisos de la interfaz de red

En este ejemplo, se describen todos los permisos de la interfaz de red.

Comando:

```
aws ec2 describe-network-interface-permissions
```

Salida:

```
{
  "NetworkInterfacePermissions": [
      {
          "PermissionState": {
              "State": "GRANTED"
          },
          "NetworkInterfacePermissionId": "eni-perm-06fd19020ede149ea",
          "NetworkInterfaceId": "eni-b909511a",
          "Permission": "INSTANCE-ATTACH",
          "AwsAccountId": "123456789012"
      }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeNetworkInterfacePermissions en la Referencia de comandos de la AWS CLI.

`describe-network-interfaces`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-network-interfaces`.

AWS CLI

Para describir las interfaces de red

En este ejemplo, se describen todas sus interfaces de red.

Comando:

```
aws ec2 describe-network-interfaces
```

Salida:

```
{
  "NetworkInterfaces": [
      {
          "Status": "in-use",
          "MacAddress": "02:2f:8f:b0:cf:75",
          "SourceDestCheck": true,
          "VpcId": "vpc-a01106c2",
          "Description": "my network interface",
          "Association": {
              "PublicIp": "203.0.113.12",
              "AssociationId": "eipassoc-0fbb766a",
              "PublicDnsName": "ec2-203-0-113-12.compute-1.amazonaws.com",
              "IpOwnerId": "123456789012"
          },
          "NetworkInterfaceId": "eni-e5aa89a3",
          "PrivateIpAddresses": [
              {
                  "PrivateDnsName": "ip-10-0-1-17.ec2.internal",
                  "Association": {
                      "PublicIp": "203.0.113.12",
                      "AssociationId": "eipassoc-0fbb766a",
                      "PublicDnsName": "ec2-203-0-113-12.compute-1.amazonaws.com",
                      "IpOwnerId": "123456789012"
                  },
                  "Primary": true,
                  "PrivateIpAddress": "10.0.1.17"
              }
          ],
          "RequesterManaged": false,
          "Ipv6Addresses": [],
          "PrivateDnsName": "ip-10-0-1-17.ec2.internal",
          "AvailabilityZone": "us-east-1d",
          "Attachment": {
              "Status": "attached",
              "DeviceIndex": 1,
              "AttachTime": "2013-11-30T23:36:42.000Z",
              "InstanceId": "i-1234567890abcdef0",
```

```
            "DeleteOnTermination": false,
            "AttachmentId": "eni-attach-66c4350a",
            "InstanceOwnerId": "123456789012"
        },
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-8637d3e3"
            }
        ],
        "SubnetId": "subnet-b61f49f0",
        "OwnerId": "123456789012",
        "TagSet": [],
        "PrivateIpAddress": "10.0.1.17"
    },
    {
        "Status": "in-use",
        "MacAddress": "02:58:f5:ef:4b:06",
        "SourceDestCheck": true,
        "VpcId": "vpc-a01106c2",
        "Description": "Primary network interface",
        "Association": {
            "PublicIp": "198.51.100.0",
            "IpOwnerId": "amazon"
        },
        "NetworkInterfaceId": "eni-f9ba99bf",
        "PrivateIpAddresses": [
            {
                "Association": {
                    "PublicIp": "198.51.100.0",
                    "IpOwnerId": "amazon"
                },
                "Primary": true,
                "PrivateIpAddress": "10.0.1.149"
            }
        ],
        "RequesterManaged": false,
        "Ipv6Addresses": [],
        "AvailabilityZone": "us-east-1d",
        "Attachment": {
            "Status": "attached",
            "DeviceIndex": 0,
            "AttachTime": "2013-11-30T23:35:33.000Z",
            "InstanceId": "i-0598c7d356eba48d7",
```

```
                "DeleteOnTermination": true,
                "AttachmentId": "eni-attach-1b9db777",
                "InstanceOwnerId": "123456789012"
            },
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-8637d3e3"
                }
            ],
            "SubnetId": "subnet-b61f49f0",
            "OwnerId": "123456789012",
            "TagSet": [],
            "PrivateIpAddress": "10.0.1.149"
        }
    ]
}
```

En este ejemplo, se describen las interfaces de red que tienen una etiqueta con la clave `Purpose` y el valor `Prod`.

Comando:

```
aws ec2 describe-network-interfaces --filters Name=tag:Purpose,Values=Prod
```

Salida:

```
{
    "NetworkInterfaces": [
        {
            "Status": "available",
            "MacAddress": "12:2c:bd:f9:bf:17",
            "SourceDestCheck": true,
            "VpcId": "vpc-8941ebec",
            "Description": "ProdENI",
            "NetworkInterfaceId": "eni-b9a5ac93",
            "PrivateIpAddresses": [
                {
                    "PrivateDnsName": "ip-10-0-1-55.ec2.internal",
                    "Primary": true,
                    "PrivateIpAddress": "10.0.1.55"
                },
```

```
            {
                "PrivateDnsName": "ip-10-0-1-117.ec2.internal",
                "Primary": false,
                "PrivateIpAddress": "10.0.1.117"
            }
        ],
        "RequesterManaged": false,
        "PrivateDnsName": "ip-10-0-1-55.ec2.internal",
        "AvailabilityZone": "us-east-1d",
        "Ipv6Addresses": [],
        "Groups": [
            {
                "GroupName": "MySG",
                "GroupId": "sg-905002f5"
            }
        ],
        "SubnetId": "subnet-31d6c219",
        "OwnerId": "123456789012",
        "TagSet": [
            {
                "Value": "Prod",
                "Key": "Purpose"
            }
        ],
        "PrivateIpAddress": "10.0.1.55"
    }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeNetworkInterfaces en la Referencia de comandos de la AWS CLI.

`describe-placement-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-placement-groups`.

AWS CLI

Para describir los grupos de ubicación

En este ejemplo de comando, se describen todos sus grupos de ubicación.

Comando:

```
aws ec2 describe-placement-groups
```

Salida:

```
{
    "PlacementGroups": [
        {
            "GroupName": "my-cluster",
            "State": "available",
            "Strategy": "cluster"
        },
        ...
    ]
}
```

- Para obtener información sobre la API, consulte DescribePlacementGroups en la Referencia de comandos de la AWS CLI.

`describe-prefix-lists`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-prefix-lists`.

AWS CLI

Para describir las listas de prefijos

En este ejemplo, se enumeran todas las listas de prefijos disponibles para la región.

Comando:

```
aws ec2 describe-prefix-lists
```

Salida:

```
{
  "PrefixLists": [
    {
      "PrefixListName": "com.amazonaws.us-east-1.s3",
      "Cidrs": [
        "54.231.0.0/17"
      ],
      "PrefixListId": "pl-63a5400a"
```

```
    }
  ]
}
```

- Para obtener información sobre la API, consulte DescribePrefixLists en la Referencia de comandos de la AWS CLI.

`describe-principal-id-format`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-principal-id-format`.

AWS CLI

Para describir el formato de ID para los usuarios y roles de IAM con el formato de ID largo activado

En el siguiente ejemplo de `describe-principal-id-format` se describen el formato de ID del usuario raíz, todos los roles de IAM y todos los usuarios de IAM con el formato de ID largo activado.

```
aws ec2 describe-principal-id-format \
    --resource instance
```

Salida:

```
{
    "Principals": [
        {
            "Arn": "arn:aws:iam::123456789012:root",
            "Statuses": [
                {
                    "Deadline": "2016-12-15T00:00:00.000Z",
                    "Resource": "reservation",
                    "UseLongIds": true
                },
                {
                    "Deadline": "2016-12-15T00:00:00.000Z",
                    "Resource": "instance",
                    "UseLongIds": true
                },
                {
                    "Deadline": "2016-12-15T00:00:00.000Z",
```

```
                    "Resource": "volume",
                    "UseLongIds": true
                },
            ]
        },
        ...
    ]
}
```

- Para obtener información sobre la API, consulte DescribePrincipalIdFormat en la Referencia de comandos de la AWS CLI.

`describe-public-ipv4-pools`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-public-ipv4-pools`.

AWS CLI

Para describir los grupos de direcciones IPv

En el siguiente ejemplo de `describe-public-ipv4-pools` se muestra la información sobre los grupos de direcciones que se crearon al aprovisionar los rangos de direcciones IPv4 públicas mediante Traiga sus propias direcciones IP (BYOIP).

```
aws ec2 describe-public-ipv4-pools
```

Salida:

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-1234567890abcdef0",
            "PoolAddressRanges": [
                {
                    "FirstAddress": "203.0.113.0",
                    "LastAddress": "203.0.113.255",
                    "AddressCount": 256,
                    "AvailableAddressCount": 256
                }
            ],
            "TotalAddressCount": 256,
            "TotalAvailableAddressCount": 256
```

```
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribePublicIpv4Pools en la Referencia de comandos de la AWS CLI.

`describe-regions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-regions`.

AWS CLI

Ejemplo 1: Describir todas las regiones habilitadas

En el siguiente ejemplo de `describe-regions`, se describen las regiones que están habilitadas para su cuenta.

```
aws ec2 describe-regions
```

Salida:

```
{
    "Regions": [
        {
            "Endpoint": "ec2.eu-north-1.amazonaws.com",
            "RegionName": "eu-north-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.ap-south-1.amazonaws.com",
            "RegionName": "ap-south-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.eu-west-3.amazonaws.com",
            "RegionName": "eu-west-3",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.eu-west-2.amazonaws.com",
            "RegionName": "eu-west-2",
```

```
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.eu-west-1.amazonaws.com",
            "RegionName": "eu-west-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.ap-northeast-3.amazonaws.com",
            "RegionName": "ap-northeast-3",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.ap-northeast-2.amazonaws.com",
            "RegionName": "ap-northeast-2",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.ap-northeast-1.amazonaws.com",
            "RegionName": "ap-northeast-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.sa-east-1.amazonaws.com",
            "RegionName": "sa-east-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.ca-central-1.amazonaws.com",
            "RegionName": "ca-central-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.ap-southeast-1.amazonaws.com",
            "RegionName": "ap-southeast-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.ap-southeast-2.amazonaws.com",
            "RegionName": "ap-southeast-2",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.eu-central-1.amazonaws.com",
```

```
            "RegionName": "eu-central-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.us-east-1.amazonaws.com",
            "RegionName": "us-east-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.us-east-2.amazonaws.com",
            "RegionName": "us-east-2",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.us-west-1.amazonaws.com",
            "RegionName": "us-west-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.us-west-2.amazonaws.com",
            "RegionName": "us-west-2",
            "OptInStatus": "opt-in-not-required"
        }
    ]
}
```

Para obtener más información, consulte Regiones y zonas en la Guía del usuario de Amazon EC2.

Ejemplo 2: Describir las regiones habilitadas con un punto de conexión cuyo nombre contiene una cadena específica

En el siguiente ejemplo de `describe-regions`, se describen todas las regiones que ha habilitado y que tienen la cadena “us” en el punto de conexión.

```
aws ec2 describe-regions \
    --filters "Name=endpoint,Values=*us*"
```

Salida:

```
{
    "Regions": [
        {
```

```
            "Endpoint": "ec2.us-east-1.amazonaws.com",
            "RegionName": "us-east-1"
        },
        {
            "Endpoint": "ec2.us-east-2.amazonaws.com",
            "RegionName": "us-east-2"
        },
        {
            "Endpoint": "ec2.us-west-1.amazonaws.com",
            "RegionName": "us-west-1"
        },
        {
            "Endpoint": "ec2.us-west-2.amazonaws.com",
            "RegionName": "us-west-2"
        }
    ]
}
```

Para obtener más información, consulte Regiones y zonas en la Guía del usuario de Amazon EC2.

Ejemplo 3: describir todas las regiones

En el siguiente ejemplo de `describe-regions`, se describen todas las regiones disponibles, incluidas las que están deshabilitadas.

```
aws ec2 describe-regions \
    --all-regions
```

Salida:

```
{
    "Regions": [
        {
            "Endpoint": "ec2.eu-north-1.amazonaws.com",
            "RegionName": "eu-north-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.ap-south-1.amazonaws.com",
            "RegionName": "ap-south-1",
            "OptInStatus": "opt-in-not-required"
        },
```

```
        {
            "Endpoint": "ec2.eu-west-3.amazonaws.com",
            "RegionName": "eu-west-3",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.eu-west-2.amazonaws.com",
            "RegionName": "eu-west-2",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.eu-west-1.amazonaws.com",
            "RegionName": "eu-west-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.ap-northeast-3.amazonaws.com",
            "RegionName": "ap-northeast-3",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.me-south-1.amazonaws.com",
            "RegionName": "me-south-1",
            "OptInStatus": "not-opted-in"
        },
        {
            "Endpoint": "ec2.ap-northeast-2.amazonaws.com",
            "RegionName": "ap-northeast-2",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.ap-northeast-1.amazonaws.com",
            "RegionName": "ap-northeast-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.sa-east-1.amazonaws.com",
            "RegionName": "sa-east-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.ca-central-1.amazonaws.com",
            "RegionName": "ca-central-1",
            "OptInStatus": "opt-in-not-required"
```

```
        },
        {
            "Endpoint": "ec2.ap-east-1.amazonaws.com",
            "RegionName": "ap-east-1",
            "OptInStatus": "not-opted-in"
        },
        {
            "Endpoint": "ec2.ap-southeast-1.amazonaws.com",
            "RegionName": "ap-southeast-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.ap-southeast-2.amazonaws.com",
            "RegionName": "ap-southeast-2",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.eu-central-1.amazonaws.com",
            "RegionName": "eu-central-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.us-east-1.amazonaws.com",
            "RegionName": "us-east-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.us-east-2.amazonaws.com",
            "RegionName": "us-east-2",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.us-west-1.amazonaws.com",
            "RegionName": "us-west-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.us-west-2.amazonaws.com",
            "RegionName": "us-west-2",
            "OptInStatus": "opt-in-not-required"
        }
    ]
}
```

Para obtener más información, consulte Regiones y zonas en la Guía del usuario de Amazon EC2.

Ejemplo 4: enumerar únicamente los nombres de las regiones

En el siguiente ejemplo de `describe-regions`, se usa el parámetro `--query` para filtrar la salida y devolver solo los nombres de las regiones como texto.

```
aws ec2 describe-regions \
    --all-regions \
    --query "Regions[].{Name:RegionName}" \
    --output text
```

Salida:

```
eu-north-1
ap-south-1
eu-west-3
eu-west-2
eu-west-1
ap-northeast-3
ap-northeast-2
me-south-1
ap-northeast-1
sa-east-1
ca-central-1
ap-east-1
ap-southeast-1
ap-southeast-2
eu-central-1
us-east-1
us-east-2
us-west-1
us-west-2
```

Para obtener más información, consulte Regiones y zonas en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeRegions en la Referencia de comandos de la AWS CLI.

describe-replace-root-volume-tasks

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-replace-root-volume-tasks`.

AWS CLI

Ejemplo 1: visualización de información sobre una tarea específica de reemplazo de un volumen raíz

En el siguiente ejemplo de `describe-replace-root-volume-tasks` se describe la tarea de reemplazo del volumen raíz replacevol-0111122223333abcd.

```
aws ec2 describe-replace-root-volume-tasks \
    --replace-root-volume-task-ids replacevol-0111122223333abcd
```

Salida:

```
{
    "ReplaceRootVolumeTasks": [
        {
            "ReplaceRootVolumeTaskId": "replacevol-0111122223333abcd",
            "Tags": [],
            "InstanceId": "i-0123456789abcdefa",
            "TaskState": "succeeded",
            "StartTime": "2022-03-14T15:16:28Z",
            "CompleteTime": "2022-03-14T15:16:52Z"
        }
    ]
}
```

Para obtener más información, consulte Replace a root volume en la Guía del usuario de Amazon Elastic Compute Cloud.

Ejemplo 2: visualización de información sobre todas las tareas de reemplazo de volumen raíz de una instancia específica

En el siguiente ejemplo de `describe-replace-root-volume-tasks` se describen todas las tareas de reemplazo de volumen raíz para la instancia i-0123456789abcdefa.

```
aws ec2 describe-replace-root-volume-tasks \
    --filters Name=instance-id,Values=i-0123456789abcdefa
```

Salida:

```
{
    "ReplaceRootVolumeTasks": [
        {
            "ReplaceRootVolumeTaskId": "replacevol-0111122223333abcd",
            "Tags": [],
            "InstanceId": "i-0123456789abcdefa",
            "TaskState": "succeeded",
            "StartTime": "2022-03-14T15:06:38Z",
            "CompleteTime": "2022-03-14T15:07:03Z"
        },
        {
            "ReplaceRootVolumeTaskId": "replacevol-0444455555555abcd",
            "Tags": [],
            "InstanceId": "i-0123456789abcdefa",
            "TaskState": "succeeded",
            "StartTime": "2022-03-14T15:16:28Z",
            "CompleteTime": "2022-03-14T15:16:52Z"
        }
    ]
}
```

Para obtener más información, consulte Replace a root volume en la Guía del usuario de Amazon Elastic Compute Cloud.

- Para obtener información sobre la API, consulte DescribeReplaceRootVolumeTasks en la Referencia de comandos de la AWS CLI.

`describe-reserved-instances-listings`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-reserved-instances-listings`.

AWS CLI

Para describir un listado de instancias reservadas

En el siguiente ejemplo de `describe-reserved-instances-listings` se recupera información sobre el listado de instancias reservada especificado.

```
aws ec2 describe-reserved-instances-listings \
```

```
    --reserved-instances-listing-id 5ec28771-05ff-4b9b-aa31-9e57dexample
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DescribeReservedInstancesListings en la Referencia de comandos de la AWS CLI.

`describe-reserved-instances-modifications`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-reserved-instances-modifications`.

AWS CLI

Para describir modificaciones de instancias reservadas

En este ejemplo de comando, se describen todas las solicitudes de modificación de instancias reservadas que se han enviado para su cuenta.

Comando:

```
aws ec2 describe-reserved-instances-modifications
```

Salida:

```
{
    "ReservedInstancesModifications": [
        {
            "Status": "fulfilled",
            "ModificationResults": [
                {
                    "ReservedInstancesId": "93bbbca2-62f1-4d9d-b225-16bada29e6c7",
                    "TargetConfiguration": {
                        "AvailabilityZone": "us-east-1b",
                        "InstanceType": "m1.large",
                        "InstanceCount": 3
                    }
                },
                {
                     "ReservedInstancesId": "1ba8e2e3-aabb-46c3-bcf5-3fe2fda922e6",
                     "TargetConfiguration": {
                         "AvailabilityZone": "us-east-1d",
                         "InstanceType": "m1.xlarge",
```

```
                        "InstanceCount": 1
                    }
                }
            ],
            "EffectiveDate": "2015-08-12T17:00:00.000Z",
            "CreateDate": "2015-08-12T17:52:52.630Z",
            "UpdateDate": "2015-08-12T18:08:06.698Z",
            "ClientToken": "c9adb218-3222-4889-8216-0cf0e52dc37e:
            "ReservedInstancesModificationId": "rimod-d3ed4335-b1d3-4de6-
ab31-0f13aaf46687",
            "ReservedInstancesIds": [
                {
                    "ReservedInstancesId": "b847fa93-e282-4f55-b59a-1342f5bd7c02"
                }
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeReservedInstancesModifications en la Referencia de comandos de la AWS CLI.

`describe-reserved-instances-offerings`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-reserved-instances-offerings`.

AWS CLI

Para describir ofertas de instancias reservadas

En este ejemplo de comando, se describen todas las instancias reservadas disponibles para su compra en la región.

Comando:

```
aws ec2 describe-reserved-instances-offerings
```

Salida:

```
{
  "ReservedInstancesOfferings": [
```

```
      {
          "OfferingType": "Partial Upfront",
          "AvailabilityZone": "us-east-1b",
          "InstanceTenancy": "default",
          "PricingDetails": [],
          "ProductDescription": "Red Hat Enterprise Linux",
          "UsagePrice": 0.0,
          "RecurringCharges": [
              {
                  "Amount": 0.088,
                  "Frequency": "Hourly"
              }
          ],
          "Marketplace": false,
          "CurrencyCode": "USD",
          "FixedPrice": 631.0,
          "Duration": 94608000,
          "ReservedInstancesOfferingId": "9a06095a-bdc6-47fe-a94a-2a382f016040",
          "InstanceType": "c1.medium"
      },
      {
          "OfferingType": "PartialUpfront",
          "AvailabilityZone": "us-east-1b",
          "InstanceTenancy": "default",
          "PricingDetails": [],
          "ProductDescription": "Linux/UNIX",
          "UsagePrice": 0.0,
          "RecurringCharges": [
              {
                  "Amount": 0.028,
                  "Frequency": "Hourly"
              }
          ],
          "Marketplace": false,
          "CurrencyCode": "USD",
          "FixedPrice": 631.0,
          "Duration": 94608000,
          "ReservedInstancesOfferingId": "bfbefc6c-0d10-418d-b144-7258578d329d",
          "InstanceType": "c1.medium"
      },
  ...
}
```

Para describir sus ofertas de instancias reservadas mediante opciones

En este ejemplo, se enumeran las instancias reservadas que AWS ofrece con las siguientes especificaciones: tipos de instancias t1.micro, productos de Windows (Amazon VPC) y ofertas de utilización intensa.

Comando:

```
aws ec2 describe-reserved-instances-offerings --no-include-marketplace --instance-type "t1.micro" --product-description "Windows (Amazon VPC)" --offering-type "no upfront"
```

Salida:

```
{
    "ReservedInstancesOfferings": [
      {
          "OfferingType": "No Upfront",
          "AvailabilityZone": "us-east-1b",
          "InstanceTenancy": "default",
          "PricingDetails": [],
          "ProductDescription": "Windows",
          "UsagePrice": 0.0,
          "RecurringCharges": [
              {
                  "Amount": 0.015,
                  "Frequency": "Hourly"
              }
          ],
          "Marketplace": false,
          "CurrencyCode": "USD",
          "FixedPrice": 0.0,
          "Duration": 31536000,
          "ReservedInstancesOfferingId": "c48ab04c-fe69-4f94-8e39-a23842292823",
          "InstanceType": "t1.micro"
      },

              ...
      {
          "OfferingType": "No Upfront",
          "AvailabilityZone": "us-east-1d",
          "InstanceTenancy": "default",
          "PricingDetails": [],
```

```
            "ProductDescription": "Windows (Amazon VPC)",
            "UsagePrice": 0.0,
            "RecurringCharges": [
                {
                    "Amount": 0.015,
                    "Frequency": "Hourly"
                }
            ],
            "Marketplace": false,
            "CurrencyCode": "USD",
            "FixedPrice": 0.0,
            "Duration": 31536000,
            "ReservedInstancesOfferingId": "3a98bf7d-2123-42d4-b4f5-8dbec4b06dc6",
            "InstanceType": "t1.micro"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeReservedInstancesOfferings en la Referencia de comandos de AWS CLI.

`describe-reserved-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-reserved-instances`.

AWS CLI

Para describir las instancias reservadas

En este ejemplo de comando, se describen las instancias reservadas que posee.

Comando:

```
aws ec2 describe-reserved-instances
```

Salida:

```
{
  "ReservedInstances": [
      {
          "ReservedInstancesId": "b847fa93-e282-4f55-b59a-1342fexample",
          "OfferingType": "No Upfront",
          "AvailabilityZone": "us-west-1c",
```

```
            "End": "2016-08-14T21:34:34.000Z",
            "ProductDescription": "Linux/UNIX",
            "UsagePrice": 0.00,
            "RecurringCharges": [
                {
                    "Amount": 0.104,
                    "Frequency": "Hourly"
                }
            ],
            "Start": "2015-08-15T21:34:35.086Z",
            "State": "active",
            "FixedPrice": 0.0,
            "CurrencyCode": "USD",
            "Duration": 31536000,
            "InstanceTenancy": "default",
            "InstanceType": "m3.medium",
            "InstanceCount": 2
        },
        ...
    ]
}
```

Para describir las instancias reservadas mediante filtros

En este ejemplo, se filtra la respuesta para incluir solo las instancias reservadas t2.micro de Linux/UNIX de tres años en us-west-1c.

Comando:

```
aws ec2 describe-reserved-instances --
filters Name=duration,Values=94608000 Name=instance-
type,Values=t2.micro Name=product-description,Values=Linux/UNIX Name=availability-
zone,Values=us-east-1e
```

Salida:

```
{
    "ReservedInstances": [
        {
            "ReservedInstancesId": "f127bd27-edb7-44c9-a0eb-0d7e09259af0",
            "OfferingType": "All Upfront",
            "AvailabilityZone": "us-east-1e",
            "End": "2018-03-26T21:34:34.000Z",
```

```
            "ProductDescription": "Linux/UNIX",
            "UsagePrice": 0.00,
            "RecurringCharges": [],
            "Start": "2015-03-27T21:34:35.848Z",
            "State": "active",
            "FixedPrice": 151.0,
            "CurrencyCode": "USD",
            "Duration": 94608000,
            "InstanceTenancy": "default",
            "InstanceType": "t2.micro",
            "InstanceCount": 1
        }
    ]
}
```

Para obtener más información, consulte Uso de instancias de Amazon EC2 en la Guía del usuario de la interfaz de la línea de comandos de AWS.

- Para obtener información sobre la API, consulte DescribeReservedInstances en la Referencia de comandos de la AWS CLI.

`describe-route-tables`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-route-tables`.

AWS CLI

Para describir las tablas de enrutamiento

En el siguiente ejemplo de `describe-route-tables` se recuperan los detalles de sus tablas de enrutamiento.

```
aws ec2 describe-route-tables
```

Salida:

```
{
    "RouteTables": [
        {
            "Associations": [
                {
                    "Main": true,
                    "RouteTableAssociationId": "rtbassoc-0df3f54e06EXAMPLE",
```

```
                "RouteTableId": "rtb-09ba434c1bEXAMPLE"
            }
        ],
        "PropagatingVgws": [],
        "RouteTableId": "rtb-09ba434c1bEXAMPLE",
        "Routes": [
            {
                "DestinationCidrBlock": "10.0.0.0/16",
                "GatewayId": "local",
                "Origin": "CreateRouteTable",
                "State": "active"
            },
            {
                "DestinationCidrBlock": "0.0.0.0/0",
                "NatGatewayId": "nat-06c018cbd8EXAMPLE",
                "Origin": "CreateRoute",
                "State": "blackhole"
            }
        ],
        "Tags": [],
        "VpcId": "vpc-0065acced4EXAMPLE",
        "OwnerId": "111122223333"
    },
    {
        "Associations": [
            {
                "Main": true,
                "RouteTableAssociationId": "rtbassoc-9EXAMPLE",
                "RouteTableId": "rtb-a1eec7de"
            }
        ],
        "PropagatingVgws": [],
        "RouteTableId": "rtb-a1eec7de",
        "Routes": [
            {
                "DestinationCidrBlock": "172.31.0.0/16",
                "GatewayId": "local",
                "Origin": "CreateRouteTable",
                "State": "active"
            },
            {
                "DestinationCidrBlock": "0.0.0.0/0",
                "GatewayId": "igw-fEXAMPLE",
                "Origin": "CreateRoute",
```

```
                    "State": "active"
                }
            ],
            "Tags": [],
            "VpcId": "vpc-3EXAMPLE",
            "OwnerId": "111122223333"
        },
        {
            "Associations": [
                {
                    "Main": false,
                    "RouteTableAssociationId": "rtbassoc-0b100c28b2EXAMPLE",
                    "RouteTableId": "rtb-07a98f76e5EXAMPLE",
                    "SubnetId": "subnet-0d3d002af8EXAMPLE"
                }
            ],
            "PropagatingVgws": [],
            "RouteTableId": "rtb-07a98f76e5EXAMPLE",
            "Routes": [
                {
                    "DestinationCidrBlock": "10.0.0.0/16",
                    "GatewayId": "local",
                    "Origin": "CreateRouteTable",
                    "State": "active"
                },
                {
                    "DestinationCidrBlock": "0.0.0.0/0",
                    "GatewayId": "igw-06cf664d80EXAMPLE",
                    "Origin": "CreateRoute",
                    "State": "active"
                }
            ],
            "Tags": [],
            "VpcId": "vpc-0065acced4EXAMPLE",
            "OwnerId": "111122223333"
        }
    ]
}
```

Para obtener más información, consulte Working with Route Tables en la Guía del usuario de AWS VPC.

- Para obtener información sobre la API, consulte DescribeRouteTables en la Referencia de comandos de la AWS CLI.

describe-scheduled-instance-availability

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-scheduled-instance-availability`.

AWS CLI

Para describir una programación disponible

En este ejemplo, se describe una programación que tiene lugar todos los domingos a partir de la fecha especificada.

Comando:

```
aws ec2 describe-scheduled-instance-availability --
recurrence Frequency=Weekly,Interval=1,OccurrenceDays=[1] --first-slot-start-time-
range EarliestTime=2016-01-31T00:00:00Z,LatestTime=2016-01-31T04:00:00Z
```

Salida:

```
{
  "ScheduledInstanceAvailabilitySet": [
    {
        "AvailabilityZone": "us-west-2b",
        "TotalScheduledInstanceHours": 1219,
        "PurchaseToken": "eyJ2IjoiMSIsInMiOjEsImMiOi...",
        "MinTermDurationInDays": 366,
        "AvailableInstanceCount": 20,
        "Recurrence": {
            "OccurrenceDaySet": [
                1
            ],
            "Interval": 1,
            "Frequency": "Weekly",
            "OccurrenceRelativeToEnd": false
        },
        "Platform": "Linux/UNIX",
        "FirstSlotStartTime": "2016-01-31T00:00:00Z",
        "MaxTermDurationInDays": 366,
        "SlotDurationInHours": 23,
        "NetworkPlatform": "EC2-VPC",
        "InstanceType": "c4.large",
        "HourlyPrice": "0.095"
```

```
    },
    ...
  ]
}
```

Para delimitar los resultados, puede agregar filtros que especifiquen el sistema operativo, la red y el tipo de instancia.

Comando:

--filters Name=platform,Values=Linux/UNIX Name=network-platform,Values=EC2-VPC Name=instance-type,Values=c4.large

- Para obtener información sobre la API, consulte DescribeScheduledInstanceAvailability en la Referencia de comandos de la AWS CLI.

`describe-scheduled-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-scheduled-instances`.

AWS CLI

Para describir las instancias programadas

En este ejemplo, se describe la instancia programada especificada.

Comando:

```
aws ec2 describe-scheduled-instances --scheduled-instance-
ids sci-1234-1234-1234-1234-123456789012
```

Salida:

```
{
  "ScheduledInstanceSet": [
      {
          "AvailabilityZone": "us-west-2b",
          "ScheduledInstanceId": "sci-1234-1234-1234-1234-123456789012",
          "HourlyPrice": "0.095",
          "CreateDate": "2016-01-25T21:43:38.612Z",
          "Recurrence": {
              "OccurrenceDaySet": [
                  1
```

```
            ],
            "Interval": 1,
            "Frequency": "Weekly",
            "OccurrenceRelativeToEnd": false,
            "OccurrenceUnit": ""
        },
        "Platform": "Linux/UNIX",
        "TermEndDate": "2017-01-31T09:00:00Z",
        "InstanceCount": 1,
        "SlotDurationInHours": 32,
        "TermStartDate": "2016-01-31T09:00:00Z",
        "NetworkPlatform": "EC2-VPC",
        "TotalScheduledInstanceHours": 1696,
        "NextSlotStartTime": "2016-01-31T09:00:00Z",
        "InstanceType": "c4.large"
    }
  ]
}
```

En este ejemplo, se describen todas las instancias programadas.

Comando:

```
aws ec2 describe-scheduled-instances
```

- Para obtener información sobre la API, consulte DescribeScheduledInstances en la Referencia de comandos de la AWS CLI.

`describe-security-group-references`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-security-group-references`.

AWS CLI

Para describir las referencias a grupos de seguridad

En este ejemplo, se describen las referencias a grupos de seguridad de `sg-bbbb2222`. La respuesta indica que el grupo de seguridad de la VPC `vpc-aaaaaaaa` hace referencia al grupo de seguridad `sg-bbbb2222`.

Comando:

```
aws ec2 describe-security-group-references --group-id sg-bbbbb22222
```

Salida:

```
{
  "SecurityGroupsReferenceSet": [
    {
      "ReferencingVpcId": "vpc-aaaaaaaa ",
      "GroupId": "sg-bbbbb22222",
      "VpcPeeringConnectionId": "pcx-b04deed9"
    }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeSecurityGroupReferences en la Referencia de comandos de la AWS CLI.

`describe-security-group-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-security-group-rules`.

AWS CLI

Ejemplo 1: descripción de las reglas de grupo de seguridad de un grupo de seguridad

En el siguiente ejemplo de `describe-security-group-rules` se describen las reglas de grupo de seguridad de un grupo de seguridad específico. Use la opción `filters` para limitar el ámbito de los resultados a un grupo de seguridad específico.

```
aws ec2 describe-security-group-rules \
    --filters Name="group-id",Values="sg-1234567890abcdef0"
```

Salida:

```
{
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-abcdef01234567890",
            "GroupId": "sg-1234567890abcdef0",
            "GroupOwnerId": "111122223333",
            "IsEgress": false,
```

```
            "IpProtocol": "-1",
            "FromPort": -1,
            "ToPort": -1,
            "ReferencedGroupInfo": {
                "GroupId": "sg-1234567890abcdef0",
                "UserId": "111122223333"
            },
            "Tags": []
        },
        {
            "SecurityGroupRuleId": "sgr-bcdef01234567890a",
            "GroupId": "sg-1234567890abcdef0",
            "GroupOwnerId": "111122223333",
            "IsEgress": true,
            "IpProtocol": "-1",
            "FromPort": -1,
            "ToPort": -1,
            "CidrIpv6": "::/0",
            "Tags": []
        },
        {
            "SecurityGroupRuleId": "sgr-cdef01234567890ab",
            "GroupId": "sg-1234567890abcdef0",
            "GroupOwnerId": "111122223333",
            "IsEgress": true,
            "IpProtocol": "-1",
            "FromPort": -1,
            "ToPort": -1,
            "CidrIpv4": "0.0.0.0/0",
            "Tags": []
        }
    ]
}
```

Ejemplo 2: descripción de una regla de grupo de seguridad

En el siguiente ejemplo de `describe-security-group-rules` se describe el grupo de seguridad especificado.

```
aws ec2 describe-security-group-rules \
    --security-group-rule-ids sgr-cdef01234567890ab
```

Salida:

```
{
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-cdef01234567890ab",
            "GroupId": "sg-1234567890abcdef0",
            "GroupOwnerId": "111122223333",
            "IsEgress": true,
            "IpProtocol": "-1",
            "FromPort": -1,
            "ToPort": -1,
            "CidrIpv4": "0.0.0.0/0",
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Reglas del grupo de seguridad en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte DescribeSecurityGroupRules en la Referencia de comandos de la AWS CLI.

`describe-security-group-vpc-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-security-group-vpc-associations`.

AWS CLI

Descripción de las asociaciones de VPC

En el siguiente ejemplo de `describe-security-group-vpc-associations`, se describen las asociaciones de VPC para el grupo de seguridad especificado.

```
aws ec2 describe-security-group-vpc-associations \
    --filters Name=group-id,Values=sg-04dbb43907d3f8a78
```

Salida:

```
{
    "SecurityGroupVpcAssociations": [
        {
```

```
            "GroupId": "sg-04dbb43907d3f8a78",
            "VpcId": "vpc-0bf4c2739bc05a694",
            "VpcOwnerId": "123456789012",
            "State": "associated"
        }
    ]
}
```

Para obtener más información, consulte Asociación de grupos de seguridad a varias VPC en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte DescribeSecurityGroupVpcAssociations en la Referencia de comandos de la AWS CLI.

`describe-security-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-security-groups`.

AWS CLI

Ejemplo 1: Describir un grupo de seguridad

En el siguiente ejemplo de `describe-security-groups`, se describe el grupo de seguridad especificado.

```
aws ec2 describe-security-groups \
    --group-ids sg-903004f8
```

Salida:

```
{
    "SecurityGroups": [
        {
            "IpPermissionsEgress": [
                {
                    "IpProtocol": "-1",
                    "IpRanges": [
                        {
                            "CidrIp": "0.0.0.0/0"
                        }
                    ],
                    "UserIdGroupPairs": [],
                    "PrefixListIds": []
```

```
            }
        ],
        "Description": "My security group",
        "Tags": [
            {
                "Value": "SG1",
                "Key": "Name"
            }
        ],
        "IpPermissions": [
            {
                "IpProtocol": "-1",
                "IpRanges": [],
                "UserIdGroupPairs": [
                    {
                        "UserId": "123456789012",
                        "GroupId": "sg-903004f8"
                    }
                ],
                "PrefixListIds": []
            },
            {
                "PrefixListIds": [],
                "FromPort": 22,
                "IpRanges": [
                    {
                        "Description": "Access from NY office",
                        "CidrIp": "203.0.113.0/24"
                    }
                ],
                "ToPort": 22,
                "IpProtocol": "tcp",
                "UserIdGroupPairs": []
                }
        ],
        "GroupName": "MySecurityGroup",
        "VpcId": "vpc-1a2b3c4d",
        "OwnerId": "123456789012",
        "GroupId": "sg-903004f8",
    }
]
}
```

Ejemplo 2: Describir los grupos de seguridad que tienen reglas específicas

En el siguiente ejemplo de `describe-security-groups` se utilizan filtros para limitar el ámbito de los resultados a los grupos de seguridad que tienen una regla que permite el tráfico SSH (puerto 22) y una regla que permite el tráfico desde todas las direcciones (`0.0.0.0/0`). En el ejemplo se usa el parámetro `--query` para mostrar solo los nombres de los grupos de seguridad. Los grupos de seguridad deben coincidir con todos los filtros para que se devuelvan en los resultados; sin embargo, una sola regla no tiene que coincidir con todos los filtros. Por ejemplo, el resultado devuelve un grupo de seguridad con una regla que permite el tráfico SSH desde una dirección IP específica y otra regla que permite el tráfico HTTP desde todas las direcciones.

```
aws ec2 describe-security-groups \
    --filters Name=ip-permission.from-port,Values=22 Name=ip-permission.to-
port,Values=22 Name=ip-permission.cidr,Values='0.0.0.0/0' \
    --query "SecurityGroups[*].[GroupName]" \
    --output text
```

Salida:

```
default
my-security-group
web-servers
launch-wizard-1
```

Ejemplo 3: describir los grupos de seguridad con base en las etiquetas

En el siguiente ejemplo de `describe-security-groups`, se usan filtros para limitar los resultados a los grupos de seguridad que incluyen `test` en el nombre del grupo de seguridad y que tienen la etiqueta `Test=To-delete`. En el ejemplo se usa el parámetro `--query` para mostrar solo los nombres y los ID de los grupos de seguridad.

```
aws ec2 describe-security-groups \
    --filters Name=group-name,Values=*test* Name=tag:Test,Values=To-delete \
    --query "SecurityGroups[*].{Name:GroupName,ID:GroupId}"
```

Salida:

```
[
    {
        "Name": "testfornewinstance",
```

```
        "ID": "sg-33bb22aa"
    },
    {
        "Name": "newgrouptest",
        "ID": "sg-1a2b3c4d"
    }
]
```

Para ver ejemplos adicionales de uso de filtros de etiquetas, consulte Trabajo con etiquetas en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeSecurityGroups en la Referencia de comandos de la AWS CLI.

`describe-snapshot-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-snapshot-attribute`.

AWS CLI

Para describir los atributos de instantánea de una instantánea

En el siguiente ejemplo de `describe-snapshot-attribute` se enumeran las cuentas con las que se comparte una instantánea.

```
aws ec2 describe-snapshot-attribute \
    --snapshot-id snap-01234567890abcedf \
    --attribute createVolumePermission
```

Salida:

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "CreateVolumePermissions": [
        {
            "UserId": "123456789012"
        }
    ]
}
```

Para obtener más información, consulte Share an Amazon EBS snapshot en la Guía del usuario de Amazon Elastic Compute Cloud.

- Para obtener información sobre la API, consulte DescribeSnapshotAttribute en la Referencia de comandos de la AWS CLI.

`describe-snapshot-tier-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-snapshot-tier-status`.

AWS CLI

Para ver la información de archivo sobre una instantánea archivada

En el siguiente ejemplo de `describe-snapshot-tier-status` se proporciona información de archivo sobre una instantánea archivada.

```
aws ec2 describe-snapshot-tier-status \
    --filters "Name=snapshot-id, Values=snap-01234567890abcedf"
```

Salida:

```
{
    "SnapshotTierStatuses": [
        {
            "Status": "completed",
            "ArchivalCompleteTime": "2021-09-15T17:33:16.147Z",
            "LastTieringProgress": 100,
            "Tags": [],
            "VolumeId": "vol-01234567890abcedf",
            "LastTieringOperationState": "archival-completed",
            "StorageTier": "archive",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-01234567890abcedf",
            "LastTieringStartTime": "2021-09-15T16:44:37.574Z"
        }
    ]
}
```

Para obtener más información, consulte Ver instantáneas archivadas en la Guía del usuario de Amazon Elastic Compute Cloud.

- Para obtener información sobre la API, consulte DescribeSnapshotTierStatus en la Referencia de comandos de la AWS CLI.

`describe-snapshots`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-snapshots`.

AWS CLI

Ejemplo 1: Describir una instantánea

En el siguiente ejemplo de `describe-snapshots`, se describe la instantánea especificada.

```
aws ec2 describe-snapshots \
    --snapshot-ids snap-1234567890abcdef0
```

Salida:

```
{
    "Snapshots": [
        {
            "Description": "This is my snapshot",
            "Encrypted": false,
            "VolumeId": "vol-049df61146c4d7901",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2019-02-28T21:28:32.000Z",
            "Progress": "100%",
            "OwnerId": "012345678910",
            "SnapshotId": "snap-01234567890abcdef",
            "Tags": [
                {
                    "Key": "Stack",
                    "Value": "test"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Instantáneas de Amazon EBS en la Guía del usuario de Amazon EC2.

Ejemplo 2: Describir las instantáneas con base en filtros

En el siguiente ejemplo de `describe-snapshots`, se usan filtros para limitar los resultados a las instantáneas que son propiedad de su cuenta de AWS y cuyo estado es `pending`. En el ejemplo se usa el parámetro `--query` para mostrar solo los ID de las instantáneas y la hora en que se inició la instantánea.

```
aws ec2 describe-snapshots \
    --owner-ids self \
    --filters Name=status,Values=pending \
    --query "Snapshots[*].{ID:SnapshotId,Time:StartTime}"
```

Salida:

```
[
    {
        "ID": "snap-1234567890abcdef0",
        "Time": "2019-08-04T12:48:18.000Z"
    },
    {
        "ID": "snap-066877671789bd71b",
        "Time": "2019-08-04T02:45:16.000Z
    },
    ...
]
```

En el siguiente ejemplo de `describe-snapshots`, se usan filtros para limitar los resultados a las instantáneas creadas a partir del volumen especificado. En el ejemplo se usa el parámetro `--query` para mostrar solo los ID de las instantáneas.

```
aws ec2 describe-snapshots \
    --filters Name=volume-id,Values=049df61146c4d7901 \
    --query "Snapshots[*].[SnapshotId]" \
    --output text
```

Salida:

```
snap-1234567890abcdef0
snap-08637175a712c3fb9
...
```

Para ver ejemplos adicionales de uso de filtros, consulte Enumerar y filtrar los recursos en la Guía del usuario de Amazon EC2.

Ejemplo 3: describir las instantáneas con base en etiquetas

En el siguiente ejemplo de `describe-snapshots`, se usan filtros de etiquetas para limitar los resultados a las instantáneas que tienen la etiqueta `Stack=Prod`.

```
aws ec2 describe-snapshots \
    --filters Name=tag:Stack,Values=prod
```

Para ver un ejemplo del resultado de `describe-snapshots`, consulte el ejemplo 1.

Para ver ejemplos adicionales de uso de filtros de etiquetas, consulte Trabajo con etiquetas en la Guía del usuario de Amazon EC2.

Ejemplo 4: describir las instantáneas con base en la antigüedad

En el siguiente ejemplo de `describe-snapshots`, se usan expresiones de JMESPath para describir todas las instantáneas creadas en su cuenta de AWS antes de la fecha especificada. Solo se muestran los ID de las instantáneas.

```
aws ec2 describe-snapshots \
    --owner-ids 012345678910 \
    --query "Snapshots[?(StartTime<='2020-03-31')].[SnapshotId]"
```

Para ver ejemplos adicionales de uso de filtros, consulte Enumerar y filtrar los recursos en la Guía del usuario de Amazon EC2.

Ejemplo 5: ver solo las instantáneas archivadas

En el siguiente ejemplo de `describe-snapshots`, se muestran solo las instantáneas que se almacenan en el nivel de archivo.

```
aws ec2 describe-snapshots \
    --filters "Name=storage-tier,Values=archive"
```

Salida:

```
{
    "Snapshots": [
        {
```

```
            "Description": "Snap A",
            "Encrypted": false,
            "VolumeId": "vol-01234567890aaaaaa",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-09-07T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-01234567890aaaaaa",
            "StorageTier": "archive",
            "Tags": []
        },
    ]
}
```

Para obtener más información, consulte Ver instantáneas archivadas en la Guía del usuario de Amazon Elastic Compute Cloud.

- Para obtener información sobre la API, consulte DescribeSnapshots en la Referencia de comandos de la AWS CLI.

`describe-spot-datafeed-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-spot-datafeed-subscription`.

AWS CLI

Para describir la suscripción a una fuente de datos de instancia de spot para una cuenta

En este ejemplo de comando, se describe la fuente de datos de la cuenta.

Comando:

```
aws ec2 describe-spot-datafeed-subscription
```

Salida:

```
{
    "SpotDatafeedSubscription": {
        "OwnerId": "123456789012",
```

```
        "Prefix": "spotdata",
        "Bucket": "amzn-s3-demo-bucket",
        "State": "Active"
    }
}
```

- Para obtener información sobre la API, consulte DescribeSpotDatafeedSubscription en la Referencia de comandos de la AWS CLI.

`describe-spot-fleet-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-spot-fleet-instances`.

AWS CLI

Para describir las instancias de spot asociadas a una flota de spot

En este ejemplo de comando, se enumeran las instancias de spot asociadas a la flota de spot especificada.

Comando:

```
aws ec2 describe-spot-fleet-instances --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Salida:

```
{
  "ActiveInstances": [
      {
          "InstanceId": "i-1234567890abcdef0",
          "InstanceType": "m3.medium",
          "SpotInstanceRequestId": "sir-08b93456"
      },
      ...
  ],
  "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

- Para obtener información sobre la API, consulte DescribeSpotFleetInstances en la Referencia de comandos de la AWS CLI.

describe-spot-fleet-request-history

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-spot-fleet-request-history`.

AWS CLI

Para describir el historial de la flota de spot

En el siguiente ejemplo de comando se devuelve el historial de la flota de spot especificada a partir de la hora especificada.

Comando:

```
aws ec2 describe-spot-fleet-request-history --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE --start-time 2015-05-26T00:00:00Z
```

En el siguiente ejemplo de salida, se muestran los lanzamientos satisfactorios de dos instancias de spot para la flota de spot.

Salida:

```
{
  "HistoryRecords": [
      {
          "Timestamp": "2015-05-26T23:17:20.697Z",
          "EventInformation": {
              "EventSubType": "submitted"
          },
          "EventType": "fleetRequestChange"
      },
      {
          "Timestamp": "2015-05-26T23:17:20.873Z",
          "EventInformation": {
              "EventSubType": "active"
          },
          "EventType": "fleetRequestChange"
      },
      {
          "Timestamp": "2015-05-26T23:21:21.712Z",
          "EventInformation": {
              "InstanceId": "i-1234567890abcdef0",
              "EventSubType": "launched"
```

```
            },
            "EventType": "instanceChange"
        },
        {
            "Timestamp": "2015-05-26T23:21:21.816Z",
            "EventInformation": {
                "InstanceId": "i-1234567890abcdef1",
                "EventSubType": "launched"
            },
            "EventType": "instanceChange"
        }
    ],
    "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
    "NextToken": "CpHNsscimcV5oH7bSbub03CI2Qms5+ypNpNm
+53MNlR0YcXAkp0xFlfKf91yVxSExmbtma3awYxMFzNA663ZskT0AHtJ6TCb2Z8bQC2EnZgyELbymtWPfpZ1ZbauVg
+P+TfGlWxWWB/Vr5dk5d4LfdgA/DRAHUrYgxzrEXAMPLE=",
    "StartTime": "2015-05-26T00:00:00Z"
}
```

- Para obtener información sobre la API, consulte DescribeSpotFleetRequestHistory en la Referencia de comandos de la AWS CLI.

`describe-spot-fleet-requests`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-spot-fleet-requests`.

AWS CLI

Para describir solicitudes de flota de spot

En este ejemplo, se describen todas las solicitudes de su flota de spot.

Comando:

```
aws ec2 describe-spot-fleet-requests
```

Salida:

```
{
    "SpotFleetRequestConfigs": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "SpotFleetRequestConfig": {
```

```
            "TargetCapacity": 20,
            "LaunchSpecifications": [
                {
                    "EbsOptimized": false,
                    "NetworkInterfaces": [
                        {
                            "SubnetId": "subnet-a61dafcf",
                            "DeviceIndex": 0,
                            "DeleteOnTermination": false,
                            "AssociatePublicIpAddress": true,
                            "SecondaryPrivateIpAddressCount": 0
                        }
                    ],
                    "InstanceType": "cc2.8xlarge",
                    "ImageId": "ami-1a2b3c4d"
                },
                {
                    "EbsOptimized": false,
                    "NetworkInterfaces": [
                        {
                            "SubnetId": "subnet-a61dafcf",
                            "DeviceIndex": 0,
                            "DeleteOnTermination": false,
                            "AssociatePublicIpAddress": true,
                            "SecondaryPrivateIpAddressCount": 0
                        }
                    ],
                    "InstanceType": "r3.8xlarge",
                    "ImageId": "ami-1a2b3c4d"
                }
            ],
            "SpotPrice": "0.05",
            "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role"
        },
        "SpotFleetRequestState": "active"
    },
    {
        "SpotFleetRequestId": "sfr-306341ed-9739-402e-881b-ce47bEXAMPLE",
        "SpotFleetRequestConfig": {
            "TargetCapacity": 20,
            "LaunchSpecifications": [
                {
                    "EbsOptimized": false,
                    "NetworkInterfaces": [
```

```
                        {
                            "SubnetId": "subnet-6e7f829e",
                            "DeviceIndex": 0,
                            "DeleteOnTermination": false,
                            "AssociatePublicIpAddress": true,
                            "SecondaryPrivateIpAddressCount": 0
                        }
                    ],
                    "InstanceType": "m3.medium",
                    "ImageId": "ami-1a2b3c4d"
                }
            ],
            "SpotPrice": "0.05",
            "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role"
        },
        "SpotFleetRequestState": "active"
    }
  ]
}
```

Para describir una solicitud de flota de spot

En este ejemplo, se describe la solicitud de flota de spot especificada.

Comando:

```
aws ec2 describe-spot-fleet-requests --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Salida:

```
{
  "SpotFleetRequestConfigs": [
    {
        "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
        "SpotFleetRequestConfig": {
            "TargetCapacity": 20,
            "LaunchSpecifications": [
                {
                    "EbsOptimized": false,
                    "NetworkInterfaces": [
                        {
                            "SubnetId": "subnet-a61dafcf",
```

```
                            "DeviceIndex": 0,
                            "DeleteOnTermination": false,
                            "AssociatePublicIpAddress": true,
                            "SecondaryPrivateIpAddressCount": 0
                        }
                    ],
                    "InstanceType": "cc2.8xlarge",
                    "ImageId": "ami-1a2b3c4d"
                },
                {
                    "EbsOptimized": false,
                    "NetworkInterfaces": [
                        {
                            "SubnetId": "subnet-a61dafcf",
                            "DeviceIndex": 0,
                            "DeleteOnTermination": false,
                            "AssociatePublicIpAddress": true,
                            "SecondaryPrivateIpAddressCount": 0
                        }
                    ],
                    "InstanceType": "r3.8xlarge",
                    "ImageId": "ami-1a2b3c4d"
                }
            ],
            "SpotPrice": "0.05",
            "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role"
        },
        "SpotFleetRequestState": "active"
    }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeSpotFleetRequests en la Referencia de comandos de la AWS CLI.

`describe-spot-instance-requests`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-spot-instance-requests`.

AWS CLI

Ejemplo 1: descripción de una solicitud de instancia de spot

En el siguiente ejemplo de `describe-spot-instance-requests` se describe la solicitud de instancia de spot especificada.

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-08b93456
```

Salida:

```
{
    "SpotInstanceRequests": [
        {
            "CreateTime": "2018-04-30T18:14:55.000Z",
            "InstanceId": "i-1234567890abcdef1",
            "LaunchSpecification": {
                "InstanceType": "t2.micro",
                "ImageId": "ami-003634241a8fcdec0",
                "KeyName": "my-key-pair",
                "SecurityGroups": [
                    {
                        "GroupName": "default",
                        "GroupId": "sg-e38f24a7"
                    }
                ],
                "BlockDeviceMappings": [
                    {
                        "DeviceName": "/dev/sda1",
                        "Ebs": {
                            "DeleteOnTermination": true,
                            "SnapshotId": "snap-0e54a519c999adbbd",
                            "VolumeSize": 8,
                            "VolumeType": "standard",
                            "Encrypted": false
                        }
                    }
                ],
                "NetworkInterfaces": [
                    {
                        "DeleteOnTermination": true,
                        "DeviceIndex": 0,
                        "SubnetId": "subnet-049df61146c4d7901"
                    }
                ],
                "Placement": {
```

```
                    "AvailabilityZone": "us-east-2b",
                    "Tenancy": "default"
                },
                "Monitoring": {
                    "Enabled": false
                }
            },
            "LaunchedAvailabilityZone": "us-east-2b",
            "ProductDescription": "Linux/UNIX",
            "SpotInstanceRequestId": "sir-08b93456",
            "SpotPrice": "0.010000"
            "State": "active",
            "Status": {
                "Code": "fulfilled",
                "Message": "Your Spot request is fulfilled.",
                "UpdateTime": "2018-04-30T18:16:21.000Z"
            },
            "Tags": [],
            "Type": "one-time",
            "InstanceInterruptionBehavior": "terminate"
        }
    ]
}
```

Ejemplo 2: descripción de las solicitudes de instancia de spot basadas en filtros

En el siguiente ejemplo de `describe-spot-instance-requests` se usan filtros para limitar el ámbito de los resultados a las instancias de spot con el tipo de instancia especificado y de la zona de disponibilidad especificada. En el ejemplo se usa el parámetro `--query` para mostrar solo los ID de las instancias.

```
aws ec2 describe-spot-instance-requests \
    --filters Name=launch.instance-type,Values=m3.medium Name=launched-availability-zone,Values=us-east-2a \
    --query "SpotInstanceRequests[*].[InstanceId]" \
    --output text
```

Salida:

```
i-057750d42936e468a
i-001efd250faaa6ffa
i-027552a73f021f3bd
```

```
...
```

Para ver ejemplos adicionales de uso de filtros, consulte Enumerar y filtrar mediante la CLI y la API en la Guía del usuario de Amazon Elastic Compute Cloud.

Ejemplo 3: descripción de las solicitudes de instancia de spot basadas en etiquetas

En el siguiente ejemplo de `describe-spot-instance-requests` se usan filtros de etiquetas para limitar el ámbito de los resultados a las solicitudes de instancias de spot que tienen la etiqueta `cost-center=cc123`.

```
aws ec2 describe-spot-instance-requests \
    --filters Name=tag:cost-center,Values=cc123
```

Para ver un ejemplo del resultado de `describe-spot-instance-requests`, consulte el ejemplo 1.

Para ver ejemplos adicionales de uso de filtros de etiquetas, consulte Trabajo con etiquetas en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeSpotInstanceRequests en la Referencia de comandos de la AWS CLI.

`describe-spot-price-history`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-spot-price-history`.

AWS CLI

Para describir el historial de precios de spot

En este ejemplo de comando se devuelve el historial de precios de spot de las instancias m1.xlarge de un día concreto de enero.

Comando:

```
aws ec2 describe-spot-price-history --instance-types m1.xlarge --start-
time 2014-01-06T07:08:09 --end-time 2014-01-06T08:09:10
```

Salida:

```
{
```

```
  "SpotPriceHistory": [
          {
              "Timestamp": "2014-01-06T07:10:55.000Z",
              "ProductDescription": "SUSE Linux",
              "InstanceType": "m1.xlarge",
              "SpotPrice": "0.087000",
              "AvailabilityZone": "us-west-1b"
          },
          {
              "Timestamp": "2014-01-06T07:10:55.000Z",
              "ProductDescription": "SUSE Linux",
              "InstanceType": "m1.xlarge",
              "SpotPrice": "0.087000",
              "AvailabilityZone": "us-west-1c"
          },
          {
              "Timestamp": "2014-01-06T05:42:36.000Z",
              "ProductDescription": "SUSE Linux (Amazon VPC)",
              "InstanceType": "m1.xlarge",
              "SpotPrice": "0.087000",
              "AvailabilityZone": "us-west-1a"
      },
      ...
}
```

Para describir el historial de precios de spot de Amazon VPC para Linux/UNIX

En este ejemplo de comando, se devuelve el historial de precios de spot de las instancias m1.xlarge de Amazon VPC para Linux/UNIX de un día concreto de enero.

Comando:

```
aws ec2 describe-spot-price-history --instance-types m1.xlarge --product-
description "Linux/UNIX (Amazon VPC)" --start-time 2014-01-06T07:08:09 --end-
time 2014-01-06T08:09:10
```

Salida:

```
{
  "SpotPriceHistory": [
      {
          "Timestamp": "2014-01-06T04:32:53.000Z",
          "ProductDescription": "Linux/UNIX (Amazon VPC)",
```

```
            "InstanceType": "m1.xlarge",
            "SpotPrice": "0.080000",
            "AvailabilityZone": "us-west-1a"
        },
        {
            "Timestamp": "2014-01-05T11:28:26.000Z",
            "ProductDescription": "Linux/UNIX (Amazon VPC)",
            "InstanceType": "m1.xlarge",
            "SpotPrice": "0.080000",
            "AvailabilityZone": "us-west-1c"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeSpotPriceHistory en la Referencia de comandos de la AWS CLI.

`describe-stale-security-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stale-security-groups`.

AWS CLI

Para describir grupos de seguridad obsoletos

En este ejemplo, se describen las reglas de grupos de seguridad obsoletos de `vpc-11223344`. En la respuesta se muestra que el grupo de seguridad sg-5fa68d3a de su cuenta tiene una regla de SSH de entrada obsoleta que hace referencia al grupo de seguridad `sg-279ab042` en la VPC emparejada y que el grupo de seguridad `sg-fe6fba9a` de su cuenta tiene una regla de SSH de salida obsoleta que hace referencia al grupo de seguridad `sg-ef6fba8b` en la VPC emparejada.

Comando:

```
aws ec2 describe-stale-security-groups --vpc-id vpc-11223344
```

Salida:

```
{
    "StaleSecurityGroupSet": [
        {
            "VpcId": "vpc-11223344",
            "StaleIpPermissionsEgress": [
```

```
            {
                "ToPort": 22,
                "FromPort": 22,
                "UserIdGroupPairs": [
                    {
                        "VpcId": "vpc-7a20e51f",
                        "GroupId": "sg-ef6fba8b",
                        "VpcPeeringConnectionId": "pcx-b04deed9",
                        "PeeringStatus": "active"
                    }
                ],
                "IpProtocol": "tcp"
            }
        ],
        "GroupName": "MySG1",
        "StaleIpPermissions": [],
        "GroupId": "sg-fe6fba9a",
        "Description": MySG1"
    },
    {
        "VpcId": "vpc-11223344",
        "StaleIpPermissionsEgress": [],
        "GroupName": "MySG2",
        "StaleIpPermissions": [
            {
                "ToPort": 22,
                "FromPort": 22,
                "UserIdGroupPairs": [
                    {
                        "VpcId": "vpc-7a20e51f",
                        "GroupId": "sg-279ab042",
                        "Description": "Access from pcx-b04deed9",
                        "VpcPeeringConnectionId": "pcx-b04deed9",
                        "PeeringStatus": "active"
                    }
                ],
                "IpProtocol": "tcp"
            }
        ],
        "GroupId": "sg-5fa68d3a",
        "Description": "MySG2"
    }
]
```

```
}
```

- Para obtener información sobre la API, consulte DescribeStaleSecurityGroups en la Referencia de comandos de la AWS CLI.

`describe-store-image-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-store-image-tasks`.

AWS CLI

Para describir el progreso de una tarea de almacén de AMI

En el siguiente ejemplo de `describe-store-image-tasks` se describe el progreso de una tarea de almacén de AMI.

```
aws ec2 describe-store-image-tasks
```

Salida:

```
{
    "StoreImageTaskResults": [
        {
            "AmiId": "ami-1234567890abcdef0",
            "Bucket": "my-ami-bucket",
            "ProgressPercentage": 17,
            "S3objectKey": "ami-1234567890abcdef0.bin",
            "StoreTaskState": "InProgress",
            "StoreTaskFailureReason": null,
            "TaskStartTime": "2022-01-01T01:01:01.001Z"
        }
    ]
}
```

Para obtener más información sobre el almacenamiento y la restauración de una AMI mediante S3, consulte Almacenar y restaurar una AMI mediante S3 <https://docs.aws.amazon.com/AWSec2/latest/UserGuide/AMI-Store-Restore.html> en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeStoreImageTasks en la Referencia de comandos de la AWS CLI.

describe-subnets

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-subnets`.

AWS CLI

Ejemplo 1: Describir todas las subredes

En el siguiente ejemplo de `describe-subnets`, se muestran los detalles de las subredes.

```
aws ec2 describe-subnets
```

Salida:

```
{
    "Subnets": [
        {
            "AvailabilityZone": "us-east-1d",
            "AvailabilityZoneId": "use1-az2",
            "AvailableIpAddressCount": 4089,
            "CidrBlock": "172.31.80.0/20",
            "DefaultForAz": true,
            "MapPublicIpOnLaunch": false,
            "MapCustomerOwnedIpOnLaunch": true,
            "State": "available",
            "SubnetId": "subnet-0bb1c79de3EXAMPLE",
            "VpcId": "vpc-0ee975135dEXAMPLE",
            "OwnerId": "111122223333",
            "AssignIpv6AddressOnCreation": false,
            "Ipv6CidrBlockAssociationSet": [],
            "CustomerOwnedIpv4Pool:": 'pool-2EXAMPLE',
            "SubnetArn": "arn:aws:ec2:us-east-2:111122223333:subnet/
subnet-0bb1c79de3EXAMPLE",
            "EnableDns64": false,
            "Ipv6Native": false,
            "PrivateDnsNameOptionsOnLaunch": {
                "HostnameType": "ip-name",
                "EnableResourceNameDnsARecord": false,
                "EnableResourceNameDnsAAAARecord": false
            }
        },
        {
            "AvailabilityZone": "us-east-1d",
```

```
            "AvailabilityZoneId": "use1-az2",
            "AvailableIpAddressCount": 4089,
            "CidrBlock": "172.31.80.0/20",
            "DefaultForAz": true,
            "MapPublicIpOnLaunch": true,
            "MapCustomerOwnedIpOnLaunch": false,
            "State": "available",
            "SubnetId": "subnet-8EXAMPLE",
            "VpcId": "vpc-3EXAMPLE",
            "OwnerId": "1111222233333",
            "AssignIpv6AddressOnCreation": false,
            "Ipv6CidrBlockAssociationSet": [],
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "MySubnet"
                }
            ],
            "SubnetArn": "arn:aws:ec2:us-east-1:111122223333:subnet/
subnet-8EXAMPLE",
            "EnableDns64": false,
            "Ipv6Native": false,
            "PrivateDnsNameOptionsOnLaunch": {
                "HostnameType": "ip-name",
                "EnableResourceNameDnsARecord": false,
                "EnableResourceNameDnsAAAARecord": false
            }
        }
    ]
}
```

Para obtener más información, consulte Trabajo con VPC y subredes en la Guía del usuario de AWS VPC.

Ejemplo 2: Describir las subredes de una VPC específica

En el ejemplo siguiente de `describe-subnets` se utiliza un filtro para recuperar detalles de las subredes de la VPC especificada.

```
aws ec2 describe-subnets \
    --filters "Name=vpc-id,Values=vpc-3EXAMPLE"
```

Salida:

```
{
    "Subnets": [
        {
            "AvailabilityZone": "us-east-1d",
            "AvailabilityZoneId": "use1-az2",
            "AvailableIpAddressCount": 4089,
            "CidrBlock": "172.31.80.0/20",
            "DefaultForAz": true,
            "MapPublicIpOnLaunch": true,
            "MapCustomerOwnedIpOnLaunch": false,
            "State": "available",
            "SubnetId": "subnet-8EXAMPLE",
            "VpcId": "vpc-3EXAMPLE",
            "OwnerId": "1111222233333",
            "AssignIpv6AddressOnCreation": false,
            "Ipv6CidrBlockAssociationSet": [],
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "MySubnet"
                }
            ],
            "SubnetArn": "arn:aws:ec2:us-east-1:111122223333:subnet/
subnet-8EXAMPLE",
            "EnableDns64": false,
            "Ipv6Native": false,
            "PrivateDnsNameOptionsOnLaunch": {
                "HostnameType": "ip-name",
                "EnableResourceNameDnsARecord": false,
                "EnableResourceNameDnsAAAARecord": false
            }
        }
    ]
}
```


Para obtener más información, consulte Trabajo con VPC y subredes en la Guía del usuario de AWS VPC.

Ejemplo 3: describir las subredes con una etiqueta específica

En el siguiente ejemplo de `describe-subnets`, se usa un filtro para recuperar los detalles de las subredes con la etiqueta `CostCenter=123` y el parámetro `--query` a fin de mostrar los ID de subred de las subredes con esta etiqueta.

```
aws ec2 describe-subnets \
    --filters "Name=tag:CostCenter,Values=123" \
    --query "Subnets[*].SubnetId" \
    --output text
```

Salida:

```
subnet-0987a87c8b37348ef
subnet-02a95061c45f372ee
subnet-03f720e7de2788d73
```

Para obtener más información, consulte Trabajo con VPC y subredes en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte DescribeSubnets en la Referencia de comandos de la AWS CLI.

`describe-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-tags`.

AWS CLI

Ejemplo 1: descripción de todas las etiquetas de un único recurso

En el siguiente ejemplo de `describe-tags` se describen las etiquetas de la instancia especificada.

```
aws ec2 describe-tags \
    --filters "Name=resource-id,Values=i-1234567890abcdef8"
```

Salida:

```
{
    "Tags": [
        {
            "ResourceType": "instance",
            "ResourceId": "i-1234567890abcdef8",
            "Value": "Test",
            "Key": "Stack"
```

```
        },
        {
            "ResourceType": "instance",
            "ResourceId": "i-1234567890abcdef8",
            "Value": "Beta Server",
            "Key": "Name"
        }
    ]
}
```

Ejemplo 2: descripción de todas las etiquetas de un tipo de recurso

En el siguiente ejemplo de `describe-tags` se describen las etiquetas de sus volúmenes.

```
aws ec2 describe-tags \
    --filters "Name=resource-type,Values=volume"
```

Salida:

```
{
    "Tags": [
        {
            "ResourceType": "volume",
            "ResourceId": "vol-1234567890abcdef0",
            "Value": "Project1",
            "Key": "Purpose"
        },
        {
            "ResourceType": "volume",
            "ResourceId": "vol-049df61146c4d7901",
            "Value": "Logs",
            "Key": "Purpose"
        }
    ]
}
```

Ejemplo 3: descripción de todas las etiquetas

En el siguiente ejemplo de `describe-tags` se describen las etiquetas de todos sus recursos.

```
aws ec2 describe-tags
```

Ejemplo 4: descripción de las etiquetas de los recursos en función de una clave de etiqueta

En el siguiente ejemplo de `describe-tags` se describen las etiquetas de sus recursos que tienen una etiqueta con la clave `Stack`.

```
aws ec2 describe-tags \
    --filters Name=key,Values=Stack
```

Salida:

```
{
    "Tags": [
        {
            "ResourceType": "volume",
            "ResourceId": "vol-027552a73f021f3b",
            "Value": "Production",
            "Key": "Stack"
        },
        {
            "ResourceType": "instance",
            "ResourceId": "i-1234567890abcdef8",
            "Value": "Test",
            "Key": "Stack"
        }
    ]
}
```

Ejemplo 5: descripción de las etiquetas de los recursos en función de una clave de etiqueta y un valor de etiqueta

En el siguiente ejemplo de `describe-tags` se describen las etiquetas de sus recursos que tienen la etiqueta `Stack=Test`.

```
aws ec2 describe-tags \
    --filters Name=key,Values=Stack Name=value,Values=Test
```

Salida:

```
{
    "Tags": [
        {
            "ResourceType": "image",
```

```
            "ResourceId": "ami-3ac336533f021f3bd",
            "Value": "Test",
            "Key": "Stack"
        },
        {
            "ResourceType": "instance",
            "ResourceId": "i-1234567890abcdef8",
            "Value": "Test",
            "Key": "Stack"
        }
    ]
}
```

En el siguiente ejemplo de `describe-tags` se utiliza una sintaxis alternativa para describir los recursos con la etiqueta `Stack=Test`.

```
aws ec2 describe-tags \
    --filters "Name=tag:Stack,Values=Test"
```

En el siguiente ejemplo de `describe-tags` se describen las etiquetas de todas sus instancias que tienen una etiqueta con la clave `Purpose` y ningún valor.

```
aws ec2 describe-tags \
    --filters "Name=resource-
type,Values=instance" "Name=key,Values=Purpose" "Name=value,Values="
```

Salida:

```
{
    "Tags": [
        {
            "ResourceType": "instance",
            "ResourceId": "i-1234567890abcdef5",
            "Value": null,
            "Key": "Purpose"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeTags en la Referencia de comandos de la AWS CLI.

`describe-traffic-mirror-filters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-traffic-mirror-filters`.

AWS CLI

Para ver los filtros de reflejo de tráfico

En el siguiente ejemplo de `describe-traffic-mirror-filters` se muestra la información de todos sus filtros de registro de tráfico.

```
aws ec2 describe-traffic-mirror-filters
```

Salida:

```
{
    "TrafficMirrorFilters": [
        {
            "TrafficMirrorFilterId": "tmf-0293f26e86EXAMPLE",
            "IngressFilterRules": [
                {
                    "TrafficMirrorFilterRuleId": "tmfr-0ca76e0e08EXAMPLE",
                    "TrafficMirrorFilterId": "tmf-0293f26e86EXAMPLE",
                    "TrafficDirection": "ingress",
                    "RuleNumber": 100,
                    "RuleAction": "accept",
                    "Protocol": 6,
                    "DestinationCidrBlock": "10.0.0.0/24",
                    "SourceCidrBlock": "10.0.0.0/24",
                    "Description": "TCP Rule"
                }
            ],
            "EgressFilterRules": [],
            "NetworkServices": [],
            "Description": "Example filter",
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte View your traffic mirror filters en la Guía de creación de reflejo de tráfico.

- Para obtener información sobre la API, consulte DescribeTrafficMirrorFilters en la Referencia de comandos de la AWS CLI.

`describe-traffic-mirror-sessions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-traffic-mirror-sessions`.

AWS CLI

Para describir una sesión de reflejo de tráfico

En el siguiente ejemplo de `describe-traffic-mirror-sessions` se muestra la información de todas sus sesiones de registro de tráfico.

```
aws ec2 describe-traffic-mirror-sessions
```

Salida:

```
{
    "TrafficMirrorSessions": [
        {
            "Tags": [],
            "VirtualNetworkId": 42,
            "OwnerId": "111122223333",
            "Description": "TCP Session",
            "NetworkInterfaceId": "eni-0a471a5cf3EXAMPLE",
            "TrafficMirrorTargetId": "tmt-0dabe9b0a6EXAMPLE",
            "TrafficMirrorFilterId": "tmf-083e18f985EXAMPLE",
            "PacketLength": 20,
            "SessionNumber": 1,
            "TrafficMirrorSessionId": "tms-0567a4c684EXAMPLE"
        },
        {
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "tag test"
                }
            ],
            "VirtualNetworkId": 13314501,
            "OwnerId": "111122223333",
```

```
            "Description": "TCP Session",
            "NetworkInterfaceId": "eni-0a471a5cf3EXAMPLE",
            "TrafficMirrorTargetId": "tmt-03665551cbEXAMPLE",
            "TrafficMirrorFilterId": "tmf-06c787846cEXAMPLE",
            "SessionNumber": 2,
            "TrafficMirrorSessionId": "tms-0060101cf8EXAMPLE"
        }
    ]
}
```

Para obtener más información, consulte View Traffic Mirror Session Details en la Guía de creación de reflejo de tráfico de AWS.

- Para obtener información sobre la API, consulte DescribeTrafficMirrorSessions en la Referencia de comandos de la AWS CLI.

`describe-traffic-mirror-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-traffic-mirror-targets`.

AWS CLI

Para describir un destino de reflejo de tráfico

En el siguiente ejemplo de `describe-traffic-mirror-targets` se muestra información sobre el destino de reflejo de tráfico especificado.

```
aws ec2 describe-traffic-mirror-targets \
    --traffic-mirror-target-ids tmt-0dabe9b0a6EXAMPLE
```

Salida:

```
{
    "TrafficMirrorTargets": [
        {
            "TrafficMirrorTargetId": "tmt-0dabe9b0a6EXAMPLE",
            "NetworkLoadBalancerArn": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/net/NLB/7cdec873fEXAMPLE",
            "Type": "network-load-balancer",
            "Description": "Example Network Load Balancer target",
            "OwnerId": "111122223333",
```

```
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Traffic mirror targets en la Guía de creación de reflejo de tráfico de Amazon VPC.

- Para obtener información sobre la API, consulte DescribeTrafficMirrorTargets en la Referencia de comandos de la AWS CLI.

`describe-transit-gateway-attachments`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-transit-gateway-attachments`.

AWS CLI

Para ver las conexiones de las puertas de enlace de tránsito

En el siguiente ejemplo de `describe-transit-gateway-attachments` se muestra la información de las conexiones de puerta de enlace de tránsito.

```
aws ec2 describe-transit-gateway-attachments
```

Salida:

```
{
    "TransitGatewayAttachments": [
        {
            "TransitGatewayAttachmentId": "tgw-attach-01f8100bc7EXAMPLE",
            "TransitGatewayId": "tgw-02f776b1a7EXAMPLE",
            "TransitGatewayOwnerId": "123456789012",
            "ResourceOwnerId": "123456789012",
            "ResourceType": "vpc",
            "ResourceId": "vpc-3EXAMPLE",
            "State": "available",
            "Association": {
                "TransitGatewayRouteTableId": "tgw-rtb-002573ed1eEXAMPLE",
                "State": "associated"
            },
            "CreationTime": "2019-08-26T14:59:25.000Z",
```

```
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Example"
                }
            ]
        },
        {
            "TransitGatewayAttachmentId": "tgw-attach-0b5968d3b6EXAMPLE",
            "TransitGatewayId": "tgw-02f776b1a7EXAMPLE",
            "TransitGatewayOwnerId": "123456789012",
            "ResourceOwnerId": "123456789012",
            "ResourceType": "vpc",
            "ResourceId": "vpc-0065acced4EXAMPLE",
            "State": "available",
            "Association": {
                "TransitGatewayRouteTableId": "tgw-rtb-002573ed1eEXAMPLE",
                "State": "associated"
            },
            "CreationTime": "2019-08-07T17:03:07.000Z",
            "Tags": []
        },
        {
            "TransitGatewayAttachmentId": "tgw-attach-08e0bc912cEXAMPLE",
            "TransitGatewayId": "tgw-02f776b1a7EXAMPLE",
            "TransitGatewayOwnerId": "123456789012",
            "ResourceOwnerId": "123456789012",
            "ResourceType": "direct-connect-gateway",
            "ResourceId": "11460968-4ac1-4fd3-bdb2-00599EXAMPLE",
            "State": "available",
            "Association": {
                "TransitGatewayRouteTableId": "tgw-rtb-002573ed1eEXAMPLE",
                "State": "associated"
            },
            "CreationTime": "2019-08-14T20:27:44.000Z",
            "Tags": []
        },
        {
            "TransitGatewayAttachmentId": "tgw-attach-0a89069f57EXAMPLE",
            "TransitGatewayId": "tgw-02f776b1a7EXAMPLE",
            "TransitGatewayOwnerId": "123456789012",
            "ResourceOwnerId": "123456789012",
            "ResourceType": "direct-connect-gateway",
            "ResourceId": "8384da05-13ce-4a91-aada-5a1baEXAMPLE",
```

```
            "State": "available",
            "Association": {
                "TransitGatewayRouteTableId": "tgw-rtb-002573ed1eEXAMPLE",
                "State": "associated"
            },
            "CreationTime": "2019-08-14T20:33:02.000Z",
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Work with transit gateways en la Guía de Transit Gateways.

- Para obtener información sobre la API, consulte DescribeTransitGatewayAttachments en la Referencia de comandos de la AWS CLI.

`describe-transit-gateway-connect-peers`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-transit-gateway-connect-peers`.

AWS CLI

Para describir un emparejamiento de Transit Gateway Connect

En el siguiente ejemplo de `describe-transit-gateway-connect-peers` se describe el emparejamiento de Connect especificado.

```
aws ec2 describe-transit-gateway-connect-peers \
    --transit-gateway-connect-peer-ids tgw-connect-peer-0666adbac4EXAMPLE
```

Salida:

```
{
    "TransitGatewayConnectPeers": [
        {
            "TransitGatewayAttachmentId": "tgw-attach-0f0927767cEXAMPLE",
            "TransitGatewayConnectPeerId": "tgw-connect-peer-0666adbac4EXAMPLE",
            "State": "available",
            "CreationTime": "2021-10-13T03:35:17.000Z",
```

```
            "ConnectPeerConfiguration": {
                "TransitGatewayAddress": "10.0.0.234",
                "PeerAddress": "172.31.1.11",
                "InsideCidrBlocks": [
                    "169.254.6.0/29"
                ],
                "Protocol": "gre",
                "BgpConfigurations": [
                    {
                        "TransitGatewayAsn": 64512,
                        "PeerAsn": 64512,
                        "TransitGatewayAddress": "169.254.6.2",
                        "PeerAddress": "169.254.6.1",
                        "BgpStatus": "down"
                    },
                    {
                        "TransitGatewayAsn": 64512,
                        "PeerAsn": 64512,
                        "TransitGatewayAddress": "169.254.6.3",
                        "PeerAddress": "169.254.6.1",
                        "BgpStatus": "down"
                    }
                ]
            },
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Transit gateway Connect attachments and Transit Gateway Connect peers en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DescribeTransitGatewayConnectPeers en la Referencia de comandos de la AWS CLI.

`describe-transit-gateway-connects`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-transit-gateway-connects`.

AWS CLI

Para describir una conexión de Transit Gateway Connect

En el siguiente ejemplo de `describe-transit-gateway-connects` se describe la conexión de Connect especificada.

```
aws ec2 describe-transit-gateway-connects \
    --transit-gateway-attachment-ids tgw-attach-037012e5dcEXAMPLE
```

Salida:

```
{
    "TransitGatewayConnects": [
        {
            "TransitGatewayAttachmentId": "tgw-attach-037012e5dcEXAMPLE",
            "TransportTransitGatewayAttachmentId": "tgw-attach-0a89069f57EXAMPLE",
            "TransitGatewayId": "tgw-02f776b1a7EXAMPLE",
            "State": "available",
            "CreationTime": "2021-03-09T19:59:17+00:00",
            "Options": {
                "Protocol": "gre"
            },
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Transit gateway Connect attachments and Transit Gateway Connect peers en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DescribeTransitGatewayConnects en la Referencia de comandos de la AWS CLI.

`describe-transit-gateway-multicast-domains`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-transit-gateway-multicast-domains`.

AWS CLI

Para describir los dominios de multidifusión de puerta de enlace de tránsito

En el siguiente ejemplo de `describe-transit-gateway-multicast-domains` se muestra información de todos sus dominios de multidifusión de puerta de enlace de tránsito.

```
aws ec2 describe-transit-gateway-multicast-domains
```

Salida:

```
{

    "TransitGatewayMulticastDomains": [
        {
            "TransitGatewayMulticastDomainId": "tgw-mcast-domain-000fb24d04EXAMPLE",
            "TransitGatewayId": "tgw-0bf0bffefaEXAMPLE",
            "TransitGatewayMulticastDomainArn": "arn:aws:ec2:us-
east-1:123456789012:transit-gateway-multicast-domain/tgw-mcast-
domain-000fb24d04EXAMPLE",
            "OwnerId": "123456789012",
            "Options": {
                "Igmpv2Support": "disable",
                "StaticSourcesSupport": "enable",
                "AutoAcceptSharedAssociations": "disable"
            },
            "State": "available",
            "CreationTime": "2019-12-10T18:32:50+00:00",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "mc1"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Managing multicast domains en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DescribeTransitGatewayMulticastDomains en la Referencia de comandos de la AWS CLI.

`describe-transit-gateway-peering-attachments`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-transit-gateway-peering-attachments`.

AWS CLI

Para describir las conexiones de emparejamiento de puerta de enlace de tránsito

En el siguiente ejemplo de `describe-transit-gateway-peering-attachments` se muestra la información de todas sus conexiones de emparejamiento de puerta de enlace de tránsito.

```
aws ec2 describe-transit-gateway-peering-attachments
```

Salida:

```
{
    "TransitGatewayPeeringAttachments": [
        {
            "TransitGatewayAttachmentId": "tgw-attach-4455667788aabbccd",
            "RequesterTgwInfo": {
                "TransitGatewayId": "tgw-123abc05e04123abc",
                "OwnerId": "123456789012",
                "Region": "us-west-2"
            },
            "AccepterTgwInfo": {
                "TransitGatewayId": "tgw-11223344aabbcc112",
                "OwnerId": "123456789012",
                "Region": "us-east-2"
            },
            "State": "pendingAcceptance",
            "CreationTime": "2019-12-09T11:38:05.000Z",
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Transit Gateway Peering Attachments en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DescribeTransitGatewayPeeringAttachments en la Referencia de comandos de la AWS CLI.

`describe-transit-gateway-policy-tables`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-transit-gateway-policy-tables`.

AWS CLI

Para describir una tabla de políticas de puerta de enlace de tránsito

En el siguiente ejemplo de `describe-transit-gateway-policy-tables` se describe la tabla de políticas de puerta de enlace de tránsito especificada.

```
aws ec2 describe-transit-gateway-policy-tables \
    --transit-gateway-policy-table-ids tgw-ptb-0a16f134b78668a81
```

Salida:

```
{
    "TransitGatewayPolicyTables": [
        {
            "TransitGatewayPolicyTableId": "tgw-ptb-0a16f134b78668a81",
            "TransitGatewayId": "tgw-067f8505c18f0bd6e",
            "State": "available",
            "CreationTime": "2023-11-28T16:36:43+00:00",
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Transit gateway policy tables en la Guía del usuario de Transit Gateway.

- Para obtener información sobre la API, consulte DescribeTransitGatewayPolicyTables en la Referencia de comandos de la AWS CLI.

`describe-transit-gateway-route-tables`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-transit-gateway-route-tables`.

AWS CLI

Para describir las tablas de enrutamiento de puerta de enlace de tránsito

En el siguiente ejemplo de `describe-transit-gateway-route-tables` se muestra la información de sus tablas de enrutamiento de puerta de enlace de tránsito.

```
aws ec2 describe-transit-gateway-route-tables
```

Salida:

```
{
    "TransitGatewayRouteTables": [
        {
            "TransitGatewayRouteTableId": "tgw-rtb-0ca78a549EXAMPLE",
            "TransitGatewayId": "tgw-0bc994abffEXAMPLE",
            "State": "available",
            "DefaultAssociationRouteTable": true,
            "DefaultPropagationRouteTable": true,
            "CreationTime": "2018-11-28T14:24:49.000Z",
            "Tags": []
        },
        {
            "TransitGatewayRouteTableId": "tgw-rtb-0e8f48f148EXAMPLE",
            "TransitGatewayId": "tgw-0043d72bb4EXAMPLE",
            "State": "available",
            "DefaultAssociationRouteTable": true,
            "DefaultPropagationRouteTable": true,
            "CreationTime": "2018-11-28T14:24:00.000Z",
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte View transit gateway route tables en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DescribeTransitGatewayRouteTables en la Referencia de comandos de la AWS CLI.

`describe-transit-gateway-vpc-attachments`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-transit-gateway-vpc-attachments`.

AWS CLI

Para describir las conexiones de VPC de puerta de enlace de tránsito

En el siguiente ejemplo de `describe-transit-gateway-vpc-attachments` se muestra la información de las conexiones de VPC de puerta de enlace de tránsito.

```
aws ec2 describe-transit-gateway-vpc-attachments
```

Salida:

```
{
    "TransitGatewayVpcAttachments": [
        {
            "TransitGatewayAttachmentId": "tgw-attach-0a08e88308EXAMPLE",
            "TransitGatewayId": "tgw-0043d72bb4EXAMPLE",
            "VpcId": "vpc-0f501f7ee8EXAMPLE",
            "VpcOwnerId": "111122223333",
            "State": "available",
            "SubnetIds": [
                "subnet-045d586432EXAMPLE",
                "subnet-0a0ad478a6EXAMPLE"
            ],
            "CreationTime": "2019-02-13T11:04:02.000Z",
            "Options": {
                "DnsSupport": "enable",
                "Ipv6Support": "disable"
            },
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "attachment name"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte View your VPC attachments en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DescribeTransitGatewayVpcAttachments en la Referencia de comandos de la AWS CLI.

`describe-transit-gateways`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-transit-gateways`.

AWS CLI

Para describir las puertas de enlace de tránsito

En el siguiente ejemplo de `describe-transit-gateways` se recuperan los detalles sobre sus puertas de enlace de tránsito.

```
aws ec2 describe-transit-gateways
```

Salida:

```
{
    "TransitGateways": [
        {
            "TransitGatewayId": "tgw-0262a0e521EXAMPLE",
            "TransitGatewayArn": "arn:aws:ec2:us-east-2:111122223333:transit-
gateway/tgw-0262a0e521EXAMPLE",
            "State": "available",
            "OwnerId": "111122223333",
            "Description": "MyTGW",
            "CreationTime": "2019-07-10T14:02:12.000Z",
            "Options": {
                "AmazonSideAsn": 64516,
                "AutoAcceptSharedAttachments": "enable",
                "DefaultRouteTableAssociation": "enable",
                "AssociationDefaultRouteTableId": "tgw-rtb-018774adf3EXAMPLE",
                "DefaultRouteTablePropagation": "enable",
                "PropagationDefaultRouteTableId": "tgw-rtb-018774adf3EXAMPLE",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable"
            },
            "Tags": []
```

```
        },
        {
            "TransitGatewayId": "tgw-0fb8421e2dEXAMPLE",
            "TransitGatewayArn": "arn:aws:ec2:us-east-2:111122223333:transit-
gateway/tgw-0fb8421e2da853bf3",
            "State": "available",
            "OwnerId": "111122223333",
            "CreationTime": "2019-03-15T22:57:33.000Z",
            "Options": {
                "AmazonSideAsn": 65412,
                "AutoAcceptSharedAttachments": "disable",
                "DefaultRouteTableAssociation": "enable",
                "AssociationDefaultRouteTableId": "tgw-rtb-06a241a3d8EXAMPLE",
                "DefaultRouteTablePropagation": "enable",
                "PropagationDefaultRouteTableId": "tgw-rtb-06a241a3d8EXAMPLE",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable"
            },
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "TGW1"
                }
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeTransitGateways en la Referencia de comandos de la AWS CLI.

`describe-verified-access-endpoints`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-verified-access-endpoints`.

AWS CLI

Para describir un punto de conexión de Acceso verificado

En el siguiente ejemplo de `describe-verified-access-endpoints`, se describe el punto de conexión de Acceso verificado especificado.

```
aws ec2 describe-verified-access-endpoints \
    --verified-access-endpoint-ids vae-066fac616d4d546f2
```

Salida:

```
{
    "VerifiedAccessEndpoints": [
        {
            "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
            "VerifiedAccessGroupId": "vagr-0dbe967baf14b7235",
            "VerifiedAccessEndpointId": "vae-066fac616d4d546f2",
            "ApplicationDomain": "example.com",
            "EndpointType": "network-interface",
            "AttachmentType": "vpc",
            "DomainCertificateArn": "arn:aws:acm:us-east-2:123456789012:certificate/
eb065ea0-26f9-4e75-a6ce-0a1a7EXAMPLE",
            "EndpointDomain": "my-ava-
app.edge-00c3372d53b1540bb.vai-0ce000c0b7643abea.prod.verified-access.us-
east-2.amazonaws.com",
            "SecurityGroupIds": [
                "sg-004915970c4c8f13a"
            ],
            "NetworkInterfaceOptions": {
                "NetworkInterfaceId": "eni-0aec70418c8d87a0f",
                "Protocol": "https",
                "Port": 443
            },
            "Status": {
                "Code": "active"
            },
            "Description": "",
            "CreationTime": "2023-08-25T20:54:43",
            "LastUpdatedTime": "2023-08-25T22:17:26",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "my-va-endpoint"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Verified Access endpoints en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte DescribeVerifiedAccessEndpoints en la Referencia de comandos de la AWS CLI.

`describe-verified-access-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-verified-access-groups`.

AWS CLI

Para describir un grupo de Acceso verificado

En el siguiente ejemplo de `describe-verified-access-groups`, se describe el grupo de Acceso verificado especificado.

```
aws ec2 describe-verified-access-groups \
    --verified-access-group-ids vagr-0dbe967baf14b7235
```

Salida:

```
{
    "VerifiedAccessGroups": [
        {
            "VerifiedAccessGroupId": "vagr-0dbe967baf14b7235",
            "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
            "Description": "Testing Verified Access",
            "Owner": "123456789012",
            "VerifiedAccessGroupArn": "arn:aws:ec2:us-east-2:123456789012:verified-
access-group/vagr-0dbe967baf14b7235",
            "CreationTime": "2023-08-25T19:55:19",
            "LastUpdatedTime": "2023-08-25T22:17:25",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "my-va-group"
                }
            ]
        }
    ]
```

```
}
```

Para obtener más información, consulte Verified Access groups en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte DescribeVerifiedAccessGroups en la Referencia de comandos de la AWS CLI.

`describe-verified-access-instance-logging-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-verified-access-instance-logging-configurations`.

AWS CLI

Para describir la configuración de registro de una instancia de Acceso verificado

En el siguiente ejemplo de `describe-verified-access-instance-logging-configurations`, se describe la configuración de registro de la instancia de Acceso verificado especificada.

```
aws ec2 describe-verified-access-instance-logging-configurations \
    --verified-access-instance-ids vai-0ce000c0b7643abea
```

Salida:

```
{
    "LoggingConfigurations": [
        {
            "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
            "AccessLogs": {
                "S3": {
                    "Enabled": false
                },
                "CloudWatchLogs": {
                    "Enabled": true,
                    "DeliveryStatus": {
                        "Code": "success"
                    },
                    "LogGroup": "my-log-group"
                },
                "KinesisDataFirehose": {
```

```
                    "Enabled": false
                },
                "LogVersion": "ocsf-1.0.0-rc.2",
                "IncludeTrustContext": false
            }
        }
    ]
}
```

Para obtener más información, consulte Verified Access logs en la Guía del usuario de acceso verificado de AWS.

- Para obtener información sobre la API, consulte DescribeVerifiedAccessInstanceLoggingConfigurations en la Referencia de comandos de la AWS CLI.

`describe-verified-access-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-verified-access-instances`.

AWS CLI

Para describir una instancia de Acceso verificado

En el siguiente ejemplo de `describe-verified-access-instances`, se describe la instancia de Acceso verificado especificada.

```
aws ec2 describe-verified-access-instances \
    --verified-access-instance-ids vai-0ce000c0b7643abea
```

Salida:

```
{
    "VerifiedAccessInstances": [
        {
            "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
            "Description": "Testing Verified Access",
            "VerifiedAccessTrustProviders": [
                {
                    "VerifiedAccessTrustProviderId": "vatp-0bb32de759a3e19e7",
                    "TrustProviderType": "user",
```

```
                    "UserTrustProviderType": "iam-identity-center"
                }
            ],
            "CreationTime": "2023-08-25T18:27:56",
            "LastUpdatedTime": "2023-08-25T19:03:32",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "my-ava-instance"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Verified Access instances en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte DescribeVerifiedAccessInstances en la Referencia de comandos de la AWS CLI.

`describe-verified-access-trust-providers`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-verified-access-trust-providers`.

AWS CLI

Para describir un proveedor de confianza de Acceso verificado

En el siguiente ejemplo de `describe-verified-access-trust-providers`, se describe el proveedor de confianza de Acceso verificado especificado.

```
aws ec2 describe-verified-access-trust-providers \
    --verified-access-trust-provider-ids vatp-0bb32de759a3e19e7
```

Salida:

```
{
    "VerifiedAccessTrustProviders": [
        {
            "VerifiedAccessTrustProviderId": "vatp-0bb32de759a3e19e7",
```

```
            "Description": "Testing Verified Access",
            "TrustProviderType": "user",
            "UserTrustProviderType": "iam-identity-center",
            "PolicyReferenceName": "idc",
            "CreationTime": "2023-08-25T19:00:38",
            "LastUpdatedTime": "2023-08-25T19:03:32",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "my-va-trust-provider"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Trust providers for Verified Access en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte DescribeVerifiedAccessTrustProviders en la Referencia de comandos de la AWS CLI.

`describe-volume-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-volume-attribute`.

AWS CLI

Para describir un atributo de volumen

En este comando de ejemplo se describe el atributo de `autoEnableIo` del volumen con el ID `vol-049df61146c4d7901`.

Comando:

```
aws ec2 describe-volume-attribute --volume-id vol-049df61146c4d7901 --
attribute autoEnableIO
```

Salida:

```
{
    "AutoEnableIO": {
```

```
        "Value": false
    },
    "VolumeId": "vol-049df61146c4d7901"
}
```

- Para obtener información sobre la API, consulte DescribeVolumeAttribute en la Referencia de comandos de la AWS CLI.

`describe-volume-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-volume-status`.

AWS CLI

Para describir el estado de un solo volumen

En este ejemplo de comando, se describe el estado del volumen `vol-1234567890abcdef0`.

Comando:

```
aws ec2 describe-volume-status --volume-ids vol-1234567890abcdef0
```

Salida:

```
{
    "VolumeStatuses": [
        {
            "VolumeStatus": {
                "Status": "ok",
                "Details": [
                    {
                        "Status": "passed",
                        "Name": "io-enabled"
                    },
                    {
                        "Status": "not-applicable",
                        "Name": "io-performance"
                    }
                ]
            },
            "AvailabilityZone": "us-east-1a",
            "VolumeId": "vol-1234567890abcdef0",
```

```
            "Actions": [],
            "Events": []
        }
    ]
}
```

Para describir el estado de los volúmenes dañados

En este ejemplo de comando, se describe el estado de todos los volúmenes que están dañados. En este ejemplo de salida no hay volúmenes dañados.

Comando:

```
aws ec2 describe-volume-status --filters Name=volume-status.status,Values=impaired
```

Salida:

```
{
    "VolumeStatuses": []
}
```

Si tiene un volumen con una comprobación de estado no superada (estado dañado), consulte cómo trabajar con un volumen dañado en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeVolumeStatus en la Referencia de comandos de la AWS CLI.

`describe-volumes-modifications`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-volumes-modifications`.

AWS CLI

Para describir el estado de modificación de un volumen

En el siguiente ejemplo de `describe-volumes-modifications` se describe el estado de modificación del volumen especificado.

```
aws ec2 describe-volumes-modifications \
    --volume-ids vol-1234567890abcdef0
```

Salida:

```
{
    "VolumeModification": {
        "TargetSize": 150,
        "TargetVolumeType": "io1",
        "ModificationState": "optimizing",
        "VolumeId": " vol-1234567890abcdef0",
        "TargetIops": 100,
        "StartTime": "2019-05-17T11:27:19.000Z",
        "Progress": 70,
        "OriginalVolumeType": "io1",
        "OriginalIops": 100,
        "OriginalSize": 100
    }
}
```

- Para obtener información sobre la API, consulte DescribeVolumesModifications en la Referencia de comandos de la AWS CLI.

`describe-volumes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-volumes`.

AWS CLI

Ejemplo 1: descripción de un volumen

En el siguiente ejemplo de `describe-volumes` se describen los volúmenes especificados en la región actual.

```
aws ec2 describe-volumes \
    --volume-ids vol-049df61146c4d7901 vol-1234567890abcdef0
```

Salida:

```
{
    "Volumes": [
        {
            "AvailabilityZone": "us-east-1a",
            "Attachments": [
```

```
                {
                    "AttachTime": "2013-12-18T22:35:00.000Z",
                    "InstanceId": "i-1234567890abcdef0",
                    "VolumeId": "vol-049df61146c4d7901",
                    "State": "attached",
                    "DeleteOnTermination": true,
                    "Device": "/dev/sda1"
                }
            ],
            "Encrypted": true,
            "KmsKeyId": "arn:aws:kms:us-east-2a:123456789012:key/8c5b2c63-b9bc-45a3-
a87a-5513eEXAMPLE,
            "VolumeType": "gp2",
            "VolumeId": "vol-049df61146c4d7901",
            "State": "in-use",
            "Iops": 100,
            "SnapshotId": "snap-1234567890abcdef0",
            "CreateTime": "2019-12-18T22:35:00.084Z",
            "Size": 8
        },
        {
            "AvailabilityZone": "us-east-1a",
            "Attachments": [],
            "Encrypted": false,
            "VolumeType": "gp2",
            "VolumeId": "vol-1234567890abcdef0",
            "State": "available",
            "Iops": 300,
            "SnapshotId": "",
            "CreateTime": "2020-02-27T00:02:41.791Z",
            "Size": 100
        }
    ]
}
```

Ejemplo 2: descripción de los volúmenes que están asociados a una instancia específica

En el siguiente ejemplo de `describe-volumes` se describen todos los volúmenes que están asociados a la instancia especificada y configurados para que se eliminen cuando la instancia termine.

```
aws ec2 describe-volumes \
    --region us-east-1 \
```

```
    --filters Name=attachment.instance-
id,Values=i-1234567890abcdef0 Name=attachment.delete-on-termination,Values=true
```

Para ver un ejemplo del resultado de `describe-volumes`, consulte el ejemplo 1.

Ejemplo 3: descripción de los volúmenes disponibles en una zona de disponibilidad específica

En el siguiente ejemplo de `describe-volumes` se describen todos los volúmenes que tienen el estado `available` y encuentran en la zona de disponibilidad especificada.

```
aws ec2 describe-volumes \
    --filters Name=status,Values=available Name=availability-zone,Values=us-east-1a
```

Para ver un ejemplo del resultado de `describe-volumes`, consulte el ejemplo 1.

Ejemplo 4: descripción de volúmenes basados en etiquetas

En el siguiente ejemplo de `describe-volumes` se describen todos los volúmenes que tienen la clave de etiqueta `Name` y un valor que comienza por `Test`. A continuación, la salida se filtra mediante una consulta que muestra únicamente las etiquetas y los ID de los volúmenes.

```
aws ec2 describe-volumes \
    --filters Name=tag:Name,Values=Test* \
    --query "Volumes[*].{ID:VolumeId,Tag:Tags}"
```

Salida:

```
[
    {
        "Tag": [
            {
                "Value": "Test2",
                "Key": "Name"
            }
        ],
        "ID": "vol-1234567890abcdef0"
    },
    {
        "Tag": [
            {
                "Value": "Test1",
```

```
                "Key": "Name"
            }
        ],
        "ID": "vol-049df61146c4d7901"
    }
]
```

Para ver ejemplos adicionales de uso de filtros de etiquetas, consulte Trabajo con etiquetas en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DescribeVolumes en la Referencia de comandos de la AWS CLI.

`describe-vpc-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-vpc-attribute`.

AWS CLI

Para describir el atributo enableDnsSupport

En este ejemplo, se describe el atributo `enableDnsSupport`. Este atributo indica si la resolución de DNS está habilitada para la VPC. Si este atributo es `true`, el servidor DNS de Amazon resuelve nombres de host de DNS para sus instancias en sus direcciones IP correspondientes; de lo contrario, no.

Comando:

```
aws ec2 describe-vpc-attribute --vpc-id vpc-a01106c2 --attribute enableDnsSupport
```

Salida:

```
{
    "VpcId": "vpc-a01106c2",
    "EnableDnsSupport": {
        "Value": true
    }
}
```

Para describir el atributo enableDnsHostnames

En este ejemplo, se describe el atributo `enableDnsHostnames`. Este atributo especifica si las instancias lanzadas en la VPC obtienen nombres de host de DNS. Si el atributo es `true`, las instancias de la VPC obtienen nombres de host de DNS; de lo contrario, no.

Comando:

```
aws ec2 describe-vpc-attribute --vpc-id vpc-a01106c2 --attribute enableDnsHostnames
```

Salida:

```
{
    "VpcId": "vpc-a01106c2",
    "EnableDnsHostnames": {
        "Value": true
    }
}
```

- Para obtener información sobre la API, consulte DescribeVpcAttribute en la Referencia de comandos de la AWS CLI.

`describe-vpc-classic-link-dns-support`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-vpc-classic-link-dns-support`.

AWS CLI

Para describir la compatibilidad de DNS de ClassicLink con las VPC

En este ejemplo, se describe el estado de compatibilidad de DNS de ClassicLink con todas sus VPC.

Comando:

```
aws ec2 describe-vpc-classic-link-dns-support
```

Salida:

```
{
  "Vpcs": [
    {
```

```
      "VpcId": "vpc-88888888",
      "ClassicLinkDnsSupported": true
    },
    {
      "VpcId": "vpc-1a2b3c4d",
      "ClassicLinkDnsSupported": false
    }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeVpcClassicLinkDnsSupport en la Referencia de comandos de la AWS CLI.

`describe-vpc-classic-link`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-vpc-classic-link`.

AWS CLI

Para describir el estado de ClassicLink de las VPC

En este ejemplo, se muestra el estado de ClassicLink de vpc-88888888.

Comando:

```
aws ec2 describe-vpc-classic-link --vpc-id vpc-88888888
```

Salida:

```
{
  "Vpcs": [
    {
      "ClassicLinkEnabled": true,
      "VpcId": "vpc-88888888",
      "Tags": [
        {
          "Value": "classiclinkvpc",
          "Key": "Name"
        }
      ]
    }
  ]
```

```
}
```

En este ejemplo, se muestran solo las VPC que están habilitadas para Classiclink (el valor del filtro `is-classic-link-enabled` está establecido en `true`).

Comando:

```
aws ec2 describe-vpc-classic-link --filter "Name=is-classic-link-
enabled,Values=true"
```

- Para obtener información sobre la API, consulte DescribeVpcClassicLink en la Referencia de comandos de la AWS CLI.

`describe-vpc-endpoint-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-vpc-endpoint-associations`.

AWS CLI

Descripción de las asociaciones de puntos de conexión de VPC

En el siguiente ejemplo de `describe-vpc-endpoint-associations`, se describen las asociaciones del punto de conexión de VPC.

```
aws ec2 describe-vpc-endpoint-associations
```

Salida:

```
{
    "VpcEndpointAssociations": [
        {
            "Id": "vpce-rsc-asc-0a810ca6ac8866bf9",
            "VpcEndpointId": "vpce-019b90d6f16d4f958",
            "AssociatedResourceAccessibility": "Accessible",
            "DnsEntry": {
                "DnsName":
 "vpce-019b90d6f16d4f958.rcfg-07129f3acded87625.4232ccc.vpc-lattice-rsc.us-
east-2.on.aws",
                "HostedZoneId": "Z03265862FOUNWMZOKUF4"
            },
```

```
            "AssociatedResourceArn": "arn:aws:vpc-lattice:us-
east-1:123456789012:resourceconfiguration/rcfg-07129f3acded87625"
        }
    ]
}
```

Para obtener más información, consulte Administración de asociaciones de punto de conexión de VPC en la Guía del usuario de AWS PrivateLink.

- Para obtener información sobre la API, consulte DescribeVpcEndpointAssociations en la Referencia de comandos de la AWS CLI.

`describe-vpc-endpoint-connection-notifications`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-vpc-endpoint-connection-notifications`.

AWS CLI

Para describir notificaciones de conexión de punto de conexión

En el siguiente ejemplo de `describe-vpc-endpoint-connection-notifications` se describen todas sus notificaciones de conexión de punto de conexión.

```
aws ec2 describe-vpc-endpoint-connection-notifications
```

Salida:

```
{
   "ConnectionNotificationSet": [
       {
           "ConnectionNotificationState": "Enabled",
           "ConnectionNotificationType": "Topic",
           "ConnectionEvents": [
               "Accept",
               "Reject",
               "Delete",
               "Connect"
           ],
           "ConnectionNotificationId": "vpce-nfn-04bcb952bc8af7abc",
           "ConnectionNotificationArn": "arn:aws:sns:us-
east-1:123456789012:VpceNotification",
```

```
            "VpcEndpointId": "vpce-0324151a02f327123"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeVpcEndpointConnectionNotifications en la Referencia de comandos de la AWS CLI.

`describe-vpc-endpoint-connections`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-vpc-endpoint-connections`.

AWS CLI

Para describir las conexiones de punto de conexión de VPC

En este ejemplo, se describen las conexiones de punto de conexión de interfaz de su servicio de punto de conexión y se filtran los resultados para mostrar los puntos de conexión que tienen el estado `PendingAcceptance`.

Comando:

```
aws ec2 describe-vpc-endpoint-connections --filters Name=vpc-endpoint-state,Values=pendingAcceptance
```

Salida:

```
{
  "VpcEndpointConnections": [
      {
          "VpcEndpointId": "vpce-0abed31004e618123",
          "ServiceId": "vpce-svc-0abced088d20def56",
          "CreationTimestamp": "2017-11-30T10:00:24.350Z",
          "VpcEndpointState": "pendingAcceptance",
          "VpcEndpointOwner": "123456789012"
      }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeVpcEndpointConnections en la Referencia de comandos de la AWS CLI.

describe-vpc-endpoint-service-configurations

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-vpc-endpoint-service-configurations`.

AWS CLI

Para describir las configuraciones del servicio de punto de conexión

En el siguiente ejemplo de `describe-vpc-endpoint-service-configurations` se describen las configuraciones del servicio de punto de conexión.

```
aws ec2 describe-vpc-endpoint-service-configurations
```

Salida:

```
{
    "ServiceConfigurations": [
        {
            "ServiceType": [
                {
                    "ServiceType": "GatewayLoadBalancer"
                }
            ],
            "ServiceId": "vpce-svc-012d33a1c4321cabc",
            "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-
svc-012d33a1c4321cabc",
            "ServiceState": "Available",
            "AvailabilityZones": [
                "us-east-1d"
            ],
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "GatewayLoadBalancerArns": [
                "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/
gwy/GWLBService/123210844e429123"
            ],
            "Tags": []
        },
        {
            "ServiceType": [
                {
```

```
                    "ServiceType": "Interface"
                }
            ],
            "ServiceId": "vpce-svc-123cabc125efa123",
            "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-123cabc125efa123",
            "ServiceState": "Available",
            "AvailabilityZones": [
                "us-east-1a"
            ],
            "AcceptanceRequired": true,
            "ManagesVpcEndpoints": false,
            "NetworkLoadBalancerArns": [
                "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/
net/NLBforService/1238753950b25123"
            ],
            "BaseEndpointDnsNames": [
                "vpce-svc-123cabc125efa123.us-east-1.vpce.amazonaws.com"
            ],
            "PrivateDnsName": "example.com",
            "PrivateDnsNameConfiguration": {
                "State": "failed",
                "Type": "TXT",
                "Value": "vpce:qUAth3FdeABCApUiXabc",
                "Name": "_1d367jvbg34znqvyefrj"
            },
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Conceptos en la Guía del usuario de AWS PrivateLink.

- Para obtener información sobre la API, consulte DescribeVpcEndpointServiceConfigurations en la Referencia de comandos de la AWS CLI.

`describe-vpc-endpoint-service-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-vpc-endpoint-service-permissions`.

AWS CLI

Para describir los permisos del servicio de punto de conexión

En este ejemplo, se describen los permisos del servicio de punto de conexión especificado.

Comando:

```
aws ec2 describe-vpc-endpoint-service-permissions --service-id vpce-svc-03d5ebb7d9579a2b3
```

Salida:

```
{
   "AllowedPrincipals": [
       {
           "PrincipalType": "Account",
           "Principal": "arn:aws:iam::123456789012:root"
       }
   ]
}
```

- Para obtener información sobre la API, consulte DescribeVpcEndpointServicePermissions en la Referencia de comandos de la AWS CLI.

`describe-vpc-endpoint-services`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-vpc-endpoint-services`.

AWS CLI

Ejemplo 1: descripción de todos los servicios de punto de conexión de VPC

En el siguiente ejemplo de `describe-vpc-endpoint-services`, se muestran todos los servicios de punto de conexión de VPC de una región de AWS.

```
aws ec2 describe-vpc-endpoint-services
```

Salida:

```
{
    "ServiceDetails": [
        {
            "ServiceType": [
                {
                    "ServiceType": "Gateway"
```

```
            }
        ],
        "AcceptanceRequired": false,
        "ServiceName": "com.amazonaws.us-east-1.dynamodb",
        "VpcEndpointPolicySupported": true,
        "Owner": "amazon",
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1b",
            "us-east-1c",
            "us-east-1d",
            "us-east-1e",
            "us-east-1f"
        ],
        "BaseEndpointDnsNames": [
            "dynamodb.us-east-1.amazonaws.com"
        ]
    },
    {
        "ServiceType": [
            {
                "ServiceType": "Interface"
            }
        ],
        "PrivateDnsName": "ec2.us-east-1.amazonaws.com",
        "ServiceName": "com.amazonaws.us-east-1.ec2",
        "VpcEndpointPolicySupported": false,
        "Owner": "amazon",
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1b",
            "us-east-1c",
            "us-east-1d",
            "us-east-1e",
            "us-east-1f"
        ],
        "AcceptanceRequired": false,
        "BaseEndpointDnsNames": [
            "ec2.us-east-1.vpce.amazonaws.com"
        ]
    },
    {
        "ServiceType": [
            {
```

```
                    "ServiceType": "Interface"
                }
            ],
            "PrivateDnsName": "ssm.us-east-1.amazonaws.com",
            "ServiceName": "com.amazonaws.us-east-1.ssm",
            "VpcEndpointPolicySupported": true,
            "Owner": "amazon",
            "AvailabilityZones": [
                "us-east-1a",
                "us-east-1b",
                "us-east-1c",
                "us-east-1d",
                "us-east-1e"
            ],
            "AcceptanceRequired": false,
            "BaseEndpointDnsNames": [
                "ssm.us-east-1.vpce.amazonaws.com"
            ]
        }
    ],
    "ServiceNames": [
        "com.amazonaws.us-east-1.dynamodb",
        "com.amazonaws.us-east-1.ec2",
        "com.amazonaws.us-east-1.ec2messages",
        "com.amazonaws.us-east-1.elasticloadbalancing",
        "com.amazonaws.us-east-1.kinesis-streams",
        "com.amazonaws.us-east-1.s3",
        "com.amazonaws.us-east-1.ssm"
    ]
}
```

Ejemplo 2: descripción de la información sobre un servicio de punto de conexión

En el siguiente ejemplo de `describe-vpc-endpoint-services`, se muestran los detalles del servicio de punto de conexión de interfaz de Amazon S3.

```
aws ec2 describe-vpc-endpoint-services \
    --filter 'Name=service-type,Values=Interface' Name=service-
name,Values=com.amazonaws.us-east-1.s3
```

Salida:

```
{
```

```
    "ServiceDetails": [
        {
            "ServiceName": "com.amazonaws.us-east-1.s3",
            "ServiceId": "vpce-svc-081d84efcdEXAMPLE",
            "ServiceType": [
                {
                    "ServiceType": "Interface"
                }
            ],
            "AvailabilityZones": [
                "us-east-1a",
                "us-east-1b",
                "us-east-1c",
                "us-east-1d",
                "us-east-1e",
            "us-east-1f"
            ],
            "Owner": "amazon",
            "BaseEndpointDnsNames": [
                "s3.us-east-1.vpce.amazonaws.com"
            ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": []
        }
    ],
    "ServiceNames": [
        "com.amazonaws.us-east-1.s3"
    ]
}
```

Para obtener más información, consulte Ver nombres de servicio de AWS disponibles en la Guía del usuario de AWS PrivateLink.

- Para obtener información sobre la API, consulte DescribeVpcEndpointServices en la Referencia de comandos de la AWS CLI.

`describe-vpc-endpoints`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-vpc-endpoints`.

AWS CLI

Para describir los puntos de conexión de VPC

En el siguiente `describe-vpc-endpoints` ejemplo, se muestra la información de todos los puntos de conexión de la VPC.

```
aws ec2 describe-vpc-endpoints
```

Salida:

```
{
    "VpcEndpoints": [
        {
            "PolicyDocument": "{\"Version\":\"2008-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Principal\":\"*\",\"Action\":\"*\",\"Resource\":\"*\"}]}",
            "VpcId": "vpc-aabb1122",
            "NetworkInterfaceIds": [],
            "SubnetIds": [],
            "PrivateDnsEnabled": true,
            "State": "available",
            "ServiceName": "com.amazonaws.us-east-1.dynamodb",
            "RouteTableIds": [
                "rtb-3d560345"
            ],
            "Groups": [],
            "VpcEndpointId": "vpce-032a826a",
            "VpcEndpointType": "Gateway",
            "CreationTimestamp": "2017-09-05T20:41:28Z",
            "DnsEntries": [],
            "OwnerId": "123456789012"
        },
        {
            "PolicyDocument": "{\n  \"Statement\": [\n    {\n      \"Action\": \"*
\", \n      \"Effect\": \"Allow\", \n      \"Principal\": \"*\", \n      \"Resource
\": \"*\"\n    }\n  ]\n}",
            "VpcId": "vpc-1a2b3c4d",
            "NetworkInterfaceIds": [
                "eni-2ec2b084",
                "eni-1b4a65cf"
            ],
            "SubnetIds": [
                "subnet-d6fcaa8d",
```

```
                "subnet-7b16de0c"
            ],
            "PrivateDnsEnabled": false,
            "State": "available",
            "ServiceName": "com.amazonaws.us-east-1.elasticloadbalancing",
            "RouteTableIds": [],
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-54e8bf31"
                }
            ],
            "VpcEndpointId": "vpce-0f89a33420c1931d7",
            "VpcEndpointType": "Interface",
            "CreationTimestamp": "2017-09-05T17:55:27.583Z",
            "DnsEntries": [
                {
                    "HostedZoneId": "Z7HUB22UULQXV",
                    "DnsName": "vpce-0f89a33420c1931d7-
bluzidnv.elasticloadbalancing.us-east-1.vpce.amazonaws.com"
                },
                {
                    "HostedZoneId": "Z7HUB22UULQXV",
                    "DnsName": "vpce-0f89a33420c1931d7-bluzidnv-us-
east-1b.elasticloadbalancing.us-east-1.vpce.amazonaws.com"
                },
                {
                    "HostedZoneId": "Z7HUB22UULQXV",
                    "DnsName": "vpce-0f89a33420c1931d7-bluzidnv-us-
east-1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com"
                }
            ],
            "OwnerId": "123456789012"
        },
        {
            "VpcEndpointId": "vpce-aabbaabbaabbaabba",
            "VpcEndpointType": "GatewayLoadBalancer",
            "VpcId": "vpc-111122223333aabbc",
            "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-
svc-123123a1c43abc123",
            "State": "available",
            "SubnetIds": [
                "subnet-0011aabbcc2233445"
            ],
```

```
            "RequesterManaged": false,
            "NetworkInterfaceIds": [
                "eni-01010120203030405"
            ],
            "CreationTimestamp": "2020-11-11T08:06:03.522Z",
            "Tags": [],
            "OwnerId": "123456789012"
        }
    ]
}
```

Para obtener más información, consulte Conceptos en la Guía del usuario de AWS PrivateLink.

- Para obtener información sobre la API, consulte DescribeVpcEndpoints en la Referencia de comandos de la AWS CLI.

`describe-vpc-peering-connections`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-vpc-peering-connections`.

AWS CLI

Para describir las conexiones de emparejamiento de VPC

En este ejemplo, se describen todas sus conexiones de emparejamiento de VPC.

Comando:

```
aws ec2 describe-vpc-peering-connections
```

Salida:

```
{
    "VpcPeeringConnections": [
        {
            "Status": {
                "Message": "Active",
                "Code": "active"
            },
            "Tags": [
                {
                    "Value": "Peering-1",
```

```
                    "Key": "Name"
                }
            ],
            "AccepterVpcInfo": {
                "OwnerId": "111122223333",
                "VpcId": "vpc-1a2b3c4d",
                "CidrBlock": "10.0.1.0/28"
            },
            "VpcPeeringConnectionId": "pcx-11122233",
            "RequesterVpcInfo": {
                "PeeringOptions": {
                    "AllowEgressFromLocalVpcToRemoteClassicLink": false,
                    "AllowEgressFromLocalClassicLinkToRemoteVpc": false
                },
                "OwnerId": "444455556666",
                "VpcId": "vpc-123abc45",
                "CidrBlock": "192.168.0.0/16"
            }
        },
        {
            "Status": {
                "Message": "Pending Acceptance by 444455556666",
                "Code": "pending-acceptance"
            },
            "Tags": [],
            "RequesterVpcInfo": {
                "PeeringOptions": {
                    "AllowEgressFromLocalVpcToRemoteClassicLink": false,
                    "AllowEgressFromLocalClassicLinkToRemoteVpc": false
                },
                "OwnerId": "444455556666",
                "VpcId": "vpc-11aa22bb",
                "CidrBlock": "10.0.0.0/28"
            },
            "VpcPeeringConnectionId": "pcx-abababab",
            "ExpirationTime": "2014-04-03T09:12:43.000Z",
            "AccepterVpcInfo": {
                "OwnerId": "444455556666",
                "VpcId": "vpc-33cc44dd"
            }
        }
    ]
}
```

Para describir conexiones de emparejamiento de VPC específicas

En este ejemplo, se describen todas sus conexiones de emparejamiento de VPC cuyo estado es pending-acceptance.

Comando:

```
aws ec2 describe-vpc-peering-connections --filters Name=status-code,Values=pending-acceptance
```

En este ejemplo, se describen todas las conexiones de emparejamiento de VPC que tienen la etiqueta Owner=Finance.

Comando:

```
aws ec2 describe-vpc-peering-connections --filters Name=tag:Owner,Values=Finance
```

En este ejemplo se describen todas las conexiones de emparejamiento de VPC que ha solicitado para la VPC especificada, vpc-1a2b3c4d.

Comando:

```
aws ec2 describe-vpc-peering-connections --filters Name=requester-vpc-info.vpc-id,Values=vpc-1a2b3c4d
```

- Para obtener información sobre la API, consulte DescribeVpcPeeringConnections en la Referencia de comandos de la AWS CLI.

`describe-vpcs`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-vpcs`.

AWS CLI

Ejemplo 1: Describir todas las VPC

En el siguiente ejemplo de `describe-vpcs`, se recuperan los detalles de todas las VPC.

```
aws ec2 describe-vpcs
```

Salida:


```
{
    "Vpcs": [
        {
            "CidrBlock": "30.1.0.0/16",
            "DhcpOptionsId": "dopt-19edf471",
            "State": "available",
            "VpcId": "vpc-0e9801d129EXAMPLE",
            "OwnerId": "111122223333",
            "InstanceTenancy": "default",
            "CidrBlockAssociationSet": [
                {
                    "AssociationId": "vpc-cidr-assoc-062c64cfafEXAMPLE",
                    "CidrBlock": "30.1.0.0/16",
                    "CidrBlockState": {
                        "State": "associated"
                    }
                }
            ],
            "IsDefault": false,
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Not Shared"
                }
            ]
        },
        {
            "CidrBlock": "10.0.0.0/16",
            "DhcpOptionsId": "dopt-19edf471",
            "State": "available",
            "VpcId": "vpc-06e4ab6c6cEXAMPLE",
            "OwnerId": "222222222222",
            "InstanceTenancy": "default",
            "CidrBlockAssociationSet": [
                {
                    "AssociationId": "vpc-cidr-assoc-00b17b4eddEXAMPLE",
                    "CidrBlock": "10.0.0.0/16",
                    "CidrBlockState": {
                        "State": "associated"
                    }
                }
            ],
```

```
            "IsDefault": false,
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Shared VPC"
                }
            ]
        }
    ]
}
```

Ejemplo 2: Describir una VPC específica

En siguiente ejemplo, `describe-vpcs` recupera los detalles de la VPC especificada.

```
aws ec2 describe-vpcs \
    --vpc-ids vpc-06e4ab6c6cEXAMPLE
```

Salida:

```
{
    "Vpcs": [
        {
            "CidrBlock": "10.0.0.0/16",
            "DhcpOptionsId": "dopt-19edf471",
            "State": "available",
            "VpcId": "vpc-06e4ab6c6cEXAMPLE",
            "OwnerId": "111122223333",
            "InstanceTenancy": "default",
            "CidrBlockAssociationSet": [
                {
                    "AssociationId": "vpc-cidr-assoc-00b17b4eddEXAMPLE",
                    "CidrBlock": "10.0.0.0/16",
                    "CidrBlockState": {
                        "State": "associated"
                    }
                }
            ],
            "IsDefault": false,
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Shared VPC"
```

```
                }
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeVpcs en la Referencia de comandos de la AWS CLI.

`describe-vpn-connections`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-vpn-connections`.

AWS CLI

Ejemplo 1: descripción de las conexiones de VPN

En el siguiente ejemplo de `describe-vpn-connections` se describen todas las conexiones de Site-to-Site VPN.

```
aws ec2 describe-vpn-connections
```

Salida:

```
{
    "VpnConnections": [
        {
            "CustomerGatewayConfiguration": "...configuration information...",
            "CustomerGatewayId": "cgw-01234567abcde1234",
            "Category": "VPN",
            "State": "available",
            "Type": "ipsec.1",
            "VpnConnectionId": "vpn-1122334455aabbccd",
            "TransitGatewayId": "tgw-00112233445566aab",
            "Options": {
                "EnableAcceleration": false,
                "StaticRoutesOnly": true,
                "LocalIpv4NetworkCidr": "0.0.0.0/0",
                "RemoteIpv4NetworkCidr": "0.0.0.0/0",
                "TunnelInsideIpVersion": "ipv4"
            },
```

```
            "Routes": [],
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "CanadaVPN"
                }
            ],
            "VgwTelemetry": [
                {
                    "AcceptedRouteCount": 0,
                    "LastStatusChange": "2020-07-29T10:35:11.000Z",
                    "OutsideIpAddress": "203.0.113.3",
                    "Status": "DOWN",
                    "StatusMessage": ""
                },
                {
                    "AcceptedRouteCount": 0,
                    "LastStatusChange": "2020-09-02T09:09:33.000Z",
                    "OutsideIpAddress": "203.0.113.5",
                    "Status": "UP",
                    "StatusMessage": ""
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte How AWS Site-to-Site VPN works en la Guía del usuario de AWS Site-to-Site VPN.

Ejemplo 2: descripción de las conexiones de VPN disponibles

En el siguiente ejemplo de `describe-vpn-connections` se describen sus conexiones de Site-to-Site VPN cuyo estado es `available`.

```
aws ec2 describe-vpn-connections \
    --filters "Name=state,Values=available"
```

Para obtener más información, consulte How AWS Site-to-Site VPN works en la Guía del usuario de AWS Site-to-Site VPN.

- Para obtener información sobre la API, consulte DescribeVpnConnections en la Referencia de comandos de la AWS CLI.

`describe-vpn-gateways`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-vpn-gateways`.

AWS CLI

Para describir las puertas de enlace privadas virtuales

En este ejemplo, se describen sus puertas de enlace privadas virtuales.

Comando:

```
aws ec2 describe-vpn-gateways
```

Salida:

```
{
    "VpnGateways": [
        {
            "State": "available",
            "Type": "ipsec.1",
            "VpnGatewayId": "vgw-f211f09b",
            "VpcAttachments": [
                {
                    "State": "attached",
                    "VpcId": "vpc-98eb5ef5"
                }
            ]
        },
        {
            "State": "available",
            "Type": "ipsec.1",
            "VpnGatewayId": "vgw-9a4cacf3",
            "VpcAttachments": [
                {
                    "State": "attaching",
                    "VpcId": "vpc-a01106c2"
                }
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeVpnGateways en la Referencia de comandos de la AWS CLI.

`detach-classic-link-vpc`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-classic-link-vpc`.

AWS CLI

Para desvincular (desasociar) una instancia EC2-Classic de una VPC

En este ejemplo, se desvincula la instancia i-0598c7d356eba48d7 de la VPC vpc-88888888.

Comando:

```
aws ec2 detach-classic-link-vpc --instance-id i-0598c7d356eba48d7 --vpc-
id vpc-88888888
```

Salida:

```
{
  "Return": true
}
```

- Para obtener información sobre la API, consulte DetachClassicLinkVpc en la Referencia de comandos de la AWS CLI.

`detach-internet-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-internet-gateway`.

AWS CLI

Para desasociar una puerta de enlace de Internet de su VPC

En el siguiente ejemplo de `detach-internet-gateway` se desasocia la puerta de enlace de Internet especificada de la VPC específica.

```
aws ec2 detach-internet-gateway \
    --internet-gateway-id igw-0d0fb496b3EXAMPLE \
    --vpc-id vpc-0a60eb65b4EXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Puertas de enlace de Internet en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte DetachInternetGateway en la Referencia de comandos de AWS CLI.

`detach-network-interface`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-network-interface`.

AWS CLI

Para desasociar una interfaz de red de la instancia

En este ejemplo, se desasocia la interfaz de red especificada de la instancia especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 detach-network-interface --attachment-id eni-attach-66c4350a
```

- Para obtener información sobre la API, consulte DetachNetworkInterface en la Referencia de comandos de AWS CLI.

`detach-verified-access-trust-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-verified-access-trust-provider`.

AWS CLI

Para desasociar un proveedor de confianza de una instancia

En el siguiente ejemplo de `detach-verified-access-trust-provider` se desasocia el proveedor de confianza de acceso verificado especificado de la instancia de acceso verificado especificada.

```
aws ec2 detach-verified-access-trust-provider \
```

```
    --verified-access-instance-id vai-0ce000c0b7643abea \
    --verified-access-trust-provider-id vatp-0bb32de759a3e19e7
```

Salida:

```
{
    "VerifiedAccessTrustProvider": {
        "VerifiedAccessTrustProviderId": "vatp-0bb32de759a3e19e7",
        "Description": "Testing Verified Access",
        "TrustProviderType": "user",
        "UserTrustProviderType": "iam-identity-center",
        "PolicyReferenceName": "idc",
        "CreationTime": "2023-08-25T19:00:38",
        "LastUpdatedTime": "2023-08-25T19:00:38"
    },
    "VerifiedAccessInstance": {
        "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
        "Description": "Testing Verified Access",
        "VerifiedAccessTrustProviders": [],
        "CreationTime": "2023-08-25T18:27:56",
        "LastUpdatedTime": "2023-08-25T18:27:56"
    }
}
```

Para obtener más información, consulte Verified Access instances en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte DetachVerifiedAccessTrustProvider en la Referencia de comandos de la AWS CLI.

`detach-volume`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-volume`.

AWS CLI

Para desasociar un volumen de una instancia

En este ejemplo de comando, se desasocia el volumen (`vol-049df61146c4d7901`) de la instancia a la que está asociado.

Comando:

```
aws ec2 detach-volume --volume-id vol-1234567890abcdef0
```

Salida:

```
{
    "AttachTime": "2014-02-27T19:23:06.000Z",
    "InstanceId": "i-1234567890abcdef0",
    "VolumeId": "vol-049df61146c4d7901",
    "State": "detaching",
    "Device": "/dev/sdb"
}
```

- Para obtener información sobre la API, consulte DetachVolume en la Referencia de comandos de la AWS CLI.

`detach-vpn-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-vpn-gateway`.

AWS CLI

Para desasociar una puerta de enlace privada virtual de la VPC

En este ejemplo, se desasocia la puerta de enlace privada virtual especificada de la VPC especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 detach-vpn-gateway --vpn-gateway-id vgw-9a4cacf3 --vpc-id vpc-a01106c2
```

- Para obtener información sobre la API, consulte DetachVpnGateway en la Referencia de comandos de la AWS CLI.

`disable-address-transfer`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-address-transfer`.

AWS CLI

Para deshabilitar la transferencia de una dirección IP elástica

En el siguiente ejemplo de `disable-address-transfer` se deshabilita la transferencia de dirección IP elástica para la dirección IP elástica especificada.

```
aws ec2 disable-address-transfer \
    --allocation-id eipalloc-09ad461b0d03f6aaf
```

Salida:

```
{
    "AddressTransfer": {
        "PublicIp": "100.21.184.216",
        "AllocationId": "eipalloc-09ad461b0d03f6aaf",
        "AddressTransferStatus": "disabled"
    }
}
```

Para obtener más información, consulte Transfer Elastic IP addresses en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte DisableAddressTransfer en la Referencia de comandos de la AWS CLI.

`disable-aws-network-performance-metric-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-aws-network-performance-metric-subscription`.

AWS CLI

Para deshabilitar una suscripción a una métrica

En el siguiente ejemplo de `disable-aws-network-performance-metric-subscription` se deshabilita el monitoreo de la latencia de red agregada entre las regiones de origen y destino especificadas.

```
aws ec2 disable-aws-network-performance-metric-subscription \
    --source us-east-1 \
    --destination eu-west-1 \
    --metric aggregate-latency \
    --statistic p50
```

Salida:

```
{
    "Output": true
}
```

Para obtener más información, consulte Administrar suscripciones de CloudWatch con la CLI en la Guía del usuario de rendimiento de la infraestructura.

- Para obtener información sobre la API, consulte DisableAwsNetworkPerformanceMetricSubscription en la Referencia de comandos de la AWS CLI.

`disable-ebs-encryption-by-default`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-ebs-encryption-by-default`.

AWS CLI

Para deshabilitar el cifrado de EBS de forma predeterminada

En el siguiente ejemplo de `disable-ebs-encryption-by-default` se deshabilita el cifrado de EBS predeterminado habilitado para su cuenta de AWS en la región actual.

```
aws ec2 disable-ebs-encryption-by-default
```

Salida:

```
{
    "EbsEncryptionByDefault": false
}
```

- Para obtener información sobre la API, consulte DisableEbsEncryptionByDefault en la Referencia de comandos de la AWS CLI.

`disable-fast-launch`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-fast-launch`.

AWS CLI

Para interrumpir el lanzamiento rápido de una imagen

En el siguiente ejemplo de `disable-fast-launch`, se interrumpe el lanzamiento rápido en la AMI especificada y se borran las instantáneas aprovisionadas previamente existentes.

```
aws ec2 disable-fast-launch \
    --image-id ami-01234567890abcedf
```

Salida:

```
{
    "ImageId": "ami-01234567890abcedf",
    "ResourceType": "snapshot",
    "SnapshotConfiguration": {},
    "LaunchTemplate": {
        "LaunchTemplateId": "lt-01234567890abcedf",
        "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
        "Version": "1"
    },
    "MaxParallelLaunches": 6,
    "OwnerId": "0123456789123",
    "State": "disabling",
    "StateTransitionReason": "Client.UserInitiated",
    "StateTransitionTime": "2022-01-27T22:47:29.265000+00:00"
}
```

Para obtener más información, consulte Configure EC2 Fast Launch settings for your Windows AMI en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DisableFastLaunch en la Referencia de comandos de la AWS CLI.

`disable-fast-snapshot-restores`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-fast-snapshot-restores`.

AWS CLI

Para deshabilitar la restauración rápida de instantáneas

En el siguiente ejemplo de `disable-fast-snapshot-restores` se deshabilitan las restauraciones rápidas de instantáneas para las instantáneas especificadas en la zona de disponibilidad especificada.

```
aws ec2 disable-fast-snapshot-restores \
    --availability-zones us-east-2a \
    --source-snapshot-ids snap-1234567890abcdef0
```

Salida:

```
{
    "Successful": [
        {
            "SnapshotId": "snap-1234567890abcdef0"
            "AvailabilityZone": "us-east-2a",
            "State": "disabling",
            "StateTransitionReason": "Client.UserInitiated",
            "OwnerId": "123456789012",
            "EnablingTime": "2020-01-25T23:57:49.602Z"
        }
    ],
    "Unsuccessful": []
}
```

- Para obtener información sobre la API, consulte DisableFastSnapshotRestores en la Referencia de comandos de la AWS CLI.

`disable-image-block-public-access`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-image-block-public-access`.

AWS CLI

Para deshabilitar el Bloqueo del acceso público de las AMI en la región especificada

En el siguiente ejemplo de `disable-image-block-public-access` se deshabilita el Bloqueo del acceso público de las AMI para la cuenta en la región especificada.

```
aws ec2 disable-image-block-public-access \
```

```
    --region us-east-1
```

Salida:

```
{
    "ImageBlockPublicAccessState": "unblocked"
}
```

Para obtener más información, consulte Bloqueo del acceso público de las AMI en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DisableImageBlockPublicAccess en la Referencia de comandos de la AWS CLI.

`disable-image-deprecation`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-image-deprecation`.

AWS CLI

Para cancelar la baja de una AMI

En el siguiente ejemplo de `disable-image-deprecation` se cancela la baja de una AMI, lo que elimina el campo `DeprecationTime` de la salida de `describe-images`. Debe ser el propietario de la AMI para realizar este procedimiento.

```
aws ec2 disable-image-deprecation \
    --image-id ami-1234567890abcdef0
```

Salida:

```
{
    "RequestID": "11aabb229-4eac-35bd-99ed-be587EXAMPLE",
    "Return": "true"
}
```

Para obtener más información, consulte Dar de baja una AMI en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DisableImageDeprecation en la Referencia de comandos de la AWS CLI.

`disable-image-deregistration-protection`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-image-deregistration-protection`.

AWS CLI

Desactivación de la protección contra la anulación del registro

En el siguiente ejemplo de `disable-image-deregistration-protection`, se desactiva la protección contra la anulación del registro para la imagen especificada.

```
aws ec2 disable-image-deregistration-protection \
    --image-id ami-0b1a928a144a74ec9
```

Salida:

```
{
    "Return": "disabled"
}
```

Para obtener más información, consulte Proteger una AMI contra la anulación del registro en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DisableImageDeregistrationProtection en la Referencia de comandos de la AWS CLI.

`disable-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-image`.

AWS CLI

Para deshabilitar una AMI

En el siguiente ejemplo de `disable-image` se deshabilita la AMI especificada.

```
aws ec2 disable-image \
    --image-id ami-1234567890abcdef0
```

Salida:

```
{
    "Return": "true"
}
```

Para obtener más información, consulte Inhabilitación de una AMI en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DisableImage en la Referencia de comandos de la AWS CLI.

`disable-ipam-organization-admin-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-ipam-organization-admin-account`.

AWS CLI

Para deshabilitar al administrador delegado de IPAM

En algunos casos, IPAM se integrará con AWS Organizations. En este caso, la cuenta de administración de AWS Organizations delega en una cuenta de miembro de AWS Organizations como administrador de IPAM.

En este ejemplo, usted es la cuenta de administración de AWS Organizations que delegó la cuenta de administrador de IPAM y desea deshabilitar esa cuenta para que no sea el administrador de IPAM.

Puede usar cualquier región de AWS para `--region` al realizar esta solicitud. No es preciso usar la región en la que se delegó originalmente al administrador o en la que se creó el IPAM, ni tampoco una región operativa de IPAM. Si deshabilita la cuenta de administrador delegado, puede volver a habilitarla en cualquier momento o delegar en una nueva cuenta como administrador de IPAM.

En el siguiente ejemplo de `disable-ipam-organization-admin-account` se deshabilita al administrador delegado de IPAM en su cuenta de AWS.

```
aws ec2 disable-ipam-organization-admin-account \
```

```
    --delegated-admin-account-id 320805250157 \
    --region ap-south-1
```

Salida:

```
{
    "Success": true
}
```

Para obtener más información, consulte Integración de IPAM con cuentas en una organización de AWS en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte DisableIpamOrganizationAdminAccount en la Referencia de comandos de AWS CLI.

`disable-serial-console-access`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-serial-console-access`.

AWS CLI

Para deshabilitar el acceso a la consola serie de EC2 en su cuenta

En el siguiente ejemplo de `disable-serial-console-access` se deshabilita el acceso de la cuenta a la consola serie.

```
aws ec2 disable-serial-console-access
```

Salida:

```
{
    "SerialConsoleAccessEnabled": false
}
```

Para obtener más información, consulte Consola serie de EC2 en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DisableSerialConsoleAccess en la Referencia de comandos de la AWS CLI.

`disable-snapshot-block-public-access`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-snapshot-block-public-access`.

AWS CLI

Deshabilitación del bloqueo del acceso público de las instantáneas

En el siguiente ejemplo de `disable-snapshot-block-public-access` se deshabilita el bloqueo del acceso público de las instantáneas para permitir que sus instantáneas se compartan públicamente.

```
aws ec2 disable-snapshot-block-public-access
```

Salida:

```
{
    "State": "unblocked"
}
```

Para obtener más información, consulte Block public access for snapshots en la Guía del usuario de Amazon EBS.

- Para obtener información sobre la API, consulte DisableSnapshotBlockPublicAccess en la Referencia de comandos de la AWS CLI.

`disable-transit-gateway-route-table-propagation`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-transit-gateway-route-table-propagation`.

AWS CLI

Para deshabilitar la conexión de puerta de enlace de tránsito a fin de propagar rutas a la tabla de enrutamiento de propagación especificada

En el siguiente ejemplo de `disable-transit-gateway-route-table-propagation` se deshabilita la conexión especificada para propagar las rutas a la tabla de enrutamiento de propagación especificada.

```
aws ec2 disable-transit-gateway-route-table-propagation \
    --transit-gateway-route-table-id tgw-rtb-0a823edbdeEXAMPLE \
    --transit-gateway-attachment-id tgw-attach-09b52ccdb5EXAMPLE
```

Salida:

```
{
    "Propagation": {
        "TransitGatewayAttachmentId": "tgw-attach-09b52ccdb5EXAMPLE",
        "ResourceId": "vpc-4d7de228",
        "ResourceType": "vpc",
        "TransitGatewayRouteTableId": "tgw-rtb-0a823edbdeEXAMPLE",
        "State": "disabled"
    }
}
```

Para obtener más información, consulte Transit gateway route tables en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DisableTransitGatewayRouteTablePropagation en la Referencia de comandos de la AWS CLI.

`disable-vgw-route-propagation`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-vgw-route-propagation`.

AWS CLI

Para deshabilitar la propagación de rutas

En este ejemplo, se impide que la puerta de enlace privada virtual especificada propague rutas estáticas a la tabla de enrutamiento especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 disable-vgw-route-propagation --route-table-id rtb-22574640 --gateway-
id vgw-9a4cacf3
```

- Para obtener información sobre la API, consulte DisableVgwRoutePropagation en la Referencia de comandos de la AWS CLI.

`disable-vpc-classic-link-dns-support`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-vpc-classic-link-dns-support`.

AWS CLI

Para deshabilitar la compatibilidad de DNS de ClassicLink con una VPC

En este ejemplo se deshabilita la compatibilidad de DNS de ClassicLink con `vpc-88888888`.

Comando:

```
aws ec2 disable-vpc-classic-link-dns-support --vpc-id vpc-88888888
```

Salida:

```
{
  "Return": true
}
```

- Para obtener información sobre la API, consulte DisableVpcClassicLinkDnsSupport en la Referencia de comandos de la AWS CLI.

`disable-vpc-classic-link`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-vpc-classic-link`.

AWS CLI

Para deshabilitar ClassicLink para una VPC

En este ejemplo se deshabilita ClassicLink para vpc-8888888.

Comando:

```
aws ec2 disable-vpc-classic-link --vpc-id vpc-88888888
```

Salida:

```
{
  "Return": true
}
```

- Para obtener información sobre la API, consulte DisableVpcClassicLink en la Referencia de comandos de la AWS CLI.

`disassociate-address`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-address`.

AWS CLI

Desasociar una dirección IP elástica en EC2-Classic

En este ejemplo, se desasocia una dirección IP elástica de una instancia en EC2-Classic. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 disassociate-address --public-ip 198.51.100.0
```

Desasociar una dirección IP elástica en EC2-VPC

En este ejemplo, se desasocia una dirección IP elástica de una instancia en una VPC. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 disassociate-address --association-id eipassoc-2bebb745
```

- Para obtener información sobre la API, consulte DisassociateAddress en la Referencia de comandos de la AWS CLI.

`disassociate-client-vpn-target-network`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-client-vpn-target-network`.

AWS CLI

Para desasociar una red de un punto de conexión de Client VPN

En el siguiente ejemplo de `disassociate-client-vpn-target-network` se desasocia la red de destino que está asociada al ID de asociación de `cvpn-assoc-12312312312312312` del punto de conexión de Client VPN especificado.

```
aws ec2 disassociate-client-vpn-target-network \
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde \
    --association-id cvpn-assoc-12312312312312312
```

Salida:

```
{
    "AssociationId": "cvpn-assoc-12312312312312312",
    "Status": {
        "Code": "disassociating"
    }
}
```

Para obtener más información, consulte Target Networks en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte DisassociateClientVpnTargetNetwork en la Referencia de comandos de AWS CLI.

`disassociate-iam-instance-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-iam-instance-profile`.

AWS CLI

Para desasociar un perfil de instancia de IAM

En este ejemplo se desasocia un perfil de instancia de IAM con el ID de asociación `iip-assoc-05020b59952902f5f`.

Comando:

```
aws ec2 disassociate-iam-instance-profile --association-id iip-
assoc-05020b59952902f5f
```

Salida:

```
{
  "IamInstanceProfileAssociation": {
      "InstanceId": "i-123456789abcde123",
      "State": "disassociating",
      "AssociationId": "iip-assoc-05020b59952902f5f",
      "IamInstanceProfile": {
          "Id": "AIPAI5IVIHMFFYY2DKV5Y",
          "Arn": "arn:aws:iam::123456789012:instance-profile/admin-role"
      }
  }
}
```

- Para obtener información sobre la API, consulte DisassociateIamInstanceProfile en la Referencia de comandos de la AWS CLI.

`disassociate-instance-event-window`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-instance-event-window`.

AWS CLI

Ejemplo 1: desasociación de una o varias instancias de un período de evento

En el siguiente ejemplo de `disassociate-instance-event-window` se desasocian una o varias instancias de un período de evento. Especifique el parámetro `instance-event-window-id` para especificar el período de evento. Para desasociar instancias, especifique el parámetro `association-target`, y para los valores del parámetro, especifique uno o varios ID de instancia.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Salida:

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Para conocer las restricciones de los períodos de evento, consulte Consideraciones en la sección sobre eventos programados de la Guía del usuario de Amazon EC2.

Ejemplo 2: desasociación de las etiquetas de instancia de un período de evento

En el siguiente ejemplo de `disassociate-instance-event-window` se desasocian las etiquetas de instancia de un período de evento. Especifique el parámetro `instance-event-window-id` para especificar el período de evento. Para desasociar las etiquetas de instancia, especifique el parámetro `association-target`, y para los valores del parámetro, especifique una o varias etiquetas.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Salida:

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
```

```
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Para conocer las restricciones de los períodos de evento, consulte Consideraciones en la sección sobre eventos programados de la Guía del usuario de Amazon EC2.

Ejemplo 3: desasociación de un host dedicado de un período de evento

En el siguiente ejemplo de `disassociate-instance-event-window` se desasocia un host dedicado de un período de evento. Especifique el parámetro `instance-event-window-id` para especificar el período de evento. Para desasociar un host dedicado, especifique el parámetro `association-target`, y para los valores del parámetro, especifique uno o varios ID de host dedicado.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target DedicatedHostIds=h-029fa35a02b99801d
```

Salida:

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Para conocer las restricciones de los períodos de evento, consulte Consideraciones en la sección sobre eventos programados de la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DisassociateInstanceEventWindow en la Referencia de comandos de la AWS CLI.

`disassociate-ipam-resource-discovery`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-ipam-resource-discovery`.

AWS CLI

Para desasociar una detección de recursos de un IPAM

En este ejemplo, usted es una cuenta de administrador delegado de IPAM y desea desasociar una detección de recursos de IPAM de su IPAM. Ha ejecutado el comando describe y ha observado que `"ResourceDiscoveryStatus": "not-found"`. Desea desasociarlo de su IPAM a fin de dejar espacio para otras asociaciones.

En el siguiente ejemplo de `disassociate-ipam-resource-discovery` se desasocia una detección de recursos de IPAM en su cuenta de AWS.

```
aws ec2 disassociate-ipam-resource-discovery \
    --ipam-resource-discovery-association-id ipam-res-disco-assoc-04382a6346357cf82
 \
    --region us-east-1
```

Salida:

```
{
    "IpamResourceDiscoveryAssociation": {
        "OwnerId": "320805250157",
        "IpamResourceDiscoveryAssociationId": "ipam-res-disco-
assoc-04382a6346357cf82",
        "IpamResourceDiscoveryAssociationArn":
 "arn:aws:ec2::320805250157:ipam-resource-discovery-association/ipam-res-disco-
assoc-04382a6346357cf82",
        "IpamResourceDiscoveryId": "ipam-res-disco-0365d2977fc1672fe",
        "IpamId": "ipam-005f921c17ebd5107",
        "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-005f921c17ebd5107",
        "IpamRegion": "us-east-1",
        "IsDefault": false,
        "ResourceDiscoveryStatus": "not-found",
```

```
        "State": "disassociate-in-progress"
    }
}
```

Para obtener más información, consulte Integración de IPAM con cuentas ajenas a su organización en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte DisassociateIpamResourceDiscovery en la Referencia de comandos de la AWS CLI.

`disassociate-nat-gateway-address`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-nat-gateway-address`.

AWS CLI

Para desasociar una dirección IP elástica de una puerta de enlace de NAT pública

En el siguiente ejemplo de `disassociate-nat-gateway-address` se desasocia la dirección IP elástica especificada de la puerta de enlace de NAT pública especificada.

```
aws ec2 disassociate-nat-gateway-address \
    --nat-gateway-id nat-1234567890abcdef0 \
    --association-ids eipassoc-0f96bdca17EXAMPLE
```

Salida:

```
{
    "NatGatewayId": "nat-1234567890abcdef0",
    "NatGatewayAddresses": [
        {
            "AllocationId": "eipalloc-0be6ecac95EXAMPLE",
            "NetworkInterfaceId": "eni-09cc4b2558794f7f9",
            "PrivateIp": "10.0.0.74",
            "PublicIp": "3.211.231.218",
            "AssociationId": "eipassoc-0f96bdca17EXAMPLE",
            "IsPrimary": false,
            "Status": "disassociating"
        }
    ]
}
```

Para obtener información, consulte Gateways NAT en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte DisassociateNatGatewayAddress en la Referencia de comandos de la AWS CLI.

`disassociate-route-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-route-table`.

AWS CLI

Para desasociar una tabla de enrutamiento

En este ejemplo, se desasocia la tabla de enrutamiento especificada de la subred especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 disassociate-route-table --association-id rtbassoc-781d0d1a
```

- Para obtener información sobre la API, consulte DisassociateRouteTable en la Referencia de comandos de la AWS CLI.

`disassociate-security-group-vpc`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-security-group-vpc`.

AWS CLI

Desasociación de un grupo de seguridad de una VPC

En el siguiente ejemplo de `disassociate-security-group-vpc`, se desasocia el grupo de seguridad especificado de la VPC especificada.

```
aws ec2 disassociate-security-group-vpc \
    --group-id sg-04dbb43907d3f8a78 \
    --vpc-id vpc-0bf4c2739bc05a694
```

Salida:

```
{
```

```
    "State": "disassociating"
}
```

Para obtener más información, consulte Asociación de grupos de seguridad a varias VPC en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte DisassociateSecurityGroupVpc en la Referencia de comandos de la AWS CLI.

`disassociate-subnet-cidr-block`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-subnet-cidr-block`.

AWS CLI

Para desasociar un bloque de CIDR de IPv6 de una subred

En este ejemplo, se desasocia un bloque de CIDR de IPv6 de una subred mediante el ID de asociación del bloque de CIDR.

Comando:

```
aws ec2 disassociate-subnet-cidr-block --association-id subnet-cidr-assoc-3aa54053
```

Salida:

```
{
  "SubnetId": "subnet-5f46ec3b",
  "Ipv6CidrBlockAssociation": {
      "Ipv6CidrBlock": "2001:db8:1234:1a00::/64",
      "AssociationId": "subnet-cidr-assoc-3aa54053",
      "Ipv6CidrBlockState": {
          "State": "disassociating"
      }
  }
}
```

- Para obtener información sobre la API, consulte DisassociateSubnetCidrBlock en la Referencia de comandos de la AWS CLI.

`disassociate-transit-gateway-multicast-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-transit-gateway-multicast-domain`.

AWS CLI

Para desasociar subredes de un dominio de multidifusión

En el siguiente ejemplo de `disassociate-transit-gateway-multicast-domain` se desasocia una subred del dominio de multidifusión especificado.

```
aws ec2 disassociate-transit-gateway-multicast-domain \
    --transit-gateway-attachment-id tgw-attach-070e571cd1EXAMPLE \
    --subnet-id subnet-000de86e3bEXAMPLE \
    --transit-gateway-multicast-domain-id tgw-mcast-domain-0c4905cef7EXAMPLE
```

Salida:

```
{
    "Associations": {
        "TransitGatewayMulticastDomainId": "tgw-mcast-domain-0c4905cef7EXAMPLE",
        "TransitGatewayAttachmentId": "tgw-attach-070e571cd1EXAMPLE",
        "ResourceId": "vpc-7EXAMPLE",
        "ResourceType": "vpc",
        "Subnets": [
            {
                "SubnetId": "subnet-000de86e3bEXAMPLE",
                "State": "disassociating"
            }
        ]
    }
}
```

Para obtener más información, consulte Dominios de multidifusión en la Guía de puertas de enlace de tránsito.

- Para obtener información sobre la API, consulte DisassociateTransitGatewayMulticastDomain en la Referencia de comandos de la AWS CLI.

`disassociate-transit-gateway-route-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-transit-gateway-route-table`.

AWS CLI

Para desasociar una tabla de enrutamiento de puerta de enlace de una conexión de recurso

En el siguiente ejemplo de `disassociate-transit-gateway-route-table` se desasocia la conexión especificada de la tabla de enrutamiento de puerta de enlace.

```
aws ec2 disassociate-transit-gateway-route-table \
    --transit-gateway-route-table-id tgw-rtb-002573ed1eEXAMPLE \
    --transit-gateway-attachment-id tgw-attach-08e0bc912cEXAMPLE
```

Salida:

```
{
    "Association": {
        "TransitGatewayRouteTableId": "tgw-rtb-002573ed1eEXAMPLE",
        "TransitGatewayAttachmentId": "tgw-attach-08e0bc912cEXAMPLE",
        "ResourceId": "11460968-4ac1-4fd3-bdb2-00599EXAMPLE",
        "ResourceType": "direct-connect-gateway",
        "State": "disassociating"
    }
}
```

Para obtener más información, consulte Transit gateway route tables en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte DisassociateTransitGatewayRouteTable en la Referencia de comandos de AWS CLI.

`disassociate-vpc-cidr-block`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-vpc-cidr-block`.

AWS CLI

Para desasociar un bloque de CIDR de IPv6 de una VPC

En este ejemplo, se desasocia un bloque de CIDR de IPv6 de una VPC utilizando el ID de asociación del bloque de CIDR.

Comando:

```
aws ec2 disassociate-vpc-cidr-block --association-id vpc-cidr-assoc-eca54085
```

Salida:

```
{
  "Ipv6CidrBlockAssociation": {
      "Ipv6CidrBlock": "2001:db8:1234:1a00::/56",
      "AssociationId": "vpc-cidr-assoc-eca54085",
      "Ipv6CidrBlockState": {
          "State": "disassociating"
      }
  },
  "VpcId": "vpc-a034d6c4"
}
```

Para desasociar un bloque de CIDR de IPv4 de una VPC

En este ejemplo, se desasocia un bloque de CIDR de IPv4 de una VPC.

Comando:

```
aws ec2 disassociate-vpc-cidr-block --association-id vpc-cidr-assoc-0287ac6b
```

Salida:

```
{
  "CidrBlockAssociation": {
      "AssociationId": "vpc-cidr-assoc-0287ac6b",
      "CidrBlock": "172.18.0.0/16",
      "CidrBlockState": {
          "State": "disassociating"
      }
  },
  "VpcId": "vpc-27621243"
}
```

- Para obtener información sobre la API, consulte DisassociateVpcCidrBlock en la Referencia de comandos de la AWS CLI.

`enable-address-transfer`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-address-transfer`.

AWS CLI

Para habilitar una transferencia de direcciones IP elásticas

En el siguiente ejemplo de `enable-address-transfer` se habilita la transferencia de direcciones IP elásticas para la dirección IP elástica especificada a la cuenta especificada.

```
aws ec2 enable-address-transfer \
    --allocation-id eipalloc-09ad461b0d03f6aaf \
    --transfer-account-id 123456789012
```

Salida:

```
{
     "AddressTransfer": {
        "PublicIp": "100.21.184.216",
        "AllocationId": "eipalloc-09ad461b0d03f6aaf",
        "TransferAccountId": "123456789012",
        "TransferOfferExpirationTimestamp": "2023-02-22T20:51:01.000Z",
        "AddressTransferStatus": "pending"
    }
}
```

Para obtener más información, consulte Transfer Elastic IP addresses en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte EnableAddressTransfer en la Referencia de comandos de la AWS CLI.

`enable-aws-network-performance-metric-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-aws-network-performance-metric-subscription`.

AWS CLI

Para habilitar una suscripción a una métrica

En el siguiente ejemplo de `enable-aws-network-performance-metric-subscription` se habilita la supervisión de la latencia de red agregada entre las regiones de origen y destino especificadas.

```
aws ec2 enable-aws-network-performance-metric-subscription \
    --source us-east-1 \
    --destination eu-west-1 \
    --metric aggregate-latency \
    --statistic p50
```

Salida:

```
{
    "Output": true
}
```

Para obtener más información, consulte Manage subscriptions en la Guía del usuario de rendimiento de la infraestructura.

- Para obtener información sobre la API, consulte EnableAwsNetworkPerformanceMetricSubscription en la Referencia de comandos de la AWS CLI.

`enable-ebs-encryption-by-default`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-ebs-encryption-by-default`.

AWS CLI

Para habilitar el cifrado de EBS de forma predeterminada

En el siguiente ejemplo de `enable-ebs-encryption-by-default` se habilita el cifrado de EBS predeterminado para su cuenta de AWS en la región actual.

```
aws ec2 enable-ebs-encryption-by-default
```

Salida:

```
{
    "EbsEncryptionByDefault": true
}
```

- Para obtener información sobre la API, consulte EnableEbsEncryptionByDefault en la Referencia de comandos de la AWS CLI.

`enable-fast-launch`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-fast-launch`.

AWS CLI

Para iniciar el lanzamiento rápido de una imagen

En el siguiente ejemplo de `enable-fast-launch`, se configura la AMI especificada para el lanzamiento rápido y se establece el número máximo de instancias paralelas que se van a lanzar en 6. El tipo de recurso que se utilizará para aprovisionar previamente la AMI se establece en `snapshot`, que también es el valor predeterminado.

```
aws ec2 enable-fast-launch \
    --image-id ami-01234567890abcedf \
    --max-parallel-launches 6 \
    --resource-type snapshot
```

Salida:

```
{
    "ImageId": "ami-01234567890abcedf",
    "ResourceType": "snapshot",
    "SnapshotConfiguration": {
        "TargetResourceCount": 10
    },
    "LaunchTemplate": {},
    "MaxParallelLaunches": 6,
    "OwnerId": "0123456789123",
    "State": "enabling",
    "StateTransitionReason": "Client.UserInitiated",
    "StateTransitionTime": "2022-01-27T22:16:03.199000+00:00"
```

```
}
```

Para obtener más información, consulte Configure EC2 Fast Launch settings for your Windows AMI en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte EnableFastLaunch en la Referencia de comandos de la AWS CLI.

`enable-fast-snapshot-restores`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-fast-snapshot-restores`.

AWS CLI

Para habilitar la restauración rápida de instantáneas

En el siguiente ejemplo de `enable-fast-snapshot-restores` se habilita la restauración rápida de instantáneas para la instantánea especificada en las zonas de disponibilidad especificadas.

```
aws ec2 enable-fast-snapshot-restores \
    --availability-zones us-east-2a us-east-2b \
    --source-snapshot-ids snap-1234567890abcdef0
```

Salida:

```
{
    "Successful": [
        {
            "SnapshotId": "snap-1234567890abcdef0"
            "AvailabilityZone": "us-east-2a",
            "State": "enabling",
            "StateTransitionReason": "Client.UserInitiated",
            "OwnerId": "123456789012",
            "EnablingTime": "2020-01-25T23:57:49.602Z"
        },
        {
            "SnapshotId": "snap-1234567890abcdef0"
            "AvailabilityZone": "us-east-2b",
            "State": "enabling",
            "StateTransitionReason": "Client.UserInitiated",
            "OwnerId": "123456789012",
```

```
            "EnablingTime": "2020-01-25T23:57:49.596Z"
        }
    ],
    "Unsuccessful": []
}
```

- Para obtener información sobre la API, consulte EnableFastSnapshotRestores en la Referencia de comandos de la AWS CLI.

`enable-image-block-public-access`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-image-block-public-access`.

AWS CLI

Para habilitar el Bloqueo del acceso público de las AMI en la región especificada

En el siguiente ejemplo de `enable-image-block-public-access` se habilita el bloqueo del acceso público de las AMI para la cuenta en la región especificada.

```
aws ec2 enable-image-block-public-access \
    --region us-east-1 \
    --image-block-public-access-state block-new-sharing
```

Salida:

```
{
    "ImageBlockPublicAccessState": "block-new-sharing"
}
```

Para obtener más información, consulte Bloqueo del acceso público de las AMI en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte EnableImageBlockPublicAccess en la Referencia de comandos de la AWS CLI.

`enable-image-deprecation`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-image-deprecation`.

AWS CLI

Dar de baja una AMI

En el siguiente ejemplo de `enable-image-deprecation` se da de baja una AMI en una fecha y hora específicas. Si especifica un valor en segundos, Amazon EC2 redondea los segundos al minuto más cercano. Debe ser el propietario de la AMI para realizar este procedimiento.

```
aws ec2 enable-image-deprecation \
    --image-id ami-1234567890abcdef0 \
    --deprecate-at '2022-10-15T13:17:12.000Z'
```

Salida:

```
{
    "RequestID": "59dbff89-35bd-4eac-99ed-be587EXAMPLE",
    "Return": "true"
}
```

Para obtener más información, consulte Dar de baja una AMI en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte EnableImageDeprecation en la Referencia de comandos de la AWS CLI.

`enable-image-deregistration-protection`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-image-deregistration-protection`.

AWS CLI

Habilitación de la protección contra la anulación del registro

En el siguiente ejemplo de `enable-image-deregistration-protection`, se habilita la protección contra la anulación del registro para la imagen especificada.

```
aws ec2 enable-image-deregistration-protection \
    --image-id ami-0b1a928a144a74ec9
```

Salida:

```
{
    "Return": "enabled-without-cooldown"
}
```

Para obtener más información, consulte Proteger una AMI de EC2 contra la anulación del registro en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte EnableImageDeregistrationProtection en la Referencia de comandos de la AWS CLI.

`enable-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-image`.

AWS CLI

Para habilitar una AMI

En el siguiente ejemplo de `enable-image` se habilita la AMI especificada.

```
aws ec2 enable-image \
    --image-id ami-1234567890abcdef0
```

Salida:

```
{
    "Return": "true"
}
```

Para obtener más información, consulte Inhabilitación de una AMI en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte EnableImage en la Referencia de comandos de la AWS CLI.

`enable-ipam-organization-admin-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-ipam-organization-admin-account`.

AWS CLI

Para realizar la integración con AWS Organizations y delegar en una cuenta de miembro como cuenta de IPAM

En el siguiente ejemplo de `enable-ipam-organization-admin-account` se realiza la integración con AWS Organizations y se delega en una cuenta de miembro como cuenta de IPAM.

```
aws ec2 enable-ipam-organization-admin-account \
    --delegated-admin-account-id 320805250157
```

Salida:

```
{
    "Success": true
}
```

Para obtener más información, consulte Integración de IPAM con AWS Organizations en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte EnableIpamOrganizationAdminAccount en la Referencia de comandos de la AWS CLI.

`enable-reachability-analyzer-organization-sharing`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-reachability-analyzer-organization-sharing`.

AWS CLI

Para habilitar el acceso de confianza del analizador de accesibilidad

En el siguiente ejemplo de `enable-reachability-analyzer-organization-sharing` se habilita el acceso de confianza al analizador de accesibilidad.

```
aws ec2 enable-reachability-analyzer-organization-sharing
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Cross-account analyses en la Guía del usuario del analizador de accesibilidad.

- Para obtener información sobre la API, consulte EnableReachabilityAnalyzerOrganizationSharing en la Referencia de comandos de la AWS CLI.

`enable-serial-console-access`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-serial-console-access`.

AWS CLI

Para habilitar el acceso de su cuenta a la consola serie

En el siguiente ejemplo de `enable-serial-console-access` se habilita el acceso de la cuenta a la consola serie.

```
aws ec2 enable-serial-console-access
```

Salida:

```
{
    "SerialConsoleAccessEnabled": true
}
```

Para obtener más información, consulte Consola serie de EC2 en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte EnableSerialConsoleAccess en la Referencia de comandos de la AWS CLI.

`enable-snapshot-block-public-access`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-snapshot-block-public-access`.

AWS CLI

Para habilitar el Bloqueo del acceso público para las instantáneas

En el siguiente ejemplo de `enable-snapshot-block-public-access` se bloquea todo el uso compartido público de sus instantáneas.

```
aws ec2 enable-snapshot-block-public-access \
    --state block-all-sharing
```

Salida:

```
{
    "State": "block-all-sharing"
}
```

Para obtener más información, consulte Block public access for snapshots en la Guía del usuario de Amazon EBS.

- Para obtener información sobre la API, consulte EnableSnapshotBlockPublicAccess en la Referencia de comandos de la AWS CLI.

`enable-transit-gateway-route-table-propagation`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-transit-gateway-route-table-propagation`.

AWS CLI

Para habilitar una conexión de puerta de enlace de tránsito a fin de propagar rutas a la tabla de enrutamiento de propagación especificada

En el siguiente ejemplo de `enable-transit-gateway-route-table-propagation` se habilita la conexión especificada para propagar las rutas a la tabla de enrutamiento de propagación especificada.

```
aws ec2 enable-transit-gateway-route-table-propagation \
    --transit-gateway-route-table-id tgw-rtb-0a823edbdeEXAMPLE \
    --transit-gateway-attachment-id tgw-attach-09b52ccdb5EXAMPLE
```

Salida:

```
{
    "Propagation": {
        "TransitGatewayAttachmentId": "tgw-attach-09b52ccdb5EXAMPLE",
        "ResourceId": "vpc-4d7de228",
        "ResourceType": "vpc",
```

```
        "TransitGatewayRouteTableId": "tgw-rtb-0a823edbdeEXAMPLE",
        "State": "disabled"
    }
}
```

Para obtener más información, consulte Transit gateway route tables en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte EnableTransitGatewayRouteTablePropagation en la Referencia de comandos de la AWS CLI.

`enable-vgw-route-propagation`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-vgw-route-propagation`.

AWS CLI

Para habilitar la propagación de rutas

En este ejemplo, se permite que la puerta de enlace privada virtual especificada propague rutas estáticas a la tabla de enrutamiento especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 enable-vgw-route-propagation --route-table-id rtb-22574640 --gateway-
id vgw-9a4cacf3
```

- Para obtener información sobre la API, consulte EnableVgwRoutePropagation en la Referencia de comandos de la AWS CLI.

`enable-volume-io`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-volume-io`.

AWS CLI

Para habilitar la E/S de un volumen

En este ejemplo, se habilita la E/S en el volumen `vol-1234567890abcdef0`.

Comando:

```
aws ec2 enable-volume-io --volume-id vol-1234567890abcdef0
```

Salida:

```
{
  "Return": true
}
```

- Para obtener información sobre la API, consulte EnableVolumeIo en la Referencia de comandos de la AWS CLI.

`enable-vpc-classic-link-dns-support`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-vpc-classic-link-dns-support`.

AWS CLI

Para habilitar la compatibilidad de DNS de ClassicLink con una VPC

En este ejemplo, se habilita la compatibilidad de DNS de ClassicLink con `vpc-88888888`.

Comando:

```
aws ec2 enable-vpc-classic-link-dns-support --vpc-id vpc-88888888
```

Salida:

```
{
  "Return": true
}
```

- Para obtener información sobre la API, consulte EnableVpcClassicLinkDnsSupport en la Referencia de comandos de la AWS CLI.

`enable-vpc-classic-link`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-vpc-classic-link`.

AWS CLI

Para habilitar una VPC en ClassicLink

En este ejemplo, se habilita vpc-8888888 para ClassicLink.

Comando:

```
aws ec2 enable-vpc-classic-link --vpc-id vpc-88888888
```

Salida:

```
{
  "Return": true
}
```

- Para obtener información sobre la API, consulte EnableVpcClassicLink en la Referencia de comandos de la AWS CLI.

`export-client-vpn-client-certificate-revocation-list`

En el siguiente ejemplo de código, se muestra cómo utilizar `export-client-vpn-client-certificate-revocation-list`.

AWS CLI

Para exportar una lista de revocación de certificados del cliente

En el siguiente ejemplo de `export-client-vpn-client-certificate-revocation-list` se exporta la lista de revocación de certificados del cliente para el punto de conexión de Client VPN especificado. En este ejemplo, la salida se devuelve en formato de texto para facilitar su lectura.

```
aws ec2 export-client-vpn-client-certificate-revocation-list \
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde \
    --output text
```

Salida:

```
-----BEGIN X509 CRL-----
```

```
MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END X509 CRL-----
STATUS      pending
```

Para obtener más información, consulte Client Certificate Revocation Lists en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte ExportClientVpnClientCertificateRevocationList en la Referencia de comandos de la AWS CLI.

`export-client-vpn-client-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `export-client-vpn-client-configuration`.

AWS CLI

Para exportar la configuración del cliente

En el siguiente ejemplo de `export-client-vpn-client-configuration` se exporta la configuración del cliente para el punto de conexión de Client VPN especificado. En este ejemplo, la salida se devuelve en formato de texto para facilitar su lectura.

```
aws ec2 export-client-vpn-client-configuration \
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde \
    --output text
```

Salida:

```
client
dev tun
proto udp
remote cvpn-endpoint-123456789123abcde.prod.clientvpn.ap-south-1.amazonaws.com 443
remote-random-hostname
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-GCM
verb 3
<ca>
-----BEGIN CERTIFICATE-----
MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----
</ca>
reneg-sec 0
```

Para obtener más información, consulte Exportación del archivo de configuración del punto de conexión de Client VPN en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte ExportClientVpnClientConfiguration en la Referencia de comandos de la AWS CLI.

`export-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `export-image`.

AWS CLI

Para exportar una máquina virtual desde una AMI

En el siguiente ejemplo de `export-image` se exporta la AMI especificada al bucket especificado en el formato especificado.

```
aws ec2 export-image \
    --image-id ami-1234567890abcdef0 \
    --disk-image-format VMDK \
    --s3-export-location S3Bucket=my-export-bucket,S3Prefix=exports/
```

Salida:

```
{
    "DiskImageFormat": "vmdk",
    "ExportImageTaskId": "export-ami-1234567890abcdef0"
    "ImageId": "ami-1234567890abcdef0",
    "RoleName": "vmimport",
    "Progress": "0",
    "S3ExportLocation": {
        "S3Bucket": "my-export-bucket",
        "S3Prefix": "exports/"
    },
    "Status": "active",
    "StatusMessage": "validating"
}
```

- Para obtener información sobre la API, consulte ExportImage en la Referencia de comandos de la AWS CLI.

`get-associated-ipv6-pool-cidrs`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-associated-ipv6-pool-cidrs`.

AWS CLI

Para obtener las asociaciones de un conjunto de direcciones IPv

En el siguiente ejemplo de `get-associated-ipv6-pool-cidrs` se obtienen las asociaciones del conjunto de direcciones IPv6 especificado.

```
aws ec2 get-associated-ipv6-pool-cidrs \
    --pool-id ipv6pool-ec2-012345abc12345abc
```

Salida:

```
{
    "Ipv6CidrAssociations": [
        {
            "Ipv6Cidr": "2001:db8:1234:1a00::/56",
            "AssociatedResource": "vpc-111111222222333ab"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetAssociatedIpv6PoolCidrs en la Referencia de comandos de la AWS CLI.

`get-aws-network-performance-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-aws-network-performance-data`.

AWS CLI

Para obtener datos de rendimiento de la red

En el siguiente ejemplo de `get-aws-network-performance-data` se recuperan datos sobre el rendimiento de la red entre las regiones especificadas en el período especificado.

```
aws ec2 get-aws-network-performance-data \
    --start-time 2022-10-26T12:00:00.000Z \
    --end-time 2022-10-26T12:30:00.000Z \
    --data-queries Id=my-query,Source=us-east-1,Destination=eu-
west-1,Metric=aggregate-latency,Statistic=p50,Period=five-minutes
```

Salida:

```
{
    "DataResponses": [
        {
            "Id": "my-query",
```

```
            "Source": "us-east-1",
            "Destination": "eu-west-1",
            "Metric": "aggregate-latency",
            "Statistic": "p50",
            "Period": "five-minutes",
            "MetricPoints": [
                {
                    "StartDate": "2022-10-26T12:00:00+00:00",
                    "EndDate": "2022-10-26T12:05:00+00:00",
                    "Value": 62.44349,
                    "Status": "OK"
                },
                {
                    "StartDate": "2022-10-26T12:05:00+00:00",
                    "EndDate": "2022-10-26T12:10:00+00:00",
                    "Value": 62.483498,
                    "Status": "OK"
                },
                {
                    "StartDate": "2022-10-26T12:10:00+00:00",
                    "EndDate": "2022-10-26T12:15:00+00:00",
                    "Value": 62.51248,
                    "Status": "OK"
                },
                {
                    "StartDate": "2022-10-26T12:15:00+00:00",
                    "EndDate": "2022-10-26T12:20:00+00:00",
                    "Value": 62.635475,
                    "Status": "OK"
                },
                {
                    "StartDate": "2022-10-26T12:20:00+00:00",
                    "EndDate": "2022-10-26T12:25:00+00:00",
                    "Value": 62.733974,
                    "Status": "OK"
                },
                {
                    "StartDate": "2022-10-26T12:25:00+00:00",
                    "EndDate": "2022-10-26T12:30:00+00:00",
                    "Value": 62.773975,
                    "Status": "OK"
                },
                {
                    "StartDate": "2022-10-26T12:30:00+00:00",
```

```
                    "EndDate": "2022-10-26T12:35:00+00:00",
                    "Value": 62.75349,
                    "Status": "OK"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Monitor network performance en la Guía del usuario de rendimiento de la infraestructura.

- Para obtener información sobre la API, consulte GetAwsNetworkPerformanceData en la Referencia de comandos de la AWS CLI.

`get-capacity-reservation-usage`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-capacity-reservation-usage`.

AWS CLI

Para consultar el uso de reservas de capacidad en todas las cuentas de AWS

En el siguiente ejemplo de `get-capacity-reservation-usage` se muestra la información de uso de la reserva de capacidad especificada.

```
aws ec2 get-capacity-reservation-usage \
    --capacity-reservation-id cr-1234abcd56EXAMPLE
```

Salida:

```
{
    "CapacityReservationId": "cr-1234abcd56EXAMPLE ",
    "InstanceUsages": [
        {
            "UsedInstanceCount": 1,
            "AccountId": "123456789012"
        }
    ],
    "AvailableInstanceCount": 4,
    "TotalInstanceCount": 5,
    "State": "active",
```

```
    "InstanceType": "t2.medium"
}
```

Para obtener más información, consulte Reservas de capacidad compartida en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte GetCapacityReservationUsage en la Referencia de comandos de la AWS CLI.

`get-coip-pool-usage`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-coip-pool-usage`.

AWS CLI

Para obtener el uso del grupo de direcciones IP propiedad del cliente

En el siguiente ejemplo de `get-coip-pool-usage` se obtiene información sobre el uso del grupo de direcciones IP propiedad del cliente especificado.

```
aws ec2 get-coip-pool-usage \
    --pool-id ipv4pool-coip-123a45678bEXAMPLE
```

Salida:

```
{
    "CoipPoolId": "ipv4pool-coip-123a45678bEXAMPLE",
    "CoipAddressUsages": [
        {
            "CoIp": "0.0.0.0"
        },
        {
            "AllocationId": "eipalloc-123ab45c6dEXAMPLE",
            "AwsAccountId": "123456789012",
            "CoIp": "0.0.0.0"
        },
        {
            "AllocationId": "eipalloc-123ab45c6dEXAMPLE",
            "AwsAccountId": "123456789111",
            "CoIp": "0.0.0.0"
        }
    ],
```

```
    "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE"
}
```

Para obtener más información, consulte Direcciones IP propiedad del cliente en la Guía del usuario de AWS Outposts para bastidores de Outposts.

- Para obtener información sobre la API, consulte GetCoipPoolUsage en la Referencia de comandos de la AWS CLI.

`get-console-output`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-console-output`.

AWS CLI

Ejemplo 1: obtención de la salida de la consola

En el siguiente ejemplo de `get-console-output` se obtiene la salida de la consola para la instancia de Linux especificada.

```
aws ec2 get-console-output \
    --instance-id i-1234567890abcdef0
```

Salida:

```
{
    "InstanceId": "i-1234567890abcdef0",
    "Timestamp": "2013-07-25T21:23:53.000Z",
    "Output": "..."
}
```

Para obtener más información, consulte Salida de la consola de instancias en la Guía del usuario de Amazon EC2.

Ejemplo 2: obtención de la salida más reciente de la consola

En el siguiente ejemplo de `get-console-output` se obtiene la salida más reciente de la consola para la instancia de Linux especificada.

```
aws ec2 get-console-output \
    --instance-id i-1234567890abcdef0 \
```

```
    --latest \
    --output text
```

Salida:

```
i-1234567890abcdef0 [    0.000000] Command line: root=LABEL=/ console=tty1
 console=ttyS0 selinux=0 nvme_core.io_timeout=4294967295
[    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point
 registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
...
Cloud-init v. 0.7.6 finished at Wed, 09 May 2018 19:01:13 +0000. Datasource
 DataSourceEc2.  Up 21.50 seconds
Amazon Linux AMI release 2018.03
Kernel 4.14.26-46.32.amzn1.x
```

Para obtener más información, consulte Salida de la consola de instancias en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte GetConsoleOutput en la Referencia de comandos de la AWS CLI.

`get-console-screenshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-console-screenshot`.

AWS CLI

Para recuperar una captura de pantalla de una instancia en ejecución

En el siguiente ejemplo de `get-console-screenshot` se recupera una captura de pantalla de la instancia especificada en formato .jpg. La captura de pantalla que se devuelve es una cadena codificada en base64.

```
aws ec2 get-console-screenshot \
    --instance-id i-1234567890abcdef0
```

Salida:

```
{
```

```
    "ImageData": "997987/8kgj49ikjhewkwwe0008084EXAMPLE",
    "InstanceId": "i-1234567890abcdef0"
}
```

- Para obtener información sobre la API, consulte GetConsoleScreenshot en la Referencia de comandos de la AWS CLI.

`get-default-credit-specification`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-default-credit-specification`.

AWS CLI

Para describir la opción de crédito predeterminada

En el siguiente ejemplo de `get-default-credit-specification` se describe la opción de crédito predeterminada de las instancias T2.

```
aws ec2 get-default-credit-specification \
    --instance-family t2
```

Salida:

```
{
    "InstanceFamilyCreditSpecification": {
        "InstanceFamily": "t2",
        "CpuCredits": "standard"
    }
}
```

- Para obtener información sobre la API, consulte GetDefaultCreditSpecification en la Referencia de comandos de la AWS CLI.

`get-ebs-default-kms-key-id`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ebs-default-kms-key-id`.

AWS CLI

Para describir su CMK predeterminada para el cifrado de EBS

En el siguiente ejemplo de `get-ebs-default-kms-key-id` se describe la CMK predeterminada para el cifrado de EBS de su cuenta de AWS.

```
aws ec2 get-ebs-default-kms-key-id
```

En la salida se muestra la CMK predeterminada para el cifrado de EBS, que es una CMK administrada por AWS con el alias `alias/aws/ebs`.

```
{
    "KmsKeyId": "alias/aws/ebs"
}
```

En la siguiente salida se muestra una CMK personalizada para el cifrado de EBS.

```
{
    "KmsKeyId": "arn:aws:kms:us-
west-2:123456789012:key/0ea3fef3-80a7-4778-9d8c-1c0c6EXAMPLE"
}
```

- Para obtener información sobre la API, consulte GetEbsDefaultKmsKeyId en la Referencia de comandos de la AWS CLI.

`get-ebs-encryption-by-default`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ebs-encryption-by-default`.

AWS CLI

Para describir si se ha habilitado el cifrado de EBS de forma predeterminada

En el siguiente ejemplo de `get-ebs-encryption-by-default` se indica si el cifrado de EBS predeterminado está habilitado para su cuenta de AWS en la región actual.

```
aws ec2 get-ebs-encryption-by-default
```

En la siguiente salida se indica que el cifrado de EBS predeterminado está deshabilitado.

```
{
    "EbsEncryptionByDefault": false
}
```

En la siguiente salida se indica que el cifrado de EBS predeterminado está habilitado.

```
{
    "EbsEncryptionByDefault": true
}
```

- Para obtener información sobre la API, consulte GetEbsEncryptionByDefault en la Referencia de comandos de la AWS CLI.

`get-flow-logs-integration-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-flow-logs-integration-template`.

AWS CLI

Para crear una plantilla de CloudFormation a fin de automatizar la integración de los registros de flujo de VPC con Amazon Athena

En el siguiente ejemplo de `get-flow-logs-integration-template` se crea una plantilla de CloudFormation a fin de automatizar la integración de los registros de flujo de VPC con Amazon Athena.

Linux:

```
aws ec2 get-flow-logs-integration-template \
    --flow-log-id fl-1234567890abcdef0 \
    --config-delivery-s3-destination-arn arn:aws:s3:::amzn-s3-demo-bucket \
    --integrate-services
 AthenaIntegrations='[{IntegrationResultS3DestinationArn=arn:aws:s3:::amzn-s3-demo-
bucket,PartitionLoadFrequency=none,PartitionStartDate=2021-07-21T00:40:00,PartitionEndDate=2
{IntegrationResultS3DestinationArn=arn:aws:s3:::amzn-s3-demo-
bucket,PartitionLoadFrequency=none,PartitionStartDate=2021-07-21T00:40:00,PartitionEndDate=2
```

Windows:

```
aws ec2 get-flow-logs-integration-template ^
    --flow-log-id fl-1234567890abcdef0 ^
    --config-delivery-s3-destination-arn arn:aws:s3:::amzn-s3-demo-bucket ^
    --integrate-
services AthenaIntegrations=[{IntegrationResultS3DestinationArn=arn:aws:s3:::amzn-
s3-demo-
```

```
bucket,PartitionLoadFrequency=none,PartitionStartDate=2021-07-21T00:40:00,PartitionEndDate=2
{IntegrationResultS3DestinationArn=arn:aws:s3:::amzn-s3-demo-
bucket,PartitionLoadFrequency=none,PartitionStartDate=2021-07-21T00:40:00,PartitionEndDate=2
```

Salida:

```
{
    "Result": "https://amzn-s3-demo-bucket.s3.us-east-2.amazonaws.com/
VPCFlowLogsIntegrationTemplate_fl-1234567890abcdef0_Wed%20Jul
%2021%2000%3A57%3A56%20UTC%202021.yml"
}
```

Para obtener más información sobre el uso de plantillas de CloudFormation, consulte Trabajo con plantillas de AWS CloudFormation en la Guía del usuario de AWS CloudFormation.

Para obtener información sobre el uso de Amazon Athena y los registros de flujo, consulte Realizar consultas en los registros de flujo mediante Amazon Athena en la Guía del usuario de Amazon Virtual Private Cloud.

- Para obtener información sobre la API, consulte GetFlowLogsIntegrationTemplate en la Referencia de comandos de la AWS CLI.

`get-groups-for-capacity-reservation`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-groups-for-capacity-reservation`.

AWS CLI

Para enumerar los grupos de recursos con una reserva de capacidad

En el siguiente ejemplo de `get-groups-for-capacity-reservation` se enumeran los grupos de recursos a los que se ha agregado la reserva de capacidad especificada.

```
aws ec2 get-groups-for-capacity-reservation \
    --capacity-reservation-id cr-1234abcd56EXAMPLE
```

Salida:

```
{
    "CapacityReservationsGroup": [
        {
```

```
            "GroupArn": "arn:aws:resource-groups:us-west-2:123456789012:group/my-
resource-group",
            "OwnerId": "123456789012"
        }
    ]
}
```

Para obtener más información, consulte Grupos de reservas de capacidad en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte GetGroupsForCapacityReservation en la Referencia de comandos de la AWS CLI.

`get-host-reservation-purchase-preview`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-host-reservation-purchase-preview`.

AWS CLI

Para obtener una vista previa de la compra de una reserva de host dedicado

En este ejemplo, se proporciona una vista previa de los costos de una reserva de host dedicado especificada para el host dedicado especificado en su cuenta.

Comando:

```
aws ec2 get-host-reservation-purchase-preview --offering-id hro-03f707bf363b6b324 --
host-id-set h-013abcd2a00cbd123
```

Salida:

```
{
  "TotalHourlyPrice": "1.499",
  "Purchase": [
      {
          "HourlyPrice": "1.499",
          "InstanceFamily": "m4",
          "PaymentOption": "NoUpfront",
          "HostIdSet": [
              "h-013abcd2a00cbd123"
          ],
```

```
            "UpfrontPrice": "0.000",
            "Duration": 31536000
        }
    ],
    "TotalUpfrontPrice": "0.000"
}
```

- Para obtener información sobre la API, consulte GetHostReservationPurchasePreview en la Referencia de comandos de la AWS CLI.

`get-image-block-public-access-state`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-image-block-public-access-state`.

AWS CLI

Para obtener el estado del Bloqueo del acceso público de las AMI en la región especificada

En el siguiente ejemplo de `get-image-block-public-access-state`, se obtiene el estado del Bloqueo del acceso público de las AMI para la cuenta en la región especificada.

```
aws ec2 get-image-block-public-access-state \
    --region us-east-1
```

Salida:

```
{
    "ImageBlockPublicAccessState": "block-new-sharing"
}
```

Para obtener más información, consulte Bloqueo del acceso público de las AMI en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte GetImageBlockPublicAccessState en la Referencia de comandos de la AWS CLI.

`get-instance-types-from-instance-requirements`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-instance-types-from-instance-requirements`.

AWS CLI

Para obtener una vista previa de los tipos de instancias que coinciden con los atributos especificados

En el siguiente ejemplo de `get-instance-types-from-instance-requirements`, primero se genera una lista de todos los atributos posibles que se pueden especificar mediante el parámetro `--generate-cli-skeleton`. Después, se guarda la lista en un archivo JSON. A continuación, el archivo JSON se usa para personalizar los atributos cuya vista previa de los tipos de instancias coincidentes se desea obtener.

Para generar todos los atributos posibles y guardar la salida directamente en un archivo JSON, use el siguiente comando.

```
aws ec2 get-instance-types-from-instance-requirements \
    --region us-east-1 \
    --generate-cli-skeleton input > attributes.json
```

Salida:

```
{
    "DryRun": true,
    "ArchitectureTypes": [
        "x86_64_mac"
    ],
    "VirtualizationTypes": [
        "paravirtual"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 0,
            "Max": 0
        },
        "MemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "CpuManufacturers": [
            "intel"
        ],
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
```

```
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
            ""
        ],
        "InstanceGenerations": [
            "current"
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "excluded",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
        "LocalStorage": "required",
        "LocalStorageTypes": [
            "hdd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorTypes": [
            "inference"
        ],
        "AcceleratorCount": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorManufacturers": [
            "xilinx"
        ],
        "AcceleratorNames": [
            "t4"
        ],
        "AcceleratorTotalMemoryMiB": {
            "Min": 0,
```

```
            "Max": 0
        }
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

Configure el archivo JSON. Debe proporcionar valores para `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` y `MemoryMiB`. Puede omitir los demás atributos. Si se omite, se utilizan los valores predeterminados. Para obtener una descripción de cada atributo y sus valores predeterminados, consulte get-instance-types-from-instance-requirements <https://docs.aws.amazon.com/cli/latest/reference/ec2/get-instance-types-from-instance-requirements.html>.

Obtenga la vista previa de los tipos de instancias que tienen los atributos especificados en `attributes.json`. Especifique el nombre y la ruta del archivo JSON mediante el parámetro `--cli-input-json`. En la siguiente solicitud, la salida tiene formato de tabla.

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
    --output table
```

Contenido del archivo `attributes.json`:

```
{

    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
        },
        "InstanceGenerations": [
            "current"
```

```
        ]
    }
}
```

Salida:

```
-----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+---------------------------------------+
||             InstanceTypes             ||
|+-------------------------------------+|
||             InstanceType              ||
|+-------------------------------------+|
||  c4.xlarge                          ||
||  c5.xlarge                          ||
||  c5a.xlarge                         ||
||  c5ad.xlarge                        ||
||  c5d.xlarge                         ||
||  c5n.xlarge                         ||
||  d2.xlarge                          ||
...
```

Para obtener más información sobre la selección del tipo de instancia basada en atributos, consulte Cómo funciona la selección de tipo de instancia basada en atributos en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte GetInstanceTypesFromInstanceRequirements en la Referencia de comandos de la AWS CLI.

`get-instance-uefi-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-instance-uefi-data`.

AWS CLI

Para recuperar datos de UEFI de una instancia

En el siguiente ejemplo de `get-instance-uefi-data` se recuperan los datos de UEFI de una instancia. Si la salida está vacía, la instancia no contiene datos UEFI.

```
aws ec2 get-instance-uefi-data \
    --instance-id i-0123456789example
```

Salida:

```
{
    "InstanceId": "i-0123456789example",
    "UefiData": "QU1aTlVFRkkf+uLXAAAAAHj5a7fZ9+3dBzxXb/.
    <snipped>
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAD4L/J/AODshho="
}
```

Para obtener más información, consulte Arranque seguro de UEFI en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte GetInstanceUefiData en la Referencia de comandos de la AWS CLI.

`get-ipam-address-history`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ipam-address-history`.

AWS CLI

Para obtener el historial de un CIDR

En el siguiente ejemplo de `get-ipam-address-history` se obtiene el historial de un CIDR.

(Linux):

```
aws ec2 get-ipam-address-history \
   --cidr 10.0.0.0/16 \
   --ipam-scope-id ipam-scope-02fc38cd4c48e7d38 \
   --start-time 2021-12-08T01:00:00.000Z \
   --end-time 2021-12-10T01:00:00.000Z
```

(Windows):

```
aws ec2 get-ipam-address-history ^
   --cidr 10.0.0.0/16 ^
   --ipam-scope-id ipam-scope-02fc38cd4c48e7d38 ^
   --start-time 2021-12-08T01:00:00.000Z ^
   --end-time 2021-12-10T01:00:00.000Z
```

Salida:

```
{
    "HistoryRecords": [
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-west-1",
            "ResourceType": "vpc",
            "ResourceId": "vpc-06cbefa9ee907e1c0",
            "ResourceCidr": "10.0.0.0/16",
            "ResourceName": "Demo",
            "ResourceComplianceStatus": "unmanaged",
            "ResourceOverlapStatus": "overlapping",
            "VpcId": "vpc-06cbefa9ee907e1c0",
            "SampledStartTime": "2021-12-08T19:54:57.675000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-2",
            "ResourceType": "vpc",
            "ResourceId": "vpc-042702f474812c9ad",
            "ResourceCidr": "10.0.0.0/16",
            "ResourceName": "test",
            "ResourceComplianceStatus": "unmanaged",
            "ResourceOverlapStatus": "overlapping",
            "VpcId": "vpc-042702f474812c9ad",
            "SampledStartTime": "2021-12-08T19:54:59.019000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-2",
            "ResourceType": "vpc",
            "ResourceId": "vpc-042b8a44f64267d67",
            "ResourceCidr": "10.0.0.0/16",
            "ResourceName": "tester",
            "ResourceComplianceStatus": "unmanaged",
            "ResourceOverlapStatus": "overlapping",
            "VpcId": "vpc-042b8a44f64267d67",
            "SampledStartTime": "2021-12-08T19:54:59.019000+00:00"
        }
    ]
}
```


Para obtener más información, consulte Ver historial de direcciones IP en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte GetIpamAddressHistory en la Referencia de comandos de la AWS CLI.

`get-ipam-discovered-accounts`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ipam-discovered-accounts`.

AWS CLI

Para ver las cuentas detectadas por un IPAM

En este caso, usted es un administrador delegado de IPAM y desea ver las cuentas de AWS que poseen los recursos detectados por el IPAM.

La región `--discovery-region` es la región operativa de IPAM en la que desea ver los estados de las cuentas supervisadas. Por ejemplo, si tiene tres regiones operativas de IPAM, puede ser conveniente realizar esta solicitud tres veces para ver las marcas de fecha y hora específicas de la detección en cada una de esas regiones concretas.

En el siguiente ejemplo de `get-ipam-discovered-accounts` se enumeran las cuentas de AWS que poseen los recursos detectados por el IPAM.

```
aws ec2 get-ipam-discovered-accounts \
   --ipam-resource-discovery-id ipam-res-disco-0365d2977fc1672fe \
   --discovery-region us-east-1
```

Salida:

```
{
    "IpamDiscoveredAccounts": [
        {
            "AccountId": "149977607591",
            "DiscoveryRegion": "us-east-1",
            "LastAttemptedDiscoveryTime": "2024-02-09T19:04:31.379000+00:00",
            "LastSuccessfulDiscoveryTime": "2024-02-09T19:04:31.379000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Integración de IPAM con cuentas ajenas a su organización en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte GetIpamDiscoveredAccounts en la Referencia de comandos de la AWS CLI.

`get-ipam-discovered-public-addresses`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ipam-discovered-public-addresses`.

AWS CLI

Para ver las direcciones IP públicas detectadas

En este ejemplo, usted es un administrador delegado de IPAM y desea ver las direcciones IP de los recursos detectados por IPAM. Puede obtener el ID de la detección de recursos mediante describe-ipam-resource-discoveries.

En el siguiente ejemplo de `get-ipam-discovered-public-addresses` se muestran las direcciones IP públicas detectadas para una detección de recurso.

```
aws ec2 get-ipam-discovered-public-addresses \
    --ipam-resource-discovery-id ipam-res-disco-0f4ef577a9f37a162 \
    --address-region us-east-1 \
    --region us-east-1
```

Salida:

```
{
    "IpamDiscoveredPublicAddresses": [
        {
           "IpamResourceDiscoveryId": "ipam-res-disco-0f4ef577a9f37a162",
            "AddressRegion": "us-east-1",
            "Address": "54.208.155.7",
            "AddressOwnerId": "320805250157",
            "AssociationStatus": "associated",
            "AddressType": "ec2-public-ip",
            "VpcId": "vpc-073b294916198ce49",
            "SubnetId": "subnet-0b6c8a8839e9a4f15",
            "NetworkInterfaceId": "eni-081c446b5284a5e06",
            "NetworkInterfaceDescription": "",
            "InstanceId": "i-07459a6fca5b35823",
            "Tags": {},
```

```
            "NetworkBorderGroup": "us-east-1c",
            "SecurityGroups": [
                {
                    "GroupName": "launch-wizard-2",
                    "GroupId": "sg-0a489dd6a65c244ce"
                }
            ],
            "SampleTime": "2024-04-05T15:13:59.228000+00:00"
        },
        {
            "IpamResourceDiscoveryId": "ipam-res-disco-0f4ef577a9f37a162",
            "AddressRegion": "us-east-1",
            "Address": "44.201.251.218",
            "AddressOwnerId": "470889052923",
            "AssociationStatus": "associated",
            "AddressType": "ec2-public-ip",
            "VpcId": "vpc-6c31a611",
            "SubnetId": "subnet-062f47608b99834b1",
            "NetworkInterfaceId": "eni-024845359c2c3ae9b",
            "NetworkInterfaceDescription": "",
            "InstanceId": "i-04ef786d9c4e03f41",
            "Tags": {},
            "NetworkBorderGroup": "us-east-1a",
            "SecurityGroups": [
                {
                    "GroupName": "launch-wizard-32",
                    "GroupId": "sg-0ed1a426e96a68374"
                }
            ],
            "SampleTime": "2024-04-05T15:13:59.145000+00:00"
        }
}
```

Para obtener más información, consulte Ver información sobre IP públicas en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte GetIpamDiscoveredPublicAddresses en la Referencia de comandos de la AWS CLI.

`get-ipam-discovered-resource-cidrs`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ipam-discovered-resource-cidrs`.

AWS CLI

Para ver los CIDR de las direcciones IP detectadas por un IPAM

En este ejemplo, usted es un administrador delegado del IPAM y desea ver los detalles relacionados con los CIDR de las direcciones IP de los recursos detectados por el IPAM.

Para llevar a cabo esta solicitud:

La detección de recursos que elija debe estar asociada al IPAM. La región `--resource-region` es la región de AWS en la que se creó el recurso.

En el siguiente ejemplo de `get-ipam-discovered-resource-cidrs` se enumeran las direcciones IP de los recursos detectados por el IPAM.

```
aws ec2 get-ipam-discovered-resource-cidrs \
   --ipam-resource-discovery-id ipam-res-disco-0365d2977fc1672fe \
   --resource-region us-east-1
```

Salida:

```
{
    {
        "IpamDiscoveredResourceCidrs": [
        {
            "IpamResourceDiscoveryId": "ipam-res-disco-0365d2977fc1672fe",
            "ResourceRegion": "us-east-1",
            "ResourceId": "vpc-0c974c95ca7ceef4a",
            "ResourceOwnerId": "149977607591",
            "ResourceCidr": "172.31.0.0/16",
            "ResourceType": "vpc",
            "ResourceTags": [],
            "IpUsage": 0.375,
            "VpcId": "vpc-0c974c95ca7ceef4a",
            "SampleTime": "2024-02-09T19:15:16.529000+00:00"
        },
        {
            "IpamResourceDiscoveryId": "ipam-res-disco-0365d2977fc1672fe",
            "ResourceRegion": "us-east-1",
            "ResourceId": "subnet-07fe028119082a8c1",
            "ResourceOwnerId": "149977607591",
            "ResourceCidr": "172.31.0.0/20",
            "ResourceType": "subnet",
```

```
            "ResourceTags": [],
            "IpUsage": 0.0012,
            "VpcId": "vpc-0c974c95ca7ceef4a",
            "SampleTime": "2024-02-09T19:15:16.529000+00:00"
        },
        {
            "IpamResourceDiscoveryId": "ipam-res-disco-0365d2977fc1672fe",
            "ResourceRegion": "us-east-1",
            "ResourceId": "subnet-0a96893763984cc4e",
            "ResourceOwnerId": "149977607591",
            "ResourceCidr": "172.31.64.0/20",
            "ResourceType": "subnet",
            "ResourceTags": [],
            "IpUsage": 0.0012,
            "VpcId": "vpc-0c974c95ca7ceef4a",
            "SampleTime": "2024-02-09T19:15:16.529000+00:00"
        }
    }
}
```

Para obtener más información, consulte Monitorear el uso de CIDR por recurso en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte GetIpamDiscoveredResourceCidrs en la Referencia de comandos de la AWS CLI.

`get-ipam-pool-allocations`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ipam-pool-allocations`.

AWS CLI

Para obtener los CIDR asignados de un grupo de IPAM

En el siguiente ejemplo de `get-ipam-pool-allocations` se obtienen los CIDR asignados de un grupo de IPAM.

(Linux):

```
aws ec2 get-ipam-pool-allocations \
    --ipam-pool-id ipam-pool-0533048da7d823723 \
    --filters Name=ipam-pool-allocation-id,Values=ipam-pool-
alloc-0e6186d73999e47389266a5d6991e6220
```

(Windows):

```
aws ec2 get-ipam-pool-allocations ^
    --ipam-pool-id ipam-pool-0533048da7d823723 ^
    --filters Name=ipam-pool-allocation-id,Values=ipam-pool-
alloc-0e6186d73999e47389266a5d6991e6220
```

Salida:

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "10.0.0.0/16",
            "IpamPoolAllocationId": "ipam-pool-
alloc-0e6186d73999e47389266a5d6991e6220",
            "ResourceType": "custom",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetIpamPoolAllocations en la Referencia de comandos de la AWS CLI.

`get-ipam-pool-cidrs`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ipam-pool-cidrs`.

AWS CLI

Para obtener los CIDR aprovisionados en un grupo de IPAM

En el siguiente ejemplo de `get-ipam-pool-cidrs` se obtienen los CIDR aprovisionados en un grupo de IPAM.

(Linux):

```
aws ec2 get-ipam-pool-cidrs \
    --ipam-pool-id ipam-pool-0533048da7d823723 \
    --filters 'Name=cidr,Values=10.*'
```

(Windows):

```
aws ec2 get-ipam-pool-cidrs ^
    --ipam-pool-id ipam-pool-0533048da7d823723 ^
    --filters Name=cidr,Values=10.*
```

Salida:

```
{
    "IpamPoolCidr": {
        "Cidr": "10.0.0.0/24",
        "State": "provisioned"
    }
}
```

- Para obtener información sobre la API, consulte GetIpamPoolCidrs en la Referencia de comandos de la AWS CLI.

`get-ipam-resource-cidrs`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ipam-resource-cidrs`.

AWS CLI

Para asignar los CIDR a un recurso

En el siguiente ejemplo de `get-ipam-resource-cidrs` se obtienen los CIDR asignados a un recurso.

(Linux):

```
aws ec2 get-ipam-resource-cidrs \
    --ipam-scope-id ipam-scope-02fc38cd4c48e7d38 \
    --filters Name=management-state,Values=unmanaged
```

(Windows):

```
aws ec2 get-ipam-resource-cidrs ^
    --ipam-scope-id ipam-scope-02fc38cd4c48e7d38 ^
    --filters Name=management-state,Values=unmanaged
```

Salida:

```
{
    "IpamResourceCidrs": [
        {
            "IpamId": "ipam-08440e7a3acde3908",
            "IpamScopeId": "ipam-scope-02fc38cd4c48e7d38",
            "ResourceRegion": "us-east-2",
            "ResourceOwnerId": "123456789012",
            "ResourceId": "vpc-621b8709",
            "ResourceName": "Default AWS VPC",
            "ResourceCidr": "172.33.0.0/16",
            "ResourceType": "vpc",
            "ResourceTags": [
                {
                    "Key": "Environment",
                    "Value": "Test"
                },
                {
                    "Key": "Name",
                    "Value": "Default AWS VPC"
                }
            ],
            "IpUsage": 0.0039,
            "ComplianceStatus": "unmanaged",
            "ManagementState": "unmanaged",
            "OverlapStatus": "nonoverlapping",
            "VpcId": "vpc-621b8709"
        }
    ]
}
```

Para obtener más información, consulte Monitorear el uso de CIDR por recurso en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte GetIpamResourceCidrs en la Referencia de comandos de la AWS CLI.

`get-launch-template-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-launch-template-data`.

AWS CLI

Para obtener datos de instancia para una plantilla de lanzamiento

En este ejemplo, se obtienen datos sobre la instancia especificada y se utiliza la opción `--query` para devolver el contenido en `LaunchTemplateData`. Puede usar la salida como base para crear una nueva plantilla de inicialización o una versión.

Comando:

```
aws ec2 get-launch-template-data --instance-id i-0123d646e8048babc --query
 'LaunchTemplateData'
```

Salida:

```
{
      "Monitoring": {},
      "ImageId": "ami-8c1be5f6",
      "BlockDeviceMappings": [
          {
              "DeviceName": "/dev/xvda",
              "Ebs": {
                  "DeleteOnTermination": true
              }
          }
      ],
      "EbsOptimized": false,
      "Placement": {
          "Tenancy": "default",
          "GroupName": "",
          "AvailabilityZone": "us-east-1a"
      },
      "InstanceType": "t2.micro",
      "NetworkInterfaces": [
          {
              "Description": "",
              "NetworkInterfaceId": "eni-35306abc",
              "PrivateIpAddresses": [
                  {
                      "Primary": true,
                      "PrivateIpAddress": "10.0.0.72"
                  }
              ],
              "SubnetId": "subnet-7b16de0c",
              "Groups": [
                  "sg-7c227019"
              ],
```

```
            "Ipv6Addresses": [
                {
                    "Ipv6Address": "2001:db8:1234:1a00::123"
                }
            ],
            "PrivateIpAddress": "10.0.0.72"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetLaunchTemplateData en la Referencia de comandos de la AWS CLI.

`get-managed-prefix-list-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-managed-prefix-list-associations`.

AWS CLI

Para obtener asociaciones de listas de prefijos

En el siguiente ejemplo de `get-managed-prefix-list-associations` se obtienen los recursos asociados a la lista de prefijos especificada.

```
aws ec2 get-managed-prefix-list-associations \
    --prefix-list-id pl-0123456abcabcabc1
```

Salida:

```
{
    "PrefixListAssociations": [
        {
            "ResourceId": "sg-0abc123456abc12345",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

Para obtener más información, consulte Managed prefix lists en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte GetManagedPrefixListAssociations en la Referencia de comandos de la AWS CLI.

`get-managed-prefix-list-entries`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-managed-prefix-list-entries`.

AWS CLI

Para obtener las entradas de una lista de prefijos

En el siguiente ejemplo de `get-managed-prefix-list-entries` se obtienen las entradas de la lista de prefijos especificada.

```
aws ec2 get-managed-prefix-list-entries \
    --prefix-list-id pl-0123456abcabcabc1
```

Salida:

```
{
    "Entries": [
        {
            "Cidr": "10.0.0.0/16",
            "Description": "vpc-a"
        },
        {
            "Cidr": "10.2.0.0/16",
            "Description": "vpc-b"
        }
    ]
}
```

Para obtener más información, consulte Managed prefix lists en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte GetManagedPrefixListEntries en la Referencia de comandos de la AWS CLI.

`get-network-insights-access-scope-analysis-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-network-insights-access-scope-analysis-findings`.

AWS CLI

Para obtener los resultados del análisis de ámbito de acceso a información de red

En el siguiente ejemplo de `get-network-insights-access-scope-analysis-findings` se obtienen los resultados del análisis de ámbito seleccionado en su cuenta de AWS.

```
aws ec2 get-network-insights-access-scope-analysis-findings \
    --region us-east-1 \
    --network-insights-access-scope-analysis-id nis \
    --nis-123456789111
```

Salida:

```
{
    "NetworkInsightsAccessScopeAnalysisId": "nisa-123456789222",
    "AnalysisFindings": [
        {
            "NetworkInsightsAccessScopeAnalysisId": "nisa-123456789222",
            "NetworkInsightsAccessScopeId": "nis-123456789111",
            "FindingComponents": [
                {
                    "SequenceNumber": 1,
                    "Component": {
                        "Id": "eni-02e3d42d5cceca67d",
                        "Arn": "arn:aws:ec2:us-east-1:936459623503:network-
interface/eni-02e3d32d9cceca17d"
                    },
                    "OutboundHeader": {
                        "DestinationAddresses": [
                            "0.0.0.0/5",
                            "11.0.0.0/8",
                            "12.0.0.0/6",
                            "128.0.0.0/3",
                            "16.0.0.0/4",
                            "160.0.0.0/5",
                            "168.0.0.0/6",
                            "172.0.0.0/12"
```

```
                        "8.0.0.0/7"
                    ],
                    "DestinationPortRanges": [
                        {
                            "From": 0,
                            "To": 65535
                        }
                    ],
                    "Protocol": "6",
                    "SourceAddresses": [
                        "10.0.2.253/32"
                    ],
                    "SourcePortRanges": [
                        {
                            "From": 0,
                            "To": 65535
                        }
                    ]
                }, [etc]
            ]
        }
    }
  ]
}
```

Para obtener más información, consulte Getting started with Network Access Analyzer using the AWS CLI en la Guía del analizador de acceso a la red.

- Para obtener información sobre la API, consulte GetNetworkInsightsAccessScopeAnalysisFindings en la Referencia de comandos de la AWS CLI.

`get-network-insights-access-scope-content`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-network-insights-access-scope-content`.

AWS CLI

Para obtener el contenido de ámbito de acceso a información de red

En el siguiente ejemplo de `get-network-insights-access-scope-content` se obtiene el contenido del ID de análisis de ámbito seleccionado en su cuenta de AWS.

```
aws ec2 get-network-insights-access-scope-content \
    --region us-east-1 \
    --network-insights-access-scope-id nis-123456789222
```

Salida:

```
{
    "NetworkInsightsAccessScopeContent": {
        "NetworkInsightsAccessScopeId": "nis-123456789222",
        "MatchPaths": [
            {
                "Source": {
                    "ResourceStatement": {
                        "ResourceTypes": [
                            "AWS::EC2::NetworkInterface"
                        ]
                    }
                },
                "Destination": {
                    "ResourceStatement": {
                        "ResourceTypes": [
                            "AWS::EC2::InternetGateway"
                        ]
                    }
                }
            }
        ]
    }
}
```

Para obtener más información, consulte Getting started with Network Access Analyzer using the AWS CLI en la Guía del analizador de acceso a la red.

- Para obtener información sobre la API, consulte GetNetworkInsightsAccessScopeContent en la Referencia de comandos de la AWS CLI.

`get-password-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-password-data`.

AWS CLI

Para obtener la contraseña cifrada

En este ejemplo, se obtiene la contraseña cifrada.

Comando:

```
aws ec2 get-password-data --instance-id i-1234567890abcdef0
```

Salida:

```
{
    "InstanceId": "i-1234567890abcdef0",
    "Timestamp": "2013-08-07T22:18:38.000Z",
    "PasswordData": "gSlJFq+VpcZXqy+iktxMF6NyxQ4qCrT4+gaOuNOenX1MmgXPTj7XEXAMPLE
UQ+YeFfb+L1U4C4AKv652Ux1iRB3CPTYP7WmU3TUnhsuBd+p6LVk7T2lKUml6OXbk6WPW1VYYm/TRPB1
e1DQ7PY4an/DgZT4mwcpRFigzhniQgDDeO1InvSDcwoUTwNs0Y1S8ouri2W4n5GNlriM3Q0AnNVelVz/
53TkDtxbNoU606M1gK9zUWSxqEgwvbV2j8c5rP0WCuaMWSFl4ziDu4bd7q+4RSyi8NUsVWnKZ4aEZffu
DPGzKrF5yLlf3etP2L4ZR6CvG7K1hx7VKOQVN32Dajw=="
}
```

Para obtener la contraseña descifrada

En este ejemplo, se obtiene la contraseña descifrada.

Comando:

```
aws ec2 get-password-data --instance-id  i-1234567890abcdef0 --priv-launch-key C:
\Keys\MyKeyPair.pem
```

Salida:

```
{
    "InstanceId": "i-1234567890abcdef0",
    "Timestamp": "2013-08-30T23:18:05.000Z",
    "PasswordData": "&ViJ652e*u"
}
```

- Para obtener información sobre la API, consulte GetPasswordData en la Referencia de comandos de la AWS CLI.

`get-reserved-instances-exchange-quote`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-reserved-instances-exchange-quote`.

AWS CLI

Para obtener un presupuesto para el intercambio de una instancia reservada convertible

En este ejemplo, se obtiene la información de intercambio de las instancias reservadas convertibles especificadas.

Comando:

```
aws ec2 get-reserved-instances-exchange-quote --reserved-
instance-ids 7b8750c3-397e-4da4-bbcb-a45ebexample --target-
configurations OfferingId=6fea5434-b379-434c-b07b-a7abexample
```

Salida:

```
{
  "CurrencyCode": "USD",
  "ReservedInstanceValueSet": [
      {
          "ReservedInstanceId": "7b8750c3-397e-4da4-bbcb-a45ebexample",
          "ReservationValue": {
              "RemainingUpfrontValue": "0.000000",
              "HourlyPrice": "0.027800",
              "RemainingTotalValue": "730.556200"
          }
      }
  ],
  "PaymentDue": "424.983828",
  "TargetConfigurationValueSet": [
      {
          "TargetConfiguration": {
              "InstanceCount": 5,
              "OfferingId": "6fea5434-b379-434c-b07b-a7abexample"
          },
          "ReservationValue": {
              "RemainingUpfrontValue": "424.983828",
              "HourlyPrice": "0.016000",
              "RemainingTotalValue": "845.447828"
```

```
            }
        }
    ],
    "IsValidExchange": true,
    "OutputReservedInstancesWillExpireAt": "2020-10-01T13:03:39Z",
    "ReservedInstanceValueRollup": {
        "RemainingUpfrontValue": "0.000000",
        "HourlyPrice": "0.027800",
        "RemainingTotalValue": "730.556200"
    },
    "TargetConfigurationValueRollup": {
        "RemainingUpfrontValue": "424.983828",
        "HourlyPrice": "0.016000",
        "RemainingTotalValue": "845.447828"
    }
}
```

- Para obtener información sobre la API, consulte GetReservedInstancesExchangeQuote en la Referencia de comandos de la AWS CLI.

`get-security-groups-for-vpc`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-security-groups-for-vpc`.

AWS CLI

Para ver los grupos de seguridad que se pueden asociar a las interfaces de red de una VPC especificada.

En el siguiente ejemplo de `get-security-groups-for-vpc` se muestran los grupos de seguridad que se pueden asociar a las interfaces de red de la VPC.

```
aws ec2 get-security-groups-for-vpc \
    --vpc-id vpc-6c31a611 \
    --region us-east-1
```

Salida:

```
{
    "SecurityGroupForVpcs": [
        {
            "Description": "launch-wizard-36 created 2022-08-29T15:59:35.338Z",
```

```
            "GroupName": "launch-wizard-36",
            "OwnerId": "470889052923",
            "GroupId": "sg-007e0c3027ee885f5",
            "Tags": [],
            "PrimaryVpcId": "vpc-6c31a611"
        },
        {
            "Description": "launch-wizard-18 created 2024-01-19T20:22:27.527Z",
            "GroupName": "launch-wizard-18",
            "OwnerId": "470889052923",
            "GroupId": "sg-0147193bef51c9eef",
            "Tags": [],
            "PrimaryVpcId": "vpc-6c31a611"
        }
}
```

- Para obtener información sobre la API, consulte GetSecurityGroupsForVpc en la Referencia de comandos de la AWS CLI.

`get-serial-console-access-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-serial-console-access-status`.

AWS CLI

Para ver el estado de acceso a la cuenta de la consola serie

En el siguiente ejemplo de `get-serial-console-access-status` se determina si el acceso a la consola serie está habilitado para su cuenta.

```
aws ec2 get-serial-console-access-status
```

Salida:

```
{
    "SerialConsoleAccessEnabled": true
}
```

Para obtener más información, consulte Consola serie de EC2 en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte GetSerialConsoleAccessStatus en la Referencia de comandos de la AWS CLI.

`get-snapshot-block-public-access-state`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-snapshot-block-public-access-state`.

AWS CLI

Para obtener el estado actual de bloqueo del acceso público de las instantáneas

En el siguiente ejemplo de `get-snapshot-block-public-access-state` se obtiene el estado actual de bloqueo del acceso público de las instantáneas.

```
aws ec2 get-snapshot-block-public-access-state
```

Salida:

```
{
    "State": "block-all-sharing"
}
```

Para obtener más información, consulte Block public access for snapshots en la Guía del usuario de Amazon EBS.

- Para obtener información sobre la API, consulte GetSnapshotBlockPublicAccessState en la Referencia de comandos de la AWS CLI.

`get-spot-placement-scores`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-spot-placement-scores`.

AWS CLI

Para calcular la puntuación de ubicación de spot para requisitos específicos

En el siguiente ejemplo de `get-spot-placement-scores`, primero se genera una lista de todos los parámetros posibles que se pueden especificar para la configuración de puntuación de ubicación de spot mediante el parámetro `--generate-cli-skeleton`. Después, se guarda la

lista en un archivo JSON. A continuación, el archivo JSON se utiliza para configurar los requisitos que se utilizarán para calcular la puntuación de ubicación de spot.

Se generan todos los parámetros posibles que se puedan especificar para la configuración de la puntuación de ubicación de spot y se guarda la salida directamente en un archivo JSON.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --generate-cli-skeleton input > attributes.json
```

Salida:

```
{
    "InstanceTypes": [
        ""
    ],
    "TargetCapacity": 0,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "RegionNames": [
        ""
    ],
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": [
            "x86_64_mac"
        ],
        "VirtualizationTypes": [
            "hvm"
        ],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 0,
                "Max": 0
            },
            "MemoryMiB": {
                "Min": 0,
                "Max": 0
            },
            "CpuManufacturers": [
                "amd"
            ],
            "MemoryGiBPerVCpu": {
                "Min": 0.0,
```

```
                "Max": 0.0
            },
            "ExcludedInstanceTypes": [
                ""
            ],
            "InstanceGenerations": [
                "previous"
            ],
            "SpotMaxPricePercentageOverLowestPrice": 0,
            "OnDemandMaxPricePercentageOverLowestPrice": 0,
            "BareMetal": "excluded",
            "BurstablePerformance": "excluded",
            "RequireHibernateSupport": true,
            "NetworkInterfaceCount": {
                "Min": 0,
                "Max": 0
            },
            "LocalStorage": "included",
            "LocalStorageTypes": [
                "hdd"
            ],
            "TotalLocalStorageGB": {
                "Min": 0.0,
                "Max": 0.0
            },
            "BaselineEbsBandwidthMbps": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorTypes": [
                "fpga"
            ],
            "AcceleratorCount": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorManufacturers": [
                "amd"
            ],
            "AcceleratorNames": [
                "vu9p"
            ],
            "AcceleratorTotalMemoryMiB": {
                "Min": 0,
```

```
                "Max": 0
            }
        }
    },
    "DryRun": true,
    "MaxResults": 0,
    "NextToken": ""
}
```

Configure el archivo JSON. Se debe proporcionar un valor para `TargetCapacity`. Para obtener una descripción de cada parámetro y sus valores predeterminados, consulte Puntuación de ubicación de spot (AWS CLI) <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-placement-score.html#calculate-sps-cli>.

Calcule la puntuación de ubicación de spot para los requisitos especificados en `attributes.json`. Especifique el nombre y la ruta del archivo JSON mediante el parámetro `--cli-input-json`.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --cli-input-json file://attributes.json
```

Salida si `SingleAvailabilityZone` se establece en `false` o se omite (si se omite, toma de forma predeterminada el valor `false`). Se devuelve una lista de regiones puntuadas.

```
"Recommendation": [
    {
        "Region": "us-east-1",
        "Score": 7
    },
    {
        "Region": "us-west-1",
        "Score": 5
    },
   ...
```

Salida si `SingleAvailabilityZone` se establece en `true`. Se devuelve una lista puntuada de zonas de disponibilidad únicas.

```
"Recommendation": [
```

```
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "use1-az1"
        "Score": 8
    },
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "usw2-az3"
        "Score": 6
    },
   ...
```

Para obtener más información sobre el cálculo de una puntuación de ubicación de spot y ejemplos de configuraciones, consulte Puntuación de ubicación de spot en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte GetSpotPlacementScores en la Referencia de comandos de la AWS CLI.

`get-subnet-cidr-reservations`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-subnet-cidr-reservations`.

AWS CLI

Para obtener información sobre una reserva de CIDR de una subred

En el siguiente ejemplo de `get-subnet-cidr-reservations`, se muestra información sobre la reserva de CIDR de subred especificada.

```
aws ec2 get-subnet-cidr-reservations \
    --subnet-id subnet-03c51e2e6cEXAMPLE
```

Salida:

```
{
    "SubnetIpv4CidrReservations": [
        {
            "SubnetCidrReservationId": "scr-044f977c4eEXAMPLE",
            "SubnetId": "subnet-03c51e2e6cEXAMPLE",
            "Cidr": "10.1.0.16/28",
            "ReservationType": "prefix",
```

```
            "OwnerId": "123456789012"
        }
    ],
    "SubnetIpv6CidrReservations": []
}
```

Para obtener más información, consulte Reservas de la subred de CIDR en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte GetSubnetCidrReservations en la Referencia de comandos de la AWS CLI.

`get-transit-gateway-attachment-propagations`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-transit-gateway-attachment-propagations`.

AWS CLI

Para enumerar las tablas de enrutamiento en las que propaga las rutas la conexión de recursos especificada

En el siguiente ejemplo de `get-transit-gateway-attachment-propagations` se muestra la tabla de enrutamiento en la que propaga las rutas la conexión de recursos especificada.

```
aws ec2 get-transit-gateway-attachment-propagations \
    --transit-gateway-attachment-id tgw-attach-09fbd47ddfEXAMPLE
```

Salida:

```
{
    "TransitGatewayAttachmentPropagations": [
        {
            "TransitGatewayRouteTableId": "tgw-rtb-0882c61b97EXAMPLE",
            "State": "enabled"
        }
    ]
}
```

Para obtener más información, consulte Transit gateway route tables en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte GetTransitGatewayAttachmentPropagations en la Referencia de comandos de la AWS CLI.

`get-transit-gateway-multicast-domain-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-transit-gateway-multicast-domain-associations`.

AWS CLI

Para ver la información sobre las asociaciones del dominio de multidifusión de puerta de enlace de tránsito

En el siguiente ejemplo de `get-transit-gateway-multicast-domain-associations` se devuelven las asociaciones del dominio de multidifusión especificado.

```
aws ec2 get-transit-gateway-multicast-domain-associations \
    --transit-gateway-multicast-domain-id tgw-mcast-domain-0c4905cef7EXAMPLE
```

Salida:

```
{
    "MulticastDomainAssociations": [
        {
            "TransitGatewayAttachmentId": "tgw-attach-028c1dd0f8EXAMPLE",
            "ResourceId": "vpc-01128d2c24EXAMPLE",
            "ResourceType": "vpc",
            "Subnet": {
                "SubnetId": "subnet-000de86e3bEXAMPLE",
                "State": "associated"
            }
        },
        {
            "TransitGatewayAttachmentId": "tgw-attach-070e571cd1EXAMPLE",
            "ResourceId": "vpc-7EXAMPLE",
            "ResourceType": "vpc",
            "Subnet": {
                "SubnetId": "subnet-4EXAMPLE",
                "State": "associated"
            }
        },
```

```
        {
            "TransitGatewayAttachmentId": "tgw-attach-070e571cd1EXAMPLE",
            "ResourceId": "vpc-7EXAMPLE",
            "ResourceType": "vpc",
            "Subnet": {
                "SubnetId": "subnet-5EXAMPLE",
                "State": "associated"
            }
        },
        {
            "TransitGatewayAttachmentId": "tgw-attach-070e571cd1EXAMPLE",
            "ResourceId": "vpc-7EXAMPLE",
            "ResourceType": "vpc",
            "Subnet": {
                "SubnetId": "subnet-aEXAMPLE",
                "State": "associated"
            }
        },
        {
            "TransitGatewayAttachmentId": "tgw-attach-070e571cd1EXAMPLE",
            "ResourceId": "vpc-7EXAMPLE",
            "ResourceType": "vpc",
            "Subnet": {
                "SubnetId": "subnet-fEXAMPLE",
                "State": "associated"
            }
        }
    ]
}
```

Para obtener más información, consulte Dominios de multidifusión en la Guía de puertas de enlace de tránsito.

- Para obtener información sobre la API, consulte GetTransitGatewayMulticastDomainAssociations en la Referencia de comandos de la AWS CLI.

`get-transit-gateway-prefix-list-references`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-transit-gateway-prefix-list-references`.

AWS CLI

Para obtener referencias de listas de prefijos en una tabla de enrutamiento de puerta de enlace de tránsito

En el siguiente ejemplo de `get-transit-gateway-prefix-list-references` se obtienen las referencias de listas de prefijos de la tabla de enrutamiento de puerta de enlace de tránsito especificada y se filtra por el ID de una lista de prefijos específica.

```
aws ec2 get-transit-gateway-prefix-list-references \
    --transit-gateway-route-table-id tgw-rtb-0123456789abcd123 \
    --filters Name=prefix-list-id,Values=pl-11111122222222333
```

Salida:

```
{
    "TransitGatewayPrefixListReferences": [
        {
            "TransitGatewayRouteTableId": "tgw-rtb-0123456789abcd123",
            "PrefixListId": "pl-11111122222222333",
            "PrefixListOwnerId": "123456789012",
            "State": "available",
            "Blackhole": false,
            "TransitGatewayAttachment": {
                "TransitGatewayAttachmentId": "tgw-attach-aabbccddaabbccaab",
                "ResourceType": "vpc",
                "ResourceId": "vpc-112233445566aabbc"
            }
        }
    ]
}
```

Para obtener más información, consulte Prefix list references en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte GetTransitGatewayPrefixListReferences en la Referencia de comandos de la AWS CLI.

`get-transit-gateway-route-table-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-transit-gateway-route-table-associations`.

AWS CLI

Para obtener información sobre las asociaciones para la tabla de enrutamiento de puerta de enlace de tránsito especificada

En el siguiente ejemplo de `get-transit-gateway-route-table-associations` se muestra información sobre las asociaciones de la tabla de enrutamiento de puerta de enlace de tránsito especificada.

```
aws ec2 get-transit-gateway-route-table-associations \
    --transit-gateway-route-table-id tgw-rtb-0a823edbdeEXAMPLE
```

Salida:

```
{
    "Associations": [
        {
            "TransitGatewayAttachmentId": "tgw-attach-09b52ccdb5EXAMPLE",
            "ResourceId": "vpc-4d7de228",
            "ResourceType": "vpc",
            "State": "associating"
        }
    ]
}
```

Para obtener más información, consulte Transit gateway route tables en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte GetTransitGatewayRouteTableAssociations en la Referencia de comandos de la AWS CLI.

`get-transit-gateway-route-table-propagations`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-transit-gateway-route-table-propagations`.

AWS CLI

Para mostrar información sobre las propagaciones de tabla de enrutamiento para la tabla de enrutamiento de la puerta de enlace de tránsito especificada

En el siguiente ejemplo de `get-transit-gateway-route-table-propagations` se devuelven las propagaciones de tabla de enrutamiento de la tabla de enrutamiento especificada.

```
aws ec2 get-transit-gateway-route-table-propagations \
    --transit-gateway-route-table-id tgw-rtb-002573ed1eEXAMPLE
```

Salida:

```
{
    "TransitGatewayRouteTablePropagations": [
        {
            "TransitGatewayAttachmentId": "tgw-attach-01f8100bc7EXAMPLE",
            "ResourceId": "vpc-3EXAMPLE",
            "ResourceType": "vpc",
            "State": "enabled"
        },
        {
            "TransitGatewayAttachmentId": "tgw-attach-08e0bc912cEXAMPLE",
            "ResourceId": "11460968-4ac1-4fd3-bdb2-00599EXAMPLE",
            "ResourceType": "direct-connect-gateway",
            "State": "enabled"
        },
        {
            "TransitGatewayAttachmentId": "tgw-attach-0a89069f57EXAMPLE",
            "ResourceId": "8384da05-13ce-4a91-aada-5a1baEXAMPLE",
            "ResourceType": "direct-connect-gateway",
            "State": "enabled"
        }
    ]
}
```

Para obtener más información, consulte Transit gateway route tables en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte GetTransitGatewayRouteTablePropagations en la Referencia de comandos de la AWS CLI.

`get-verified-access-endpoint-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-verified-access-endpoint-policy`.

AWS CLI

Para obtener la política de acceso verificado de un punto de conexión

En el siguiente ejemplo de `get-verified-access-endpoint-policy` se obtiene la política de acceso verificado del punto de conexión especificado.

```
aws ec2 get-verified-access-endpoint-policy \
    --verified-access-endpoint-id vae-066fac616d4d546f2
```

Salida:

```
{
    "PolicyEnabled": true,
    "PolicyDocument": "permit(principal,action,resource)\nwhen
 {\n    context.identity.groups.contains(\"finance\") &&\n
 context.identity.email_verified == true\n};"
}
```

Para obtener más información, consulte Verified Access policies en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte GetVerifiedAccessEndpointPolicy en la Referencia de comandos de la AWS CLI.

`get-verified-access-group-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-verified-access-group-policy`.

AWS CLI

Para obtener la política de acceso verificado de un grupo

En el siguiente ejemplo de `get-verified-access-group-policy` se obtiene la política de acceso verificado del grupo especificado.

```
aws ec2 get-verified-access-group-policy \
    --verified-access-group-id vagr-0dbe967baf14b7235
```

Salida:

```
{
    "PolicyEnabled": true,
    "PolicyDocument": "permit(principal,action,resource)\nwhen
 {\n    context.identity.groups.contains(\"finance\") &&\n
 context.identity.email_verified == true\n};"
}
```

Para obtener más información, consulte Verified Access groups en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte GetVerifiedAccessGroupPolicy en la Referencia de comandos de la AWS CLI.

`get-vpn-connection-device-sample-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-vpn-connection-device-sample-configuration`.

AWS CLI

Para descargar un archivo de configuración de ejemplo

En el siguiente ejemplo de `get-vpn-connection-device-sample-configuration` se descarga el archivo de configuración de ejemplo especificado. Para enumerar los dispositivos de puerta de enlace con un archivo de configuración de ejemplo, llame al comando `get-vpn-connection-device-types`.

```
aws ec2 get-vpn-connection-device-sample-configuration \
    --vpn-connection-id vpn-123456789abc01234 \
    --vpn-connection-device-type-id 5fb390ba
```

Salida:

```
{
    "VpnConnectionDeviceSampleConfiguration": "contents-of-the-sample-configuration-
file"
}
```

Para obtener más información, consulte Download the configuration file en la Guía del usuario de AWS Site-to-Site VPN.

- Para obtener información sobre la API, consulte GetVpnConnectionDeviceSampleConfiguration en la Referencia de comandos de la AWS CLI.

`get-vpn-connection-device-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-vpn-connection-device-types`.

AWS CLI

Para enumerar los dispositivos de puerta de enlace con un archivo de configuración de ejemplo

En el siguiente ejemplo de `get-vpn-connection-device-types` se enumeran los dispositivos de puerta de enlace de Palo Alto Networks que tienen archivos de configuración de ejemplo.

```
aws ec2 get-vpn-connection-device-types \
    --query "VpnConnectionDeviceTypes[?Vendor==`Palo Alto Networks`]"
```

Salida:

```
[
    {
        "VpnConnectionDeviceTypeId": "754a6372",
        "Vendor": "Palo Alto Networks",
        "Platform": "PA Series",
        "Software": "PANOS 4.1.2+"
    },
    {
        "VpnConnectionDeviceTypeId": "9612cbed",
        "Vendor": "Palo Alto Networks",
        "Platform": "PA Series",
        "Software": "PANOS 4.1.2+ (GUI)"
    },
    {
        "VpnConnectionDeviceTypeId": "5fb390ba",
        "Vendor": "Palo Alto Networks",
        "Platform": "PA Series",
        "Software": "PANOS 7.0+"
    }
]
```

Para obtener más información, consulte Download the configuration file en la Guía del usuario de AWS Site-to-Site VPN.

- Para obtener información sobre la API, consulte GetVpnConnectionDeviceTypes en la Referencia de comandos de la AWS CLI.

`import-client-vpn-client-certificate-revocation-list`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-client-vpn-client-certificate-revocation-list`.

AWS CLI

Para importar una lista de revocación de certificados del cliente

En el siguiente ejemplo de `import-client-vpn-client-certificate-revocation-list` se importa una lista de revocación de certificados del cliente al punto de conexión de Client VPN especificando la ubicación del archivo en el equipo local.

```
aws ec2 import-client-vpn-client-certificate-revocation-list \
    --certificate-revocation-list file:///path/to/crl.pem \
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde
```

Salida:

```
{
    "Return": true
}
```

Para obtener más información, consulte Client Certificate Revocation Lists en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte ImportClientVpnClientCertificateRevocationList en la Referencia de comandos de la AWS CLI.

`import-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-image`.

AWS CLI

Para importar un archivo de imagen de máquina virtual como AMI

En el siguiente ejemplo de `import-image` se importa el archivo de virtualización abierto (OVA) especificado.

```
aws ec2 import-image \
  --disk-containers Format=ova,UserBucket="{S3Bucket=my-import-bucket,S3Key=vms/my-server-vm.ova}"
```

Salida:

```
{
    "ImportTaskId": "import-ami-1234567890abcdef0",
    "Progress": "2",
    "SnapshotDetails": [
        {
            "DiskImageSize": 0.0,
            "Format": "ova",
            "UserBucket": {
                "S3Bucket": "my-import-bucket",
                "S3Key": "vms/my-server-vm.ova"
            }
        }
    ],
    "Status": "active",
    "StatusMessage": "pending"
}
```

- Para obtener información sobre la API, consulte ImportImage en la Referencia de comandos de la AWS CLI.

`import-key-pair`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-key-pair`.

AWS CLI

Para importar una clave pública

Primero, genere un par de claves con la herramienta de su elección. Por ejemplo, utilice este comando ssh-keygen:

Comando:

```
ssh-keygen -t rsa -C "my-key" -f ~/.ssh/my-key
```

Salida:

```
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ec2-user/.ssh/my-key.
Your public key has been saved in /home/ec2-user/.ssh/my-key.pub.
...
```

En este ejemplo de comando, se importa la clave pública especificada.

Comando:

```
aws ec2 import-key-pair --key-name "my-key" --public-key-material fileb://~/.ssh/my-key.pub
```

Salida:

```
{
  "KeyName": "my-key",
  "KeyFingerprint": "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca"
}
```

- Para obtener información sobre la API, consulte ImportKeyPair en la Referencia de comandos de la AWS CLI.

`import-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-snapshot`.

AWS CLI

Para importar una instantánea

En el siguiente ejemplo de `import-snapshot` se importa el disco especificado como una instantánea.

```
aws ec2 import-snapshot \
    --description "My server VMDK" \
```

```
    --disk-container Format=VMDK,UserBucket={'S3Bucket=my-import-bucket,S3Key=vms/
my-server-vm.vmdk'}
```

Salida:

```
{
    "Description": "My server VMDK",
    "ImportTaskId": "import-snap-1234567890abcdef0",
    "SnapshotTaskDetail": {
        "Description": "My server VMDK",
        "DiskImageSize": "0.0",
        "Format": "VMDK",
        "Progress": "3",
        "Status": "active",
        "StatusMessage": "pending"
        "UserBucket": {
            "S3Bucket": "my-import-bucket",
            "S3Key": "vms/my-server-vm.vmdk"
        }
    }
}
```

- Para obtener información sobre la API, consulte ImportSnapshot en la Referencia de comandos de la AWS CLI.

`list-images-in-recycle-bin`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-images-in-recycle-bin`.

AWS CLI

Para enumerar las imágenes de la papelera de reciclaje

En el siguiente ejemplo de `list-images-in-recycle-bin` se enumeran todas las imágenes retenidas en la papelera de reciclaje en este momento.

```
aws ec2 list-images-in-recycle-bin
```

Salida:

```
{
```

```
    "Images": [
        {
            "RecycleBinEnterTime": "2022-03-14T15:35:08.000Z",
            "Description": "Monthly AMI One",
            "RecycleBinExitTime": "2022-03-15T15:35:08.000Z",
            "Name": "AMI_01",
            "ImageId": "ami-0111222333444abcd"
        }
    ]
}
```

Para obtener más información, consulte Recuperar AMI eliminadas de la papelera de reciclaje en la Guía del usuario de Amazon EBS.

- Para obtener información sobre la API, consulte ListImagesInRecycleBin en la Referencia de comandos de la AWS CLI.

`list-snapshots-in-recycle-bin`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-snapshots-in-recycle-bin`.

AWS CLI

Para ver las instantáneas en la papelera de reciclaje

En el siguiente ejemplo de `list-snapshots-in-recycle-bin` se enumera información sobre las instantáneas que hay en la papelera de reciclaje, incluidos el ID de la instantánea, una descripción de la instantánea, el ID del volumen a partir del cual se creó la instantánea, la fecha y la hora en que se eliminó la instantánea y entró en la papelera de reciclaje, y la fecha y la hora de vencimiento del período de retención.

```
aws ec2 list-snapshots-in-recycle-bin \
    --snapshot-id snap-01234567890abcdef
```

Salida:

```
{
    "SnapshotRecycleBinInfo": [
        {
            "Description": "Monthly data backup snapshot",
            "RecycleBinEnterTime": "2022-12-01T13:00:00.000Z",
            "RecycleBinExitTime": "2022-12-15T13:00:00.000Z",
```

```
            "VolumeId": "vol-abcdef09876543210",
            "SnapshotId": "snap-01234567890abcdef"
        }
    ]
}
```

Para obtener más información sobre la papelera de reciclaje, consulte Recuperar instantáneas eliminadas de la papelera de reciclaje en la Guía del usuario de Amazon EBS.

- Para obtener información sobre la API, consulte ListSnapshotsInRecycleBin en la Referencia de comandos de la AWS CLI.

`lock-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `lock-snapshot`.

AWS CLI

Ejemplo 1: bloqueo de una instantánea en el modo de gobernanza

En el siguiente ejemplo de `lock-snapshot` se bloquea la instantánea especificada en el modo de gobernanza.

```
aws ec2 lock-snapshot \
    --snapshot-id snap-0b5e733b4a8df6e0d \
    --lock-mode governance \
    --lock-duration 365
```

Salida:

```
{
    "SnapshotId": "snap-0b5e733b4a8df6e0d",
    "LockState": "governance",
    "LockDuration": 365,
    "LockCreatedOn": "2024-05-05T00:56:06.208000+00:00",
    "LockExpiresOn": "2025-05-05T00:56:06.208000+00:00",
    "LockDurationStartTime": "2024-05-05T00:56:06.208000+00:00"
}
```

Para obtener más información, consulte Snapshot lock en la Guía del usuario de Amazon EBS.

Ejemplo 2: bloqueo de una instantánea en modo de cumplimiento

En el siguiente ejemplo de `lock-snapshot` se bloquea la instantánea especificada en el modo de cumplimiento.

```
aws ec2 lock-snapshot \
    --snapshot-id snap-0163a8524c5b9901f \
    --lock-mode compliance \
    --cool-off-period 24 \
    --lock-duration 365
```

Salida:

```
{
    "SnapshotId": "snap-0b5e733b4a8df6e0d",
    "LockState": "compliance-cooloff",
    "LockDuration": 365,
    "CoolOffPeriod": 24,
    "CoolOffPeriodExpiresOn": "2024-05-06T01:02:20.527000+00:00",
    "LockCreatedOn": "2024-05-05T01:02:20.527000+00:00",
    "LockExpiresOn": "2025-05-05T01:02:20.527000+00:00",
    "LockDurationStartTime": "2024-05-05T01:02:20.527000+00:00"
}
```

Para obtener más información, consulte Snapshot lock en la Guía del usuario de Amazon EBS.

- Para obtener información sobre la API, consulte LockSnapshot en la Referencia de comandos de la AWS CLI.

`modify-address-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-address-attribute`.

AWS CLI

Para modificar los atributos del nombre de dominio asociado a una dirección IP elástica

En los siguientes ejemplos de `modify-address-attribute` se modifica el atributo de nombre de dominio de una dirección IP elástica.

Linux:

```
aws ec2 modify-address-attribute \
    --allocation-id eipalloc-abcdef01234567890 \
```

```
    --domain-name example.com
```

Windows:

```
aws ec2 modify-address-attribute ^
    --allocation-id eipalloc-abcdef01234567890 ^
    --domain-name example.com
```

Salida:

```
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.net."
            "PtrRecordUpdate": {
                "Value": "example.com.",
                "Status": "PENDING"
        }
    ]
}
```

Para supervisar el cambio pendiente y ver los atributos modificados de una dirección IP elástica, consulte describe-addresses-attribute en la Referencia de comandos de la AWS CLI.

- Para obtener información sobre la API, consulte ModifyAddressAttribute en la Referencia de comandos de la AWS CLI.

`modify-availability-zone-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-availability-zone-group`.

AWS CLI

Para habilitar un grupo de zonas

En el siguiente ejemplo de `modify-availability-zone-group` se habilita el grupo de zonas especificado.

```
aws ec2 modify-availability-zone-group \
```

```
    --group-name us-west-2-lax-1 \
    --opt-in-status opted-in
```

Salida:

```
{
    "Return": true
}
```

Para obtener más información, consulte Regiones y zonas en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte ModifyAvailabilityZoneGroup en la Referencia de comandos de la AWS CLI.

`modify-capacity-reservation-fleet`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-capacity-reservation-fleet`.

AWS CLI

Ejemplo 1: modificación de la capacidad objetivo total de una flota de reserva de capacidad

En el siguiente ejemplo de `modify-capacity-reservation-fleet` se modifica la capacidad de destino total de la flota de reserva de capacidad especificada. Al modificar la capacidad de destino total de una Flota de Reservas de capacidad, la flota crea automáticamente nuevas Reservas de capacidad o modifica o cancela las Reservas de capacidad existentes en la flota para cumplir la nueva capacidad de destino total. No puede intentar realizar modificaciones adicionales en una flota mientras esté en el estado `modifying`.

```
aws ec2 modify-capacity-reservation-fleet \
    --capacity-reservation-fleet-id crf-01234567890abcedf \
    --total-target-capacity 160
```

Salida:

```
{
    "Return": true
}
```

Ejemplo 2: modificación de la fecha de finalización de una flota de reserva de capacidad

En el siguiente ejemplo de `modify-capacity-reservation-fleet` se modifica la fecha de finalización de la flota de reserva de capacidad especificada. Al modificar la fecha de finalización de la flota, las fechas de finalización de todas las Reservas de capacidad individuales se actualizan en consecuencia. No puede intentar realizar modificaciones adicionales en una flota mientras esté en el estado `modifying`.

```
aws ec2 modify-capacity-reservation-fleet \
    --capacity-reservation-fleet-id crf-01234567890abcedf \
    --end-date 2022-07-04T23:59:59.000Z
```

Salida:

```
{
    "Return": true
}
```

Para obtener más información sobre flotas de reserva de capacidad, consulte Flotas de reservas de capacidad en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte ModifyCapacityReservationFleet en la Referencia de comandos de la AWS CLI.

`modify-capacity-reservation`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-capacity-reservation`.

AWS CLI

Ejemplo 1: cambio del número de instancias reservadas por una reserva de capacidad existente

En el siguiente ejemplo de `modify-capacity-reservation` se cambia el número de instancias para las que la reserva de capacidad reserva capacidad.

```
aws ec2 modify-capacity-reservation \
    --capacity-reservation-id cr-1234abcd56EXAMPLE \
    --instance-count 5
```

Salida:

```
{
    "Return": true
}
```

Para obtener más información, consulte Modificar una reserva de capacidad en la Guía del usuario de Amazon EC2.

Ejemplo 2: cambio de la fecha y la hora de finalización de una reserva de capacidad existente

En el siguiente ejemplo de `modify-capacity-reservation` se modifica una reserva de capacidad existente para que finalice en la fecha y hora especificadas.

```
aws ec2 modify-capacity-reservation \
    --capacity-reservation-id cr-1234abcd56EXAMPLE \
    --end-date-type limited \
    --end-date 2019-08-31T23:59:59Z
```

Para obtener más información, consulte Modificar una reserva de capacidad en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte ModifyCapacityReservation en la Referencia de comandos de la AWS CLI.

`modify-client-vpn-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-client-vpn-endpoint`.

AWS CLI

Para modificar un punto de conexión de Client VPN

En el siguiente ejemplo de `modify-client-vpn-endpoint` se habilita el registro de conexiones del cliente para el punto de conexión de Client VPN especificado.

```
aws ec2 modify-client-vpn-endpoint \
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde \
    --connection-log-options Enabled=true,CloudwatchLogGroup=ClientVPNLogs
```

Salida:

```
{
```

```
    "Return": true
}
```

Para obtener más información, consulte Client VPN Endpoints en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte ModifyClientVpnEndpoint en la Referencia de comandos de la AWS CLI.

`modify-default-credit-specification`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-default-credit-specification`.

AWS CLI

Para modificar la opción de crédito predeterminada

En el siguiente ejemplo de `modify-default-credit-specification` se describe la opción de crédito predeterminada de las instancias T2.

```
aws ec2 modify-default-credit-specification \
    --instance-family t2 \
    --cpu-credits unlimited
```

Salida:

```
{
    "InstanceFamilyCreditSpecification": {
        "InstanceFamily": "t2",
        "CpuCredits": "unlimited"
    }
}
```

- Para obtener información sobre la API, consulte ModifyDefaultCreditSpecification en la Referencia de comandos de la AWS CLI.

`modify-ebs-default-kms-key-id`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-ebs-default-kms-key-id`.

AWS CLI

Para establecer su CMK predeterminada para el cifrado de EBS

En el siguiente ejemplo de `modify-ebs-default-kms-key-id` se establece la CMK especificada como CMK predeterminada para el cifrado de EBS en su cuenta de AWS en la región actual.

```
aws ec2 modify-ebs-default-kms-key-id \
    --kms-key-id alias/my-cmk
```

Salida:

```
{
    "KmsKeyId": "arn:aws:kms:us-
west-2:123456789012:key/0ea3fef3-80a7-4778-9d8c-1c0c6EXAMPLE"
}
```

- Para obtener información sobre la API, consulte ModifyEbsDefaultKmsKeyId en la Referencia de comandos de la AWS CLI.

`modify-fleet`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-fleet`.

AWS CLI

Para escalar una flota de EC

En el siguiente ejemplo de `modify-fleet` se modifica la capacidad de destino de la flota de EC2 especificada. Si el valor especificado es superior a la capacidad actual, la flota de EC2 lanza instancias adicionales. Si el valor especificado es inferior a la capacidad actual, la flota de EC2 cancela todas las solicitudes abiertas y, si la política de terminación es `terminate`, la flota de EC2 termina todas las instancias que superen la nueva capacidad de destino.

```
aws ec2 modify-fleet \
    --fleet-ids fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE \
    --target-capacity-specification TotalTargetCapacity=5
```

Salida:

```
{
    "Return": true
}
```

Para obtener más información, consulte Administrar una flota de EC2 en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte ModifyFleet en la Referencia de comandos de la AWS CLI.

`modify-fpga-image-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-fpga-image-attribute`.

AWS CLI

Para modificar los atributos de una imagen de Amazon FPGA

En este ejemplo, se agregan permisos de carga para el ID de cuenta `123456789012` de la AFI especificada.

Comando:

```
aws ec2 modify-fpga-image-attribute --attribute loadPermission --fpga-image-
id afi-0d123e123bfc85abc --load-permission Add=[{UserId=123456789012}]
```

Salida:

```
{
  "FpgaImageAttribute": {
      "FpgaImageId": "afi-0d123e123bfc85abc",
      "LoadPermissions": [
          {
              "UserId": "123456789012"
          }
      ]
  }
}
```

- Para obtener información sobre la API, consulte ModifyFpgaImageAttribute en la Referencia de comandos de la AWS CLI.

`modify-hosts`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-hosts`.

AWS CLI

Ejemplo 1: habilitación de la ubicación automática de un host dedicado

En el siguiente ejemplo de `modify-hosts` se habilita la ubicación automática de un host dedicado para que acepte cualquier lanzamiento de instancia sin destino que coincida con su configuración de tipo de instancia.

```
aws ec2 modify-hosts \
    --host-id h-06c2f189b4EXAMPLE \
    --auto-placement on
```

Salida:

```
{
    "Successful": [
        "h-06c2f189b4EXAMPLE"
    ],
    "Unsuccessful": []
}
```

Para obtener más información, consulte Modify the auto-placement setting for a Dedicated Host en la Guía del usuario de Amazon EC2.

Ejemplo 2: habilitación de la recuperación del host para un host dedicado

En los siguientes ejemplos de `modify-hosts` se habilita la recuperación de host del host dedicado especificado.

```
aws ec2 modify-hosts \
    --host-id h-06c2f189b4EXAMPLE \
    --host-recovery on
```

Salida:

```
{
```

```
    "Successful": [
        "h-06c2f189b4EXAMPLE"
    ],
    "Unsuccessful": []
}
```

Para obtener más información, consulte Modify the auto-placement setting for a Dedicated Host en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte ModifyHosts en la Referencia de comandos de la AWS CLI.

`modify-id-format`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-id-format`.

AWS CLI

Para habilitar el formato de ID más largo para un recurso

En el siguiente ejemplo de `modify-id-format` se habilita el formato de ID más largo para el tipo de recurso `instance`.

```
aws ec2 modify-id-format \
    --resource instance \
    --use-long-ids
```

Para deshabilitar el formato de ID más largo para un recurso

En el siguiente ejemplo de `modify-id-format` se deshabilita el formato de ID más largo para el tipo de recurso `instance`.

```
aws ec2 modify-id-format \
    --resource instance \
    --no-use-long-ids
```

En el siguiente ejemplo de `modify-id-format` se habilita el formato de ID más largo para todos los tipos de recursos admitidos que se encuentran dentro de su período de inscripción.

```
aws ec2 modify-id-format \
```

```
    --resource all-current \
    --use-long-ids
```

- Para obtener información sobre la API, consulte ModifyIdFormat en la Referencia de comandos de la AWS CLI.

`modify-identity-id-format`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-identity-id-format`.

AWS CLI

Para permitir que un rol de IAM utilice ID más largos para un recurso

En el siguiente ejemplo de `modify-identity-id-format` se permite que el rol de IAM `EC2Role` de su cuenta de AWS utilice un formato de ID largo para el tipo de recurso `instance`.

```
aws ec2 modify-identity-id-format \
    --principal-arn arn:aws:iam::123456789012:role/EC2Role \
    --resource instance \
    --use-long-ids
```

Para permitir que un usuario de IAM utilice ID más largos para un recurso

En el siguiente ejemplo de `modify-identity-id-format` se permite que el usuario de IAM `AdminUser` de su cuenta de AWS utilice el formato de ID más largo para el tipo de recurso `volume`.

```
aws ec2 modify-identity-id-format \
    --principal-arn arn:aws:iam::123456789012:user/AdminUser \
    --resource volume \
    --use-long-ids
```

En el siguiente ejemplo de `modify-identity-id-format` se permite que el usuario de IAM `AdminUser` de su cuenta de AWS utilice el formato de ID más largo para todos los tipos de recursos admitidos que se encuentran dentro de su período de inscripción.

```
aws ec2 modify-identity-id-format \
    --principal-arn arn:aws:iam::123456789012:user/AdminUser \
    --resource all-current \
```

```
    --use-long-ids
```

- Para obtener información sobre la API, consulte ModifyIdentityIdFormat en la Referencia de comandos de la AWS CLI.

`modify-image-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-image-attribute`.

AWS CLI

Ejemplo 1: operación de hacer pública una AMI

En el siguiente ejemplo de `modify-instance-attribute` se hace pública la AMI especificada.

```
aws ec2 modify-image-attribute \
    --image-id ami-5731123e \
    --launch-permission "Add=[{Group=all}]"
```

Este comando no genera ninguna salida.

Ejemplo 2: operación de hacer privada una AMI

En el siguiente ejemplo de `modify-instance-attribute` se hace privada la AMI especificada.

```
aws ec2 modify-image-attribute \
    --image-id ami-5731123e \
    --launch-permission "Remove=[{Group=all}]"
```

Este comando no genera ninguna salida.

Ejemplo 3: concesión de permiso de lanzamiento a una cuenta de AWS

En el siguiente ejemplo de `modify-instance-attribute` se conceden permisos de lanzamiento a la cuenta de AWS especificada.

```
aws ec2 modify-image-attribute \
    --image-id ami-5731123e \
    --launch-permission "Add=[{UserId=123456789012}]"
```

Este comando no genera ninguna salida.

Ejemplo 4: retirada de permiso de lanzamiento a una cuenta de AWS

En el siguiente ejemplo de `modify-instance-attribute` se retiran los permisos de lanzamiento a la cuenta de AWS especificada.

```
aws ec2 modify-image-attribute \
    --image-id ami-5731123e \
    --launch-permission "Remove=[{UserId=123456789012}]"
```

- Para obtener información sobre la API, consulte ModifyImageAttribute en la Referencia de comandos de la AWS CLI.

`modify-instance-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-instance-attribute`.

AWS CLI

Ejemplo 1: modificación del tipo de instancia

En el siguiente ejemplo de `modify-instance-attribute` se modifica el tipo de instancia de la instancia especificada. La instancia debe tener el estado `stopped`.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --instance-type "{\"Value\": \"m1.small\"}"
```

Este comando no genera ninguna salida.

Ejemplo 2: habilitación de redes mejoradas en una instancia

En el siguiente ejemplo de `modify-instance-attribute` se habilitan las redes mejoradas para la instancia especificada. La instancia debe tener el estado `stopped`.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --sriov-net-support simple
```

Este comando no genera ninguna salida.

Ejemplo 3: modificación del atributo sourceDestCheck

En el siguiente ejemplo de `modify-instance-attribute` se establece el atributo `sourceDestCheck` de la instancia especificada en `true`. La instancia debe encontrarse en una VPC.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --source-dest-check "{\"Value\": true}"
```

Este comando no genera ninguna salida.

Ejemplo 4: modificación del atributo deleteOnTermination del volumen raíz

En el siguiente ejemplo de `modify-instance-attribute` se establece en `false` el atributo `deleteOnTermination` para el volumen raíz de la instancia respaldada por Amazon EBS especificada. De forma predeterminada, este atributo es `true` para el volumen raíz.

Comando:

```
aws ec2 modify-instance-attribute \
  --instance-id i-1234567890abcdef0 \
  --block-device-mappings "[{\"DeviceName\": \"/dev/sda1\",\"Ebs\": {\"DeleteOnTermination\":false}}]"
```

Este comando no genera ninguna salida.

Ejemplo 5: modificación de los datos de usuario asociados a una instancia

En el siguiente ejemplo de `modify-instance-attribute` se agrega el contenido del archivo `UserData.txt` como UserData de la instancia especificada.

Contenido del archivo original `UserData.txt`:

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

El contenido del archivo debe estar codificado en base64. El primer comando convierte el archivo de texto a base64 y lo guarda como un archivo nuevo.

Versión del comando para Linux/macOS:

```
base64 UserData.txt > UserData.base64.txt
```

Este comando no genera ninguna salida.

Versión del comando para Windows:

```
certutil -encode UserData.txt tmp.b64 && findstr /v /c:- tmp.b64 >
 UserData.base64.txt
```

Salida:

```
Input Length = 67
Output Length = 152
CertUtil: -encode command completed successfully.
```

Ahora puede hacer referencia a ese archivo en el siguiente comando de la CLI:

```
aws ec2 modify-instance-attribute \
    --instance-id=i-09b5a14dbca622e76 \
    --attribute userData --value file://UserData.base64.txt
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Datos de usuario y las AWS CLI en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte ModifyInstanceAttribute en la Referencia de comandos de la AWS CLI.

`modify-instance-capacity-reservation-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-instance-capacity-reservation-attributes`.

AWS CLI

Ejemplo 1: modificación de los ajustes de destino de reserva de capacidad de una instancia

En el siguiente ejemplo de `modify-instance-capacity-reservation-attributes` se modifica una instancia detenida para utilizar como destino una reserva de capacidad determinada.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-EXAMPLE8765abcd4e \
    --capacity-reservation-specification
 'CapacityReservationTarget={CapacityReservationId= cr-1234abcd56EXAMPLE }'
```

Salida:

```
{
    "Return": true
}
```

Para obtener más información, consulte Modificar la configuración de reserva de capacidad de la instancia en la Guía del usuario de Amazon EC2.

Ejemplo 2: modificación de los ajustes de destino de reserva de capacidad de una instancia

En el siguiente ejemplo de `modify-instance-capacity-reservation-attributes` se modifica una instancia detenida que tiene como destino la reserva de capacidad especificada para lanzarla en cualquier reserva de capacidad que tenga atributos coincidentes (tipo de instancia, plataforma, zona de disponibilidad) y criterios de coincidencia de instancia abierta.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-EXAMPLE8765abcd4e \
    --capacity-reservation-specification 'CapacityReservationPreference=open'
```

Salida:

```
{
    "Return": true
}
```

Para obtener más información, consulte Modificar la configuración de reserva de capacidad de la instancia en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte ModifyInstanceCapacityReservationAttributes en la Referencia de comandos de la AWS CLI.

`modify-instance-credit-specification`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-instance-credit-specification`.

AWS CLI

Para modificar la opción de crédito para el uso de CPU de una instancia

En este ejemplo, se modifica a unlimited la opción de crédito para el uso de la CPU de la instancia especificada en la región especificada. Las opciones de crédito válidas son standard y unlimited.

Comando:

```
aws ec2 modify-instance-credit-specification --instance-credit-specification "InstanceId=i-1234567890abcdef0,CpuCredits=unlimited"
```

Salida:

```
{
  "SuccessfulInstanceCreditSpecifications": [
    {
      "InstanceId": "i-1234567890abcdef0"
    }
  ],
  "UnsuccessfulInstanceCreditSpecifications": []
}
```

- Para obtener información sobre la API, consulte ModifyInstanceCreditSpecification en la Referencia de comandos de la AWS CLI.

`modify-instance-event-start-time`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-instance-event-start-time`.

AWS CLI

Para modificar la hora de inicio del evento de una instancia

En el siguiente comando `modify-instance-event-start-time` se muestra cómo modificar la hora de inicio del evento de la instancia especificada. Especifique el ID de evento mediante el parámetro `--instance-event-id`. Especifique la nueva fecha y hora mediante el parámetro `--not-before`.

```
aws ec2 modify-instance-event-start-time --instance-id i-1234567890abcdef0
 --instance-event-id instance-event-0abcdef1234567890 --not-
before 2019-03-25T10:00:00.000
```

Salida:

```
"Event": {
    "InstanceEventId": "instance-event-0abcdef1234567890",
    "Code": "system-reboot",
    "Description": "scheduled reboot",
    "NotAfter": "2019-03-25T12:00:00.000Z",
    "NotBefore": "2019-03-25T10:00:00.000Z",
    "NotBeforeDeadline": "2019-04-22T21:00:00.000Z"
}
```

Para obtener más información, consulte Instances Scheduled for Reboot en la Guía del usuario de Amazon Elastic Compute Cloud.

- Para obtener información sobre la API, consulte ModifyInstanceEventStartTime en la Referencia de comandos de la AWS CLI.

`modify-instance-event-window`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-instance-event-window`.

AWS CLI

Ejemplo 1: modificación del intervalo de tiempo de un período de evento

En el siguiente ejemplo de `modify-instance-event-window` se modifica el intervalo de tiempo de un período de evento. Especifique el parámetro `time-range` para modificar el intervalo de tiempo. No puede especificar el parámetro `cron-expression`.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890
```

```
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8
```

Salida:

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Para conocer las restricciones de los períodos de evento, consulte Consideraciones en la sección sobre eventos programados de la Guía del usuario de Amazon EC2.

Ejemplo 2: modificación de un conjunto de intervalos de tiempo para un período de evento

En el siguiente ejemplo de `modify-instance-event-window` se modifica el intervalo de tiempo de un período de evento. Especifique el parámetro `time-range` para modificar el intervalo de tiempo. No puede especificar el parámetro `cron-expression`.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range '[{"StartWeekDay": "monday", "StartHour": 2, "EndWeekDay":
 "wednesday", "EndHour": 8},
        {"StartWeekDay": "thursday", "StartHour": 2, "EndWeekDay": "friday",
 "EndHour": 8}]'
```

Salida:

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            },
            {
                "StartWeekDay": "thursday",
                "StartHour": 2,
                "EndWeekDay": "friday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
```

```
    }
}
```

Para conocer las restricciones de los períodos de evento, consulte Consideraciones en la sección sobre eventos programados de la Guía del usuario de Amazon EC2.

Ejemplo 3: modificación de la expresión cron de un período de evento

En el siguiente ejemplo de `modify-instance-event-window` se modifica la expresión cron de un período de evento. Especifique el parámetro `cron-expression` para modificar la expresión cron. No puede especificar el parámetro `time-range`.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --cron-expression "* 21-23 * * 2,3"
```

Salida:

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Para conocer las restricciones de los períodos de evento, consulte Consideraciones en la sección sobre eventos programados de la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte ModifyInstanceEventWindow en la Referencia de comandos de la AWS CLI.

`modify-instance-maintenance-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-instance-maintenance-options`.

AWS CLI

Ejemplo 1: deshabilitación del comportamiento de recuperación de una instancia

En el siguiente ejemplo de `modify-instance-maintenance-options` se deshabilita la recuperación automática simplificada para una instancia en ejecución o detenida.

```
aws ec2 modify-instance-maintenance-options \
    --instance-id i-0abcdef1234567890 \
    --auto-recovery disabled
```

Salida:

```
{
    "InstanceId": "i-0abcdef1234567890",
    "AutoRecovery": "disabled"
}
```

Para obtener más información, consulte Configurar la recuperación automática simplificada en la Guía del usuario de Amazon EC2.

Ejemplo 2: configuración del comportamiento predeterminado de recuperación de una instancia

En el siguiente ejemplo de `modify-instance-maintenance-options` se establece el comportamiento de recuperación automática como predeterminado, lo que permite una recuperación automática simplificada para los tipos de instancias compatibles.

```
aws ec2 modify-instance-maintenance-options \
    --instance-id i-0abcdef1234567890 \
    --auto-recovery default
```

Salida:

```
{
    "InstanceId": "i-0abcdef1234567890",
    "AutoRecovery": "default"
}
```

Para obtener más información, consulte Configurar la recuperación automática simplificada en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte ModifyInstanceMaintenanceOptions en la Referencia de comandos de la AWS CLI.

`modify-instance-metadata-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-instance-metadata-options`.

AWS CLI

Ejemplo 1: habilitación de IMDSv2

En el siguiente ejemplo de `modify-instance-metadata-options` se configura el uso de IMDSv2 en la instancia especificada.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-tokens required \
    --http-endpoint enabled
```

Salida:

```
{
    "InstanceId": "i-1234567898abcdef0",
    "InstanceMetadataOptions": {
        "State": "pending",
        "HttpTokens": "required",
        "HttpPutResponseHopLimit": 1,
        "HttpEndpoint": "enabled"
    }
}
```

Para obtener más información, consulte Metadatos de instancia en la Guía del usuario de Amazon EC2.

Ejemplo 2: deshabilitación de los metadatos de la instancia

En el siguiente ejemplo de `modify-instance-metadata-options` se deshabilita el uso de todas las versiones de los metadatos de instancia en la instancia especificada.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-endpoint disabled
```

Salida:

```
{
    "InstanceId": "i-1234567898abcdef0",
    "InstanceMetadataOptions": {
        "State": "pending",
        "HttpTokens": "required",
        "HttpPutResponseHopLimit": 1,
        "HttpEndpoint": "disabled"
    }
}
```

Para obtener más información, consulte Metadatos de instancia en la Guía del usuario de Amazon EC2.

Ejemplo 3: habilitación del punto de conexión de IPv6 de metadatos de instancia para su instancia

En el ejemplo siguiente de `modify-instance-metadata-options`, se muestra cómo activar el punto de conexión de IPv6 para el servicio de metadatos de instancia. El punto de conexión IPv6 está desactivado de forma predeterminada. Esto es cierto incluso si ha iniciando una instancia en una subred de solo IPv6. El punto de conexión de IPv6 únicamente está accesible en instancias integradas en el Nitro System.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-protocol-ipv6 enabled \
    --http-endpoint enabled
```

Salida:

```
{
    "InstanceId": "i-1234567898abcdef0",
    "InstanceMetadataOptions": {
        "State": "pending",
        "HttpTokens": "required",
        "HttpPutResponseHopLimit": 1,
        "HttpEndpoint": "enabled",
        HttpProtocolIpv6": "enabled"
    }
}
```

Para obtener más información, consulte Metadatos de instancia en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte ModifyInstanceMetadataOptions en la Referencia de comandos de la AWS CLI.

`modify-instance-placement`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-instance-placement`.

AWS CLI

Ejemplo 1: eliminación de la afinidad de una instancia con un host dedicado

En el siguiente ejemplo de `modify-instance-placement` se elimina la afinidad de una instancia con un host dedicado y se permite que se lance en cualquier host dedicado disponible de su cuenta que admita ese tipo de instancia.

```
aws ec2 modify-instance-placement \
    --instance-id i-0e6ddf6187EXAMPLE \
    --affinity default
```

Salida:

```
{
    "Return": true
}
```

Ejemplo 2: establecimiento de la afinidad entre una instancia y el host dedicado especificado

En el siguiente ejemplo de `modify-instance-placement` se establece una relación de lanzamiento entre una instancia y un host dedicado. La instancia solo se puede ejecutar en el host dedicado especificado.

```
aws ec2 modify-instance-placement \
    --instance-id i-0e6ddf6187EXAMPLE \
    --affinity host \
    --host-id i-0e6ddf6187EXAMPLE
```

Salida:

```
{
    "Return": true
}
```

Ejemplo 3: movimiento de una instancia a un grupo con ubicación

En el siguiente ejemplo de `modify-instance-placement` se mueve una instancia a un grupo con ubicación, se detiene la instancia, se modifica la ubicación de la instancia y, a continuación, se reinicia la instancia.

```
aws ec2 stop-instances \
    --instance-ids i-0123a456700123456

aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name MySpreadGroup

aws ec2 start-instances \
    --instance-ids i-0123a456700123456
```

Ejemplo 4: eliminación de instancia de un grupo con ubicación

En el siguiente ejemplo de `modify-instance-placement` se elimina una instancia de un grupo con ubicación; para ello, se detiene la instancia, se modifica la ubicación de la instancia y, a continuación, se reinicia la instancia. En el siguiente ejemplo, se especifica una cadena vacía ("") como nombre del grupo con ubicación para indicar que la instancia no debe ubicarse en un grupo con ubicación.

Detenga la instancia:

```
aws ec2 stop-instances \
    --instance-ids i-0123a456700123456
```

Modifique la ubicación (símbolo del sistema de Windows):

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name ""
```

Modifique la ubicación (Windows PowerShell, Linux y macOS):

```
aws ec2 modify-instance-placement `
    --instance-id i-0123a456700123456 `
    --group-name ''
```

Reinicie la instancia:

```
aws ec2 start-instances \
    --instance-ids i-0123a456700123456
```

Salida:

```
{
    "Return": true
}
```

Para obtener más información, consulte Modificar la tenencia y afinidad del host dedicado en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte ModifyInstancePlacement en la Referencia de comandos de la AWS CLI.

`modify-ipam-pool`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-ipam-pool`.

AWS CLI

Para modificar un grupo de IPAM

En el siguiente ejemplo de `modify-ipam-pool` se modifica un grupo de IPAM.

(Linux):

```
aws ec2 modify-ipam-pool \
    --ipam-pool-id ipam-pool-0533048da7d823723 \
    --add-allocation-resource-tags "Key=Owner,Value=Build Team" \
    --clear-allocation-default-netmask-length \
    --allocation-min-netmask-length 14
```

(Windows):

```
aws ec2 modify-ipam-pool ^
    --ipam-pool-id ipam-pool-0533048da7d823723 ^
    --add-allocation-resource-tags "Key=Owner,Value=Build Team" ^
    --clear-allocation-default-netmask-length ^
    --allocation-min-netmask-length 14
```

Salida:

```
{
    "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0533048da7d823723",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0533048da7d823723",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-02fc38cd4c48e7d38",
        "IpamScopeType": "private",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-08440e7a3acde3908",
        "IpamRegion": "us-east-1",
        "Locale": "None",
        "PoolDepth": 1,
        "State": "modify-complete",
        "AutoImport": true,
        "AddressFamily": "ipv4",
        "AllocationMinNetmaskLength": 14,
        "AllocationMaxNetmaskLength": 26,
        "AllocationResourceTags": [
            {
                "Key": "Environment",
                "Value": "Preprod"
            },
            {
```

```
                "Key": "Owner",
                "Value": "Build Team"
            }
        ]
    }
}
```

Para obtener más información, consulte Edición de un grupo en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte ModifyIpamPool en la Referencia de comandos de la AWS CLI.

`modify-ipam-resource-cidr`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-ipam-resource-cidr`.

AWS CLI

Para modificar los CIDR asignados a un recurso

En el siguiente ejemplo de `modify-ipam-resource-cidr` se modifica el CIDR de un recurso.

(Linux):

```
aws ec2 modify-ipam-resource-cidr \
    --current-ipam-scope-id ipam-scope-02fc38cd4c48e7d38 \
    --destination-ipam-scope-id ipam-scope-0da34c61fd189a141 \
    --resource-id vpc-010e1791024eb0af9 \
    --resource-cidr 10.0.1.0/24 \
    --resource-region us-east-1 \
    --monitored
```

(Windows):

```
aws ec2 modify-ipam-resource-cidr ^
    --current-ipam-scope-id ipam-scope-02fc38cd4c48e7d38 ^
    --destination-ipam-scope-id ipam-scope-0da34c61fd189a141 ^
    --resource-id vpc-010e1791024eb0af9 ^
    --resource-cidr 10.0.1.0/24 ^
    --resource-region us-east-1 ^
    --monitored
```

Salida:

```
{
    "IpamResourceCidr": {
        "IpamId": "ipam-08440e7a3acde3908",
        "IpamScopeId": "ipam-scope-0da34c61fd189a141",
        "IpamPoolId": "ipam-pool-0533048da7d823723",
        "ResourceRegion": "us-east-1",
        "ResourceOwnerId": "123456789012",
        "ResourceId": "vpc-010e1791024eb0af9",
        "ResourceCidr": "10.0.1.0/24",
        "ResourceType": "vpc",
        "ResourceTags": [
            {
                "Key": "Environment",
                "Value": "Preprod"
            },
            {
                "Key": "Owner",
                "Value": "Build Team"
            }
        ],
        "IpUsage": 0.0,
        "ComplianceStatus": "noncompliant",
        "ManagementState": "managed",
        "OverlapStatus": "overlapping",
        "VpcId": "vpc-010e1791024eb0af9"
    }
}
```

Para obtener más información sobre cómo mover recursos, consulte Mover CIDR de VPC entre alcances en la Guía del usuario de Amazon VPC IPAM.

Para obtener más información sobre cómo cambiar los estados de supervisión, consulte Cambiar el estado de monitoreo de los CIDR de recursos en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte ModifyIpamResourceCidr en la Referencia de comandos de la AWS CLI.

`modify-ipam-resource-discovery`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-ipam-resource-discovery`.

AWS CLI

Para modificar las regiones operativas de una detección de recursos

En este ejemplo, usted es un administrador delegado de IPAM y desea modificar las regiones operativas de una detección de recursos.

Para llevar a cabo esta solicitud:

No puede modificar una detección de recursos predeterminada y debe ser el propietario de la detección de recursos. Necesita el ID de la detección de recursos, que puede obtener mediante describe-ipam-resource-discoveries.

En el siguiente ejemplo de `modify-ipam-resource-discovery` se modifica una detección de recursos no predeterminada de su cuenta de AWS.

```
aws ec2 modify-ipam-resource-discovery \
    --ipam-resource-discovery-id ipam-res-disco-0f4ef577a9f37a162 \
    --add-operating-regions RegionName='us-west-1' \
    --remove-operating-regions RegionName='us-east-2' \
    --region us-east-1
```

Salida:

```
{
    "IpamResourceDiscovery": {
        "OwnerId": "149977607591",
        "IpamResourceDiscoveryId": "ipam-res-disco-0365d2977fc1672fe",
        "IpamResourceDiscoveryArn": "arn:aws:ec2::149977607591:ipam-resource-
discovery/ipam-res-disco-0365d2977fc1672fe",
        "IpamResourceDiscoveryRegion": "us-east-1",
        "Description": "Example",
        "OperatingRegions": [
            {
                "RegionName": "us-east-1"
            },
            {
                "RegionName": "us-west-1"
            }
        ],
        "IsDefault": false,
        "State": "modify-in-progress"
    }
```

```
}
```

Para obtener más información, consulte Cómo trabajar con las detecciones de recursos en la Guía del usuario de IPAM de Amazon VPC.

- Para obtener información sobre la API, consulte ModifyIpamResourceDiscovery en la Referencia de comandos de la AWS CLI.

`modify-ipam-scope`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-ipam-scope`.

AWS CLI

Para modificar la descripción de un ámbito

En este caso, usted es un administrador delegado de IPAM y desea modificar la descripción de un ámbito de IPAM.

Para llevar a cabo esta solicitud, necesitará el ID del ámbito, que puede obtener mediante describe-ipam-scopes.

En el siguiente ejemplo de `modify-ipam-scope` se actualiza la descripción del ámbito.

```
aws ec2 modify-ipam-scope \
    --ipam-scope-id ipam-scope-0d3539a30b57dcdd1 \
    --description example \
    --region us-east-1
```

Salida:

```
{
"IpamScope": {
        "OwnerId": "320805250157",
        "IpamScopeId": "ipam-scope-0d3539a30b57dcdd1",
        "IpamScopeArn": "arn:aws:ec2::320805250157:ipam-scope/ipam-
scope-0d3539a30b57dcdd1",
        "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-005f921c17ebd5107",
        "IpamRegion": "us-east-1",
        "IpamScopeType": "public",
        "IsDefault": true,
        "Description": "example",
```

```
        "PoolCount": 1,
        "State": "modify-in-progress"
    }
}
```

Para obtener más información, consulte Cómo funciona IPAM en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte ModifyIpamScope en la Referencia de comandos de la AWS CLI.

`modify-ipam`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-ipam`.

AWS CLI

Para modificar un IPAM

En el siguiente ejemplo de `modify-ipam` se modifica un IPAM agregándole una región operativa.

(Linux):

```
aws ec2 modify-ipam \
    --ipam-id ipam-08440e7a3acde3908 \
    --add-operating-regions RegionName=us-west-2
```

(Windows):

```
aws ec2 modify-ipam ^
    --ipam-id ipam-08440e7a3acde3908 ^
    --add-operating-regions RegionName=us-west-2
```

Salida:

```
{
    "Ipam": {
        "OwnerId": "123456789012",
        "IpamId": "ipam-08440e7a3acde3908",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-08440e7a3acde3908",
```

```
        "IpamRegion": "us-east-1",
        "PublicDefaultScopeId": "ipam-scope-0b9eed026396dbc16",
        "PrivateDefaultScopeId": "ipam-scope-02fc38cd4c48e7d38",
        "ScopeCount": 3,
        "OperatingRegions": [
            {
                "RegionName": "us-east-1"
            },
            {
                "RegionName": "us-east-2"
            },
            {
                "RegionName": "us-west-1"
            },
            {
                "RegionName": "us-west-2"
            }
        ],
        "State": "modify-in-progress"
    }
}
```

- Para obtener información sobre la API, consulte ModifyIpam en la Referencia de comandos de la AWS CLI.

`modify-launch-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-launch-template`.

AWS CLI

Para cambiar la versión de la plantilla de lanzamiento predeterminada

En este ejemplo, se especifica la versión 2 de la plantilla de lanzamiento especificada como versión predeterminada.

Comando:

```
aws ec2 modify-launch-template --launch-template-id lt-0abcd290751193123 --default-version 2
```

Salida:

```
{
  "LaunchTemplate": {
      "LatestVersionNumber": 2,
      "LaunchTemplateId": "lt-0abcd290751193123",
      "LaunchTemplateName": "WebServers",
      "DefaultVersionNumber": 2,
      "CreatedBy": "arn:aws:iam::123456789012:root",
      "CreateTime": "2017-12-01T13:35:46.000Z"
  }
}
```

- Para obtener información sobre la API, consulte ModifyLaunchTemplate en la Referencia de comandos de la AWS CLI.

`modify-managed-prefix-list`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-managed-prefix-list`.

AWS CLI

Para modificar una lista de prefijos

En el siguiente ejemplo de `modify-managed-prefix-list` se agrega una entrada a la lista de prefijos especificada.

```
aws ec2 modify-managed-prefix-list \
    --prefix-list-id pl-0123456abcabcabc1 \
    --add-entries Cidr=10.1.0.0/16,Description=vpc-c \
    --current-version 1
```

Salida:

```
{
    "PrefixList": {
        "PrefixListId": "pl-0123456abcabcabc1",
        "AddressFamily": "IPv4",
        "State": "modify-in-progress",
        "PrefixListArn": "arn:aws:ec2:us-west-2:123456789012:prefix-list/
pl-0123456abcabcabc1",
        "PrefixListName": "vpc-cidrs",
        "MaxEntries": 10,
```

```
        "Version": 1,
        "OwnerId": "123456789012"
    }
}
```

Para obtener más información, consulte Managed prefix lists en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte ModifyManagedPrefixList en la Referencia de comandos de la AWS CLI.

`modify-network-interface-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-network-interface-attribute`.

AWS CLI

Para modificar el atributo de conexión de una interfaz de red

En este ejemplo de comando, se modifica el atributo `attachment` de la interfaz de red especificada.

Comando:

```
aws ec2 modify-network-interface-attribute --network-interface-id eni-686ea200 --attachment AttachmentId=eni-attach-43348162,DeleteOnTermination=false
```

Para modificar el atributo description de una interfaz de red

En este ejemplo de comando, se modifica el atributo `description` de la interfaz de red especificada.

Comando:

```
aws ec2 modify-network-interface-attribute --network-interface-id eni-686ea200 --description "My description"
```

Para modificar el atributo groupSet de una interfaz de red

En este ejemplo de comando, se modifica el atributo `groupSet` de la interfaz de red especificada.

Comando:

```
aws ec2 modify-network-interface-attribute --network-interface-id eni-686ea200 --
groups sg-903004f8 sg-1a2b3c4d
```

Para modificar el atributo sourceDestCheck de una interfaz de red

En este ejemplo de comando, se modifica el atributo `sourceDestCheck` de la interfaz de red especificada.

Comando:

```
aws ec2 modify-network-interface-attribute --network-interface-id eni-686ea200 --no-
source-dest-check
```

- Para obtener información sobre la API, consulte ModifyNetworkInterfaceAttribute en la Referencia de comandos de la AWS CLI.

`modify-private-dns-name-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-private-dns-name-options`.

AWS CLI

Para modificar las opciones para los nombres de host de instancia

En el siguiente ejemplo de `modify-private-dns-name-options` se deshabilita la opción de responder a las consultas de DNS de nombres de host de instancia con registros A de DNS.

```
aws ec2 modify-private-dns-name-options \
    --instance-id i-1234567890abcdef0 \
    --no-enable-resource-name-dns-a-record
```

Salida:

```
{
    "Return": true
}
```

Para obtener más información, consulte Tipos de nombres de host de instancias de Amazon EC2 en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte ModifyPrivateDnsNameOptions en la Referencia de comandos de la AWS CLI.

`modify-reserved-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-reserved-instances`.

AWS CLI

Para modificar instancias reservadas

En este ejemplo de comando, se mueve una instancia reservada a otra zona de disponibilidad de la misma región.

Comando:

```
aws ec2 modify-reserved-instances --reserved-instances-ids b847fa93-e282-4f55-b59a-1342f5bd7c02 --target-configurations AvailabilityZone=us-west-1c,Platform=EC2-Classic,InstanceCount=10
```

Salida:

```
{
  "ReservedInstancesModificationId": "rimod-d3ed4335-b1d3-4de6-ab31-0f13aaf46687"
}
```

Para modificar la plataforma de red de las instancias reservadas

En este ejemplo de comando, se convierten instancias reservadas EC2-Classic en EC2-VPC.

Comando:

```
aws ec2 modify-reserved-instances --reserved-instances-ids f127bd27-edb7-44c9-a0eb-0d7e09259af0 --target-configurations AvailabilityZone=us-west-1c,Platform=EC2-VPC,InstanceCount=5
```

Salida:

```
{
  "ReservedInstancesModificationId": "rimod-82fa9020-668f-4fb6-945d-61537009d291"
}
```

Para obtener más información, consulte Modificar instancias reservadas en la Guía del usuario de Amazon EC2.

Para modificar el tamaño de instancia de instancias reservadas

En este ejemplo de comando, se modifica una instancia reservada que tiene 10 instancias m1.small de Linux/UNIX en us-west-1c, de modo que 8 instancias m1.small se convierten en 2 instancias m1.large y las 2 instancias m1.small restantes se convierten en 1 instancia m1.medium en la misma zona de disponibilidad. Comando:

```
aws ec2 modify-reserved-instances --reserved-instances-
ids 1ba8e2e3-3556-4264-949e-63ee671405a9 --target-
configurations AvailabilityZone=us-west-1c,Platform=EC2-
Classic,InstanceCount=2,InstanceType=m1.large AvailabilityZone=us-
west-1c,Platform=EC2-Classic,InstanceCount=1,InstanceType=m1.medium
```

Salida:

```
{
    "ReservedInstancesModificationId": "rimod-acc5f240-080d-4717-b3e3-1c6b11fa00b6"
}
```

Para obtener más información, consulte Modifying the Instance Size of Your Reservations en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte ModifyReservedInstances en la Referencia de comandos de la AWS CLI.

`modify-security-group-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-security-group-rules`.

AWS CLI

Para modificar las reglas de un grupo de seguridad y actualizar la descripción de la regla, el protocolo IP y el rango de direcciones de CidrIpv

En el siguiente ejemplo de `modify-security-group-rules` se actualizan la descripción, el protocolo IP y el rango de CIDR de IPV4 de una regla de grupo de seguridad especificada. Utilice el parámetro `security-group-rules` para introducir las actualizaciones de las reglas de grupo de seguridad especificadas. `-1` especifica todos los protocolos.

```
aws ec2 modify-security-group-rules \
    --group-id sg-1234567890abcdef0 \
    --security-group-rules SecurityGroupRuleId=sgr-
abcdef01234567890,SecurityGroupRule='{Description=test,IpProtocol=-1,CidrIpv4=0.0.0.0/0}'
```

Salida:

```
{
    "Return": true
}
```

Si desea obtener más información acerca de las reglas de grupo de seguridad, consulte Reglas de grupo de seguridad en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte ModifySecurityGroupRules en la Referencia de comandos de la AWS CLI.

`modify-snapshot-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-snapshot-attribute`.

AWS CLI

Ejemplo 1: modificación de un atributo de instantánea

En el siguiente ejemplo de `modify-snapshot-attribute` se actualiza el atributo `createVolumePermission` de la instantánea especificada y se eliminan los permisos de volumen del usuario especificado.

```
aws ec2 modify-snapshot-attribute \
    --snapshot-id snap-1234567890abcdef0 \
    --attribute createVolumePermission \
    --operation-type remove \
    --user-ids 123456789012
```

Ejemplo 2: operación de hacer pública una instantánea

En el siguiente ejemplo de `modify-snapshot-attribute` se hace pública la instantánea especificada.

```
aws ec2 modify-snapshot-attribute \
    --snapshot-id snap-1234567890abcdef0 \
    --attribute createVolumePermission \
    --operation-type add \
    --group-names all
```

- Para obtener información sobre la API, consulte ModifySnapshotAttribute en la Referencia de comandos de la AWS CLI.

`modify-snapshot-tier`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-snapshot-tier`.

AWS CLI

Archivo de una instantánea

En el siguiente ejemplo de `modify-snapshot-tier` se archiva la instantánea especificada. El parámetro de respuesta `TieringStartTime` indica la fecha y la hora en que se inició el proceso de archivo en formato de hora UTC (AAAA-MM-DDTHH:MM:SSZ).

```
aws ec2 modify-snapshot-tier \
    --snapshot-id snap-01234567890abcedf \
    --storage-tier archive
```

Salida:

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "TieringStartTime": "2021-09-15T16:44:37.574Z"
}
```

Para obtener más información sobre el archivado de instantáneas, consulte Archivo de instantáneas de Amazon EBS en la Guía del usuario de Amazon EBS.

- Para obtener información sobre la API, consulte ModifySnapshotTier en la Referencia de comandos de la AWS CLI.

`modify-spot-fleet-request`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-spot-fleet-request`.

AWS CLI

Para modificar una solicitud de flota de spot

En este ejemplo de comando, se actualiza la capacidad de destino de la solicitud de flota de spot especificada.

Comando:

```
aws ec2 modify-spot-fleet-request --target-capacity 20 --spot-fleet-request-
id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Salida:

```
{
    "Return": true
}
```

En este ejemplo de comando, se disminuye la capacidad de destino de la flota de spot especificada sin que ello suponga terminar ninguna de las instancias de spot.

Comando:

```
aws ec2 modify-spot-fleet-request --target-capacity 10 --excess-capacity-
termination-policy NoTermination --spot-fleet-request-ids sfr-73fbd2ce-
aa30-494c-8788-1cee4EXAMPLE
```

Salida:

```
{
    "Return": true
}
```

- Para obtener información sobre la API, consulte ModifySpotFleetRequest en la Referencia de comandos de la AWS CLI.

`modify-subnet-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-subnet-attribute`.

AWS CLI

Para cambiar el comportamiento del direccionamiento de IPv4 público de una subred

En este ejemplo, se modifica subnet-1a2b3c4d de modo que se especifique que a todas las instancias lanzadas en esta subred se les asigne una dirección IPv4 pública. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 modify-subnet-attribute --subnet-id subnet-1a2b3c4d --map-public-ip-on-launch
```

Para cambiar el comportamiento del direccionamiento de IPv6 público de una subred

En este ejemplo, se modifica subnet-1a2b3c4d de modo que se especifique que a todas las instancias lanzadas en esta subred se les asigne una dirección IPv6 pública.

Comando:

```
aws ec2 modify-subnet-attribute --subnet-id subnet-1a2b3c4d --assign-ipv6-address-on-creation
```

Para obtener más información, consulte Direccionamiento IP para VPC en la Guía del usuario de AWS Virtual Private Cloud.

- Para obtener información sobre la API, consulte ModifySubnetAttribute en la Referencia de comandos de la AWS CLI.

`modify-traffic-mirror-filter-network-services`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-traffic-mirror-filter-network-services`.

AWS CLI

Para añadir servicios de red a un filtro de reflejo de tráfico

En el siguiente ejemplo de `modify-traffic-mirror-filter-network-services` se agregan los servicios de red de DNS de Amazon al filtro especificado.

```
aws ec2 modify-traffic-mirror-filter-network-services \
    --traffic-mirror-filter-id tmf-04812ff784EXAMPLE \
    --add-network-service amazon-dns
```

Salida:

```
{
    "TrafficMirrorFilter": {
        "Tags": [
            {
                "Key": "Name",
                "Value": "Production"
            }
        ],
        "EgressFilterRules": [],
        "NetworkServices": [
            "amazon-dns"
        ],
        "TrafficMirrorFilterId": "tmf-04812ff784EXAMPLE",
        "IngressFilterRules": [
            {
                "SourceCidrBlock": "0.0.0.0/0",
                "RuleNumber": 1,
                "DestinationCidrBlock": "0.0.0.0/0",
                "Description": "TCP Rule",
                "Protocol": 6,
                "TrafficDirection": "ingress",
                "TrafficMirrorFilterId": "tmf-04812ff784EXAMPLE",
                "RuleAction": "accept",
                "TrafficMirrorFilterRuleId": "tmf-04812ff784EXAMPLE"
            }
        ]
    }
}
```

Para obtener más información, consulte Modify Traffic Mirror Filter Network Services en la Guía de creación de reflejo de tráfico de AWS.

- Para obtener información sobre la API, consulte ModifyTrafficMirrorFilterNetworkServices en la Referencia de comandos de la AWS CLI.

modify-traffic-mirror-filter-rule

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-traffic-mirror-filter-rule`.

AWS CLI

Para modificar una regla de filtro de reflejo de tráfico

En el siguiente ejemplo de `modify-traffic-mirror-filter-rule` se modifica la descripción de la regla de filtro de reflejo de tráfico especificada.

```
aws ec2 modify-traffic-mirror-filter-rule \
    --traffic-mirror-filter-rule-id tmfr-0ca76e0e08EXAMPLE \
    --description "TCP Rule"
```

Salida:

```
{
    "TrafficMirrorFilterRule": {
        "TrafficMirrorFilterRuleId": "tmfr-0ca76e0e08EXAMPLE",
        "TrafficMirrorFilterId": "tmf-0293f26e86EXAMPLE",
        "TrafficDirection": "ingress",
        "RuleNumber": 100,
        "RuleAction": "accept",
        "Protocol": 6,
        "DestinationCidrBlock": "10.0.0.0/24",
        "SourceCidrBlock": "10.0.0.0/24",
        "Description": "TCP Rule"
    }
}
```

Para obtener más información, consulte Modify Your Traffic Mirror Filter Rules en la Guía de creación de reflejo de tráfico de AWS.

- Para obtener información sobre la API, consulte ModifyTrafficMirrorFilterRule en la Referencia de comandos de la AWS CLI.

modify-traffic-mirror-session

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-traffic-mirror-session`.

AWS CLI

Para modificar una sesión de reflejo de tráfico

En el siguiente ejemplo de `modify-traffic-mirror-session` se cambian la descripción de la sesión de reflejo de tráfico y la cantidad de paquetes que se van a reflejar.

```
aws ec2 modify-traffic-mirror-session \
    --description "Change packet length" \
    --traffic-mirror-session-id tms-08a33b1214EXAMPLE \
    --remove-fields "packet-length"
```

Salida:

```
{
    "TrafficMirrorSession": {
        "TrafficMirrorSessionId": "tms-08a33b1214EXAMPLE",
        "TrafficMirrorTargetId": "tmt-07f75d8feeEXAMPLE",
        "TrafficMirrorFilterId": "tmf-04812ff784EXAMPLE",
        "NetworkInterfaceId": "eni-070203f901EXAMPLE",
        "OwnerId": "111122223333",
        "SessionNumber": 1,
        "VirtualNetworkId": 7159709,
        "Description": "Change packet length",
        "Tags": []
    }
}
```

Para obtener más información, consulte Modify your traffic mirror session en la Guía de creación de reflejo de tráfico.

- Para obtener información sobre la API, consulte ModifyTrafficMirrorSession en la Referencia de comandos de la AWS CLI.

`modify-transit-gateway-prefix-list-reference`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-transit-gateway-prefix-list-reference`.

AWS CLI

Para modificar una referencia a una lista de prefijos

En el siguiente ejemplo de `modify-transit-gateway-prefix-list-reference` se modifica la referencia a la lista de prefijos de la tabla de enrutamiento especificada; para ello, se cambia la conexión a la que se enruta el tráfico.

```
aws ec2 modify-transit-gateway-prefix-list-reference \
    --transit-gateway-route-table-id tgw-rtb-0123456789abcd123 \
    --prefix-list-id pl-1111112222222333 \
    --transit-gateway-attachment-id tgw-attach-aabbccddaabbccaab
```

Salida:

```
{
    "TransitGatewayPrefixListReference": {
        "TransitGatewayRouteTableId": "tgw-rtb-0123456789abcd123",
        "PrefixListId": "pl-11111122222222333",
        "PrefixListOwnerId": "123456789012",
        "State": "modifying",
        "Blackhole": false,
        "TransitGatewayAttachment": {
            "TransitGatewayAttachmentId": "tgw-attach-aabbccddaabbccaab",
            "ResourceType": "vpc",
            "ResourceId": "vpc-112233445566aabbc"
        }
    }
}
```

Para obtener más información, consulte Prefix list references en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte ModifyTransitGatewayPrefixListReference en la Referencia de comandos de la AWS CLI.

`modify-transit-gateway-vpc-attachment`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-transit-gateway-vpc-attachment`.

AWS CLI

Para modificar una conexión de VPC de puerta de enlace de tránsito

En el siguiente ejemplo de `modify-transit-gateway-vpc-attachment` se agrega una subred a la conexión de VPC de puerta de enlace de tránsito especificada.

```
aws ec2 modify-transit-gateway-vpc-attachment \
    --transit-gateway-attachment-id tgw-attach-09fbd47ddfEXAMPLE \
    --add-subnet-ids subnet-0e51f45802EXAMPLE
```

Salida:

```
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-09fbd47ddfEXAMPLE",
        "TransitGatewayId": "tgw-0560315ccfEXAMPLE",
        "VpcId": "vpc-5eccc927",
        "VpcOwnerId": "111122223333",
        "State": "modifying",
        "SubnetIds": [
            "subnet-0e51f45802EXAMPLE",
            "subnet-1EXAMPLE"
        ],
        "CreationTime": "2019-08-08T16:47:38.000Z",
        "Options": {
            "DnsSupport": "enable",
            "Ipv6Support": "disable"
        }
    }
}
```

Para obtener más información, consulte Transit gateway attachments to a VPC en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte ModifyTransitGatewayVpcAttachment en la Referencia de comandos de la AWS CLI.

`modify-transit-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-transit-gateway`.

AWS CLI

Para modificar una puerta de enlace de tránsito

En el siguiente ejemplo de `modify-transit-gateway` se modifica la puerta de enlace de tránsito especificada; para ello, se habilita la compatibilidad con ECMP en las conexiones de VPN.

```
aws ec2 modify-transit-gateway \
    --transit-gateway-id tgw-111111222222aaaaa \
    --options VpnEcmpSupport=enable
```

Salida:

```
{
    "TransitGateway": {
        "TransitGatewayId": "tgw-111111222222aaaaa",
        "TransitGatewayArn": "64512",
        "State": "modifying",
        "OwnerId": "123456789012",
        "CreationTime": "2020-04-30T08:41:37.000Z",
        "Options": {
            "AmazonSideAsn": 64512,
            "AutoAcceptSharedAttachments": "disable",
            "DefaultRouteTableAssociation": "enable",
            "AssociationDefaultRouteTableId": "tgw-rtb-0123456789abcd123",
            "DefaultRouteTablePropagation": "enable",
            "PropagationDefaultRouteTableId": "tgw-rtb-0123456789abcd123",
            "VpnEcmpSupport": "enable",
            "DnsSupport": "enable"
        }
    }
}
```

Para obtener más información, consulte Transit gateways en la Guía de Transit Gateways.

- Para obtener información sobre la API, consulte ModifyTransitGateway en la Referencia de comandos de la AWS CLI.

`modify-verified-access-endpoint-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-verified-access-endpoint-policy`.

AWS CLI

Para configurar la política de acceso verificado de un punto de conexión

En el siguiente ejemplo de `modify-verified-access-endpoint-policy` se agrega la política de acceso verificado especificada al punto de conexión de acceso verificado especificado.

```
aws ec2 modify-verified-access-endpoint-policy \
    --verified-access-endpoint-id vae-066fac616d4d546f2 \
    --policy-enabled \
    --policy-document file://policy.txt
```

Contenido de `policy.txt`:

```
permit(principal,action,resource)
when {
    context.identity.groups.contains("finance") &&
    context.identity.email.verified == true
};
```

Salida:

```
{
    "PolicyEnabled": true,
    "PolicyDocument": "permit(principal,action,resource)\nwhen
 {\n    context.identity.groups.contains(\"finance\") &&\n
 context.identity.email_verified == true\n};"
}
```

Para obtener más información, consulte Verified Access policies en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte ModifyVerifiedAccessEndpointPolicy en la Referencia de comandos de la AWS CLI.

`modify-verified-access-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-verified-access-endpoint`.

AWS CLI

Para modificar la configuración de un punto de conexión de acceso verificado

En el siguiente ejemplo de `modify-verified-access-endpoint` se agrega la descripción especificada al punto de conexión de acceso verificado especificado.

```
aws ec2 modify-verified-access-endpoint \
```

```
    --verified-access-endpoint-id vae-066fac616d4d546f2 \
    --description 'Testing Verified Access'
```

Salida:

```
{
    "VerifiedAccessEndpoint": {
        "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
        "VerifiedAccessGroupId": "vagr-0dbe967baf14b7235",
        "VerifiedAccessEndpointId": "vae-066fac616d4d546f2",
        "ApplicationDomain": "example.com",
        "EndpointType": "network-interface",
        "AttachmentType": "vpc",
        "DomainCertificateArn": "arn:aws:acm:us-east-2:123456789012:certificate/
eb065ea0-26f9-4e75-a6ce-0a1a7EXAMPLE",
        "EndpointDomain": "my-ava-
app.edge-00c3372d53b1540bb.vai-0ce000c0b7643abea.prod.verified-access.us-
east-2.amazonaws.com",
        "SecurityGroupIds": [
            "sg-004915970c4c8f13a"
        ],
        "NetworkInterfaceOptions": {
            "NetworkInterfaceId": "eni-0aec70418c8d87a0f",
            "Protocol": "https",
            "Port": 443
        },
        "Status": {
            "Code": "updating"
        },
        "Description": "Testing Verified Access",
        "CreationTime": "2023-08-25T20:54:43",
        "LastUpdatedTime": "2023-08-25T22:46:32"
    }
}
```

Para obtener más información, consulte Verified Access endpoints en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte ModifyVerifiedAccessEndpoint en la Referencia de comandos de la AWS CLI.

`modify-verified-access-group-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-verified-access-group-policy`.

AWS CLI

Para configurar una política de acceso verificado para un grupo

En el siguiente ejemplo de `modify-verified-access-group-policy` se agrega la política de acceso verificado especificada al grupo de acceso verificado especificado.

```
aws ec2 modify-verified-access-group-policy \
    --verified-access-group-id vagr-0dbe967baf14b7235 \
    --policy-enabled \
    --policy-document file://policy.txt
```

Contenido de `policy.txt`:

```
permit(principal,action,resource)
when {
    context.identity.groups.contains("finance") &&
    context.identity.email.verified == true
};
```

Salida:

```
{
    "PolicyEnabled": true,
    "PolicyDocument": "permit(principal,action,resource)\nwhen
 {\n    context.identity.groups.contains(\"finance\") &&\n
 context.identity.email_verified == true\n};"
}
```

Para obtener más información, consulte Verified Access groups en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte ModifyVerifiedAccessGroupPolicy en la Referencia de comandos de la AWS CLI.

`modify-verified-access-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-verified-access-group`.

AWS CLI

Para modificar la configuración de un grupo de acceso verificado

En el siguiente ejemplo de `modify-verified-access-group` se agrega la descripción especificada al grupo de acceso verificado especificado.

```
aws ec2 modify-verified-access-group \
    --verified-access-group-id vagr-0dbe967baf14b7235 \
    --description "Testing Verified Access"
```

Salida:

```
{
    "VerifiedAccessGroup": {
        "VerifiedAccessGroupId": "vagr-0dbe967baf14b7235",
        "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
        "Description": "Testing Verified Access",
        "Owner": "123456789012",
        "VerifiedAccessGroupArn": "arn:aws:ec2:us-east-2:123456789012:verified-
access-group/vagr-0dbe967baf14b7235",
        "CreationTime": "2023-08-25T19:55:19",
        "LastUpdatedTime": "2023-08-25T22:17:25"
    }
}
```

Para obtener más información, consulte Verified Access groups en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte ModifyVerifiedAccessGroup en la Referencia de comandos de la AWS CLI.

`modify-verified-access-instance-logging-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-verified-access-instance-logging-configuration`.

AWS CLI

Para habilitar el registro de una instancia de acceso verificado

En el siguiente ejemplo de `modify-verified-access-instance-logging-configuration` se habilita el registro de acceso para la instancia de acceso verificado especificada. Los registros se entregarán al grupo de registro de registros de CloudWatch especificado.

```
aws ec2 modify-verified-access-instance-logging-configuration \
    --verified-access-instance-id vai-0ce000c0b7643abea \
    --access-logs CloudWatchLogs={Enabled=true,LogGroup=my-log-group}
```

Salida:

```
{
    "LoggingConfiguration": {
        "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
        "AccessLogs": {
            "S3": {
                "Enabled": false
            },
            "CloudWatchLogs": {
                "Enabled": true,
                "DeliveryStatus": {
                    "Code": "success"
                },
                "LogGroup": "my-log-group"
            },
            "KinesisDataFirehose": {
                "Enabled": false
            },
            "LogVersion": "ocsf-1.0.0-rc.2",
            "IncludeTrustContext": false
        }
    }
}
```

Para obtener más información, consulte Verified Access logs en la Guía del usuario de acceso verificado de AWS.

- Para obtener información sobre la API, consulte ModifyVerifiedAccessInstanceLoggingConfiguration en la Referencia de comandos de la AWS CLI.

`modify-verified-access-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-verified-access-instance`.

AWS CLI

Para modificar la configuración de una instancia de acceso verificado

En el siguiente ejemplo de `modify-verified-access-instance` se agrega la descripción especificada a la instancia de acceso verificado especificada.

```
aws ec2 modify-verified-access-instance \
    --verified-access-instance-id vai-0ce000c0b7643abea \
    --description "Testing Verified Access"
```

Salida:

```
{
    "VerifiedAccessInstance": {
        "VerifiedAccessInstanceId": "vai-0ce000c0b7643abea",
        "Description": "Testing Verified Access",
        "VerifiedAccessTrustProviders": [
            {
                "VerifiedAccessTrustProviderId": "vatp-0bb32de759a3e19e7",
                "TrustProviderType": "user",
                "UserTrustProviderType": "iam-identity-center"
            }
        ],
        "CreationTime": "2023-08-25T18:27:56",
        "LastUpdatedTime": "2023-08-25T22:41:04"
    }
}
```

Para obtener más información, consulte Verified Access instances en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte ModifyVerifiedAccessInstance en la Referencia de comandos de la AWS CLI.

`modify-verified-access-trust-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-verified-access-trust-provider`.

AWS CLI

Para modificar la configuración de un proveedor de confianza de acceso verificado

En el siguiente ejemplo de `modify-verified-access-trust-provider` se agrega la descripción especificada al proveedor de confianza de acceso verificado especificado.

```
aws ec2 modify-verified-access-trust-provider \
    --verified-access-trust-provider-id vatp-0bb32de759a3e19e7 \
    --description "Testing Verified Access"
```

Salida:

```
{
    "VerifiedAccessTrustProvider": {
        "VerifiedAccessTrustProviderId": "vatp-0bb32de759a3e19e7",
        "Description": "Testing Verified Access",
        "TrustProviderType": "user",
        "UserTrustProviderType": "iam-identity-center",
        "PolicyReferenceName": "idc",
        "CreationTime": "2023-08-25T19:00:38",
        "LastUpdatedTime": "2023-08-25T19:18:21"
    }
}
```

Para obtener más información, consulte Trust providers for Verified Access en la Guía del usuario de Acceso verificado de AWS.

- Para obtener información sobre la API, consulte ModifyVerifiedAccessTrustProvider en la Referencia de comandos de la AWS CLI.

`modify-volume-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-volume-attribute`.

AWS CLI

Para modificar un atributo de volumen

En este ejemplo se establece en `true` el atributo `autoEnableIo` del volumen con el ID `vol-1234567890abcdef0`. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 modify-volume-attribute --volume-id vol-1234567890abcdef0 --auto-enable-io
```

- Para obtener información sobre la API, consulte ModifyVolumeAttribute en la Referencia de comandos de la AWS CLI.

`modify-volume`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-volume`.

AWS CLI

Ejemplo 1: modificación de un volumen mediante el cambio de su tamaño

En el siguiente ejemplo de `modify-volume` se cambia el tamaño del volumen especificado a 150 GB.

Comando:

```
aws ec2 modify-volume --size 150 --volume-id vol-1234567890abcdef0
```

Salida:

```
{
    "VolumeModification": {
        "TargetSize": 150,
        "TargetVolumeType": "io1",
```

```
        "ModificationState": "modifying",
        "VolumeId": " vol-1234567890abcdef0",
        "TargetIops": 100,
        "StartTime": "2019-05-17T11:27:19.000Z",
        "Progress": 0,
        "OriginalVolumeType": "io1",
        "OriginalIops": 100,
        "OriginalSize": 100
    }
}
```

Ejemplo 2: modificación de un volumen mediante el cambio de su tipo, tamaño y valor de IOPS

En el siguiente ejemplo de `modify-volume` se cambia el tipo de volumen a SSD de IOPS aprovisionadas, se establece la tasa de IOPS de destino en 10 000 y se establece el tamaño del volumen en 350 GB.

```
aws ec2 modify-volume \
    --volume-type io1 \
    --iops 10000 \
    --size 350 \
    --volume-id vol-1234567890abcdef0
```

Salida:

```
{
    "VolumeModification": {
        "TargetSize": 350,
        "TargetVolumeType": "io1",
        "ModificationState": "modifying",
        "VolumeId": "vol-0721c1a9d08c93bf6",
        "TargetIops": 10000,
        "StartTime": "2019-05-17T11:38:57.000Z",
        "Progress": 0,
        "OriginalVolumeType": "gp2",
        "OriginalIops": 150,
        "OriginalSize": 50
    }
}
```

- Para obtener información sobre la API, consulte ModifyVolume en la Referencia de comandos de la AWS CLI.

`modify-vpc-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-vpc-attribute`.

AWS CLI

Para modificar el atributo enableDnsSupport

En este ejemplo, se modifica el atributo `enableDnsSupport`. Este atributo indica si la resolución de DNS está habilitada para la VPC. Si este atributo es `true`, el servidor DNS de Amazon resuelve nombres de host de DNS para sus instancias en sus direcciones IP correspondientes; de lo contrario, no. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 modify-vpc-attribute --vpc-id vpc-a01106c2 --enable-dns-support "{\"Value
\":false}"
```

Para modificar el atributo enableDnsHostnames

En este ejemplo, se modifica el atributo `enableDnsHostnames`. Este atributo especifica si las instancias lanzadas en la VPC obtienen nombres de host de DNS. Si el atributo es `true`, las instancias de la VPC obtienen nombres de host de DNS; de lo contrario, no. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 modify-vpc-attribute --vpc-id vpc-a01106c2 --enable-dns-hostnames "{\"Value
\":false}"
```

- Para obtener información sobre la API, consulte ModifyVpcAttribute en la Referencia de comandos de la AWS CLI.

`modify-vpc-endpoint-connection-notification`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-vpc-endpoint-connection-notification`.

AWS CLI

Para modificar una notificación de conexión de punto de conexión

En este ejemplo, se cambia el tema de SNS de la notificación de conexión de punto de conexión especificada.

Comando:

```
aws ec2 modify-vpc-endpoint-connection-notification --connection-notification-id vpce-nfn-008776de7e03f5abc --connection-events Accept Reject --connection-notification-arn arn:aws:sns:us-east-2:123456789012:mytopic
```

Salida:

```
{
   "ReturnValue": true
}
```

- Para obtener información sobre la API, consulte ModifyVpcEndpointConnectionNotification en la Referencia de comandos de la AWS CLI.

`modify-vpc-endpoint-service-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-vpc-endpoint-service-configuration`.

AWS CLI

Para modificar una configuración de servicio de punto de conexión

En este ejemplo, se cambia el requisito de aceptación del servicio de punto de conexión especificado.

Comando:

```
aws ec2 modify-vpc-endpoint-service-configuration --service-id vpce-svc-09222513e6e77dc86 --no-acceptance-required
```

Salida:

```
{
   "ReturnValue": true
}
```

- Para obtener información sobre la API, consulte ModifyVpcEndpointServiceConfiguration en la Referencia de comandos de la AWS CLI.

`modify-vpc-endpoint-service-payer-responsibility`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-vpc-endpoint-service-payer-responsibility`.

AWS CLI

Para modificar la responsabilidad del pagador

En el siguiente ejemplo de `modify-vpc-endpoint-service-payer-responsibility` se modifica la responsabilidad del pagador del servicio de punto de conexión especificado.

```
aws ec2 modify-vpc-endpoint-service-payer-responsibility \
    --service-id vpce-svc-071afff70666e61e0 \
    --payer-responsibility ServiceOwner
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte ModifyVpcEndpointServicePayerResponsibility en la Referencia de comandos de la AWS CLI.

`modify-vpc-endpoint-service-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-vpc-endpoint-service-permissions`.

AWS CLI

Para modificar los permisos del servicio de punto de conexión

En este ejemplo, se agrega el permiso para que una cuenta de AWS se conecte al servicio de punto de conexión especificado.

Comando:

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-
svc-03d5ebb7d9579a2b3 --add-allowed-principals '["arn:aws:iam::123456789012:root"]'
```

Salida:

```
{
   "ReturnValue": true
}
```

En este ejemplo, se agrega el permiso para que un usuario de IAM (`admin`) específico se conecte al servicio de punto de conexión especificado.

Comando:

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-
svc-03d5ebb7d9579a2b3 --add-allowed-principals '["arn:aws:iam::123456789012:user/
admin"]'
```

- Para obtener información sobre la API, consulte ModifyVpcEndpointServicePermissions en la Referencia de comandos de la AWS CLI.

`modify-vpc-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-vpc-endpoint`.

AWS CLI

Para modificar un punto de conexión de puerta de enlace

En este ejemplo, se modifica el punto de conexión de puerta de enlace `vpce-1a2b3c4d`; para ello, asocia la tabla de enrutamiento `rtb-aaa222bb` al punto de conexión y restablece el documento de política.

Comando:

```
aws ec2 modify-vpc-endpoint --vpc-endpoint-id vpce-1a2b3c4d --add-route-table-
ids rtb-aaa222bb --reset-policy
```

Salida:

```
{
  "Return": true
}
```

Para modificar un punto de conexión de interfaz

En este ejemplo, se modifica el punto de conexión de la interfaz `vpce-0fe5b17a0707d6fa5` agregando la subred `subnet-d6fcaa8d` al punto de conexión.

Comando:

```
aws ec2 modify-vpc-endpoint --vpc-endpoint-id vpce-0fe5b17a0707d6fa5 --add-subnet-id subnet-d6fcaa8d
```

Salida:

```
{
  "Return": true
}
```

- Para obtener información sobre la API, consulte ModifyVpcEndpoint en la Referencia de comandos de la AWS CLI.

`modify-vpc-peering-connection-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-vpc-peering-connection-options`.

AWS CLI

Para habilitar la comunicación a través de una conexión de emparejamiento de VPC desde su conexión de ClassicLink local

En este ejemplo, para la conexión de emparejamiento `pcx-aaaabbb`, el propietario de la VPC solicitante modifica las opciones de conexión de emparejamiento de VPC para permitir que una conexión de ClassicLink local se comunique con la VPC emparejada.

Comando:

```
aws ec2 modify-vpc-peering-connection-options --vpc-peering-connection-id pcx-aaaabbbb --requester-peering-connection-options AllowEgressFromLocalClassicLinkToRemoteVpc=true
```

Salida:

```
{
```

```
  "RequesterPeeringConnectionOptions": {
      "AllowEgressFromLocalClassicLinkToRemoteVpc": true
  }
}
```

Para habilitar la comunicación a través de una conexión de emparejamiento de VPC desde una conexión de ClassicLink remota

En este ejemplo, el propietario de la VPC aceptadora modifica las opciones de conexión de emparejamiento de VPC para permitir que la VPC local se comunique con la conexión de ClassicLink de la VPC emparejada.

Comando:

```
aws ec2 modify-vpc-peering-connection-options --vpc-peering-
connection-id pcx-aaaabbbb --accepter-peering-connection-
options AllowEgressFromLocalVpcToRemoteClassicLink=true
```

Salida:

```
{
  "AccepterPeeringConnectionOptions": {
    "AllowEgressFromLocalVpcToRemoteClassicLink": true
  }
}
```

Para habilitar el soporte de resolución de DNS para conexión de emparejamiento de VPC

En este ejemplo, el propietario de la VPC solicitante modifica las opciones de conexión de emparejamiento de VPC de `pcx-aaaabbbb` para permitir que la VPC local resuelva los nombres de host de DNS públicos en direcciones IP privadas al realizar consultas desde instancias de la VPC emparejada.

Comando:

```
aws ec2 modify-vpc-peering-connection-options --vpc-peering-connection-id pcx-
aaaabbbb --requester-peering-connection-options AllowDnsResolutionFromRemoteVpc=true
```

Salida:

```
{
```

```
  "RequesterPeeringConnectionOptions": {
      "AllowDnsResolutionFromRemoteVpc": true
  }
}
```

- Para obtener información sobre la API, consulte ModifyVpcPeeringConnectionOptions en la Referencia de comandos de la AWS CLI.

`modify-vpc-tenancy`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-vpc-tenancy`.

AWS CLI

Para modificar la tenencia de una VPC

En este ejemplo, se modifica la tenencia de la VPC `vpc-1a2b3c4d` a `default`.

Comando:

```
aws ec2 modify-vpc-tenancy --vpc-id vpc-1a2b3c4d --instance-tenancy default
```

Salida:

```
{
  "Return": true
}
```

- Para obtener información sobre la API, consulte ModifyVpcTenancy en la Referencia de comandos de la AWS CLI.

`modify-vpn-connection-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-vpn-connection-options`.

AWS CLI

Modificación de las opciones de conexión de la VPN

En el siguiente ejemplo de `modify-vpn-connection-options` se modifica el CIDR de IPv4 local de la puerta de enlace de cliente de la conexión de VPN especificada.

```
aws ec2 modify-vpn-connection-options \
    --vpn-connection-id vpn-1122334455aabbccd \
    --local-ipv4-network-cidr 10.0.0.0/16
```

Salida:

```
{
    "VpnConnections": [
        {
            "CustomerGatewayConfiguration": "...configuration information...",
            "CustomerGatewayId": "cgw-01234567abcde1234",
            "Category": "VPN",
            "State": "modifying",
            "Type": "ipsec.1",
            "VpnConnectionId": "vpn-1122334455aabbccd",
            "TransitGatewayId": "tgw-00112233445566aab",
            "Options": {
                "EnableAcceleration": false,
                "StaticRoutesOnly": true,
                "LocalIpv4NetworkCidr": "10.0.0.0/16",
                "RemoteIpv4NetworkCidr": "0.0.0.0/0",
                "TunnelInsideIpVersion": "ipv4"
            },
            "Routes": [],
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "CanadaVPN"
                }
            ],
            "VgwTelemetry": [
                {
                    "AcceptedRouteCount": 0,
                    "LastStatusChange": "2020-07-29T10:35:11.000Z",
                    "OutsideIpAddress": "203.0.113.3",
                    "Status": "DOWN",
                    "StatusMessage": ""
                },
                {
                    "AcceptedRouteCount": 0,
                    "LastStatusChange": "2020-09-02T09:09:33.000Z",
                    "OutsideIpAddress": "203.0.113.5",
                    "Status": "UP",
```

```
                    "StatusMessage": ""
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Modifying Site-to-Site VPN connection options en la Guía del usuario de AWS Site-to-Site VPN.

- Para obtener información sobre la API, consulte ModifyVpnConnectionOptions en la Referencia de comandos de la AWS CLI.

`modify-vpn-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-vpn-connection`.

AWS CLI

Para modificar una conexión de VPN

En el siguiente ejemplo de `modify-vpn-connection` se cambia la puerta de enlace de destino de la conexión VPN `vpn-12345678901234567` a la puerta de enlace privada virtual `vgw-11223344556677889`:

```
aws ec2 modify-vpn-connection \
    --vpn-connection-id vpn-12345678901234567 \
    --vpn-gateway-id vgw-11223344556677889
```

Salida:

```
{
    "VpnConnection": {
        "CustomerGatewayConfiguration": "...configuration information...",
        "CustomerGatewayId": "cgw-aabbccddee1122334",
        "Category": "VPN",
        "State": "modifying",
        "Type": "ipsec.1",
        "VpnConnectionId": "vpn-12345678901234567",
        "VpnGatewayId": "vgw-11223344556677889",
        "Options": {
            "StaticRoutesOnly": false
```

```
        },
        "VgwTelemetry": [
            {
                "AcceptedRouteCount": 0,
                "LastStatusChange": "2019-07-17T07:34:00.000Z",
                "OutsideIpAddress": "18.210.3.222",
                "Status": "DOWN",
                "StatusMessage": "IPSEC IS DOWN"
            },
            {
                "AcceptedRouteCount": 0,
                "LastStatusChange": "2019-07-20T21:20:16.000Z",
                "OutsideIpAddress": "34.193.129.33",
                "Status": "DOWN",
                "StatusMessage": "IPSEC IS DOWN"
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte ModifyVpnConnection en la Referencia de comandos de la AWS CLI.

`modify-vpn-tunnel-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-vpn-tunnel-certificate`.

AWS CLI

Para rotar un certificado de túnel de VPN

En el siguiente ejemplo de `modify-vpn-tunnel-certificate` se rota el certificado del túnel especificado para una conexión de VPN.

```
aws ec2 modify-vpn-tunnel-certificate \
    --vpn-tunnel-outside-ip-address 203.0.113.17 \
    --vpn-connection-id vpn-12345678901234567
```

Salida:

```
{
    "VpnConnection": {
```

```
        "CustomerGatewayConfiguration": ...configuration information...,
        "CustomerGatewayId": "cgw-aabbccddee1122334",
        "Category": "VPN",
        "State": "modifying",
        "Type": "ipsec.1",
        "VpnConnectionId": "vpn-12345678901234567",
        "VpnGatewayId": "vgw-11223344556677889",
        "Options": {
            "StaticRoutesOnly": false
        },
        "VgwTelemetry": [
            {
                "AcceptedRouteCount": 0,
                "LastStatusChange": "2019-09-11T17:27:14.000Z",
                "OutsideIpAddress": "203.0.113.17",
                "Status": "DOWN",
                "StatusMessage": "IPSEC IS DOWN",
                "CertificateArn": "arn:aws:acm:us-east-1:123456789101:certificate/
c544d8ce-20b8-4fff-98b0-example"
            },
            {
                "AcceptedRouteCount": 0,
                "LastStatusChange": "2019-09-11T17:26:47.000Z",
                "OutsideIpAddress": "203.0.114.18",
                "Status": "DOWN",
                "StatusMessage": "IPSEC IS DOWN",
                "CertificateArn": "arn:aws:acm:us-
east-1:123456789101:certificate/5ab64566-761b-4ad3-b259-example"
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte ModifyVpnTunnelCertificate en la Referencia de comandos de la AWS CLI.

`modify-vpn-tunnel-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-vpn-tunnel-options`.

AWS CLI

Para modificar las opciones de túnel de una conexión de VPN

En el siguiente ejemplo de `modify-vpn-tunnel-options` se actualizan los grupos de Diffie-Hellman permitidos para el túnel y la conexión de VPN especificados.

```
aws ec2 modify-vpn-tunnel-options \
    --vpn-connection-id vpn-12345678901234567 \
    --vpn-tunnel-outside-ip-address 203.0.113.17 \
    --tunnel-options Phase1DHGroupNumbers=[{Value=14},{Value=15},{Value=16},
{Value=17},{Value=18}],Phase2DHGroupNumbers=[{Value=14},{Value=15},{Value=16},
{Value=17},{Value=18}]
```

Salida:

```
{
    "VpnConnection": {
        "CustomerGatewayConfiguration": "...configuration information...",
        "CustomerGatewayId": "cgw-aabbccddee1122334",
        "Category": "VPN",
        "State": "available",
        "Type": "ipsec.1",
        "VpnConnectionId": "vpn-12345678901234567",
        "VpnGatewayId": "vgw-11223344556677889",
        "Options": {
            "StaticRoutesOnly": false,
            "TunnelOptions": [
                {
                    "OutsideIpAddress": "203.0.113.17",
                    "Phase1DHGroupNumbers": [
                        {
                            "Value": 14
                        },
                        {
                            "Value": 15
                        },
                        {
                            "Value": 16
                        },
                        {
                            "Value": 17
                        },
                        {
                            "Value": 18
                        }
                    ],
```

```
                    "Phase2DHGroupNumbers": [
                        {
                            "Value": 14
                        },
                        {
                            "Value": 15
                        },
                        {
                            "Value": 16
                        },
                        {
                            "Value": 17
                        },
                        {
                            "Value": 18
                        }
                    ]
                },
                {
                    "OutsideIpAddress": "203.0.114.19"
                }
            ]
        },
        "VgwTelemetry": [
            {
                "AcceptedRouteCount": 0,
                "LastStatusChange": "2019-09-10T21:56:54.000Z",
                "OutsideIpAddress": "203.0.113.17",
                "Status": "DOWN",
                "StatusMessage": "IPSEC IS DOWN"
            },
            {
                "AcceptedRouteCount": 0,
                "LastStatusChange": "2019-09-10T21:56:43.000Z",
                "OutsideIpAddress": "203.0.114.19",
                "Status": "DOWN",
                "StatusMessage": "IPSEC IS DOWN"
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte ModifyVpnTunnelOptions en la Referencia de comandos de la AWS CLI.

`monitor-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `monitor-instances`.

AWS CLI

Habilitar el monitoreo detallado para una instancia

Este comando de ejemplo habilita el monitoreo detallado de la instancia especificada.

Comando:

```
aws ec2 monitor-instances --instance-ids i-1234567890abcdef0
```

Salida:

```
{
  "InstanceMonitorings": [
      {
          "InstanceId": "i-1234567890abcdef0",
          "Monitoring": {
              "State": "pending"
          }
      }
  ]
}
```

- Para obtener información sobre la API, consulte MonitorInstances en la Referencia de comandos de la AWS CLI.

`move-address-to-vpc`

En el siguiente ejemplo de código, se muestra cómo utilizar `move-address-to-vpc`.

AWS CLI

Para mover una dirección a EC2-VPC

En este ejemplo, se mueve la dirección IP elástica 54.123.4.56 a la plataforma EC2-VPC.

Comando:

```
aws ec2 move-address-to-vpc --public-ip 54.123.4.56
```

Salida:

```
{
  "Status": "MoveInProgress"
}
```

- Para obtener información sobre la API, consulte MoveAddressToVpc en la Referencia de comandos de la AWS CLI.

`move-byoip-cidr-to-ipam`

En el siguiente ejemplo de código, se muestra cómo utilizar `move-byoip-cidr-to-ipam`.

AWS CLI

Para transferir un CIDR de BYOIP a IPAM

En el siguiente ejemplo de `move-byoip-cidr-to-ipam` se transfiere un CIDR de BYOIP a IPAM.

(Linux):

```
aws ec2 move-byoip-cidr-to-ipam \
    --region us-west-2 \
    --ipam-pool-id ipam-pool-0a03d430ca3f5c035 \
    --ipam-pool-owner 111111111111 \
    --cidr 130.137.249.0/24
```

(Windows):

```
aws ec2 move-byoip-cidr-to-ipam ^
    --region us-west-2 ^
    --ipam-pool-id ipam-pool-0a03d430ca3f5c035 ^
    --ipam-pool-owner 111111111111 ^
```

```
    --cidr 130.137.249.0/24
```

Salida:

```
{
    "ByoipCidr": {
        "Cidr": "130.137.249.0/24",
        "State": "pending-transfer"
    }
}
```

Para obtener más información, consulte el Tutorial: Transferir un CIDR IPv4 de BYOIP a IPAM en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte MoveByoipCidrToIpam en la Referencia de comandos de la AWS CLI.

`network-insights-access-scope`

En el siguiente ejemplo de código, se muestra cómo utilizar `network-insights-access-scope`.

AWS CLI

Para crear ámbitos de acceso a la información de red

En el siguiente ejemplo de `create-network-insights-access-scope` se crea un ámbito de acceso a la información de red en su cuenta de AWS.

```
aws ec2 create-network-insights-access-scope \
    --cli-input-json file://access-scope-file.json
```

Contenido de `access-scope-file.json`:

```
{
    {
        "MatchPaths": [
            {
                "Source": {
                    "ResourceStatement": {
                        "Resources": [
                            "vpc-abcd12e3"
```

```
                        ]
                    }
                }
            }
        ],
        "ExcludePaths": [
            {
                "Source": {
                    "ResourceStatement": {
                        "ResourceTypes": [
                            "AWS::EC2::InternetGateway"
                        ]
                    }
                }
            }
        ]
    }
}
```

Salida:

```
{
    "NetworkInsightsAccessScopeAnalysisId": "nisa-123456789111"
    }{
    "NetworkInsightsAccessScope": {
        "NetworkInsightsAccessScopeId": "nis-123456789222",
        "NetworkInsightsAccessScopeArn": "arn:aws:ec2:us-
east-1:123456789222:network-insights-access-scope/nis-123456789222",
        "CreatedDate": "2022-01-25T19:20:28.796000+00:00",
        "UpdatedDate": "2022-01-25T19:20:28.797000+00:00"
    },
    "NetworkInsightsAccessScopeContent": {
        "NetworkInsightsAccessScopeId": "nis-04c0c0fbca737c404",
        "MatchPaths": [
            {
                "Source": {
                    "ResourceStatement": {
                        "Resources": [
                            "vpc-abcd12e3"
                        ]
                    }
                }
            }
```

```
        ],
        "ExcludePaths": [
            {
                "Source": {
                    "ResourceStatement": {
                        "ResourceTypes": [
                            "AWS::EC2::InternetGateway"
                        ]
                    }
                }
            }
        ]
    }
}
```

Para obtener más información, consulte Getting started with Network Access Analyzer using the AWS CLI en la Guía del analizador de acceso a la red.

- Para obtener información sobre la API, consulte NetworkInsightsAccessScope en la Referencia de comandos de la AWS CLI.

`provision-byoip-cidr`

En el siguiente ejemplo de código, se muestra cómo utilizar `provision-byoip-cidr`.

AWS CLI

Para aprovisionar un rango de direcciones

En el siguiente ejemplo de `provision-byoip-cidr` se proporciona un rango de direcciones IP públicas para su uso con AWS.

```
aws ec2 provision-byoip-cidr \
    --cidr 203.0.113.25/24 \
    --cidr-authorization-context Message="$text_message",Signature="$signed_message"
```

Salida:

```
{
    "ByoipCidr": {
        "Cidr": "203.0.113.25/24",
        "State": "pending-provision"
```

```
    }
}
```

Para obtener más información sobre la creación de las cadenas de mensajes en el contexto de autorización, consulte Traiga sus propias direcciones IP (BYOIP) en la Guía del usuario de Amazon EC2.

- Para obtener información sobre de la API, consulte ProvisionByoipCidr en la Referencia de comandos de la AWS CLI.

`provision-ipam-pool-cidr`

En el siguiente ejemplo de código, se muestra cómo utilizar `provision-ipam-pool-cidr`.

AWS CLI

Para aprovisionar un CIDR en un grupo de IPAM

En el siguiente ejemplo de `provision-ipam-pool-cidr` se aprovisiona un CIDR en un grupo de IPAM.

(Linux):

```
aws ec2 provision-ipam-pool-cidr \
    --ipam-pool-id ipam-pool-0533048da7d823723 \
    --cidr 10.0.0.0/24
```

(Windows):

```
aws ec2 provision-ipam-pool-cidr ^
    --ipam-pool-id ipam-pool-0533048da7d823723 ^
    --cidr 10.0.0.0/24
```

Salida:

```
{
    "IpamPoolCidr": {
        "Cidr": "10.0.0.0/24",
        "State": "pending-provision"
    }
```

```
}
```

Para obtener más información, consulte Aprovisionamiento de CIDR en un grupo en la Guía del usuario de Amazon VPC IPAM.

- Para obtener información sobre la API, consulte ProvisionIpamPoolCidr en la Referencia de comandos de la AWS CLI.

`purchase-host-reservation`

En el siguiente ejemplo de código, se muestra cómo utilizar `purchase-host-reservation`.

AWS CLI

Para adquirir una reserva de host dedicado

En este ejemplo, se proporciona una vista previa de los costos de una reserva de host dedicado especificada para el host dedicado especificado en su cuenta.

Comando:

```
aws ec2 purchase-host-reservation --offering-id hro-03f707bf363b6b324 --host-id-
set h-013abcd2a00cbd123
```

Salida:

```
{
  "TotalHourlyPrice": "1.499",
  "Purchase": [
      {
          "HourlyPrice": "1.499",
          "InstanceFamily": "m4",
          "PaymentOption": "NoUpfront",
          "HostIdSet": [
              "h-013abcd2a00cbd123"
          ],
          "HostReservationId": "hr-0d418a3a4ffc669ae",
          "UpfrontPrice": "0.000",
          "Duration": 31536000
      }
  ],
  "TotalUpfrontPrice": "0.000"
```

```
}
```

- Para obtener información sobre de la API, consulte PurchaseHostReservation en la Referencia de comandos de la AWS CLI.

`purchase-reserved-instances-offering`

En el siguiente ejemplo de código, se muestra cómo utilizar `purchase-reserved-instances-offering`.

AWS CLI

Para adquirir una oferta de instancia reservada

En este ejemplo de comando, se ilustra la adquisición de una oferta de instancias reservadas; para ello, se especifican un ID de oferta y la cantidad de instancias.

Comando:

```
aws ec2 purchase-reserved-instances-offering --reserved-instances-offering-
id ec06327e-dd07-46ee-9398-75b5fexample --instance-count 3
```

Salida:

```
{
  "ReservedInstancesId": "af9f760e-6f91-4559-85f7-4980eexample"
}
```

- Para obtener información sobre la API, consulte PurchaseReservedInstancesOffering en la Referencia de comandos de la AWS CLI.

`purchase-scheduled-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `purchase-scheduled-instances`.

AWS CLI

Para adquirir una instancia programada

En este ejemplo, se adquiere una instancia programada.

Comando:

```
aws ec2 purchase-scheduled-instances --purchase-requests file://purchase-request.json
```

Purchase-request.json:

```
[
    {
        "PurchaseToken": "eyJ2IjoiMSIsInMiOjEsImMiOi...",
        "InstanceCount": 1
    }
]
```

Salida:

```
{
  "ScheduledInstanceSet": [
      {
          "AvailabilityZone": "us-west-2b",
          "ScheduledInstanceId": "sci-1234-1234-1234-1234-123456789012",
          "HourlyPrice": "0.095",
          "CreateDate": "2016-01-25T21:43:38.612Z",
          "Recurrence": {
              "OccurrenceDaySet": [
                  1
              ],
              "Interval": 1,
              "Frequency": "Weekly",
              "OccurrenceRelativeToEnd": false,
              "OccurrenceUnit": ""
          },
          "Platform": "Linux/UNIX",
          "TermEndDate": "2017-01-31T09:00:00Z",
          "InstanceCount": 1,
          "SlotDurationInHours": 32,
          "TermStartDate": "2016-01-31T09:00:00Z",
          "NetworkPlatform": "EC2-VPC",
          "TotalScheduledInstanceHours": 1696,
          "NextSlotStartTime": "2016-01-31T09:00:00Z",
          "InstanceType": "c4.large"
      }
```

```
  ]
}
```

- Para obtener información sobre la API, consulte PurchaseScheduledInstances en la Referencia de comandos de la AWS CLI.

`reboot-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `reboot-instances`.

AWS CLI

Reiniciar una instancia de Amazon EC

En este ejemplo, se reinicia la instancia especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 reboot-instances --instance-ids i-1234567890abcdef5
```

Para obtener más información, consulte Reiniciar su instancia en la Guía del usuario de Amazon Elastic Compute Cloud.

- Para obtener información sobre la API, consulte RebootInstances en la Referencia de comandos de la AWS CLI.

`register-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-image`.

AWS CLI

Ejemplo 1: registro de una AMI mediante un archivo de manifiesto

En el siguiente ejemplo de `register-image` se registra una AMI mediante el archivo de manifiesto especificado en Amazon S3.

```
aws ec2 register-image \
    --name my-image \
    --image-location amzn-s3-demo-bucket/myimage/image.manifest.xml
```

Salida:

```
{
    "ImageId": "ami-1234567890EXAMPLE"
}
```

Para obtener más información, consulte Imágenes de máquina de Amazon (AMI) en la Guía del usuario de Amazon EC2.

Ejemplo 2: registro de una AMI mediante una instantánea de un dispositivo raíz

En el siguiente ejemplo de `register-image` se registra una AMI mediante la instantánea especificada de un volumen raíz de EBS como dispositivo `/dev/xvda`. La asignación de dispositivos de bloques también incluye un volumen de EBS vacío de 100 GiB como dispositivo `/dev/xvdf`.

```
aws ec2 register-image \
    --name my-image \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0db2cf683925d191f} DeviceName=/dev/
xvdf,Ebs={VolumeSize=100}
```

Salida:

```
{
    "ImageId": "ami-1a2b3c4d5eEXAMPLE"
}
```

Para obtener más información, consulte Imágenes de máquina de Amazon (AMI) en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte RegisterImage en la Referencia de comandos de la AWS CLI.

`register-instance-event-notification-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-instance-event-notification-attributes`.

AWS CLI

Ejemplo 1: inclusión de todas las etiquetas en las notificaciones de eventos

En el siguiente ejemplo de `register-instance-event-notification-attributes` se incluyen todas las etiquetas en las notificaciones de eventos.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute IncludeAllTagsOfInstance=true
```

Salida:

```
{
    "InstanceTagAttribute": {
        "InstanceTagKeys": [],
        "IncludeAllTagsOfInstance": true
    }
}
```

Para obtener más información, consulte Eventos programados para las instancias en la Guía del usuario de Amazon EC2.

Ejemplo 2: inclusión de etiquetas específicas en las notificaciones de eventos

En el siguiente ejemplo de `register-instance-event-notification-attributes` se incluyen las etiquetas especificadas en las notificaciones de eventos. No se pueden especificar etiquetas si `IncludeAllTagsOfInstance` es `true`.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute InstanceTagKeys="tag-key1","tag-key2"
```

Salida:

```
{
    "InstanceTagAttribute": {
        "InstanceTagKeys": [
            "tag-key1",
            "tag-key2"
        ],
        "IncludeAllTagsOfInstance": false
    }
```

```
}
```

Para obtener más información, consulte Eventos programados para las instancias en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte RegisterInstanceEventNotificationAttributes en la Referencia de comandos de la AWS CLI.

`register-transit-gateway-multicase-group-sources`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-transit-gateway-multicase-group-sources`.

AWS CLI

Para registrar un origen en un grupo de multidifusión de puerta de enlace de tránsito.

En este ejemplo de `register-transit-gateway-multicast-group-sources` se registra el origen del grupo de interfaz de red especificado en un grupo de multidifusión.

```
aws ec2 register-transit-gateway-multicast-group-sources \
    --transit-gateway-multicast-domain-id tgw-mcast-domain-0c4905cef79d6e597 \
    --group-ip-address 224.0.1.0 \
    --network-interface-ids eni-07f290fc3c090cbae
```

Salida:

```
{
    "RegisteredMulticastGroupSources": {
        "TransitGatewayMulticastDomainId": "tgw-mcast-domain-0c4905cef79d6e597",
        "RegisteredNetworkInterfaceIds": [
            "eni-07f290fc3c090cbae"
        ],
        "GroupIpAddress": "224.0.1.0"
    }
}
```

Para obtener más información, consulte Register Sources with a Multicast Group en la Guía del usuario de AWS Transit Gateway.

- Para obtener información sobre la API, consulte RegisterTransitGatewayMulticaseGroupSources en la Referencia de comandos de la AWS CLI.

`register-transit-gateway-multicast-group-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-transit-gateway-multicast-group-members`.

AWS CLI

Para ver la información sobre las asociaciones del dominio de multidifusión de puerta de enlace de tránsito

En el siguiente ejemplo de `register-transit-gateway-multicast-group-members` se devuelven las asociaciones del dominio de multidifusión especificado.

```
aws ec2 register-transit-gateway-multicast-group-members \
    --transit-gateway-multicast-domain-id tgw-mcast-domain-0c4905cef79d6e597 \
    --group-ip-address 224.0.1.0 \
    --network-interface-ids eni-0e246d32695012e81
```

Salida:

```
{
    "RegisteredMulticastGroupMembers": {
        "TransitGatewayMulticastDomainId": "tgw-mcast-domain-0c4905cef79d6e597",
        "RegisteredNetworkInterfaceIds": [
            "eni-0e246d32695012e81"
        ],
        "GroupIpAddress": "224.0.1.0"
    }
}
```

Para obtener más información, consulte Dominios de multidifusión en la Guía del usuario de puertas de enlace de tránsito.

- Para obtener información sobre la API, consulte RegisterTransitGatewayMulticastGroupMembers en la Referencia de comandos de la AWS CLI.

`register-transit-gateway-multicast-group-sources`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-transit-gateway-multicast-group-sources`.

AWS CLI

Para registrar un origen en un grupo de multidifusión de puerta de enlace de tránsito.

En este ejemplo de `register-transit-gateway-multicast-group-sources` se registra el origen del grupo de interfaz de red especificado en un grupo de multidifusión.

```
aws ec2 register-transit-gateway-multicast-group-sources \
    --transit-gateway-multicast-domain-id tgw-mcast-domain-0c4905cef79d6e597 \
    --group-ip-address 224.0.1.0 \
    --network-interface-ids eni-07f290fc3c090cbae
```

Salida:

```
{
    "RegisteredMulticastGroupSources": {
        "TransitGatewayMulticastDomainId": "tgw-mcast-domain-0c4905cef79d6e597",
        "RegisteredNetworkInterfaceIds": [
            "eni-07f290fc3c090cbae"
        ],
        "GroupIpAddress": "224.0.1.0"
    }
}
```

Para obtener más información, consulte Dominios de multidifusión en la Guía de puertas de enlace de tránsito.

- Para obtener información sobre la API, consulte RegisterTransitGatewayMulticastGroupSources en la Referencia de comandos de la AWS CLI.

`reject-transit-gateway-peering-attachment`

En el siguiente ejemplo de código, se muestra cómo utilizar `reject-transit-gateway-peering-attachment`.

AWS CLI

Para rechazar una conexión de emparejamiento de puerta de enlace de tránsito

En el siguiente ejemplo de `reject-transit-gateway-peering-attachment` se rechaza la conexión de emparejamiento de puerta de enlace de tránsito especificada. El parámetro `--region` especifica la región en la que se encuentra la puerta de enlace de tránsito aceptadora.

```
aws ec2 reject-transit-gateway-peering-attachment \
    --transit-gateway-attachment-id tgw-attach-4455667788aabbccd \
    --region us-east-2
```

Salida:

```
{
    "TransitGatewayPeeringAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-4455667788aabbccd",
        "RequesterTgwInfo": {
            "TransitGatewayId": "tgw-123abc05e04123abc",
            "OwnerId": "123456789012",
            "Region": "us-west-2"
        },
        "AccepterTgwInfo": {
            "TransitGatewayId": "tgw-11223344aabbcc112",
            "OwnerId": "123456789012",
            "Region": "us-east-2"
        },
        "State": "rejecting",
        "CreationTime": "2019-12-09T11:50:31.000Z"
    }
}
```

Para obtener más información, consulte Transit Gateway Peering Attachments en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte RejectTransitGatewayPeeringAttachment en la Referencia de comandos de la AWS CLI.

`reject-transit-gateway-vpc-attachment`

En el siguiente ejemplo de código, se muestra cómo utilizar `reject-transit-gateway-vpc-attachment`.

AWS CLI

Para rechazar una conexión de VPC de puerta de enlace de tránsito

En el siguiente ejemplo de `reject-transit-gateway-vpc-attachment` se rechaza la conexión de VPC de puerta de enlace de tránsito especificada.

```
aws ec2 reject-transit-gateway-vpc-attachment \
    --transit-gateway-attachment-id tgw-attach-0a34fe6b4fEXAMPLE
```

Salida:

```
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-0a34fe6b4fEXAMPLE",
        "TransitGatewayId": "tgw-0262a0e521EXAMPLE",
        "VpcId": "vpc-07e8ffd50fEXAMPLE",
        "VpcOwnerId": "111122223333",
        "State": "pending",
        "SubnetIds": [
            "subnet-0752213d59EXAMPLE"
        ],
        "CreationTime": "2019-07-10T17:33:46.000Z",
        "Options": {
            "DnsSupport": "enable",
            "Ipv6Support": "disable"
        }
    }
}
```

Para obtener más información, consulte Transit gateway attachments to a VPC en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte RejectTransitGatewayVpcAttachment en la Referencia de comandos de la AWS CLI.

`reject-transit-gateway-vpc-attachments`

En el siguiente ejemplo de código, se muestra cómo utilizar `reject-transit-gateway-vpc-attachments`.

AWS CLI

Para rechazar una conexión de VPC de puerta de enlace de tránsito

En el siguiente ejemplo de `reject-transit-gateway-vpc-attachment` se rechaza la conexión de VPC de puerta de enlace de tránsito especificada.

```
aws ec2 reject-transit-gateway-vpc-attachment \
```

```
    --transit-gateway-attachment-id tgw-attach-0a34fe6b4fEXAMPLE
```

Salida:

```
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-0a34fe6b4fEXAMPLE",
        "TransitGatewayId": "tgw-0262a0e521EXAMPLE",
        "VpcId": "vpc-07e8ffd50fEXAMPLE",
        "VpcOwnerId": "111122223333",
        "State": "pending",
        "SubnetIds": [
            "subnet-0752213d59EXAMPLE"
        ],
        "CreationTime": "2019-07-10T17:33:46.000Z",
        "Options": {
            "DnsSupport": "enable",
            "Ipv6Support": "disable"
        }
    }
}
```

Para obtener más información, consulte Transit gateway attachments to a VPC en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte RejectTransitGatewayVpcAttachments en la Referencia de comandos de la AWS CLI.

`reject-vpc-endpoint-connections`

En el siguiente ejemplo de código, se muestra cómo utilizar `reject-vpc-endpoint-connections`.

AWS CLI

Para rechazar una solicitud de conexión de punto de conexión de interfaz

En este ejemplo, se rechaza la solicitud de conexión de punto de conexión especificada para el servicio de punto de conexión especificado.

Comando:

```
aws ec2 reject-vpc-endpoint-connections --service-id vpce-svc-03d5ebb7d9579a2b3 --
vpc-endpoint-ids vpce-0c1308d7312217abc
```

Salida:

```
{
  "Unsuccessful": []
}
```

- Para obtener información sobre la API, consulte RejectVpcEndpointConnections en la Referencia de comandos de la AWS CLI.

`reject-vpc-peering-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `reject-vpc-peering-connection`.

AWS CLI

Para rechazar una conexión de emparejamiento de VPC

En este ejemplo, se rechaza la solicitud de conexión de emparejamiento de VPC especificada.

Comando:

```
aws ec2 reject-vpc-peering-connection --vpc-peering-connection-id pcx-1a2b3c4d
```

Salida:

```
{
    "Return": true
}
```

- Para obtener información sobre la API, consulte RejectVpcPeeringConnection en la Referencia de comandos de la AWS CLI.

`release-address`

En el siguiente ejemplo de código, se muestra cómo utilizar `release-address`.

AWS CLI

Liberar direcciones IP elásticas para EC2-Classic

En este ejemplo, se libera una dirección IP elástica para su uso con instancias en EC2-Classic. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 release-address --public-ip 198.51.100.0
```

Liberar una dirección IP elástica para EC2-VPC

En este ejemplo, se libera una dirección IP elástica para su uso con instancias en una VPC. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 release-address --allocation-id eipalloc-64d5890a
```

- Para obtener información sobre la API, consulte ReleaseAddress en la Referencia de comandos de la AWS CLI.

`release-hosts`

En el siguiente ejemplo de código, se muestra cómo utilizar `release-hosts`.

AWS CLI

Para liberar un host dedicado de su cuenta

Para liberar un host dedicado de su cuenta. Las instancias que se encuentran en el host deben detenerse o terminarse antes para poder liberar el host.

Comando:

```
aws ec2 release-hosts --host-id=h-0029d6e3cacf1b3da
```

Salida:

```
{
```

```
    "Successful":  [
        "h-0029d6e3cacf1b3da"
         ],
  "Unsuccessful": []

}
```

- Para obtener información sobre la API, consulte ReleaseHosts en la Referencia de comandos de la AWS CLI.

`release-ipam-pool-allocation`

En el siguiente ejemplo de código, se muestra cómo utilizar `release-ipam-pool-allocation`.

AWS CLI

Para liberar una asignación de grupo de IPAM

En este ejemplo, usted es un administrador delegado de IPAM. Ha intentado eliminar un grupo de IPAM, pero ha recibido un error que indica que no puede eliminarlo mientras el grupo tenga asignaciones. Está utilizando este comando para liberar una asignación de grupo.

Tenga en cuenta lo siguiente:

Solo puede usar este comando para asignaciones personalizadas. Para eliminar una asignación de un recurso sin eliminar el recurso, defina su estado de supervisión en false mediante modify-ipam-resource-cidr. Para completar esta solicitud, necesitará el ID del grupo de IPAM, que puede obtener mediante describe-ipam-pools. También necesitará el ID de asignación, que puede obtener mediante get-ipam-pool-allocations. Si no desea eliminar las asignaciones una por una, puede utilizar `--cascade option` al eliminar un grupo de IPAM para liberar automáticamente todas las asignaciones del grupo antes de eliminarlo. Hay varios requisitos previos que debe cumplir antes de ejecutar este comando. Para obtener más información, consulte Liberar una asignación en la Guía del usuario de Amazon VPC IPAM. La región `--region` en la que se ejecuta este comando debe ser la configuración regional del grupo de IPAM donde se encuentra la asignación.

En el siguiente ejemplo de `release-ipam-pool-allocation` se libera una asignación de un grupo de IPAM.

```
aws ec2 release-ipam-pool-allocation \
```

```
    --ipam-pool-id ipam-pool-07bdd12d7c94e4693 \
    --cidr 10.0.0.0/23 \
    --ipam-pool-allocation-id ipam-pool-alloc-0e66a1f730da54791b99465b79e7d1e89 \
    --region us-west-1
```

Salida:

```
{
    "Success": true
}
```

Una vez liberada la asignación, puede ser conveniente ejecutar delete-ipam-pool.

- Para obtener información sobre la API, consulte ReleaseIpamPoolAllocation en la Referencia de comandos de la AWS CLI.

`replace-iam-instance-profile-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `replace-iam-instance-profile-association`.

AWS CLI

Reemplazar un perfil de instancia de IAM para una instancia

En este ejemplo, se reemplaza el perfil de instancia de IAM, representado por la asociación `iip-assoc-060bae234aac2e7fa`, con el perfil de instancia de IAM denominado `AdminRole`.

```
aws ec2 replace-iam-instance-profile-association \
    --iam-instance-profile Name=AdminRole \
    --association-id iip-assoc-060bae234aac2e7fa
```

Salida:

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-087711ddaf98f9489",
        "State": "associating",
        "AssociationId": "iip-assoc-0b215292fab192820",
        "IamInstanceProfile": {
            "Id": "AIPAJLNLDX3AMYZNWYYAY",
```

```
            "Arn": "arn:aws:iam::123456789012:instance-profile/AdminRole"
        }
    }
}
```

- Para obtener información sobre la API, consulte ReplaceIamInstanceProfileAssociation en la Referencia de comandos de la AWS CLI.

`replace-network-acl-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `replace-network-acl-association`.

AWS CLI

Para sustituir la ACL de red asociada a una subred

En este ejemplo, se asocia la ACL de red especificada a la subred para la asociación de ACL de red especificada.

Comando:

```
aws ec2 replace-network-acl-association --association-id aclassoc-e5b95c8c --
network-acl-id acl-5fb85d36
```

Salida:

```
{
    "NewAssociationId": "aclassoc-3999875b"
}
```

- Para obtener información sobre la API, consulte ReplaceNetworkAclAssociation en la Referencia de comandos de la AWS CLI.

`replace-network-acl-entry`

En el siguiente ejemplo de código, se muestra cómo utilizar `replace-network-acl-entry`.

AWS CLI

Para sustituir una entrada de ACL de red

En este ejemplo, se sustituye una entrada para la ACL de red especificada. La nueva regla 100 permite la entrada de tráfico desde 203.0.113.12/24 en el puerto 53 de UDP (DNS) a cualquier subred asociada.

Comando:

```
aws ec2 replace-network-acl-entry --network-acl-id acl-5fb85d36 --ingress --rule-number 100 --protocol udp --port-range From=53,To=53 --cidr-block 203.0.113.12/24 --rule-action allow
```

- Para obtener información sobre la API, consulte ReplaceNetworkAclEntry en la Referencia de comandos de la AWS CLI.

`replace-route-table-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `replace-route-table-association`.

AWS CLI

Para sustituir la tabla de enrutamiento asociada a la subred

En este ejemplo, se asocia la tabla de enrutamiento especificada a la subred especificada.

Comando:

```
aws ec2 replace-route-table-association --association-id rtbassoc-781d0d1a --route-table-id rtb-22574640
```

Salida:

```
{
    "NewAssociationId": "rtbassoc-3a1f0f58"
}
```

- Para obtener información sobre la API, consulte ReplaceRouteTableAssociation en la Referencia de comandos de la AWS CLI.

`replace-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `replace-route`.

AWS CLI

Para reemplazar una ruta

En este ejemplo, se reemplaza la ruta especificada de la tabla de enrutamiento especificada. La nueva ruta coincide con el CIDR especificado y envía el tráfico a la puerta de enlace privada virtual especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 replace-route --route-table-id rtb-22574640 --destination-cidr-
block 10.0.0.0/16 --gateway-id vgw-9a4cacf3
```

- Para obtener información sobre la API, consulte ReplaceRoute en la Referencia de comandos de la AWS CLI.

`replace-transit-gateway-route`

En el siguiente ejemplo de código, se muestra cómo utilizar `replace-transit-gateway-route`.

AWS CLI

Para reemplazar la ruta especificada en la tabla de enrutamiento de puerta de enlace de tránsito especificada

En el siguiente ejemplo de `replace-transit-gateway-route` se reemplaza la ruta en la tabla de enrutamiento de puerta de enlace de tránsito especificada.

```
aws ec2 replace-transit-gateway-route \
    --destination-cidr-block 10.0.2.0/24 \
    --transit-gateway-attachment-id tgw-attach-09b52ccdb5EXAMPLE \
    --transit-gateway-route-table-id tgw-rtb-0a823edbdeEXAMPLE
```

Salida:

```
{
    "Route": {
        "DestinationCidrBlock": "10.0.2.0/24",
        "TransitGatewayAttachments": [
            {
```

```
                "ResourceId": "vpc-4EXAMPLE",
                "TransitGatewayAttachmentId": "tgw-attach-09b52ccdb5EXAMPLE",
                "ResourceType": "vpc"
            }
        ],
        "Type": "static",
        "State": "active"
    }
}
```

Para obtener más información, consulte Transit gateway route tables en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte ReplaceTransitGatewayRoute en la Referencia de comandos de la AWS CLI.

`report-instance-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `report-instance-status`.

AWS CLI

Para informar sobre el estado de una instancia

En este ejemplo de comando, se informa sobre el estado de la instancia especificada.

Comando:

```
aws ec2 report-instance-status --instances i-1234567890abcdef0 --status impaired --
reason-codes unresponsive
```

- Para obtener información sobre la API, consulte ReportInstanceStatus en la Referencia de comandos de la AWS CLI.

`request-spot-fleet`

En el siguiente ejemplo de código, se muestra cómo utilizar `request-spot-fleet`.

AWS CLI

Para solicitar una flota de spot en la subred con el precio más bajo

En este ejemplo de comando, se crea una solicitud de flota de spot con dos especificaciones de lanzamiento que solo se diferencian en la subred. La flota de spot lanza las instancias en la subred especificada con el precio más bajo. Si las instancias se lanzan en una VPC predeterminada, reciben una dirección IP pública de forma predeterminada. Si las instancias se lanzan en una VPC no predeterminada, no reciben una dirección IP pública de forma predeterminada.

Tenga en cuenta que no puede especificar diferentes subredes de la misma zona de disponibilidad en una solicitud de flota de spot.

Comando:

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Config.json:

```
{
  "SpotPrice": "0.04",
  "TargetCapacity": 2,
  "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "SubnetId": "subnet-1a2b3c4d, subnet-3c4d5e6f",
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Salida:

```
{
  "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
```

```
}
```

Para solicitar una flota de spot en la zona de disponibilidad con el precio más bajo

En este ejemplo de comando, se crea una solicitud de flota de spot con dos especificaciones de lanzamiento que solo se diferencian en la zona de disponibilidad. La flota de spot lanza las instancias en la zona de disponibilidad especificada con el precio más bajo. Si su cuenta admite EC2-VPC únicamente, Amazon EC2 lanza las instancias de spot en la subred predeterminada de la zona de disponibilidad. Si su cuenta admite EC2-Classic, Amazon EC2 lanza las instancias en EC2-Classic en la zona de disponibilidad.

Comando:

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Config.json:

```
{
  "SpotPrice": "0.04",
  "TargetCapacity": 2,
  "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "Placement": {
              "AvailabilityZone": "us-west-2a, us-west-2b"
          },
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Para lanzar instancias de spot en una subred y asignarles direcciones IP públicas

En este ejemplo de comando, se asignan direcciones públicas a instancias lanzadas en una VPC no predeterminada. Tenga en cuenta que, si especifica una interfaz de red, debe incluir el ID de subred y el ID de grupo de seguridad mediante la interfaz de red.

Comando:

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Config.json:

```
{
  "SpotPrice": "0.04",
  "TargetCapacity": 2,
  "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "InstanceType": "m3.medium",
          "NetworkInterfaces": [
              {
                  "DeviceIndex": 0,
                  "SubnetId": "subnet-1a2b3c4d",
                  "Groups": [ "sg-1a2b3c4d" ],
                  "AssociatePublicIpAddress": true
              }
          ],
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::880185128111:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Para solicitar una flota de spot con la estrategia de asignación diversificada

En este ejemplo de comando, se crea una solicitud de flota de spot que lanza 30 instancias mediante la estrategia de asignación diversificada. Las especificaciones de lanzamiento varían según el tipo de instancia. La flota de spot distribuye las instancias entre las especificaciones de inicialización, de tal forma que haya 10 instancias de cada tipo.

Comando:

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Config.json:

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/my-spot-fleet-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      }
  ]
}
```

Para obtener más información, consulte las solicitudes de flota de spot en la Guía del usuario de Amazon Elastic Compute Cloud.

- Para obtener información sobre la API, consulte RequestSpotFleet en la Referencia de comandos de la AWS CLI.

`request-spot-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `request-spot-instances`.

AWS CLI

Para solicitar instancias de spot

En este ejemplo de comando, se crea una solicitud de instancia de spot única para cinco instancias en la zona de disponibilidad especificada. Si su cuenta admite EC2-VPC únicamente, Amazon EC2 lanza las instancias en la subred predeterminada de la zona de disponibilidad especificada. Si su cuenta admite EC2-Classic, Amazon EC2 lanza las instancias en EC2-Classic en la zona de disponibilidad.

Comando:

```
aws ec2 request-spot-instances --spot-price "0.03" --instance-count 5 --type "one-time" --launch-specification file://specification.json
```

Specification.json:

```
{
  "ImageId": "ami-1a2b3c4d",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d" ],
  "InstanceType": "m3.medium",
  "Placement": {
    "AvailabilityZone": "us-west-2a"
  },
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Salida:

```
{
  "SpotInstanceRequests": [
      {
          "Status": {
              "UpdateTime": "2014-03-25T20:54:21.000Z",
              "Code": "pending-evaluation",
              "Message": "Your Spot request has been submitted for review, and is
 pending evaluation."
          },
          "ProductDescription": "Linux/UNIX",
          "SpotInstanceRequestId": "sir-df6f405d",
          "State": "open",
          "LaunchSpecification": {
              "Placement": {
```

```
                "AvailabilityZone": "us-west-2a"
            },
            "ImageId": "ami-1a2b3c4d",
            "KeyName": "my-key-pair",
            "SecurityGroups": [
                {
                    "GroupName": "my-security-group",
                    "GroupId": "sg-1a2b3c4d"
                }
            ],
            "Monitoring": {
                "Enabled": false
            },
            "IamInstanceProfile": {
                "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
            },
            "InstanceType": "m3.medium"
        },
        "Type": "one-time",
        "CreateTime": "2014-03-25T20:54:20.000Z",
        "SpotPrice": "0.050000"
    },
    ...
  ]
}
```

En este ejemplo de comando, se crea una solicitud de instancia de spot única para cinco instancias en la subred especificada. Amazon EC2 inicia las instancias en la subred especificada. Si la VPC es una VPC no predeterminada, las instancias no reciben una dirección IP pública de forma predeterminada.

Comando:

```
aws ec2 request-spot-instances --spot-price "0.050" --instance-count 5 --type "one-time" --launch-specification file://specification.json
```

Specification.json:

```
{
  "ImageId": "ami-1a2b3c4d",
  "SecurityGroupIds": [ "sg-1a2b3c4d" ],
  "InstanceType": "m3.medium",
```

```
  "SubnetId": "subnet-1a2b3c4d",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Salida:

```
{
  "SpotInstanceRequests": [
      {
          "Status": {
             "UpdateTime": "2014-03-25T22:21:58.000Z",
             "Code": "pending-evaluation",
             "Message": "Your Spot request has been submitted for review, and is
 pending evaluation."
          },
          "ProductDescription": "Linux/UNIX",
          "SpotInstanceRequestId": "sir-df6f405d",
          "State": "open",
          "LaunchSpecification": {
             "Placement": {
                 "AvailabilityZone": "us-west-2a"
             }
             "ImageId": "ami-1a2b3c4d"
             "SecurityGroups": [
                 {
                     "GroupName": "my-security-group",
                     "GroupID": "sg-1a2b3c4d"
                 }
             ]
             "SubnetId": "subnet-1a2b3c4d",
             "Monitoring": {
                 "Enabled": false
             },
             "IamInstanceProfile": {
                 "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
             },
             "InstanceType": "m3.medium",
         },
         "Type": "one-time",
         "CreateTime": "2014-03-25T22:21:58.000Z",
         "SpotPrice": "0.050000"
```

```
      },
      ...
  ]
}
```

En este ejemplo de comando, se asigna una dirección IP pública a instancias de spot que se lanzan en una VPC no predeterminada. Tenga en cuenta que, si especifica una interfaz de red, debe incluir el ID de subred y el ID de grupo de seguridad mediante la interfaz de red.

Comando:

```
aws ec2 request-spot-instances --spot-price "0.050" --instance-count 1 --type "one-time" --launch-specification file://specification.json
```

Specification.json:

```
{
  "ImageId": "ami-1a2b3c4d",
  "KeyName": "my-key-pair",
  "InstanceType": "m3.medium",
  "NetworkInterfaces": [
    {
      "DeviceIndex": 0,
      "SubnetId": "subnet-1a2b3c4d",
      "Groups": [ "sg-1a2b3c4d" ],
      "AssociatePublicIpAddress": true
    }
  ],
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

- Para obtener información sobre la API, consulte RequestSpotInstances en la Referencia de comandos de la AWS CLI.

`reset-address-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-address-attribute`.

AWS CLI

Para restablecer el atributo de nombre de dominio asociado a una dirección IP elástica

En los siguientes ejemplos de `reset-address-attribute` se restablece el atributo de nombre de dominio de una dirección IP elástica.

Linux:

```
aws ec2 reset-address-attribute \
    --allocation-id eipalloc-abcdef01234567890 \
    --attribute domain-name
```

Windows:

```
aws ec2 reset-address-attribute ^
    --allocation-id eipalloc-abcdef01234567890 ^
    --attribute domain-name
```

Salida:

```
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.com."
            "PtrRecordUpdate": {
                "Value": "example.net.",
                "Status": "PENDING"
        }
    ]
}
```

Para supervisar el cambio pendiente describe-addresses-attribute en la Referencia de comandos de la AWS CLI.

- Para obtener información sobre la API, consulte ResetAddressAttribute en la Referencia de comandos de la AWS CLI.

`reset-ebs-default-kms-key-id`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-ebs-default-kms-key-id`.

AWS CLI

Para restablecer la CMK predeterminada para el cifrado de EBS

En el siguiente ejemplo de `reset-ebs-default-kms-key-id` se restablece la CMK predeterminada para el cifrado de EBS en su cuenta de AWS en la región actual.

```
aws ec2 reset-ebs-default-kms-key-id
```

Salida:

```
{
   "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/8c5b2c63-b9bc-45a3-
a87a-5513eEXAMPLE"
}
```

- Para obtener información sobre la API, consulte ResetEbsDefaultKmsKeyId en la Referencia de comandos de la AWS CLI.

`reset-fpga-image-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-fpga-image-attribute`.

AWS CLI

Para restablecer los atributos de una imagen de Amazon FPGA

En este ejemplo, se restablecen los permisos de carga de la AFI especificada.

Comando:

```
aws ec2 reset-fpga-image-attribute --fpga-image-id afi-0d123e123bfc85abc --
attribute loadPermission
```

Salida:

```
{
  "Return": true
```

```
}
```

- Para obtener información sobre la API, consulte ResetFpgaImageAttribute en la Referencia de comandos de la AWS CLI.

`reset-image-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-image-attribute`.

AWS CLI

Para restablecer el atributo launchPermission

En este ejemplo, se restablece el atributo `launchPermission` de la AMI especificada en su valor predeterminado. De forma predeterminada, las AMI son privadas. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 reset-image-attribute --image-id ami-5731123e --attribute launchPermission
```

- Para obtener información sobre la API, consulte ResetImageAttribute en la Referencia de comandos de la AWS CLI.

`reset-instance-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-instance-attribute`.

AWS CLI

Para restablecer el atributo sourceDestCheck

En este ejemplo, se restablece el atributo `sourceDestCheck` de la instancia especificada. La instancia debe encontrarse en una VPC. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 reset-instance-attribute --instance-id i-1234567890abcdef0 --
attribute sourceDestCheck
```

Para restablecer el atributo kernel

En este ejemplo, se restablece el atributo `kernel` de la instancia especificada. La instancia debe tener el estado `stopped`. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 reset-instance-attribute --instance-id i-1234567890abcdef0 --
attribute kernel
```

Para restablecer el atributo ramdisk

En este ejemplo, se restablece el atributo `ramdisk` de la instancia especificada. La instancia debe tener el estado `stopped`. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 reset-instance-attribute --instance-id i-1234567890abcdef0 --
attribute ramdisk
```

- Para obtener información sobre la API, consulte ResetInstanceAttribute en la Referencia de comandos de la AWS CLI.

`reset-network-interface-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-network-interface-attribute`.

AWS CLI

Para restablecer un atributo de interfaz de red

En el siguiente ejemplo de `reset-network-interface-attribute` se restablece en `true` el valor del atributo de comprobación de origen/destino.

```
aws ec2 reset-network-interface-attribute \
    --network-interface-id eni-686ea200 \
    --source-dest-check
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte ResetNetworkInterfaceAttribute en la Referencia de comandos de la AWS CLI.

`reset-snapshot-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-snapshot-attribute`.

AWS CLI

Para restablecer un atributo de instantánea

En este ejemplo, se restablecen los permisos de creación de volúmenes para la instantánea `snap-1234567890abcdef0`. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 reset-snapshot-attribute --snapshot-id snap-1234567890abcdef0 --
attribute createVolumePermission
```

- Para obtener información sobre la API, consulte ResetSnapshotAttribute en la Referencia de comandos de la AWS CLI.

`restore-address-to-classic`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-address-to-classic`.

AWS CLI

Para restaurar una dirección en EC2-Classic

En este ejemplo, se restaura la dirección IP elástica 198.51.100.0 a la plataforma EC2-Classic.

Comando:

```
aws ec2 restore-address-to-classic --public-ip 198.51.100.0
```

Salida:

```
{
```

```
  "Status": "MoveInProgress",
  "PublicIp": "198.51.100.0"
}
```

- Para obtener información sobre la API, consulte RestoreAddressToClassic en la Referencia de comandos de la AWS CLI.

`restore-image-from-recycle-bin`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-image-from-recycle-bin`.

AWS CLI

Para restaurar una imagen desde la papelera de reciclaje

En el siguiente ejemplo de `restore-image-from-recycle-bin` se restaura la AMI ami-0111222333444abcd desde la papelera de reciclaje.

```
aws ec2 restore-image-from-recycle-bin \
    --image-id ami-0111222333444abcd
```

Salida:

```
{
    "Return": true
}
```

Para obtener más información, consulte Recuperar AMI eliminadas de la papelera de reciclaje en la Guía del usuario de Amazon EBS.

- Para obtener información sobre la API, consulte RestoreImageFromRecycleBin en la Referencia de comandos de la AWS CLI.

`restore-managed-prefix-list-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-managed-prefix-list-version`.

AWS CLI

us-west-2**To restore a prefix list version**

En el siguiente ejemplo de `restore-managed-prefix-list-version`, se restauran las entradas de la versión 1 de la lista de prefijos especificada.

```
aws ec2 restore-managed-prefix-list-version \
    --prefix-list-id pl-0123456abcabcabc1 \
    --current-version 2 \
    --previous-version 1
```

Salida:

```
{
    "PrefixList": {
        "PrefixListId": "pl-0123456abcabcabc1",
        "AddressFamily": "IPv4",
        "State": "restore-in-progress",
        "PrefixListArn": "arn:aws:ec2:us-west-2:123456789012:prefix-list/
pl-0123456abcabcabc1",
        "PrefixListName": "vpc-cidrs",
        "MaxEntries": 10,
        "Version": 2,
        "OwnerId": "123456789012"
    }
}
```

Para obtener más información, consulte Managed prefix lists en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte RestoreManagedPrefixListVersion en la Referencia de comandos de la AWS CLI.

`restore-snapshot-from-recycle-bin`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-snapshot-from-recycle-bin`.

AWS CLI

Para restaurar instantáneas desde la papelera de reciclaje

En el siguiente ejemplo de `restore-snapshot-from-recycle-bin` se restaura una instantánea desde la papelera de reciclaje. Cuando restaura una instantánea desde la papelera de reciclaje, la instantánea está disponible inmediatamente para su uso y se quita de la papelera

de reciclaje. Puede utilizar una instantánea restaurada de la misma manera en que utiliza cualquier otra instantánea de la cuenta.

```
aws ec2 restore-snapshot-from-recycle-bin \
    --snapshot-id snap-01234567890abcdef
```

Este comando no genera ninguna salida.

Para obtener más información sobre la papelera de reciclaje, consulte Recuperar instantáneas eliminadas de la papelera de reciclaje en la Guía del usuario de Amazon EBS.

- Para obtener información sobre la API, consulte RestoreSnapshotFromRecycleBin en la Referencia de comandos de la AWS CLI.

`restore-snapshot-tier`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-snapshot-tier`.

AWS CLI

Ejemplo 1: restauración permanente de una instantánea archivada

En el siguiente ejemplo de `restore-snapshot-tier` se restaura la instantánea especificada de forma permanente. Especifique el valor de `--snapshot-id` e incluya la opción `permanent-restore`.

```
aws ec2 restore-snapshot-tier \
    --snapshot-id snap-01234567890abcedf \
    --permanent-restore
```

Salida:

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "IsPermanentRestore": true
}
```

Para obtener más información sobre el archivado de instantáneas, consulte Archivo de instantáneas de Amazon EBS en la Guía del usuario de Amazon EBS.

Ejemplo 2: restauración temporal de una instantánea archivada

En el siguiente ejemplo de `restore-snapshot-tier` se restaura la instantánea especificada de forma temporal. Omita la opción `--permanent-restore`. Especifique el valor de `--snapshot-id` y, en `temporary-restore-days`, especifique la cantidad de días durante los que desea restaurar la instantánea. `temporary-restore-days` debe especificarse en días. El rango permitido es de 1 a 180. Si no especifica ningún valor, el valor predeterminado es 1 día.

```
aws ec2 restore-snapshot-tier \
    --snapshot-id snap-01234567890abcedf \
    --temporary-restore-days 5
```

Salida:

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "RestoreDuration": 5,
    "IsPermanentRestore": false
}
```

Para obtener más información sobre el archivado de instantáneas, consulte Archivo de instantáneas de Amazon EBS en la Guía del usuario de Amazon EBS.

Ejemplo 3: modificación del período de restauración

En el siguiente ejemplo de `restore-snapshot-tier` se cambia el período de restauración de la instantánea especificada a 10 días.

```
aws ec2 restore-snapshot-tier \
    --snapshot-id snap-01234567890abcedf
    --temporary-restore-days 10
```

Salida:

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "RestoreDuration": 10,
    "IsPermanentRestore": false
}
```

Para obtener más información sobre el archivado de instantáneas, consulte Archivo de instantáneas de Amazon EBS en la Guía del usuario de Amazon EBS.

Ejemplo 4: modificación del tipo de restauración

En el siguiente ejemplo de `restore-snapshot-tier` se cambia el tipo de restauración de la instantánea especificada de temporal a permanente.

```
aws ec2 restore-snapshot-tier \
    --snapshot-id snap-01234567890abcedf
    --permanent-restore
```

Salida:

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "IsPermanentRestore": true
}
```

Para obtener más información sobre el archivado de instantáneas, consulte Archivo de instantáneas de Amazon EBS en la Guía del usuario de Amazon EBS.

- Para obtener información sobre la API, consulte RestoreSnapshotTier en la Referencia de comandos de la AWS CLI.

`revoke-client-vpn-ingress`

En el siguiente ejemplo de código, se muestra cómo utilizar `revoke-client-vpn-ingress`.

AWS CLI

Para revocar una regla de autorización de un punto de conexión de Client VPN

En el siguiente ejemplo de `revoke-client-vpn-ingress` se revoca una regla de acceso a Internet (`0.0.0.0/0`) para todos los grupos.

```
aws ec2 revoke-client-vpn-ingress \
    --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde \
    --target-network-cidr 0.0.0.0/0 --revoke-all-groups
```

Salida:

```
{
    "Status": {
        "Code": "revoking"
```

```
    }
}
```

Para obtener más información, consulte Authorization Rules en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte RevokeClientVpnIngress en la Referencia de comandos de la AWS CLI.

`revoke-security-group-egress`

En el siguiente ejemplo de código, se muestra cómo utilizar `revoke-security-group-egress`.

AWS CLI

Ejemplo 1: eliminación de la regla que permite el tráfico saliente a un rango de direcciones específico

En el siguiente ejemplo del comando `revoke-security-group-egress` se elimina la regla que otorga acceso en el puerto TCP 80 a los rangos de direcciones especificados.

```
aws ec2 revoke-security-group-egress \
    --group-id sg-026c12253ce15eff7 \
    --ip-
permissions [{IpProtocol=tcp,FromPort=80,ToPort=80,IpRanges=[{CidrIp=10.0.0.0/16}]
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Grupos de seguridad en la Guía del usuario de Amazon EC2.

Ejemplo 2: eliminación de la regla que permite el tráfico saliente a un grupo de seguridad específico

En el siguiente ejemplo del comando `revoke-security-group-egress` se elimina la regla que otorga acceso en el puerto TCP 80 al grupo de seguridad especificado.

```
aws ec2 revoke-security-group-egress \
    --group-id sg-026c12253ce15eff7 \
    --ip-permissions '[{"IpProtocol": "tcp", "FromPort": 443, "ToPort":
 443,"UserIdGroupPairs": [{"GroupId": "sg-06df23a01ff2df86d"}]}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Grupos de seguridad en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte RevokeSecurityGroupEgress en la Referencia de comandos de la AWS CLI.

`revoke-security-group-ingress`

En el siguiente ejemplo de código, se muestra cómo utilizar `revoke-security-group-ingress`.

AWS CLI

Ejemplo 1: eliminación de una regla de un grupo de seguridad

En el siguiente ejemplo de `revoke-security-group-ingress` se elimina el acceso al puerto TCP 22 al rango de direcciones `203.0.113.0/24` del grupo de seguridad especificado para una VPC predeterminada.

```
aws ec2 revoke-security-group-ingress \
    --group-name mySecurityGroup
    --protocol tcp \
    --port 22 \
    --cidr 203.0.113.0/24
```

Este comando no genera ninguna salida si se ejecuta correctamente.

Para obtener más información, consulte Grupos de seguridad en la Guía del usuario de Amazon EC2.

Ejemplo 2: eliminación de una regla mediante el conjunto de permisos de IP

En el siguiente ejemplo de `revoke-security-group-ingress` se usa el parámetro `ip-permissions` para eliminar una regla de entrada que permite enviar el mensaje ICMP `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (tipo 3, código 4).

```
aws ec2 revoke-security-group-ingress \
    --group-id sg-026c12253ce15eff7 \
    --ip-
permissions IpProtocol=icmp,FromPort=3,ToPort=4,IpRanges=[{CidrIp=0.0.0.0/0}]
```

Este comando no genera ninguna salida si se ejecuta correctamente.

Para obtener más información, consulte Grupos de seguridad en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte RevokeSecurityGroupIngress en la Referencia de comandos de la AWS CLI.

`run-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `run-instances`.

AWS CLI

Ejemplo 1: Lanzar una instancia en una subred predeterminada

En el siguiente ejemplo de `run-instances`, se lanza una única instancia de tipo `t2.micro` en la subred predeterminada de la región actual y se la asocia a la subred predeterminada de la VPC predeterminada de la región. El par de claves es opcional si no tiene pensado conectarse a la instancia mediante SSH (Linux) o RDP (Windows).

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --key-name MyKeyPair
```

Salida:

```
{
    "Instances": [
        {
            "AmiLaunchIndex": 0,
            "ImageId": "ami-0abcdef1234567890",
            "InstanceId": "i-1231231230abcdef0",
            "InstanceType": "t2.micro",
            "KeyName": "MyKeyPair",
            "LaunchTime": "2018-05-10T08:05:20.000Z",
            "Monitoring": {
                "State": "disabled"
            },
            "Placement": {
                "AvailabilityZone": "us-east-2a",
```

```
            "GroupName": "",
            "Tenancy": "default"
        },
        "PrivateDnsName": "ip-10-0-0-157.us-east-2.compute.internal",
        "PrivateIpAddress": "10.0.0.157",
        "ProductCodes": [],
        "PublicDnsName": "",
        "State": {
            "Code": 0,
            "Name": "pending"
        },
        "StateTransitionReason": "",
        "SubnetId": "subnet-04a636d18e83cfacb",
        "VpcId": "vpc-1234567890abcdef0",
        "Architecture": "x86_64",
        "BlockDeviceMappings": [],
        "ClientToken": "",
        "EbsOptimized": false,
        "Hypervisor": "xen",
        "NetworkInterfaces": [
            {
                "Attachment": {
                    "AttachTime": "2018-05-10T08:05:20.000Z",
                    "AttachmentId": "eni-attach-0e325c07e928a0405",
                    "DeleteOnTermination": true,
                    "DeviceIndex": 0,
                    "Status": "attaching"
                },
                "Description": "",
                "Groups": [
                    {
                        "GroupName": "MySecurityGroup",
                        "GroupId": "sg-0598c7d356eba48d7"
                    }
                ],
                "Ipv6Addresses": [],
                "MacAddress": "0a:ab:58:e0:67:e2",
                "NetworkInterfaceId": "eni-0c0a29997760baee7",
                "OwnerId": "123456789012",
                "PrivateDnsName": "ip-10-0-0-157.us-east-2.compute.internal",
                "PrivateIpAddress": "10.0.0.157",
                "PrivateIpAddresses": [
                    {
                        "Primary": true,
```

```
                            "PrivateDnsName": "ip-10-0-0-157.us-
east-2.compute.internal",
                            "PrivateIpAddress": "10.0.0.157"
                        }
                    ],
                    "SourceDestCheck": true,
                    "Status": "in-use",
                    "SubnetId": "subnet-04a636d18e83cfacb",
                    "VpcId": "vpc-1234567890abcdef0",
                    "InterfaceType": "interface"
                }
            ],
            "RootDeviceName": "/dev/xvda",
            "RootDeviceType": "ebs",
            "SecurityGroups": [
                {
                    "GroupName": "MySecurityGroup",
                    "GroupId": "sg-0598c7d356eba48d7"
                }
            ],
            "SourceDestCheck": true,
            "StateReason": {
                "Code": "pending",
                "Message": "pending"
            },
            "Tags": [],
            "VirtualizationType": "hvm",
            "CpuOptions": {
                "CoreCount": 1,
                "ThreadsPerCore": 1
            },
            "CapacityReservationSpecification": {
                "CapacityReservationPreference": "open"
            },
            "MetadataOptions": {
                "State": "pending",
                "HttpTokens": "optional",
                "HttpPutResponseHopLimit": 1,
                "HttpEndpoint": "enabled"
            }
        }
    ],
    "OwnerId": "123456789012",
    "ReservationId": "r-02a3f596d91211712"
```

```
}
```

Ejemplo 2: Lanzar una instancia en una subred no predeterminada y agregar una dirección IP pública

En el siguiente ejemplo de `run-instances`, se solicita una dirección IP pública para una instancia que se va a lanzar en una subred no predeterminada. La instancia se asocia a los grupos de seguridad especificados.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --subnet-id subnet-08fc749671b2d077c \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --associate-public-ip-address \
    --key-name MyKeyPair
```

Para ver un ejemplo del resultado de `run-instances`, consulte el ejemplo 1.

Ejemplo 3: lanzar una instancia con volúmenes adicionales

En el siguiente ejemplo de `run-instances`, se usa una asignación de dispositivos de bloques, especificada en mapping.json, para asociar volúmenes adicionales en el momento del lanzamiento. Una asignación de dispositivos de bloques puede especificar volúmenes de EBS, volúmenes de almacén de instancias o tanto volúmenes de EBS como volúmenes de almacén de instancias.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --subnet-id subnet-08fc749671b2d077c \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --key-name MyKeyPair \
    --block-device-mappings file://mapping.json
```

Contenido de `mapping.json`. En este ejemplo, se le agrega a `/dev/sdh` un volumen de EBS vacío con un tamaño de 100 GiB.

```
[
    {
```

```
        "DeviceName": "/dev/sdh",
        "Ebs": {
            "VolumeSize": 100
        }
    }
]
```

Contenido de `mapping.json`. En este ejemplo, se le agrega a `ephemeral1` un volumen de almacén de instancias.

```
[
    {
        "DeviceName": "/dev/sdc",
        "VirtualName": "ephemeral1"
    }
]
```

Para ver un ejemplo del resultado de `run-instances`, consulte el ejemplo 1.

Para obtener más información acerca de la asignación de dispositivos de bloques, consulte Asignación de dispositivos de bloques en la Guía del usuario de Amazon EC2.

Ejemplo 4: lanzar una instancia y agregar etiquetas al crearla

En el siguiente ejemplo de `run-instances`, se agrega una etiqueta con una clave de `webserver` y un valor de `production` a la instancia. El comando también aplica una etiqueta con una clave de `cost-center` y un valor de `cc123` a cualquier volumen de EBS que se cree (en este caso, el volumen raíz).

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 1 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --tag-specifications
 'ResourceType=instance,Tags=[{Key=webserver,Value=production}]'
 'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

Para ver un ejemplo del resultado de `run-instances`, consulte el ejemplo 1.

Ejemplo 5: lanzar una instancia con datos de usuario

En el siguiente ejemplo de `run-instances`, se transfieren los datos del usuario a un archivo denominado `my_script.txt` que contiene un script de configuración para la instancia. El script se ejecuta en el momento del lanzamiento.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 1 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --user-data file://my_script.txt
```

Para ver un ejemplo del resultado de `run-instances`, consulte el ejemplo 1.

Para obtener más información, consulte Trabajo con datos de usuario en instancias en la Guía del usuario de Amazon EC2.

Ejemplo 6: lanzar una instancia de rendimiento ampliable

En el siguiente ejemplo de `run-instances`, se lanza una instancia t2.micro con la opción de crédito `unlimited`. Al lanzar una instancia T2, si no especifica `--credit-specification`, la opción de crédito predeterminada es `standard`. Al lanzar una instancia T3, la opción de crédito predeterminada es `unlimited`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 1 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --credit-specification CpuCredits=unlimited
```

Para ver un ejemplo del resultado de `run-instances`, consulte el ejemplo 1.

Para obtener más información sobre las instancias de rendimiento ampliable, consulte Instancias de rendimiento ampliable en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte RunInstances en la Referencia de comandos de la AWS CLI.

`run-scheduled-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `run-scheduled-instances`.

AWS CLI

Para lanzar una instancia programada

En este ejemplo, se lanza la instancia programada especificada en una VPC.

Comando:

```
aws ec2 run-scheduled-instances --scheduled-instance-
id sci-1234-1234-1234-1234-123456789012 --instance-count 1 --launch-
specification file://launch-specification.json
```

Launch-specification.json:

```
{
  "ImageId": "ami-12345678",
  "KeyName": "my-key-pair",
  "InstanceType": "c4.large",
  "NetworkInterfaces": [
    {
        "DeviceIndex": 0,
        "SubnetId": "subnet-12345678",
        "AssociatePublicIpAddress": true,
        "Groups": ["sg-12345678"]
    }
  ],
  "IamInstanceProfile": {
      "Name": "my-iam-role"
  }
}
```

Salida:

```
{
  "InstanceIdSet": [
```

```
      "i-1234567890abcdef0"
  ]
}
```

En este ejemplo, se lanza la instancia programada especificada en EC2-Classic.

Comando:

```
aws ec2 run-scheduled-instances --scheduled-instance-
id sci-1234-1234-1234-1234-123456789012 --instance-count 1 --launch-
specification file://launch-specification.json
```

Launch-specification.json:

```
{
  "ImageId": "ami-12345678",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": ["sg-12345678"],
  "InstanceType": "c4.large",
  "Placement": {
    "AvailabilityZone": "us-west-2b"
  }
  "IamInstanceProfile": {
      "Name": "my-iam-role"
  }
}
```

Salida:

```
{
  "InstanceIdSet": [
      "i-1234567890abcdef0"
  ]
}
```

- Para obtener información sobre la API, consulte RunScheduledInstances en la Referencia de comandos de la AWS CLI.

`search-local-gateway-routes`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-local-gateway-routes`.

AWS CLI

Para buscar rutas en una tabla de enrutamiento de puerta de enlace local

En el siguiente ejemplo de `search-local-gateway-routes` se buscan rutas estáticas en la tabla de enrutamiento de la puerta de enlace local especificada.

```
aws ec2 search-local-gateway-routes \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --filters "Name=type,Values=static"
```

Salida:

```
{
    "Route": {
        "DestinationCidrBlock": "0.0.0.0/0",
        "LocalGatewayVirtualInterfaceGroupId": "lgw-vif-grp-07145b276bEXAMPLE",
        "Type": "static",
        "State": "deleted",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7EXAMPLE"
    }
}
```

- Para obtener información sobre la API, consulte SearchLocalGatewayRoutes en la Referencia de comandos de la AWS CLI.

`search-transit-gateway-multicast-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-transit-gateway-multicast-groups`.

AWS CLI

Para buscar uno o más grupos de multidifusión de puerta de enlace de tránsito y devolver información de pertenencia al grupo

En el siguiente ejemplo de `search-transit-gateway-multicast-groups` se devuelve la pertenencia al grupo del grupo de multidifusión especificado.

```
aws ec2 search-transit-gateway-multicast-groups \
```

```
    --transit-gateway-multicast-domain-id tgw-mcast-domain-000fb24d04EXAMPLE
```

Salida:

```
{
    "MulticastGroups": [
        {
            "GroupIpAddress": "224.0.1.0",
            "TransitGatewayAttachmentId": "tgw-attach-0372e72386EXAMPLE",
            "SubnetId": "subnet-0187aff814EXAMPLE",
            "ResourceId": "vpc-0065acced4EXAMPLE",
            "ResourceType": "vpc",
            "NetworkInterfaceId": "eni-03847706f6EXAMPLE",
            "GroupMember": false,
            "GroupSource": true,
            "SourceType": "static"
        }
    ]
}
```

Para obtener más información, consulte Multidifusión en puertas de enlace de tránsito en la Guía de puertas de enlace de tránsito.

- Para obtener información sobre la API, consulte SearchTransitGatewayMulticastGroups en la Referencia de comandos de la AWS CLI.

`search-transit-gateway-routes`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-transit-gateway-routes`.

AWS CLI

Para buscar rutas en la tabla de enrutamiento de puerta de enlace de tránsito especificada

En el siguiente ejemplo de `search-transit-gateway-routes` se devuelven todas las rutas que son del tipo `static` de la tabla de enrutamiento especificada.

```
aws ec2 search-transit-gateway-routes \
    --transit-gateway-route-table-id tgw-rtb-0a823edbdeEXAMPLE \
    --filters "Name=type,Values=static"
```

Salida:

```
{
    "Routes": [
        {
            "DestinationCidrBlock": "10.0.2.0/24",
            "TransitGatewayAttachments": [
                {
                    "ResourceId": "vpc-4EXAMPLE",
                    "TransitGatewayAttachmentId": "tgw-attach-09b52ccdb5EXAMPLE",
                    "ResourceType": "vpc"
                }
            ],
            "Type": "static",
            "State": "active"
        },
        {
            "DestinationCidrBlock": "10.1.0.0/24",
            "TransitGatewayAttachments": [
                {
                    "ResourceId": "vpc-4EXAMPLE",
                    "TransitGatewayAttachmentId": "tgw-attach-09b52ccdb5EXAMPLE",
                    "ResourceType": "vpc"
                }
            ],
            "Type": "static",
            "State": "active"
        }
    ],
    "AdditionalRoutesAvailable": false
}
```

Para obtener más información, consulte Transit gateway route tables en la Guía de Transit Gateway.

- Para obtener información sobre la API, consulte SearchTransitGatewayRoutes en la Referencia de comandos de la AWS CLI.

`send-diagnostic-interrupt`

En el siguiente ejemplo de código, se muestra cómo utilizar `send-diagnostic-interrupt`.

AWS CLI

Para enviar una interrupción de diagnóstico

En el siguiente ejemplo de `send-diagnostic-interrupt` se envía una interrupción de diagnóstico a la instancia especificada.

```
aws ec2 send-diagnostic-interrupt \
    --instance-id i-1234567890abcdef0
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte SendDiagnosticInterrupt en la Referencia de comandos de la AWS CLI.

`start-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-instances`.

AWS CLI

Iniciar una instancia de Amazon EC

En este ejemplo, se inicia la instancia respaldada por Amazon EBS.

Comando:

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

Salida:

```
{
    "StartingInstances": [
        {
            "InstanceId": "i-1234567890abcdef0",
            "CurrentState": {
                "Code": 0,
                "Name": "pending"
            },
            "PreviousState": {
                "Code": 80,
                "Name": "stopped"
            }
        }
    ]
}
```

Para obtener más información, consulte Detener e iniciar la instancia en la Guía del usuario de Amazon Elastic Compute Cloud.

- Para obtener información sobre la API, consulte StartInstances en la Referencia de comandos de la AWS CLI.

`start-network-insights-access-scope-analysis`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-network-insights-access-scope-analysis`.

AWS CLI

Para iniciar un análisis de ámbito de acceso a información de la red

En el siguiente ejemplo de `start-network-insights-access-scope-analysis` se inicia el análisis de ámbito en su cuenta de AWS.

```
aws ec2 start-network-insights-access-scope-analysis \
    --region us-east-1 \
    --network-insights-access-scope-id nis-123456789111
```

Salida:

```
{
    "NetworkInsightsAccessScopeAnalysis": {
        "NetworkInsightsAccessScopeAnalysisId": "nisa-123456789222",
        "NetworkInsightsAccessScopeAnalysisArn": "arn:aws:ec2:us-
east-1:123456789012:network-insights-access-scope-analysis/nisa-123456789222",
        "NetworkInsightsAccessScopeId": "nis-123456789111",
        "Status": "running",
        "StartDate": "2022-01-26T00:47:06.814000+00:00"
    }
}
```

Para obtener más información, consulte Getting started with Network Access Analyzer using the AWS CLI en la Guía del analizador de acceso a la red.

- Para obtener información sobre la API, consulte StartNetworkInsightsAccessScopeAnalysis en la Referencia de comandos de la AWS CLI.

`start-network-insights-analysis`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-network-insights-analysis`.

AWS CLI

Para analizar una ruta

En el siguiente ejemplo de `start-network-insights-analysis` se analiza la ruta entre el origen y el destino. Para ver los resultados del análisis de la ruta, utilice el comando `describe-network-insights-analyses`.

```
aws ec2 start-network-insights-analysis \
    --network-insights-path-id nip-0b26f224f1d131fa8
```

Salida:

```
{
    "NetworkInsightsAnalysis": {
        "NetworkInsightsAnalysisId": "nia-02207aa13eb480c7a",
        "NetworkInsightsAnalysisArn": "arn:aws:ec2:us-east-1:123456789012:network-
insights-analysis/nia-02207aa13eb480c7a",
        "NetworkInsightsPathId": "nip-0b26f224f1d131fa8",
        "StartDate": "2021-01-20T22:58:37.495Z",
        "Status": "running"
    }
}
```

Para obtener más información, consulte Getting started using the AWS CLI en la Guía del analizador de accesibilidad.

- Para obtener información sobre la API, consulte StartNetworkInsightsAnalysis en la Referencia de comandos de la AWS CLI.

`start-vpc-endpoint-service-private-dns-verification`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-vpc-endpoint-service-private-dns-verification`.

AWS CLI

Para iniciar el proceso de verificación de DNS

En el siguiente ejemplo de `start-vpc-endpoint-service-private-dns-verification` se inicia el proceso de verificación de DNS para el servicio de punto de conexión especificado.

```
aws ec2 start-vpc-endpoint-service-private-dns-verification \
    --service-id vpce-svc-071afff70666e61e0
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Manage DNS names en la Guía del usuario de AWS PrivateLink.

- Para obtener información sobre la API, consulte StartVpcEndpointServicePrivateDnsVerification en la Referencia de comandos de la AWS CLI.

`stop-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-instances`.

AWS CLI

Ejemplo 1: Detener una instancia de Amazon EC

En el siguiente ejemplo de `stop-instances`, se detiene la instancia respaldada por Amazon EBS especificada.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0
```

Salida:

```
{
    "StoppingInstances": [
        {
            "InstanceId": "i-1234567890abcdef0",
            "CurrentState": {
                "Code": 64,
                "Name": "stopping"
            },
```

```
            "PreviousState": {
                "Code": 16,
                "Name": "running"
            }
        }
    ]
}
```

Para obtener más información, consulte Detener e iniciar la instancia en la Guía del usuario de Amazon Elastic Compute Cloud.

Ejemplo 2: Hibernar una instancia de Amazon EC

En el siguiente ejemplo de `stop-instances`, se hiberna una instancia respaldada por Amazon EBS siempre y cuando la instancia sea compatible con la hibernación y cumpla con los requisitos previos para la hibernación. Luego de que la instancia sea puesta en hibernación, la instancia se detiene.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --hibernate
```

Salida:

```
{
    "StoppingInstances": [
        {
            "CurrentState": {
                "Code": 64,
                "Name": "stopping"
            },
            "InstanceId": "i-1234567890abcdef0",
            "PreviousState": {
                "Code": 16,
                "Name": "running"
            }
        }
    ]
}
```

Para obtener más información, consulte Hibernar la instancia de Linux bajo demanda en la Guía del usuario de Amazon Elastic Compute Cloud.

- Para obtener información sobre la API, consulte StopInstances en la Referencia de comandos de la AWS CLI.

`terminate-client-vpn-connections`

En el siguiente ejemplo de código, se muestra cómo utilizar `terminate-client-vpn-connections`.

AWS CLI

Para terminar una conexión a un punto de conexión de Client VPN

En el siguiente ejemplo de `terminate-client-vpn-connections` se termina la conexión especificada al punto de conexión de Client VPN.

```
aws ec2 terminate-client-vpn-connections \
    --client-vpn-endpoint-id vpn-endpoint-123456789123abcde \
    --connection-id cvpn-connection-04edd76f5201e0cb8
```

Salida:

```
{
    "ClientVpnEndpointId": "vpn-endpoint-123456789123abcde",
    "ConnectionStatuses": [
        {
            "ConnectionId": "cvpn-connection-04edd76f5201e0cb8",
            "PreviousStatus": {
                "Code": "active"
            },
            "CurrentStatus": {
                "Code": "terminating"
            }
        }
    ]
}
```

Para obtener más información, consulte Client Connections en la Guía del administrador de AWS Client VPN.

- Para obtener información sobre la API, consulte TerminateClientVpnConnections en la Referencia de comandos de la AWS CLI.

`terminate-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `terminate-instances`.

AWS CLI

Terminar una instancia de Amazon EC

En este ejemplo, se termina la instancia especificada.

Comando:

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

Salida:

```
{
    "TerminatingInstances": [
        {
            "InstanceId": "i-1234567890abcdef0",
            "CurrentState": {
                "Code": 32,
                "Name": "shutting-down"
            },
            "PreviousState": {
                "Code": 16,
                "Name": "running"
            }
        }
    ]
}
```

Para obtener más información, consulte Uso de instancias de Amazon EC2 en la Guía del usuario de la interfaz de la línea de comandos de AWS.

- Para obtener información sobre la API, consulte TerminateInstances en la Referencia de comandos de la AWS CLI.

`unassign-ipv6-addresses`

En el siguiente ejemplo de código, se muestra cómo utilizar `unassign-ipv6-addresses`.

AWS CLI

Para anular la asignación de una dirección IPv6 de una interfaz de red

En este ejemplo, se anula la asignación de las direcciones IPv6 especificadas de la interfaz de red especificada.

Comando:

```
aws ec2 unassign-ipv6-addresses --ipv6-
addresses 2001:db8:1234:1a00:3304:8879:34cf:4071 --network-interface-id eni-23c49b68
```

Salida:

```
{
  "NetworkInterfaceId": "eni-23c49b68",
  "UnassignedIpv6Addresses": [
      "2001:db8:1234:1a00:3304:8879:34cf:4071"
  ]
}
```

- Para obtener información sobre la API, consulte UnassignIpv6Addresses en la Referencia de comandos de la AWS CLI.

`unassign-private-ip-addresses`

En el siguiente ejemplo de código, se muestra cómo utilizar `unassign-private-ip-addresses`.

AWS CLI

Para anular la asignación de una dirección IP privada secundaria de una interfaz de red

En este ejemplo, se anula la asignación de las direcciones IP especificadas de la interfaz de red especificada. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

Comando:

```
aws ec2 unassign-private-ip-addresses --network-interface-id eni-e5aa89a3 --private-
ip-addresses 10.0.0.82
```

- Para obtener información sobre la API, consulte UnassignPrivateIpAddresses en la Referencia de comandos de la AWS CLI.

`unassign-private-nat-gateway-address`

En el siguiente ejemplo de código, se muestra cómo utilizar `unassign-private-nat-gateway-address`.

AWS CLI

Para cancelar la asignación de direcciones IP privadas de la puerta de enlace de NAT privada

En el siguiente ejemplo de `unassign-private-nat-gateway-address` se anula la asignación de la dirección IP especificada de la puerta de enlace NAT privada especificada.

```
aws ec2 unassign-private-nat-gateway-address \
    --nat-gateway-id nat-1234567890abcdef0 \
    --private-ip-addresses 10.0.20.197
```

Salida:

```
{
    "NatGatewayId": "nat-0ee3edd182361f662",
    "NatGatewayAddresses": [
        {
            "NetworkInterfaceId": "eni-0065a61b324d1897a",
            "PrivateIp": "10.0.20.197",
            "IsPrimary": false,
            "Status": "unassigning"
        }
    ]
}
```

Para obtener información, consulte Gateways NAT en la Guía del usuario de Amazon VPC.

- Para obtener información sobre la API, consulte UnassignPrivateNatGatewayAddress en la Referencia de comandos de la AWS CLI.

`unlock-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `unlock-snapshot`.

AWS CLI

Para desbloquear una instantánea

En el siguiente ejemplo de `unlock-snapshot` se desbloquea la instantánea especificada.

```
aws ec2 unlock-snapshot \
    --snapshot-id snap-0b5e733b4a8df6e0d
```

Salida:

```
{
    "SnapshotId": "snap-0b5e733b4a8df6e0d"
}
```

Para obtener más información, consulte Snapshot lock en la Guía del usuario de Amazon EBS.

- Para obtener información sobre la API, consulte UnlockSnapshot en la Referencia de comandos de la AWS CLI.

`unmonitor-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `unmonitor-instances`.

AWS CLI

Deshabilitar el monitoreo detallado de una instancia

Este comando de ejemplo deshabilita el monitoreo detallado de la instancia especificada.

Comando:

```
aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

Salida:

```
{
  "InstanceMonitorings": [
      {
          "InstanceId": "i-1234567890abcdef0",
          "Monitoring": {
```

```
            "State": "disabling"
        }
    }
  ]
}
```

- Para obtener información sobre la API, consulte UnmonitorInstances en la Referencia de comandos de la AWS CLI.

`update-security-group-rule-descriptions-egress`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-security-group-rule-descriptions-egress`.

AWS CLI

Para actualizar la descripción de una regla de grupo de seguridad de salida

En el siguiente ejemplo de `update-security-group-rule-descriptions-egress` se actualiza la descripción de la regla de grupo de seguridad para el protocolo y el rango de direcciones IPv4 especificados. La descripción `Outbound HTTP access to server 2` reemplaza a cualquier descripción existente de la regla.

```
aws ec2 update-security-group-rule-descriptions-egress \
    --group-id sg-02f0d35a850ba727f \
    --ip-permissions
 IpProtocol=tcp,FromPort=80,ToPort=80,IpRanges=[{CidrIp=203.0.113.0/24,Description="Outbound
 HTTP access to server 2"}]
```

Salida:

```
{
    "Return": true
}
```

Para obtener más información, consulte Reglas del grupo de seguridad en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte UpdateSecurityGroupRuleDescriptionsEgress en la Referencia de comandos de la AWS CLI.

update-security-group-rule-descriptions-ingress

En el siguiente ejemplo de código, se muestra cómo utilizar `update-security-group-rule-descriptions-ingress`.

AWS CLI

Ejemplo 1: actualización de la descripción de una regla de grupo de seguridad entrante con un origen de CIDR

En el siguiente ejemplo de `update-security-group-rule-descriptions-ingress` se actualiza la descripción de la regla de grupo de seguridad para el protocolo y el rango de direcciones IPv4 especificados. La descripción `SSH access from ABC office` reemplaza a cualquier descripción existente de la regla.

```
aws ec2 update-security-group-rule-descriptions-ingress \
    --group-id sg-02f0d35a850ba727f \
    --ip-permissions
 IpProtocol=tcp,FromPort=22,ToPort=22,IpRanges='[{CidrIp=203.0.113.0/16,Description="SSH
 access from corpnet"}]'
```

Salida:

```
{
    "Return": true
}
```

Para obtener más información, consulte Reglas del grupo de seguridad en la Guía del usuario de Amazon EC2.

Ejemplo 2: actualización de la descripción de una regla de grupo de seguridad entrante con un origen de lista de prefijos

En el siguiente ejemplo de `update-security-group-rule-descriptions-ingress` se actualiza la descripción de la regla de grupo de seguridad para el puerto y la lista de prefijos especificados. La descripción `SSH access from ABC office` reemplaza a cualquier descripción existente de la regla.

```
aws ec2 update-security-group-rule-descriptions-ingress \
```

```
    --group-id sg-02f0d35a850ba727f \
    --ip-permissions
 IpProtocol=tcp,FromPort=22,ToPort=22,PrefixListIds='[{PrefixListId=pl-12345678,Description=
 access from corpnet"}]'
```

Salida:

```
{
    "Return": true
}
```

Para obtener más información, consulte Reglas del grupo de seguridad en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte UpdateSecurityGroupRuleDescriptionsIngress en la Referencia de comandos de la AWS CLI.

`withdraw-byoip-cidr`

En el siguiente ejemplo de código, se muestra cómo utilizar `withdraw-byoip-cidr`.

AWS CLI

Para dejar de anunciar un rango de direcciones

En el siguiente ejemplo de `withdraw-byoip-cidr` se deja de anunciar el rango de direcciones especificado.

```
aws ec2 withdraw-byoip-cidr
    --cidr 203.0.113.25/24
```

Salida:

```
{
    "ByoipCidr": {
        "Cidr": "203.0.113.25/24",
        "StatusMessage": "ipv4pool-ec2-1234567890abcdef0",
        "State": "advertised"
    }
}
```

- Para obtener información sobre la API, consulte WithdrawByoipCidr en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon EC2 Instance Connect que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante la AWS Command Line Interface con Conexión de la instancia de Amazon EC2.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`send-ssh-public-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `send-ssh-public-key`.

AWS CLI

Envío de una clave pública SSH a una instancia

En el siguiente ejemplo de `send-ssh-public-key`, se envía la clave pública SSH especificada a la instancia especificada. La clave se usa para autenticar al usuario especificado.

```
aws ec2-instance-connect send-ssh-public-key \
    --instance-id i-1234567890abcdef0 \
    --instance-os-user ec2-user \
    --availability-zone us-east-2b \
    --ssh-public-key file://path/my-rsa-key.pub
```

Este comando no genera ninguna salida.

- Para obtener detalles sobre la API, consulte SendSshPublicKey en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon ECR que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante el uso de la AWS Command Line Interface con Amazon ECR.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`batch-check-layer-availability`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-check-layer-availability`.

AWS CLI

Para comprobar la disponibilidad de una capa

En el siguiente ejemplo de `batch-check-layer-availability`, se comprueba la disponibilidad de una capa con el resumen `sha256:6171c7451a50945f8ddd72f7732cc04d7a0d1f48138a426b2e64387fdeb834ed` en el repositorio `cluster-autoscaler`.

```
aws ecr batch-check-layer-availability \
    --repository-name cluster-autoscaler \
    --layer-
digests sha256:6171c7451a50945f8ddd72f7732cc04d7a0d1f48138a426b2e64387fdeb834ed
```

Salida:

```
{
    "layers": [
        {
            "layerDigest":
 "sha256:6171c7451a50945f8ddd72f7732cc04d7a0d1f48138a426b2e64387fdeb834ed",
            "layerAvailability": "AVAILABLE",
            "layerSize": 2777,
            "mediaType": "application/vnd.docker.container.image.v1+json"
        }
    ],
    "failures": []
}
```

- Para obtener información sobre la API, consulte BatchCheckLayerAvailability en la Referencia de comandos de la AWS CLI.

`batch-delete-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-delete-image`.

AWS CLI

Ejemplo 1: eliminación de una imagen

En el siguiente ejemplo de `batch-delete-image`, se elimina una imagen con la etiqueta `precise` del repositorio especificado del registro predeterminado de una cuenta.

```
aws ecr batch-delete-image \
    --repository-name ubuntu \
    --image-ids imageTag=precise
```

Salida:

```
{
    "failures": [],
    "imageIds": [
        {
            "imageTag": "precise",
            "imageDigest":
 "sha256:19665f1e6d1e504117a1743c0a3d3753086354a38375961f2e665416ef4b1b2f"
        }
```

```
    ]
}
```

Ejemplo 2: eliminación de varias imágenes

En el siguiente ejemplo de `batch-delete-image`, se eliminan todas las imágenes con las etiquetas `prod` y `team1` del repositorio especificado.

```
aws ecr batch-delete-image \
    --repository-name MyRepository \
    --image-ids imageTag=prod imageTag=team1
```

Salida:

```
{
    "imageIds": [
        {
            "imageDigest": "sha256:123456789012",
            "imageTag": "prod"
        },
        {
            "imageDigest": "sha256:567890121234",
            "imageTag": "team1"
        }
    ],
    "failures": []
}
```

Para obtener más información, consulte Deleting an Image en la Guía del usuario de Amazon ECR.

- Para obtener información sobre la API, consulte BatchDeleteImage en la Referencia de comandos de la AWS CLI.

`batch-get-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-image`.

AWS CLI

Ejemplo 1: obtención de una imagen

En el siguiente ejemplo de `batch-get-image`, se obtiene una imagen con la etiqueta `v1.13.6` de un repositorio llamado `cluster-autoscaler` del registro predeterminado de una cuenta.

```
aws ecr batch-get-image \
    --repository-name cluster-autoscaler \
    --image-ids imageTag=v1.13.6
```

Salida:

```
{
    "images": [
        {
            "registryId": "012345678910",
            "repositoryName": "cluster-autoscaler",
            "imageId": {
                "imageDigest":
 "sha256:4a1c6567c38904384ebc64e35b7eeddd8451110c299e3368d2210066487d97e5",
                "imageTag": "v1.13.6"
            },
            "imageManifest": "{\n   \"schemaVersion\": 2,\n
 \"mediaType\": \"application/vnd.docker.distribution.manifest.v2+json
\",\n   \"config\": {\n      \"mediaType\": \"application/
vnd.docker.container.image.v1+json\",\n      \"size\": 2777,\n      \"digest
\": \"sha256:6171c7451a50945f8ddd72f7732cc04d7a0d1f48138a426b2e64387fdeb834ed
\"\n   },\n   \"layers\": [\n      {\n         \"mediaType
\": \"application/vnd.docker.image.rootfs.diff.tar.gzip
\",\n         \"size\": 17743696,\n         \"digest\":
 \"sha256:39fafc05754f195f134ca11ecdb1c9a691ab0848c697fffeb5a85f900caaf6e1\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 2565026,\n
 \"digest\":
 \"sha256:8c8a779d3a537b767ae1091fe6e00c2590afd16767aa6096d1b318d75494819f
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 28005981,\n
 \"digest\":
 \"sha256:c44ba47496991c9982ee493b47fd25c252caabf2b4ae7dd679c9a27b6a3c8fb7\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 775,\n         \"digest
\": \"sha256:e2c388b44226544363ca007be7b896bcce1baebea04da23cbd165eac30be650f\"\n
   }\n   ]\n}"
        }
    ],
    "failures": []
```

```
}
```

Ejemplo 2: obtención de varias imágenes

En el siguiente ejemplo de `batch-get-image`, se muestran detalles de todas las imágenes con las etiquetas `prod` y `team1` del repositorio especificado.

```
aws ecr batch-get-image \
    --repository-name MyRepository \
    --image-ids imageTag=prod imageTag=team1
```

Salida:

```
{
    "images": [
        {
            "registryId": "123456789012",
            "repositoryName": "MyRepository",
            "imageId": {
                "imageDigest": "sha256:123456789012",
                "imageTag": "prod"
            },
            "imageManifest": "manifestExample1"
        },
        {
            "registryId": "567890121234",
            "repositoryName": "MyRepository",
            "imageId": {
                "imageDigest": "sha256:123456789012",
                "imageTag": "team1"
            },
            "imageManifest": "manifestExample2"
        }
    ],
    "failures": []
}
```

Para obtener más información, consulte Images en la Guía del usuario de Amazon ECR.

- Para obtener información sobre la API, consulte BatchGetImage en la Referencia de comandos de la AWS CLI.

`complete-layer-upload`

En el siguiente ejemplo de código, se muestra cómo utilizar `complete-layer-upload`.

AWS CLI

Para finalizar la carga de una capa de imágenes

En el siguiente ejemplo de `complete-layer-upload` se finaliza la carga de una capa de imágenes en el repositorio `layer-test`.

```
aws ecr complete-layer-upload \
    --repository-name layer-test \
    --upload-id 6cb64b8a-9378-0e33-2ab1-b780fab8a9e9 \
    --layer-digests 6cb64b8a-9378-0e33-2ab1-
b780fab8a9e9:48074e6d3a68b39aad8ccc002cdad912d4148c0f92b3729323e
```

Salida:

```
{
    "uploadId": "6cb64b8a-9378-0e33-2ab1-b780fab8a9e9",
    "layerDigest":
 "sha256:9a77f85878aa1906f2020a0ecdf7a7e962d57e882250acd773383224b3fe9a02",
    "repositoryName": "layer-test",
    "registryId": "130757420319"
}
```

- Para obtener información sobre la API, consulte CompleteLayerUpload en la Referencia de comandos de la AWS CLI.

`create-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-repository`.

AWS CLI

Ejemplo 1: creación de un repositorio

En el siguiente ejemplo de `create-repository` se crea un repositorio dentro del espacio de nombres especificado en el registro predeterminado de una cuenta.

```
aws ecr create-repository \
```

```
    --repository-name project-a/sample-repo
```

Salida:

```
{
    "repository": {
        "registryId": "123456789012",
        "repositoryName": "project-a/sample-repo",
        "repositoryArn": "arn:aws:ecr:us-west-2:123456789012:repository/project-a/
sample-repo"
    }
}
```

Para obtener más información, consulte Creating a Repository en la Guía del usuario de Amazon ECR.

Ejemplo 2: creación de un repositorio configurado con inmutabilidad de las etiquetas de imagen

En el siguiente ejemplo de `create-repository` se crea un repositorio configurado para la inmutabilidad de etiquetas en el registro predeterminado de una cuenta.

```
aws ecr create-repository \
    --repository-name project-a/sample-repo \
    --image-tag-mutability IMMUTABLE
```

Salida:

```
{
    "repository": {
        "registryId": "123456789012",
        "repositoryName": "project-a/sample-repo",
        "repositoryArn": "arn:aws:ecr:us-west-2:123456789012:repository/project-a/
sample-repo",
        "imageTagMutability": "IMMUTABLE"
    }
}
```

Para obtener más información, consulte Mutabilidad de las etiquetas de imagen en la Guía del usuario de Amazon ECR.

Ejemplo 3: creación de un repositorio configurado con una configuración de escaneo

En el siguiente ejemplo de `create-repository` se crea un repositorio configurado para realizar un escaneo de vulnerabilidad a una inserción de imagen en el registro predeterminado de una cuenta.

```
aws ecr create-repository \
    --repository-name project-a/sample-repo \
    --image-scanning-configuration scanOnPush=true
```

Salida:

```
{
    "repository": {
        "registryId": "123456789012",
        "repositoryName": "project-a/sample-repo",
        "repositoryArn": "arn:aws:ecr:us-west-2:123456789012:repository/project-a/
sample-repo",
        "imageScanningConfiguration": {
            "scanOnPush": true
        }
    }
}
```

Para obtener más información, consulte Escaneo de imágenes en la Guía del usuario de Amazon ECR.

- Para obtener información sobre la API, consulte CreateRepository en la Referencia de comandos de la AWS CLI.

`delete-lifecycle-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-lifecycle-policy`.

AWS CLI

Para eliminar la política de ciclo de vida para un repositorio

En el siguiente ejemplo de `delete-lifecycle-policy`, se elimina la política de ciclo de vida del repositorio `hello-world`.

```
aws ecr delete-lifecycle-policy \
```

```
    --repository-name hello-world
```

Salida:

```
{
    "registryId": "012345678910",
    "repositoryName": "hello-world",
    "lifecyclePolicyText": "{\"rules\":[{\"rulePriority\":1,\"description\":\"Remove
 untagged images.\",\"selection\":{\"tagStatus\":\"untagged\",\"countType\":
\"sinceImagePushed\",\"countUnit\":\"days\",\"countNumber\":10},\"action\":{\"type
\":\"expire\"}}]}",
    "lastEvaluatedAt": 0.0
}
```

- Para obtener información sobre la API, consulte DeleteLifecyclePolicy en la Referencia de comandos de la AWS CLI.

`delete-repository-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-repository-policy`.

AWS CLI

Para eliminar la política de repositorio de un repositorio

En el siguiente ejemplo de `delete-repository-policy`, se elimina la política de repositorio del repositorio `cluster-autoscaler`.

```
aws ecr delete-repository-policy \
    --repository-name cluster-autoscaler
```

Salida:

```
{
    "registryId": "012345678910",
    "repositoryName": "cluster-autoscaler",
    "policyText": "{\n  \"Version\" : \"2008-10-17\",\n  \"Statement\" : [ {\n
 \"Sid\" : \"allow public pull\",\n    \"Effect\" : \"Allow\",\n    \"Principal\" :
 \"*\",\n    \"Action\" : [ \"ecr:BatchCheckLayerAvailability\", \"ecr:BatchGetImage
\", \"ecr:GetDownloadUrlForLayer\" ]\n  } ]\n}"
```

```
}
```

- Para obtener información sobre la API, consulte DeleteRepositoryPolicy en la Referencia de comandos de la AWS CLI.

`delete-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-repository`.

AWS CLI

Eliminación de un repositorio

En el siguiente ejemplo de `delete-repository` el comando fuerza la eliminación del repositorio especificado del registro predeterminado de una cuenta. La marca `--force` es obligatoria si el repositorio contiene imágenes.

```
aws ecr delete-repository \
    --repository-name ubuntu \
    --force
```

Salida:

```
{
    "repository": {
        "registryId": "123456789012",
        "repositoryName": "ubuntu",
        "repositoryArn": "arn:aws:ecr:us-west-2:123456789012:repository/ubuntu"
    }
}
```

Para obtener más información, consulte Deleting a Repository en la Guía del usuario de Amazon ECR.

- Para obtener información sobre la API, consulte DeleteRepository en la Referencia de comandos de la AWS CLI.

`describe-image-scan-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-image-scan-findings`.

AWS CLI

Para describir los resultados de escaneo de una imagen

En el siguiente ejemplo de `describe-image-scan-findings`,se devuelven los resultados del escaneo de una imagen utilizando el resumen de imágenes del repositorio especificado en el registro predeterminado de una cuenta.

```
aws ecr describe-image-scan-findings \
    --repository-name sample-repo \
    --image-
id imageDigest=sha256:74b2c688c700ec95a93e478cdb959737c148df3fbf5ea706abe0318726e885e6
```

Salida:

```
{
    "imageScanFindings": {
      "findings": [
          {
              "name": "CVE-2019-5188",
              "description": "A code execution vulnerability exists in the directory
 rehashing functionality of E2fsprogs e2fsck 1.45.4. A specially crafted ext4
 directory can cause an out-of-bounds write on the stack, resulting in code
 execution. An attacker can corrupt a partition to trigger this vulnerability.",
              "uri": "http://people.ubuntu.com/~ubuntu-security/cve/CVE-2019-5188",
              "severity": "MEDIUM",
              "attributes": [
                  {
                      "key": "package_version",
                      "value": "1.44.1-1ubuntu1.1"
                  },
                  {
                      "key": "package_name",
                      "value": "e2fsprogs"
                  },
                  {
                      "key": "CVSS2_VECTOR",
                      "value": "AV:L/AC:L/Au:N/C:P/I:P/A:P"
                  },
                  {
                      "key": "CVSS2_SCORE",
                      "value": "4.6"
                  }
```

```
                ]
            }
        ],
        "imageScanCompletedAt": 1579839105.0,
        "vulnerabilitySourceUpdatedAt": 1579811117.0,
        "findingSeverityCounts": {
            "MEDIUM": 1
        }
    },
    "registryId": "123456789012",
    "repositoryName": "sample-repo",
    "imageId": {
        "imageDigest":
 "sha256:74b2c688c700ec95a93e478cdb959737c148df3fbf5ea706abe0318726e885e6"
    },
    "imageScanStatus": {
        "status": "COMPLETE",
        "description": "The scan was completed successfully."
    }
}
```

Para obtener más información, consulte Image Scanning en la Guía del usuario de Amazon ECR.

- Para obtener información sobre la API, consulte DescribeImageScanFindings en la Referencia de comandos de la AWS CLI.

`describe-images`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-images`.

AWS CLI

Para describir una imagen en un repositorio

En el siguiente ejemplo de `describe-images` se muestran detalles sobre una imagen del repositorio `cluster-autoscaler` con la etiqueta `v1.13.6`.

```
aws ecr describe-images \
    --repository-name cluster-autoscaler \
    --image-ids imageTag=v1.13.6
```

Salida:

```
{
    "imageDetails": [
        {
            "registryId": "012345678910",
            "repositoryName": "cluster-autoscaler",
            "imageDigest":
 "sha256:4a1c6567c38904384ebc64e35b7eeddd8451110c299e3368d2210066487d97e5",
            "imageTags": [
                "v1.13.6"
            ],
            "imageSizeInBytes": 48318255,
            "imagePushedAt": 1565128275.0
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeImages en la Referencia de comandos de la AWS CLI.

`describe-repositories`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-repositories`.

AWS CLI

Para describir los repositorios de imágenes en un registro

En este ejemplo, se describen los repositorios del registro predeterminado de una cuenta.

Comando:

```
aws ecr describe-repositories
```

Salida:

```
{
    "repositories": [
        {
            "registryId": "012345678910",
            "repositoryName": "ubuntu",
            "repositoryArn": "arn:aws:ecr:us-west-2:012345678910:repository/ubuntu"
```

```
        },
        {
            "registryId": "012345678910",
            "repositoryName": "test",
            "repositoryArn": "arn:aws:ecr:us-west-2:012345678910:repository/test"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeRepositories en la Referencia de comandos de la AWS CLI.

`get-authorization-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-authorization-token`.

AWS CLI

Para obtener un token de autorización para el registro predeterminado

En el siguiente ejemplo de comando de `get-authorization-token` se obtiene un token de autorización para el registro predeterminado.

```
aws ecr get-authorization-token
```

Salida:

```
{
    "authorizationData": [
        {
            "authorizationToken": "QVdTOkN...",
            "expiresAt": 1448875853.241,
            "proxyEndpoint": "https://123456789012.dkr.ecr.us-west-2.amazonaws.com"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetAuthorizationToken en la Referencia de comandos de la AWS CLI.

`get-download-url-for-layer`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-download-url-for-layer`.

AWS CLI

Para obtener la dirección URL de descarga de una capa

En el siguiente ejemplo de `get-download-url-for-layer`, se comprueba la dirección URL descargada de una capa con el resumen `sha256:6171c7451a50945f8ddd72f7732cc04d7a0d1f48138a426b2e64387fdeb834ed` en el repositorio `cluster-autoscaler`.

```
aws ecr get-download-url-for-layer \
    --repository-name cluster-autoscaler  \
    --layer-
digest sha256:6171c7451a50945f8ddd72f7732cc04d7a0d1f48138a426b2e64387fdeb834ed
```

Salida:

```
{
    "downloadUrl": "https://prod-us-west-2-starport-layer-bucket.s3.us-
west-2.amazonaws.com/e501-012345678910-9cb60dc0-7284-5643-3987-
da6dac0465f0/04620aac-66a5-4167-8232-55ee7ef6d565?X-Amz-Algorithm=AWS4-HMAC-
SHA256&X-Amz-Date=20190814T220617Z&X-Amz-SignedHeaders=host&X-Amz-Expires=3600&X-
Amz-Credential=AKIA32P3D2JDNMVAJLGF%2F20190814%2Fus-west-2%2Fs3%2Faws4_request&X-
Amz-Signature=9161345894947a1672467a0da7a1550f2f7157318312fe4941b59976239c3337",
    "layerDigest":
 "sha256:6171c7451a50945f8ddd72f7732cc04d7a0d1f48138a426b2e64387fdeb834ed"
}
```

- Para obtener información sobre la API, consulte GetDownloadUrlForLayer en la Referencia de comandos de la AWS CLI.

`get-lifecycle-policy-preview`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-lifecycle-policy-preview`.

AWS CLI

Para recuperar los detalles de una vista previa de política de ciclo de vida

En el siguiente ejemplo de `get-lifecycle-policy-preview`, se recupera el resultado de una vista previa de política de ciclo de vida del repositorio especificado en el registro predeterminado de una cuenta.

Comando:

```
aws ecr get-lifecycle-policy-preview \
    --repository-name "project-a/amazon-ecs-sample"
```

Salida:

```
{
    "registryId": "012345678910",
    "repositoryName": "project-a/amazon-ecs-sample",
    "lifecyclePolicyText": "{\n    \"rules\": [\n        {\n
 \"rulePriority\": 1,\n            \"description\": \"Expire images older than 14
 days\",\n            \"selection\": {\n                \"tagStatus\": \"untagged\",
\n                \"countType\": \"sinceImagePushed\",\n                \"countUnit
\": \"days\",\n                \"countNumber\": 14\n            },\n
 \"action\": {\n                \"type\": \"expire\"\n            }\n        }\n
  ]\n}\n",
    "status": "COMPLETE",
    "previewResults": [],
    "summary": {
        "expiringImageTotalCount": 0
    }
}
```

Para obtener más información, consulte Lifecycle Policies en la Guía del usuario de Amazon ECR.

- Para obtener información sobre la API, consulte GetLifecyclePolicyPreview en la Referencia de comandos de la AWS CLI.

`get-lifecycle-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-lifecycle-policy`.

AWS CLI

Para recuperar una política de ciclo de vida

En el siguiente ejemplo de `get-lifecycle-policy`, se muestran detalles de la política de ciclo de vida del repositorio especificado en el registro predeterminado de una cuenta.

```
aws ecr get-lifecycle-policy \
    --repository-name "project-a/amazon-ecs-sample"
```

Salida:

```
{
     "registryId": "123456789012",
     "repositoryName": "project-a/amazon-ecs-sample",
     "lifecyclePolicyText": "{\"rules\":[{\"rulePriority\":1,\"description\":
\"Expire images older than 14 days\",\"selection\":{\"tagStatus\":\"untagged\",
\"countType\":\"sinceImagePushed\",\"countUnit\":\"days\",\"countNumber\":14},
\"action\":{\"type\":\"expire\"}}]}",
     "lastEvaluatedAt": 1504295007.0
}
```

Para obtener más información, consulte Lifecycle Policies en la Guía del usuario de Amazon ECR.

- Para obtener información sobre la API, consulte GetLifecyclePolicy en la Referencia de comandos de la AWS CLI.

`get-login-password`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-login-password`.

AWS CLI

Para recuperar una contraseña para autenticarse en un registro

En el siguiente ejemplo de `get-login-password`, se muestra una contraseña que puede usar con el cliente de contenedor de su elección para autenticarse en un registro de Amazon ECR al que tenga acceso la entidad principal de IAM.

```
aws ecr get-login-password
```

Salida:

```
<password>
```

Para usarlo con la CLI de Docker, canalice el resultado del comando `get-login-password` al comando `docker login`. Al recuperar la contraseña, asegúrese de especificar la misma región en la que se encuentra su registro de Amazon ECR.

```
aws ecr get-login-password \
    --region <region>
 \
| docker login \
    --username AWS \
    --password-stdin <aws_account_id>.dkr.ecr.<region>.amazonaws.com
```

Para obtener más información, consulte Registry Authentication en la Guía del usuario de Amazon ECR.

- Para obtener información sobre la API, consulte GetLoginPassword en la Referencia de comandos de la AWS CLI.

`get-login`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-login`.

AWS CLI

Para recuperar un comando de inicio de sesión de Docker en el registro predeterminado

En este ejemplo se imprime un comando que se puede utilizar para iniciar sesión en el registro de Amazon ECR predeterminado.

Comando:

```
aws ecr get-login
```

Salida:

```
docker login -u AWS -p <password> -e none https://
<aws_account_id>.dkr.ecr.<region>.amazonaws.com
```

Para iniciar sesión en el registro de otra cuenta

En este ejemplo se imprimen uno o varios comandos que se pueden utilizar para iniciar sesión en los registros de Amazon ECR asociados a otras cuentas.

Comando:

```
aws ecr get-login --registry-ids 012345678910 023456789012
```

Salida:

```
docker login -u <username> -p <token-1> -e none <endpoint-1>
docker login -u <username> -p <token-2> -e none <endpoint-2>
```

- Para obtener información sobre la API, consulte GetLogin en la Referencia de comandos de la AWS CLI.

`get-repository-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-repository-policy`.

AWS CLI

Para recuperar la política de repositorio de un repositorio

En el siguiente ejemplo de `get-repository-policy` se muestran detalles sobre la política de repositorio del repositorio `cluster-autoscaler`.

```
aws ecr get-repository-policy \
    --repository-name cluster-autoscaler
```

Salida:

```
{
    "registryId": "012345678910",
    "repositoryName": "cluster-autoscaler",
    "policyText": "{\n  \"Version\" : \"2008-10-17\",\n  \"Statement\" : [ {\n
 \"Sid\" : \"allow public pull\",\n    \"Effect\" : \"Allow\",\n    \"Principal\" :
 \"*\",\n    \"Action\" : [ \"ecr:BatchCheckLayerAvailability\", \"ecr:BatchGetImage
\", \"ecr:GetDownloadUrlForLayer\" ]\n  } ]\n}"
}
```

- Para obtener información sobre la API, consulte GetRepositoryPolicy en la Referencia de comandos de la AWS CLI.

`initiate-layer-upload`

En el siguiente ejemplo de código, se muestra cómo utilizar `initiate-layer-upload`.

AWS CLI

Para iniciar la carga de una capa de imágenes

En el siguiente ejemplo de `initiate-layer-upload`, se inicia la carga de una capa de imágenes en el repositorio `layer-test`.

```
aws ecr initiate-layer-upload \
    --repository-name layer-test
```

Salida:

```
{
    "partSize": 10485760,
    "uploadId": "6cb64b8a-9378-0e33-2ab1-b780fab8a9e9"
}
```

- Para obtener información sobre la API, consulte InitiateLayerUpload en la Referencia de comandos de la AWS CLI.

`list-images`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-images`.

AWS CLI

Para crear una lista de las imágenes en un repositorio

En el siguiente ejemplo de `list-images` se muestra una lista de las imágenes del repositorio `cluster-autoscaler`.

```
aws ecr list-images \
    --repository-name cluster-autoscaler
```

Salida:

```
{
    "imageIds": [
```

```
        {
            "imageDigest":
 "sha256:99c6fb4377e9a420a1eb3b410a951c9f464eff3b7dbc76c65e434e39b94b6570",
            "imageTag": "v1.13.8"
        },
        {
            "imageDigest":
 "sha256:99c6fb4377e9a420a1eb3b410a951c9f464eff3b7dbc76c65e434e39b94b6570",
            "imageTag": "v1.13.7"
        },
        {
            "imageDigest":
 "sha256:4a1c6567c38904384ebc64e35b7eeddd8451110c299e3368d2210066487d97e5",
            "imageTag": "v1.13.6"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListImages en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un repositorio

En el siguiente ejemplo de `list-tags-for-resource`, se muestra una lista de las etiquetas asociadas con el repositorio `hello-world`.

```
aws ecr list-tags-for-resource \
    --resource-arn arn:aws:ecr:us-west-2:012345678910:repository/hello-world
```

Salida:

```
{
    "tags": [
        {
            "Key": "Stage",
            "Value": "Integ"
```

```
        }
    ]
}
```

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-image-scanning-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-image-scanning-configuration`.

AWS CLI

Para actualizar la configuración de escaneo de imágenes de un repositorio

En el siguiente ejemplo de `put-image-scanning-configuration`, se actualiza la configuración de escaneo de imágenes del repositorio especificado.

```
aws ecr put-image-scanning-configuration \
    --repository-name sample-repo \
    --image-scanning-configuration scanOnPush=true
```

Salida:

```
{
   "registryId": "012345678910",
   "repositoryName": "sample-repo",
   "imageScanningConfiguration": {
     "scanOnPush": true
   }
}
```

Para obtener más información, consulte Image Scanning en la Guía del usuario de Amazon ECR.

- Para obtener información sobre la API, consulte PutImageScanningConfiguration en la Referencia de comandos de la AWS CLI.

`put-image-tag-mutability`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-image-tag-mutability`.

AWS CLI

Para actualizar la configuración de mutabilidad de las etiquetas de imagen en un repositorio

En el siguiente ejemplo de `put-image-tag-mutability`, se configura el repositorio especificado para la inmutabilidad de las etiquetas. De este modo, se evita que se sobrescriban todas las etiquetas de imagen dentro del repositorio.

```
aws ecr put-image-tag-mutability \
    --repository-name hello-repository \
    --image-tag-mutability IMMUTABLE
```

Salida:

```
{
   "registryId": "012345678910",
   "repositoryName": "sample-repo",
   "imageTagMutability": "IMMUTABLE"
}
```

Para obtener más información, consulte Image Tag Mutability en la Guía del usuario de Amazon ECR.

- Para obtener información sobre la API, consulte PutImageTagMutability en la Referencia de comandos de la AWS CLI.

`put-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-image`.

AWS CLI

Para reetiquetar una imagen con su manifiesto

En el siguiente ejemplo de `put-image`, se crea una etiqueta nueva en el repositorio `hello-world` con un manifiesto de imagen existente.

```
aws ecr put-image \
    --repository-name hello-world \
    --image-tag 2019.08 \
    --image-manifest file://hello-world.manifest.json
```

Contenido de `hello-world.manifest.json`:

```
{
    "schemaVersion": 2,
    "mediaType": "application/vnd.docker.distribution.manifest.v2+json",
    "config": {
        "mediaType": "application/vnd.docker.container.image.v1+json",
        "size": 5695,
        "digest":
 "sha256:cea5fe7701b7db3dd1c372f3cea6f43cdda444fcc488f530829145e426d8b980"
    },
    "layers": [
        {
            "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
            "size": 39096921,
            "digest":
 "sha256:d8868e50ac4c7104d2200d42f432b661b2da8c1e417ccfae217e6a1e04bb9295"
        },
        {
            "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
            "size": 57938,
            "digest":
 "sha256:83251ac64627fc331584f6c498b3aba5badc01574e2c70b2499af3af16630eed"
        },
        {
            "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
            "size": 423,
            "digest":
 "sha256:589bba2f1b36ae56f0152c246e2541c5aa604b058febfcf2be32e9a304fec610"
        },
        {
            "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
            "size": 680,
            "digest":
 "sha256:d62ecaceda3964b735cdd2af613d6bb136a52c1da0838b2ff4b4dab4212bcb1c"
        },
        {
            "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
            "size": 162,
            "digest":
 "sha256:6d93b41cfc6bf0d2522b7cf61588de4cd045065b36c52bd3aec2ba0622b2b22b"
        },
        {
            "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
```

```
            "size": 28268840,
            "digest":
 "sha256:6986b4d4c07932c680b3587f2eac8b0e013568c003cc23b04044628a5c5e599f"
        },
        {
            "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
            "size": 35369152,
            "digest":
 "sha256:8c5ec60f10102dc8da0649d866c7c2f706e459d0bdc25c83ad2de86f4996c276"
        },
        {
            "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
            "size": 155,
            "digest":
 "sha256:cde50b1c594539c5f67cbede9aef95c9ae321ccfb857f7b251b45b84198adc85"
        },
        {
            "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
            "size": 28737,
            "digest":
 "sha256:2e102807ab72a73fc9abf53e8c50e421bdc337a0a8afcb242176edeec65977e4"
        },
        {
            "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
            "size": 190,
            "digest":
 "sha256:fc379bbd5ed37808772bef016553a297356c59b8f134659e6ee4ecb563c2f5a7"
        },
        {
            "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
            "size": 28748,
            "digest":
 "sha256:021db240dfccf5a1aff19507d17c0177e5888e518acf295b52204b1825e8b7ee"
        }
    ]
}
```

Salida:

```
{
    "image": {
        "registryId": "130757420319",
        "repositoryName": "hello-world",
```

```
        "imageId": {
            "imageDigest":
 "sha256:8ece96b74f87652876199d83bd107d0435a196133af383ac54cb82b6cc5283ae",
            "imageTag": "2019.08"
        },
        "imageManifest": "{\n  \"schemaVersion\": 2,\n  \"mediaType
\": \"application/vnd.docker.distribution.manifest.v2+json
\",\n  \"config\": {\n    \"mediaType\": \"application/
vnd.docker.container.image.v1+json\",\n    \"size\": 5695,\n    \"digest\":
 \"sha256:cea5fe7701b7db3dd1c372f3cea6f43cdda444fcc488f530829145e426d8b980\"\n
  },\n  \"layers\": [\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 39096921,\n      \"digest
\": \"sha256:d8868e50ac4c7104d2200d42f432b661b2da8c1e417ccfae217e6a1e04bb9295\"\n
  },\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 57938,\n      \"digest
\": \"sha256:83251ac64627fc331584f6c498b3aba5badc01574e2c70b2499af3af16630eed
\"\n    },\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 423,\n      \"digest\":
 \"sha256:589bba2f1b36ae56f0152c246e2541c5aa604b058febfcf2be32e9a304fec610\"\n    },
\n    {\n      \"mediaType\": \"application/vnd.docker.image.rootfs.diff.tar.gzip\",
\n      \"size\": 680,\n      \"digest\":
 \"sha256:d62ecaceda3964b735cdd2af613d6bb136a52c1da0838b2ff4b4dab4212bcb1c
\"\n    },\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 162,\n      \"digest
\": \"sha256:6d93b41cfc6bf0d2522b7cf61588de4cd045065b36c52bd3aec2ba0622b2b22b
\"\n    },\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 28268840,\n      \"digest
\": \"sha256:6986b4d4c07932c680b3587f2eac8b0e013568c003cc23b04044628a5c5e599f
\"\n    },\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 35369152,\n      \"digest
\": \"sha256:8c5ec60f10102dc8da0649d866c7c2f706e459d0bdc25c83ad2de86f4996c276\"\n
  },\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 155,\n      \"digest\":
 \"sha256:cde50b1c594539c5f67cbede9aef95c9ae321ccfb857f7b251b45b84198adc85\"\n    },
\n    {\n      \"mediaType\": \"application/vnd.docker.image.rootfs.diff.tar.gzip\",
\n      \"size\": 28737,\n      \"digest\":
 \"sha256:2e102807ab72a73fc9abf53e8c50e421bdc337a0a8afcb242176edeec65977e4\"\n    },
\n    {\n      \"mediaType\": \"application/vnd.docker.image.rootfs.diff.tar.gzip\",
\n      \"size\": 190,\n      \"digest\":
 \"sha256:fc379bbd5ed37808772bef016553a297356c59b8f134659e6ee4ecb563c2f5a7\"\n    },
\n    {\n      \"mediaType\": \"application/vnd.docker.image.rootfs.diff.tar.gzip\",
\n      \"size\": 28748,\n      \"digest\":
 \"sha256:021db240dfccf5a1aff19507d17c0177e5888e518acf295b52204b1825e8b7ee\"\n
  }\n  ]\n}\n"
```

```
    }
}
```

- Para obtener información sobre la API, consulte PutImage en la Referencia de comandos de la AWS CLI.

`put-lifecycle-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-lifecycle-policy`.

AWS CLI

Para crear una política de ciclo de vida

En el siguiente ejemplo de `put-lifecycle-policy`,se crea una política de ciclo de vida para el repositorio especificado en el registro predeterminado de una cuenta.

```
aws ecr put-lifecycle-policy \
    --repository-name "project-a/amazon-ecs-sample" \
    --lifecycle-policy-text "file://policy.json"
```

Contenido de `policy.json`:

```
{
   "rules": [
       {
           "rulePriority": 1,
           "description": "Expire images older than 14 days",
           "selection": {
               "tagStatus": "untagged",
               "countType": "sinceImagePushed",
               "countUnit": "days",
               "countNumber": 14
           },
           "action": {
               "type": "expire"
           }
       }
   ]
}
```

Salida:

```
{
   "registryId": "<aws_account_id>",
   "repositoryName": "project-a/amazon-ecs-sample",
   "lifecyclePolicyText": "{\"rules\":[{\"rulePriority\":1,\"description\":\"Expire
 images older than 14 days\",\"selection\":{\"tagStatus\":\"untagged\",\"countType
\":\"sinceImagePushed\",\"countUnit\":\"days\",\"countNumber\":14},\"action\":
{\"type\":\"expire\"}}]}"
}
```

Para obtener más información, consulte Lifecycle Policies en la Guía del usuario de Amazon ECR.

- Para obtener información sobre la API, consulte PutLifeCyclePolicy en la Referencia de comandos de la AWS CLI.

`set-repository-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-repository-policy`.

AWS CLI

Para establecer la política de repositorio de un repositorio

En el siguiente ejemplo de `set-repository-policy`, se asocia al repositorio `cluster-autoscaler` una política de repositorio incluida en un archivo.

```
aws ecr set-repository-policy \
    --repository-name cluster-autoscaler \
    --policy-text file://my-policy.json
```

Contenido de `my-policy.json`:

```
{
    "Version":"2012-10-17",
    "Statement" : [
        {
            "Sid" : "allow public pull",
            "Effect" : "Allow",
            "Principal" : "*",
            "Action" : [
                "ecr:BatchCheckLayerAvailability",
                "ecr:BatchGetImage",
```

```
                "ecr:GetDownloadUrlForLayer"
            ]
        }
    ]
}
```

Salida:

```
{
    "registryId": "012345678910",
    "repositoryName": "cluster-autoscaler",
    "policyText": "{\n  \"Version\" : \"2008-10-17\",\n  \"Statement\" : [ {\n
 \"Sid\" : \"allow public pull\",\n    \"Effect\" : \"Allow\",\n    \"Principal\" :
 \"*\",\n    \"Action\" : [ \"ecr:BatchCheckLayerAvailability\", \"ecr:BatchGetImage
\", \"ecr:GetDownloadUrlForLayer\" ]\n  } ]\n}"
}
```

- Para obtener información sobre la API, consulte SetRepositoryPolicy en la Referencia de comandos de la AWS CLI.

`start-image-scan`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-image-scan`.

AWS CLI

Para iniciar un escaneo de vulnerabilidades de imágenes

En el siguiente ejemplo de `start-image-scan`, se inicia un escaneo de imágenes en busca de las imágenes especificadas en el resumen de imágenes del repositorio especificado.

```
aws ecr start-image-scan \
    --repository-name sample-repo \
    --image-
id imageDigest=sha256:74b2c688c700ec95a93e478cdb959737c148df3fbf5ea706abe0318726e885e6
```

Salida:

```
{
   "registryId": "012345678910",
   "repositoryName": "sample-repo",
   "imageId": {
```

```
        "imageDigest":
 "sha256:74b2c688c700ec95a93e478cdb959737c148df3fbf5ea706abe0318726e885e6"
    },
    "imageScanStatus": {
        "status": "IN_PROGRESS"
    }
}
```

Para obtener más información, consulte Image Scanning en la Guía del usuario de Amazon ECR.

- Para obtener información sobre la API, consulte StartImageScan en la Referencia de comandos de la AWS CLI.

`start-lifecycle-policy-preview`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-lifecycle-policy-preview`.

AWS CLI

Para crear una vista previa de política de ciclo de vida

En el siguiente ejemplo de `start-lifecycle-policy-preview` se crea una vista previa de la política de ciclo de vida definida por un archivo JSON para el repositorio especificado.

```
aws ecr start-lifecycle-policy-preview \
    --repository-name "project-a/amazon-ecs-sample" \
    --lifecycle-policy-text "file://policy.json"
```

Contenido de `policy.json`:

```
{
   "rules": [
       {
           "rulePriority": 1,
           "description": "Expire images older than 14 days",
           "selection": {
               "tagStatus": "untagged",
               "countType": "sinceImagePushed",
               "countUnit": "days",
               "countNumber": 14
           },
           "action": {
               "type": "expire"
```

```
            }
        }
    ]
}
```

Salida:

```
{
    "registryId": "012345678910",
    "repositoryName": "project-a/amazon-ecs-sample",
    "lifecyclePolicyText": "{\n    \"rules\": [\n        {\n
 \"rulePriority\": 1,\n            \"description\": \"Expire images older than 14
 days\",\n            \"selection\": {\n                \"tagStatus\": \"untagged\",
\n                \"countType\": \"sinceImagePushed\",\n                \"countUnit
\": \"days\",\n                \"countNumber\": 14\n            },\n
 \"action\": {\n                \"type\": \"expire\"\n            }\n        }\n
  ]\n}\n",
    "status": "IN_PROGRESS"
}
```

- Para obtener información sobre la API, consulte StartLifecyclePolicyPreview en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para etiquetar un repositorio

En el siguiente ejemplo de `tag-resource`, se establece una etiqueta con una clave `Stage` y el valor `Integ` en el repositorio `hello-world`.

```
aws ecr tag-resource \
    --resource-arn arn:aws:ecr:us-west-2:012345678910:repository/hello-world \
    --tags Key=Stage,Value=Integ
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para desetiquetar un repositorio

En el siguiente ejemplo de `untag-resource`, se quita la etiqueta con la clave `Stage` del repositorio `hello-world`.

```
aws ecr untag-resource \
    --resource-arn arn:aws:ecr:us-west-2:012345678910:repository/hello-world \
    --tag-keys Stage
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`upload-layer-part`

En el siguiente ejemplo de código, se muestra cómo utilizar `upload-layer-part`.

AWS CLI

Para cargar una parte de una capa

En el siguiente ejemplo de `upload-layer-part` se carga una parte de una capa de imagen en el repositorio `layer-test`.

```
aws ecr upload-layer-part \
    --repository-name layer-test \
    --upload-id 6cb64b8a-9378-0e33-2ab1-b780fab8a9e9 \
    --part-first-byte 0 \
    --part-last-byte 8323314 \
    --layer-part-blob file:///var/lib/docker/image/overlay2/layerdb/sha256/
ff986b10a018b48074e6d3a68b39aad8ccc002cdad912d4148c0f92b3729323e/layer.b64
```

Salida:

```
{
```

```
    "uploadId": "6cb64b8a-9378-0e33-2ab1-b780fab8a9e9",
    "registryId": "012345678910",
    "lastByteReceived": 8323314,
    "repositoryName": "layer-test"
}
```

- Para obtener información sobre la API, consulte UploadLayerPart en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon ECR Public que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante el uso de la AWS Command Line Interface con Amazon ECR Public.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`batch-delete-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-delete-image`.

AWS CLI

Ejemplo 1: eliminación de una imagen mediante identificadores de resumen de imágenes, la imagen y todas sus etiquetas se eliminan en un repositorio de un registro público

En el siguiente ejemplo de `batch-delete-image`, se elimina una imagen al especificar el resumen de imágenes:

```
aws ecr-public batch-delete-image \
    --repository-name project-a/nginx-web-app \
```

```
    --image-
ids imageDigest=sha256:b1f9deb5fe3711a3278379ebbcaefbc5d70a2263135db86bd27a0dae150546c2
```

Salida:

```
{
"imageIds": [
    {
        "imageDigest":
 "sha256:b1f9deb5fe3711a3278379ebbcaefbc5d70a2263135db86bd27a0dae150546c2",
        "imageTag": "latest"
    }
],
"failures": []
}
```

Para obtener más información, consulte Eliminación de una imagen de un repositorio público en la Guía del usuario de Amazon ECR Public.

Ejemplo 2: eliminación de una imagen al especificar la etiqueta asociada a la imagen que desea eliminar del repositorio.

En el siguiente ejemplo de `batch-delete-image`, se elimina una imagen especificando la etiqueta asociada al repositorio de imágenes denominado `project-a/nginx-web-app` en un registro público. Si solo tiene una etiqueta y ejecuta este comando, se eliminará la imagen. De lo contrario, si tiene varias etiquetas para la misma imagen, especifique una y solo se eliminará la etiqueta del repositorio y no la imagen.

```
aws ecr-public batch-delete-image \
    --repository-name project-a/nginx-web-app \
    --image-ids imageTag=_temp
```

Salida:

```
{
    "imageIds": [
        {
            "imageDigest":
 "sha256:f7a86a0760e2f8d7eff07e515fc87bf4bac45c35376c06f9a280f15ecad6d7e0",
            "imageTag": "_temp"
        }
```

```
    ],
    "failures": []
}
```

Para obtener más información, consulte Eliminación de una imagen de un repositorio público en la Guía del usuario de Amazon ECR Public.

Ejemplo 3: para eliminar varias imágenes, puede especificar varias etiquetas de imagen o resúmenes de imagen en la solicitud para un repositorio en un registro público.

En el siguiente ejemplo de `batch-delete-image`, se eliminan varias imágenes de un repositorio denominado project-a/nginx-web-app al especificar varias etiquetas de imagen o resúmenes de imágenes en la solicitud.

```
aws ecr-public batch-delete-image \
    --repository-name project-a/nginx-web-app \
    --image-ids imageTag=temp2.0
  imageDigest=sha256:47ba980bc055353d9c0af89b1894f68faa43ca93856917b8406316be86f01278
```

Salida:

```
{
     "imageIds": [
         {
             "imageDigest":
 "sha256:47ba980bc055353d9c0af89b1894f68faa43ca93856917b8406316be86f01278"
         },
         {
             "imageDigest":
 "sha256:f7a86a0760e2f8d7eff07e515fc87bf4bac45c35376c06f9a280f15ecad6d7e0",
             "imageTag": "temp2.0"
         }
     ],
     "failures": []
 }
```

Para obtener más información, consulte Eliminación de una imagen de un repositorio público en la Guía del usuario de Amazon ECR Public.

Ejemplo 4: para eliminar una imagen entre cuentas de AWS mediante identificadores de registro e ID de resumen de imágenes, la imagen y todas sus etiquetas se eliminan en un repositorio de un registro público

En el siguiente ejemplo de `batch-delete-image`, se elimina una imagen al especificar el resumen de imágenes entre cuentas de AWS:

```
aws ecr-public batch-delete-image \
    --registry-id 123456789098 \
    --repository-name project-a/nginx-web-app \
    --image-
ids imageDigest=sha256:b1f9deb5fe3711a3278379ebbcaefbc5d70a2263135db86bd27a0dae150546c2
 \
    --region us-east-1
```

Salida:

```
{
    "imageIds": [
        {
            "imageDigest":
 "sha256:b1f9deb5fe3711a3278379ebbcaefbc5d70a2263135db86bd27a0dae150546c2",
            "imageTag": "temp2.0"
        }
    ],
    "failures": []
}
```

Para obtener más información, consulte Eliminación de una imagen de un repositorio público en la Guía del usuario de Amazon ECR Public.

- Para obtener información sobre la API, consulte BatchDeleteImage en la Referencia de comandos de la AWS CLI.

`create-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-repository`.

AWS CLI

Ejemplo 1: creación de un repositorio en un registro público

En el siguiente ejemplo de `create-repository`, se crea un repositorio con el nombre project-a/nginx-web-app en un registro público.

```
aws ecr-public create-repository \
```

```
    --repository-name project-a/nginx-web-app
```

Salida:

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr-public::123456789012:repository/project-a/
nginx-web-app",
        "registryId": "123456789012",
        "repositoryName": "project-a/nginx-web-app",
        "repositoryUri": "public.ecr.aws/public-registry-custom-alias/project-a/
nginx-web-app",
        "createdAt": "2024-07-01T21:08:55.131000+00:00"
    },
    "catalogData": {}
}
```

Para obtener más información, consulte Creating a public repository en la Guía del usuario de Amazon ECR Public.

Ejemplo 2: creación de un repositorio en un registro público con una breve descripción del contenido del repositorio, el sistema y la arquitectura operativa con los que son compatibles las imágenes del repositorio

En el siguiente ejemplo de `create-repository`, se crea un repositorio con el nombre project-a/nginx-web-app en un registro público con una breve descripción del contenido del repositorio, el sistema y la arquitectura operativa con los que son compatibles las imágenes del repositorio.

```
aws ecr-public create-repository \
    --repository-name project-a/nginx-web-app \
    --catalog-data 'description=My project-a ECR Public
 Repository,architectures=ARM,ARM 64,x86,x86-64,operatingSystems=Linux'
```

Salida:

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr-public::123456789012:repository/project-a/
nginx-web-app",
        "registryId": "123456789012",
        "repositoryName": "project-a/nginx-web-app",
```

```
        "repositoryUri": "public.ecr.aws/public-registry-custom-alias/project-a/
nginx-web-app",
        "createdAt": "2024-07-01T21:23:20.455000+00:00"
    },
    "catalogData": {
        "description": "My project-a ECR Public Repository",
        "architectures": [
            "ARM",
            "ARM 64",
            "x86",
            "x86-64"
        ],
        "operatingSystems": [
            "Linux"
        ]
    }
}
```

Para obtener más información, consulte Creating a public repository en la Guía del usuario de Amazon ECR Public.

Ejemplo 3: creación de un repositorio en un registro público, junto con información sobre logoImageBlob, aboutText, usageText y etiquetas

En el siguiente ejemplo de `create-repository`, se crea un repositorio denominado project-a/nginx-web-app en un registro público, junto con información de logoImageBlob, aboutText, usageText y etiquetas.

```
aws ecr-public create-repository \
    --cli-input-json file://myfile.json
```

Contenidos de `myfile.json`:

```
{
    "repositoryName": "project-a/nginx-web-app",
    "catalogData": {
        "description": "My project-a ECR Public Repository",
        "architectures": [
            "ARM",
            "ARM 64",
            "x86",
            "x86-64"
```

```
        ],
        "operatingSystems": [
            "Linux"
        ],
        "logoImageBlob": "iVBORw0KGgoA<<truncated-for-better-reading>>ErkJggg==",
        "aboutText": "## Quick reference\n\nMaintained by: [the Amazon Linux Team]
(https://github.com/aws/amazon-linux-docker-images)\n\nWhere to get help: [the
 Docker Community Forums](https://forums.docker.com/), [the Docker Community Slack]
(https://dockr.ly/slack), or [Stack Overflow](https://stackoverflow.com/search?
tab=newest&q=docker)\n\n## Supported tags and respective `dockerfile` links\n\n*
 [`2.0.20200722.0`, `2`, `latest`](https://github.com/amazonlinux/container-images/
blob/03d54f8c4d522bf712cffd6c8f9aafba0a875e78/Dockerfile)\n* [`2.0.20200722.0-
with-sources`, `2-with-sources`, `with-sources`](https://github.com/
amazonlinux/container-images/blob/1e7349845e029a2e6afe6dc473ef17d052e3546f/
Dockerfile)\n* [`2018.03.0.20200602.1`, `2018.03`, `1`](https://github.com/
amazonlinux/container-images/blob/f10932e08c75457eeb372bf1cc47ea2a4b8e98c8/
Dockerfile)\n* [`2018.03.0.20200602.1-with-sources`, `2018.03-with-sources`,
 `1-with-sources`](https://github.com/amazonlinux/container-images/
blob/8c9ee491689d901aa72719be0ec12087a5fa8faf/Dockerfile)\n\n## What is Amazon
 Linux?\n\nAmazon Linux is provided by Amazon Web Services (AWS). It is designed
 to provide a stable, secure, and high-performance execution environment for
 applications running on Amazon EC2. The full distribution includes packages that
 enable easy integration with AWS, including launch configuration tools and many
 popular AWS libraries and tools. AWS provides ongoing security and maintenance
 updates to all instances running Amazon Linux.\n\nThe Amazon Linux container image
 contains a minimal set of packages. To install additional packages, [use `yum`]
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/managing-software.html).\n\nAWS
 provides two versions of Amazon Linux: [Amazon Linux 2](https://aws.amazon.com/
amazon-linux-2/) and [Amazon Linux AMI](https://aws.amazon.com/amazon-linux-ami/).
\n\nFor information on security updates for Amazon Linux, please refer to [Amazon
 Linux 2 Security Advisories](https://alas.aws.amazon.com/alas2.html) and [Amazon
 Linux AMI Security Advisories](https://alas.aws.amazon.com/). Note that Docker
 Hub's vulnerability scanning for Amazon Linux is currently based on RPM versions,
 which does not reflect the state of backported patches for vulnerabilities.\n
\n## Where can I run Amazon Linux container images?\n\nYou can run Amazon Linux
 container images in any Docker based environment. Examples include, your laptop,
 in Amazon EC2 instances, and Amazon ECS clusters.\n\n## License\n\nAmazon Linux is
 available under the [GNU General Public License, version 2.0](https://github.com/
aws/amazon-linux-docker-images/blob/master/LICENSE). Individual software packages
 are available under their own licenses; run `rpm -qi [package name]` or check
 `/usr/share/doc/[package name]-*` and `/usr/share/licenses/[package name]-*` for
 details.\n\nAs with all Docker images, these likely also contain other software
 which may be under other licenses (such as Bash, etc from the base distribution,
 along with any direct or indirect dependencies of the primary software being
```

```
 contained).\n\nSome additional license information which was able to be auto-
detected might be found in [the `repo-info` repository's `amazonlinux/` directory]
(https://github.com/docker-library/repo-info/tree/master/repos/amazonlinux).\n\n##
 Security\n\nFor information on security updates for Amazon Linux, please refer
 to [Amazon Linux 2 Security Advisories](https://alas.aws.amazon.com/alas2.html)
 and [Amazon Linux AMI Security Advisories](https://alas.aws.amazon.com/). Note
 that Docker Hub's vulnerability scanning for Amazon Linux is currently based
 on RPM versions, which does not reflect the state of backported patches for
 vulnerabilities.",
       "usageText": "## Supported architectures\n\namd64, arm64v8\n\n## Where
 can I run Amazon Linux container images?\n\nYou can run Amazon Linux container
 images in any Docker based environment. Examples include, your laptop, in Amazon
 EC2 instances, and ECS clusters.\n\n## How do I install a software package from
 Extras repository in Amazon Linux 2?\n\nAvailable packages can be listed with the
 `amazon-linux-extras` command. Packages can be installed with the `amazon-linux-
extras install <package>` command. Example: `amazon-linux-extras install rust1`\n
\n## Will updates be available for Amazon Linux containers?\n\nSimilar to the Amazon
 Linux images for Amazon EC2 and on-premises use, Amazon Linux container images will
 get ongoing updates from Amazon in the form of security updates, bug fix updates,
 and other enhancements. Security bulletins for Amazon Linux are available at
 https://alas.aws.amazon.com/\n\n## Will AWS Support the current version of Amazon
 Linux going forward?\n\nYes; in order to avoid any disruption to your existing
 applications and to facilitate migration to Amazon Linux 2, AWS will provide
 regular security updates for Amazon Linux 2018.03 AMI and container image for 2
 years after the final LTS build is announced. You can also use all your existing
 support channels such as AWS Support and Amazon Linux Discussion Forum to continue
 to submit support requests."
    },
    "tags": [
        {
            "Key": "Name",
            "Value": "project-a/nginx-web-app"
        },
        {
            "Key": "Environment",
            "Value": "Prod"
        }
    ]
}
```

Salida:

```
{
```

```
    "repository": {
        "repositoryArn": "arn:aws:ecr-public::123456789012:repository/project-a/
nginx-web-app",
        "registryId": "123456789012",
        "repositoryName": "project-a/nginx-web-app",
        "repositoryUri": "public.ecr.aws/public-registry-custom-alias/project-a/
nginx-web-app",
        "createdAt": "2024-07-01T21:53:05.749000+00:00"
    },
    "catalogData": {
        "description": "My project-a ECR Public Repository",
        "architectures": [
            "ARM",
            "ARM 64",
            "x86",
            "x86-64"
        ],
        "operatingSystems": [
            "Linux"
        ],
        "logoUrl": "https://d3g9o9u8re44ak.cloudfront.net/
logo/23861450-4b9b-403c-9a4c-7aa0ef140bb8/2f9bf5a7-a32f-45b4-b5cd-c5770a35e6d7.png",
        "aboutText": "## Quick reference\n\nMaintained by: [the Amazon Linux Team]
(https://github.com/aws/amazon-linux-docker-images)\n\nWhere to get help: [the
 Docker Community Forums](https://forums.docker.com/), [the Docker Community Slack]
(https://dockr.ly/slack), or [Stack Overflow](https://stackoverflow.com/search?
tab=newest&q=docker)\n\n## Supported tags and respective `dockerfile` links\n\n*
 [`2.0.20200722.0`, `2`, `latest`](https://github.com/amazonlinux/container-images/
blob/03d54f8c4d522bf712cffd6c8f9aafba0a875e78/Dockerfile)\n* [`2.0.20200722.0-
with-sources`, `2-with-sources`, `with-sources`](https://github.com/
amazonlinux/container-images/blob/1e7349845e029a2e6afe6dc473ef17d052e3546f/
Dockerfile)\n* [`2018.03.0.20200602.1`, `2018.03`, `1`](https://github.com/
amazonlinux/container-images/blob/f10932e08c75457eeb372bf1cc47ea2a4b8e98c8/
Dockerfile)\n* [`2018.03.0.20200602.1-with-sources`, `2018.03-with-sources`,
 `1-with-sources`](https://github.com/amazonlinux/container-images/
blob/8c9ee491689d901aa72719be0ec12087a5fa8faf/Dockerfile)\n\n## What is Amazon
 Linux?\n\nAmazon Linux is provided by Amazon Web Services (AWS). It is designed
 to provide a stable, secure, and high-performance execution environment for
 applications running on Amazon EC2. The full distribution includes packages that
 enable easy integration with AWS, including launch configuration tools and many
 popular AWS libraries and tools. AWS provides ongoing security and maintenance
 updates to all instances running Amazon Linux.\n\nThe Amazon Linux container image
 contains a minimal set of packages. To install additional packages, [use `yum`]
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/managing-software.html).\n\nAWS
```

```
 provides two versions of Amazon Linux: [Amazon Linux 2](https://aws.amazon.com/
amazon-linux-2/) and [Amazon Linux AMI](https://aws.amazon.com/amazon-linux-ami/).
\n\nFor information on security updates for Amazon Linux, please refer to [Amazon
 Linux 2 Security Advisories](https://alas.aws.amazon.com/alas2.html) and [Amazon
 Linux AMI Security Advisories](https://alas.aws.amazon.com/). Note that Docker
 Hub's vulnerability scanning for Amazon Linux is currently based on RPM versions,
 which does not reflect the state of backported patches for vulnerabilities.\n
\n## Where can I run Amazon Linux container images?\n\nYou can run Amazon Linux
 container images in any Docker based environment. Examples include, your laptop,
 in Amazon EC2 instances, and Amazon ECS clusters.\n\n## License\n\nAmazon Linux is
 available under the [GNU General Public License, version 2.0](https://github.com/
aws/amazon-linux-docker-images/blob/master/LICENSE). Individual software packages
 are available under their own licenses; run `rpm -qi [package name]` or check
 `/usr/share/doc/[package name]-*` and `/usr/share/licenses/[package name]-*` for
 details.\n\nAs with all Docker images, these likely also contain other software
 which may be under other licenses (such as Bash, etc from the base distribution,
 along with any direct or indirect dependencies of the primary software being
 contained).\n\nSome additional license information which was able to be auto-
detected might be found in [the `repo-info` repository's `amazonlinux/` directory]
(https://github.com/docker-library/repo-info/tree/master/repos/amazonlinux).\n\n##
 Security\n\nFor information on security updates for Amazon Linux, please refer
 to [Amazon Linux 2 Security Advisories](https://alas.aws.amazon.com/alas2.html)
 and [Amazon Linux AMI Security Advisories](https://alas.aws.amazon.com/). Note
 that Docker Hub's vulnerability scanning for Amazon Linux is currently based
 on RPM versions, which does not reflect the state of backported patches for
 vulnerabilities.",
       "usageText": "## Supported architectures\n\namd64, arm64v8\n\n## Where
 can I run Amazon Linux container images?\n\nYou can run Amazon Linux container
 images in any Docker based environment. Examples include, your laptop, in Amazon
 EC2 instances, and ECS clusters.\n\n## How do I install a software package from
 Extras repository in Amazon Linux 2?\n\nAvailable packages can be listed with the
 `amazon-linux-extras` command. Packages can be installed with the `amazon-linux-
extras install <package>` command. Example: `amazon-linux-extras install rust1`\n
\n## Will updates be available for Amazon Linux containers?\n\nSimilar to the Amazon
 Linux images for Amazon EC2 and on-premises use, Amazon Linux container images will
 get ongoing updates from Amazon in the form of security updates, bug fix updates,
 and other enhancements. Security bulletins for Amazon Linux are available at
 https://alas.aws.amazon.com/\n\n## Will AWS Support the current version of Amazon
 Linux going forward?\n\nYes; in order to avoid any disruption to your existing
 applications and to facilitate migration to Amazon Linux 2, AWS will provide
 regular security updates for Amazon Linux 2018.03 AMI and container image for 2
 years after the final LTS build is announced. You can also use all your existing
 support channels such as AWS Support and Amazon Linux Discussion Forum to continue
 to submit support requests."
```

```
    }
}
```

Para obtener más información, consulte Creating a public repository en la Guía del usuario de Amazon ECR Public y Repository catalog data en la Guía del usuario de Amazon ECR Public.

- Para obtener información sobre la API, consulte CreateRepository en la Referencia de comandos de la AWS CLI.

`delete-repository-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-repository-policy`.

AWS CLI

Eliminación de una política de repositorio de un registro público

En el siguiente ejemplo de `delete-repository-policy`, se elimina la política de repositorio del repositorio público de ERC en la cuenta de AWS.

```
aws ecr-public delete-repository-policy \
     --repository-name project-a/nginx-web-app \
     --region us-east-1
```

Salida:

```
{
    "registryId": "123456789012",
    "repositoryName": "project-a/nginx-web-app",
    "policyText": "{\n  \"Version\" : \"2008-10-17\",\n  \"Statement\" : [ {\n
    \"Sid\" : \"AllowPush\",\n    \"Effect\" : \"Allow\",\n    \"Principal
\" : {\n      \"AWS\" : [ \"arn:aws:iam:"123456789012":user/eksuser1\",
 \"arn:aws:iam:"123456789012":user/admin\" ]\n    },\n    \"Action\" :
 [ \"ecr-public:BatchCheckLayerAvailability\", \"ecr-public:PutImage\",
 \"ecr-public:InitiateLayerUpload\", \"ecr-public:UploadLayerPart\", \"ecr-
public:CompleteLayerUpload\" ]\n  } ]\n}"
}
```

Para obtener más información, consulte Eliminación de una instrucción de política de repositorio público en la Guía del usuario de Amazon ECR Public.

- Para obtener información sobre la API, consulte DeleteRepositoryPolicy en la Referencia de comandos de la AWS CLI.

`delete-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-repository`.

AWS CLI

Para eliminar un repositorio de un registro público

En el siguiente ejemplo de `delete-repository`, se elimina un repositorio con el nombre `project-a/nginx-web-app` de su registro público.

```
aws ecr-public delete-repository \
    --repository-name project-a/nginx-web-app
```

Salida:

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr-public::123456789012:repository/project-a/
nginx-web-app",
        "registryId": "123456789012",
        "repositoryName": "project-a/nginx-web-app",
        "repositoryUri": "public.ecr.aws/public-registry-custom-alias/project-a/
nginx-web-app",
        "createdAt": "2024-07-01T22:14:50.103000+00:00"
    }
}
```

Para obtener más información, consulte Eliminación de un repositorio público en Amazon ECR Public.

- Para obtener información sobre la API, consulte DeleteRepository en la Referencia de comandos de la AWS CLI.

`describe-image-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-image-tags`.

AWS CLI

Ejemplo 1: descripción de los detalles de las etiquetas de imagen en un repositorio público

En el siguiente ejemplo de `describe-image-tags`, se describen las etiquetas de imagen del repositorio de muestras de `project-a/nginx-web-app`.

```
aws ecr-public describe-image-tags \
    --repository-name project-a/nginx-web-app \
    --region us-east-1
```

Salida:

```
{
    "imageTagDetails": [
        {
            "imageTag": "latest",
            "createdAt": "2024-07-10T22:29:00-05:00",
            "imageDetail": {
                "imageDigest":
 "sha256:b1f9deb5fe3711a3278379ebbcaefbc5d70a2263135db86bd27a0dae150546c2",
                "imageSizeInBytes": 121956548,
                "imagePushedAt": "2024-07-10T22:29:00-05:00",
                "imageManifestMediaType": "application/
vnd.docker.distribution.manifest.v2+json",
                "artifactMediaType": "application/
vnd.docker.container.image.v1+json"
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeImageTags en la Referencia de comandos de la AWS CLI.

`describe-images`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-images`.

AWS CLI

Ejemplo 1: descripción de imágenes en un repositorio de registro público

En el siguiente ejemplo de `describe-images`, se describen detalles de imágenes en un repositorio con el nombre `project-a/nginx-web-app` en un registro público.

```
aws ecr-public describe-images \
    --repository-name project-a/nginx-web-app \
    --region us-east-1
```

Salida:

```
{
    "imageDetails": [
        {
            "registryId": "123456789012",
            "repositoryName": "project-a/nginx-web-app",
            "imageDigest":
 "sha256:0d8c93e72e82fa070d49565c00af32abbe8ddfd7f75e39f4306771ae0628c7e8",
            "imageTags": [
                "temp1.0"
            ],
            "imageSizeInBytes": 123184716,
            "imagePushedAt": "2024-07-23T11:32:49-05:00",
            "imageManifestMediaType": "application/
vnd.docker.distribution.manifest.v2+json",
            "artifactMediaType": "application/vnd.docker.container.image.v1+json"
        },
        {
            "registryId": "123456789012",
            "repositoryName": "project-a/nginx-web-app",
            "imageDigest":
 "sha256:b1f9deb5fe3711a3278379ebbcaefbc5d70a2263135db86bd27a0dae150546c2",
            "imageTags": [
                "temp2.0"
            ],
            "imageSizeInBytes": 121956548,
            "imagePushedAt": "2024-07-23T11:39:38-05:00",
            "imageManifestMediaType": "application/
vnd.docker.distribution.manifest.v2+json",
            "artifactMediaType": "application/vnd.docker.container.image.v1+json"
        },
        {
            "registryId": "123456789012",
            "repositoryName": "project-a/nginx-web-app",
```

```
            "imageDigest":
 "sha256:f7a86a0760e2f8d7eff07e515fc87bf4bac45c35376c06f9a280f15ecad6d7e0",
            "imageTags": [
                "temp3.0",
                "latest"
            ],
            "imageSizeInBytes": 232108879,
            "imagePushedAt": "2024-07-22T00:54:34-05:00",
            "imageManifestMediaType": "application/
vnd.docker.distribution.manifest.v2+json",
            "artifactMediaType": "application/vnd.docker.container.image.v1+json"
        }
    ]
}
```

Para obtener más información, consulte Descripción de una imagen en un repositorio público en Amazon ECR Public.

Ejemplo 2: descripción de las imágenes del repositorio ordenando imageTags e imagePushedAt

En el siguiente ejemplo de `describe-images`, se describen imágenes de un repositorio con el nombre project-a/nginx-web-app en un registro público.

```
aws ecr-public describe-images \
    --repository-name project-a/nginx-web-app \
    --query 'sort_by(imageDetails,& imagePushedAt)[*].imageTags[*]' \
    --output text
```

Salida:

```
temp3.0 latest
temp1.0
temp2.0
```

Ejemplo 3: descripción de las imágenes del repositorio para generar las dos últimas etiquetas de imagen insertadas en el repositorio

En el siguiente ejemplo de `describe-images`, se obtienen los detalles de las etiquetas de imagen del repositorio con nombre `project-a/nginx-web-app` en un registro público y se consulta el resultado para mostrar solo los dos primeros registros.

```
aws ecr-public describe-images \
```

```
    --repository-name project-a/nginx-web-app  \
    --query 'sort_by(imageDetails,& imagePushedAt)[*].imageTags[*] | [0:2]' \
    --output text
```

Salida:

```
temp3.0 latest
temp1.0
```

- Para obtener información sobre la API, consulte DescribeImages en la Referencia de comandos de la AWS CLI.

`describe-registries`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-registries`.

AWS CLI

Descripción de todos los registros de un registro público

En el siguiente ejemplo de `describe-registries`, se describen todos los registros de la cuenta.

```
aws ecr-public describe-registries
```

Salida:

```
{
 "registries": [
     {
         "registryId": "123456789012",
         "registryArn": "arn:aws:ecr-public::123456789012:registry/123456789012",
         "registryUri": "public.ecr.aws/publicregistrycustomalias",
         "verified": false,
         "aliases": [
             {
                 "name": "publicregistrycustomalias",
                 "status": "ACTIVE",
                 "primaryRegistryAlias": true,
                 "defaultRegistryAlias": true
             }
         ]
```

```
    }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeRegistries en la Referencia de comandos de la AWS CLI.

`describe-repository`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-repository`.

AWS CLI

Ejemplo 1: descripción de un repositorio en un registro público

En el siguiente ejemplo de `describe-repositories`, se describe un repositorio con el nombre `project-a/nginx-web-app` en un registro público.

```
aws ecr-public describe-repositories \
    --repository-name project-a/nginx-web-app
```

Salida:

```
{
    "repositories": [
        {
            "repositoryArn": "arn:aws:ecr-public::123456789012:repository/project-a/
nginx-web-app",
            "registryId": "123456789012",
            "repositoryName": "project-a/nginx-web-app",
            "repositoryUri": "public.ecr.aws/public-registry-custom-alias/project-a/
nginx-web-app",
            "createdAt": "2024-07-07T00:07:56.526000-05:00"
        }
    ]
}
```

Ejemplo 2: descripción de todos los repositorios en un registro público en una tabla

En el siguiente `describe-repositories` ejemplo, se describen todos los repositorios de un registro público y, a continuación, se muestran los nombres de los repositorios en un formato de tabla.

```
aws ecr-public describe-repositories \
    --region us-east-1 \
    --output table \
    --query "repositories[*].repositoryName"
```

Salida:

```
----------------------------
|   DescribeRepositories    |
+---------------------------+
|  project-a/nginx-web-app  |
|  nginx                    |
|  myfirstrepo1             |
|  helm-test-chart          |
|  test-ecr-public          |
|  nginx-web-app            |
|  sample-repo              |
+---------------------------+
```

- Para obtener información sobre la API, consulte DescribeRepository en la Referencia de comandos de la AWS CLI.

`get-authorization-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-authorization-token`.

AWS CLI

Ejemplo 1: recuperación de un token de autorización para cualquier registro público de Amazon ECR al que tenga acceso la entidad principal de IAM

En el siguiente ejemplo de `get-authorization-token`, se obtiene un token de autorización con AWS CLI y se establece en una variable de entorno.

```
aws ecr-public get-authorization-token \
    --region us-east-1
```

Salida:

```
{
    "authorizationData": {
```

```
        "authorizationToken":
 "QVdTOmV5SndZWGxzYjJKJFHDSFKJHERWUY65IOU36TRYEGFNSDLRIUOTUYTHJKLDFGOcmFUQk9OSFV2UVV4a0x6Sm1
        "expiresAt": "2024-07-25T21:37:26.301000-04:00"
    }
}
```

Para obtener más información, consulte Registros públicos de Amazon ECR en Amazon ECR Public.

Ejemplo 2: recuperación de un token de autorización para cualquier registro público de Amazon ECR al que tenga acceso la entidad principal de IAM

En el siguiente ejemplo de `get-authorization-token`, se obtiene un token de autorización con AWS CLI y se establece en una variable de entorno.

```
aws ecr-public get-authorization-token \
    --region us-east-1 \
    --output=text \
    --query 'authorizationData.authorizationToken'
```

Salida:

```
QVdTOmV5SndZWGxzYjJKJFHDSFKJHERWUY65IOU36TRYEGFNSDLRIUOTUYTHJKLDFGOcmFUQk9OSFV2UVV4a0x6Sm1ZV
```

Para obtener más información, consulte Registros públicos de Amazon ECR en Amazon ECR Public.

- Para obtener información sobre la API, consulte GetAuthorizationToken en la Referencia de comandos de la AWS CLI.

`get-login-password`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-login-password`.

AWS CLI

Ejemplo 1: autenticación docker en un registro público de Amazon ECR

En el siguiente ejemplo de `get-login-password`, se recupera y muestra un token de autenticación mediante la API GetAuthorizationToken que puede usar para autenticarse en un registro público de Amazon ECR.

```
aws ecr-public get-login-password \
    --region us-
east-1
| docker login \
    --username AWS \
    --password-stdin public.ecr.aws
```

Este comando no produce ningún resultado en el terminal, sino que lo canaliza a Docker.

Para obtener más información, consulte Authenticate to the public registry de Amazon ECR Public.

Ejemplo 2: autenticación docker en el propio registro público personalizado de AmazonECR

En el siguiente ejemplo de `get-login-password`, se recupera y muestra un token de autenticación mediante la API GetAuthorizationToken, que puede usar para autenticarse en su propio registro público de Amazon ECR personalizado.

```
 aws ecr-public get-login-password \
    --region us-east-1 \
| docker login \
    --username AWS \
    --password-stdin public.ecr.aws/<your-public-registry-custom-alias>
```

Este comando no produce ningún resultado en el terminal, sino que lo canaliza a Docker.

Para obtener más información, consulte Autenticarse en su propio Amazon ECR Public en Amazon ECR Public.

- Para obtener información sobre la API, consulte GetLoginPassword en la Referencia de comandos de la AWS CLI.

`get-registry-catalog-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-registry-catalog-data`.

AWS CLI

Recuperación de los metadatos del catálogo para un registro de ECR público

El siguiente `get-registry-catalog-data` recupera los metadatos del catálogo para un registro de ECR público.

```
aws ecr-public get-registry-catalog-data \
    --region us-east-1
```

Salida:

```
{
    "registryCatalogData": {
        "displayName": "YourCustomPublicRepositoryalias"
    }
}
```

- Para obtener información sobre la API, consulte GetRegistryCatalogData en la Referencia de comandos de la AWS CLI.

`get-repository-catalog-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-repository-catalog-data`.

AWS CLI

Recuperación de los metadatos del catálogo para un repositorio en un registro público

En el siguiente ejemplo de `get-repository-catalog-data`, se muestran los metadatos del catálogo del repositorio `project-a/nginx-web-app` en un registro público.

```
aws ecr-public get-repository-catalog-data \
    --repository-name project-a/nginx-web-app \
    --region us-east-1
```

Salida:

```
{
    "catalogData": {
        "description": "My project-a ECR Public Repository",
        "architectures": [
            "ARM",
            "ARM 64",
            "x86",
            "x86-64"
        ],
        "operatingSystems": [
```

```
            "Linux"
        ],
        "logoUrl": "https://d3g9o9u8re44ak.cloudfront.net/logo/491d3846-8f33-4d8b-
a10c-c2ce271e6c0d/4f09d87c-2569-4916-a932-5c296bf6f88a.png",
        "aboutText": "## Quick reference\n\nMaintained <truncated>",
        "usageText": "## Supported architectures\n\namd64, arm64v8\n\n##
 <truncated>"
    }
}
```

Para obtener más información, consulte los Datos del catálogo del repositorio en Amazon ECR Public.

- Para obtener información sobre la API, consulte GetRepositoryCatalogData en la Referencia de comandos de la AWS CLI.

`get-repository-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-repository-policy`.

AWS CLI

Obtención de una política de repositorio asociada al repositorio

En el siguiente ejemplo de `get-repository-policy`, se obtiene una política de repositorio asociada al repositorio.

```
aws ecr-public get-repository-policy \
    --repository-name project-a/nginx-web-app \
    --region us-east-1
```

Salida:

```
{
    "registryId": "123456789012",
    "repositoryName": "project-a/nginx-web-app",
    "policyText": "{\n  \"Version\" : \"2008-10-17\",\n  \"Statement\" : [ {\n
    \"Sid\" : \"AllowPush\",\n    \"Effect\" : \"Allow\",\n    \"Principal
\" : {\n      \"AWS\" : [ \"arn:aws:iam::123456789012:user/eksuser1\",
 \"arn:aws:iam::123456789012:user/admin\" ]\n    },\n    \"Action\" :
 [ \"ecr-public:BatchCheckLayerAvailability\", \"ecr-public:PutImage\",
 \"ecr-public:InitiateLayerUpload\", \"ecr-public:UploadLayerPart\", \"ecr-
public:CompleteLayerUpload\" ]\n  } ]\n}"
```

```
}
```

Para obtener más información, consulte Uso de GetRepositoryPolicy con un AWS SDK o CLI en la Guía de usuario de Amazon ECR Public.

- Para obtener información sobre la API, consulte GetRepositoryPolicy en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Muestra de etiquetas de un repositorio público en un registro público

En el siguiente ejemplo de `list-tags-for-resource`, se muestran las etiquetas de un recurso denominado `project-a/nginx-web-app` en un registro público.

```
aws ecr-public list-tags-for-resource \
    --resource-arn arn:aws:ecr-public::123456789012:repository/project-a/nginx-web-app \
    --region us-east-1
```

Salida:

```
{
    "tags": [
        {
            "Key": "Environment",
            "Value": "Prod"
        },
        {
            "Key": "stack",
            "Value": "dev1"
        },
        {
            "Key": "Name",
            "Value": "project-a/nginx-web-app"
        }
    ]
}
```

Para obtener más información, consulte Muestra de etiquetas para un repositorio público en Amazon ECR Public.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-registry-catalog-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-registry-catalog-data`.

AWS CLI

Creación o actualización de los metadatos del catálogo de un registro de ECR público

El siguiente `put-registry-catalog-data` crea o actualiza los metadatos del catálogo para un registro de ECR público. Solo las cuentas que tengan el distintivo de cuenta verificada pueden tener un nombre para mostrar de registro.

```
aws ecr-public put-registry-catalog-data \
    --region us-east-1 \
    --display-name <YourCustomPublicRepositoryalias>
```

Salida:

```
{
    "registryCatalogData": {
        "displayName": "YourCustomPublicRepositoryalias"
    }
}
```

- Para obtener información sobre la API, consulte PutRegistryCatalogData en la Referencia de comandos de la AWS CLI.

`put-repository-catalog-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-repository-catalog-data`.

AWS CLI

Creación o actualización de los datos del catálogo de un repositorio en un registro público

En el siguiente ejemplo de `put-repository-catalog-data`, se crean o actualizan datos del catálogo para un repositorio denominado project-a/nginx-web-app en un registro público, junto con información de logoImageBlob, aboutText, usageText y etiquetas.

```
aws ecr-public put-repository-catalog-data \
    --repository-name project-a/nginx-web-app \
    --cli-input-json file://repository-catalog-data.json \
    --region us-east-1
```

Contenido de `repository-catalog-data.json`:

```
{
    "repositoryName": "project-a/nginx-web-app",
    "catalogData": {
        "description": "My project-a ECR Public Repository",
        "architectures": [
            "ARM",
            "ARM 64",
            "x86",
            "x86-64"
        ],
        "operatingSystems": [
            "Linux"
        ],
        "logoImageBlob": "iVBORw0KGgoA<<truncated-for-better-reading>>ErkJggg==",
        "aboutText": "## Quick reference.",
        "usageText": "## Supported architectures are as follows."
    }
}
```

Salida:

```
{
    "catalogData": {
        "description": "My project-a ECR Public Repository",
        "architectures": [
            "ARM",
            "ARM 64",
            "x86",
            "x86-64"
        ],
        "operatingSystems": [
```

```
            "Linux"
        ],
        "logoUrl": "https://d3g9o9u8re44ak.cloudfront.net/logo/df86cf58-ee60-4061-
b804-0be24d97ccb1/4a9ed9b2-69e4-4ede-b924-461462d20ef0.png",
        "aboutText": "## Quick reference.",
        "usageText": "## Supported architectures are as follows."
    }
}
```

Para obtener más información, consulte los Datos del catálogo del repositorio en Amazon ECR Public.

- Para obtener información sobre la API, consulte PutRepositoryCatalogData en la Referencia de comandos de la AWS CLI.

`set-repository-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-repository-policy`.

AWS CLI

Ejemplo 1: establecimiento de una política de repositorio que permita extraer información del repositorio

En el siguiente ejemplo de `set-repository-policy`, se aplica una política de repositorio público de ECR al repositorio especificado para controlar los permisos de acceso.

```
aws ecr-public set-repository-policy \
    --repository-name project-a/nginx-web-app \
    --policy-text file://my-repository-policy.json
```

Contenido de `my-repository-policy.json`:

```
{
    "Version":"2012-10-17",
    "Statement" : [
        {
            "Sid" : "allow public pull",
            "Effect" : "Allow",
            "Principal" : "*",
            "Action" : [
                "ecr:BatchCheckLayerAvailability",
```

```
                "ecr:BatchGetImage",
                "ecr:GetDownloadUrlForLayer"
            ]
        }
    ]
}
```

Salida:

```
{
    "registryId": "12345678901",
    "repositoryName": "project-a/nginx-web-app",
    "policyText": "{\n  \"Version\" : \"2008-10-17\",\n  \"Statement\" : [ {\n
 \"Sid\" : \"allow public pull\",\n    \"Effect\" : \"Allow\",\n    \"Principal\" :
 \"*\",\n    \"Action\" : [ \"ecr:BatchCheckLayerAvailability\", \"ecr:BatchGetImage
\", \"ecr:GetDownloadUrlForLayer\" ]\n  } ]\n}"
}
```

Para obtener más información, consulte Establecimiento de una instrucción de política de repositorio en la Guía del usuario de Amazon ECR Public.

Ejemplo 2: establecimiento de una política de repositorio que permita a un usuario de IAM de la cuenta insertar imágenes

En el siguiente ejemplo de `set-repository-policy`, se permite a un usuario de IAM de la cuenta insertar imágenes mediante un repositorio de ECR de la cuenta de AWS con el archivo de entrada denominado `file://my-repository-policy.json` como texto de la política.

```
aws ecr-public set-repository-policy \
    --repository-name project-a/nginx-web-app \
    --policy-text file://my-repository-policy.json
```

Contenido de `my-repository-policy.json`:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPush",
            "Effect": "Allow",
            "Principal": {
```

```
                "AWS": [
                    "arn:aws:iam::account-id:user/push-pull-user-1",
                    "arn:aws:iam::account-id:user/push-pull-user-2"
                ]
            },
            "Action": [
                "ecr-public:BatchCheckLayerAvailability",
                "ecr-public:PutImage",
                "ecr-public:InitiateLayerUpload",
                "ecr-public:UploadLayerPart",
                "ecr-public:CompleteLayerUpload"
            ]
        }
    ]
}
```

Salida:

```
{
    "registryId": "12345678901",
    "repositoryName": "project-a/nginx-web-app",
    "policyText": "{\n  \"Version\" : \"2008-10-17\",\n  \"Statement\" :
 [ {\n    \"Sid\" : \"AllowPush\",\n    \"Effect\" : \"Allow\",\n
 \"Principal\" : {\n      \"AWS\" : [ \"arn:aws:iam::12345678901:user/admin
\", \"arn:aws:iam::12345678901:user/eksuser1\" ]\n    },\n    \"Action\" :
 [ \"ecr-public:BatchCheckLayerAvailability\", \"ecr-public:PutImage\",
 \"ecr-public:InitiateLayerUpload\", \"ecr-public:UploadLayerPart\", \"ecr-
public:CompleteLayerUpload\" ]\n  } ]\n}"
}
```

Para obtener más información, consulte Establecimiento de una instrucción de política de repositorio en la Guía del usuario de Amazon ECR Public.

Ejemplo 3: establecimiento de una política de repositorio que permita a un usuario de IAM de la cuenta diferente insertar imágenes

En el siguiente ejemplo de `set-repository-policy`, se permite que una cuenta específica inserte imágenes mediante la entrada de la CLI file://my-repository-policy.json en la cuenta de AWS.

```
aws ecr-public set-repository-policy \
    --repository-name project-a/nginx-web-app \
```

```
    --policy-text file://my-repository-policy.json
```

Contenido de `my-repository-policy.json`:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCrossAccountPush",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::other-or-same-account-id:role/RoleName"
            },
            "Action": [
                "ecr-public:BatchCheckLayerAvailability",
                "ecr-public:PutImage",
                "ecr-public:InitiateLayerUpload",
                "ecr-public:UploadLayerPart",
                "ecr-public:CompleteLayerUpload"
            ]
        }
    ]
}
```

Salida:

```
{
    "registryId": "12345678901",
    "repositoryName": "project-a/nginx-web-app",
    "policyText": "{\n  \"Version\" : \"2008-10-17\",\n  \"Statement\" : [ {\n
 \"Sid\" : \"AllowCrossAccountPush\",\n    \"Effect\" : \"Allow\",\n    \"Principal
\" : {\n      \"AWS\" : \"arn:aws:iam::12345678901:role/RoleName\"\n    },\n
 \"Action\" : [ \"ecr-public:BatchCheckLayerAvailability\", \"ecr-public:PutImage
\", \"ecr-public:InitiateLayerUpload\", \"ecr-public:UploadLayerPart\", \"ecr-
public:CompleteLayerUpload\" ]\n  } ]\n}"
}
```

Para obtener más información, consulte Ejemplos de políticas de repositorio público en la Guía del usuario de Amazon ECR Public.

- Para obtener información sobre la API, consulte SetRepositoryPolicy en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Ejemplo 1: etiquetado de un repositorio público existente en un registro público

En el siguiente ejemplo de `tag-resource`, se etiqueta un repositorio con el nombre `project-a/nginx-web-app` en un registro público.

```
aws ecr-public tag-resource \
    --resource-arn arn:aws:ecr-public::123456789012:repository/project-a/nginx-web-app \
    --tags Key=stack,Value=dev \
    --region us-east-1
```

Para obtener más información, consulte Uso de etiquetas para un repositorio público en Amazon ECR Public.

Ejemplo 2: etiquetado de un repositorio público existente con varias etiquetas en un registro público.

En el siguiente ejemplo de `tag-resource`, se etiqueta un repositorio existente con varias etiquetas.

```
aws ecr-public tag-resource \
    --resource-arn arn:aws:ecr-public::890517186334:repository/project-a/nginx-web-app  \
    --tags Key=key1,Value=value1 Key=key2,Value=value2 Key=key3,Value=value3 \
    --region us-east-1
```

Para obtener más información, consulte Uso de etiquetas para un repositorio público en Amazon ECR Public.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Ejemplo 1: eliminación de etiquetas de un repositorio público existente en un registro público

En el siguiente ejemplo de `untag-resource`, se etiqueta un repositorio con el nombre `project-a/nginx-web-app` en un registro público.

```
aws ecr-public untag-resource \
    --resource-arn arn:aws:ecr-public::123456789012:repository/project-a/nginx-web-app \
    --tag-keys stack \
    --region us-east-1
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de etiquetas para un repositorio público en Amazon ECR Public.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon ECS que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon ECS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`capacity-provider-update`

En el siguiente ejemplo de código, se muestra cómo utilizar `capacity-provider-update`.

AWS CLI

Actualización del proveedor de capacidad en un clúster de ECS

En el siguiente ejemplo de `update-capacity-provider`, se muestra cómo podemos modificar los parámetros del proveedor de capacidad en un clúster de ECS.

```
aws ecs update-capacity-provider \
    --name Infra-ECS-Cluster-ECS-project-update-cluster-d6bb6d5b-
EC2CapacityProvider-3fIpdkLywwFt \
    --auto-scaling-group-
provider "managedScaling={status=DISABLED,targetCapacity=50,minimumScalingStepSize=2,maximum
```

Salida:

```
{
    "capacityProvider": {
        "capacityProviderArn": "arn:aws:ecs:us-west-2:123456789012:capacity-
provider/Infra-ECS-Cluster-ECS-project-update-cluster-d6bb6d5b-
EC2CapacityProvider-3fIpdkLywwFt",
        "name": "Infra-ECS-Cluster-ECS-project-update-cluster-d6bb6d5b-
EC2CapacityProvider-3fIpdkLywwFt",
        "status": "ACTIVE",
        "autoScalingGroupProvider": {
            "autoScalingGroupArn": "arn:aws:autoscaling:us-
west-2:123456789012:autoScalingGroup:424941d1-b43f-4a17-
adbb-08b6a6e397e1:autoScalingGroupName/Infra-ECS-Cluster-ECS-project-update-cluster-
d6bb6d5b-ECSAutoScalingGroup-f44jrQHS2nRB",
            "managedScaling": {
                "status": "ENABLED",
                "targetCapacity": 100,
                "minimumScalingStepSize": 1,
                "maximumScalingStepSize": 10000,
                "instanceWarmupPeriod": 300
            },
            "managedTerminationProtection": "DISABLED",
            "managedDraining": "ENABLED"
        },
        "updateStatus": "UPDATE_IN_PROGRESS",
        "tags": []
    }
}
```

Para obtener más información sobre el proveedor de capacidad, consulte Amazon ECS capacity providers for the EC2 launch type en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte CapacityProviderUpdate en la Referencia de comandos de la AWS CLI.

`create-capacity-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-capacity-provider`.

AWS CLI

Para crear un proveedor de capacidad

En el siguiente ejemplo de create-capacity-provider se crea un proveedor de capacidad que utiliza el grupo de escalado automático MyASG, que tiene habilitados el escalado administrado y la protección contra terminación administrada. Esta configuración se utiliza para el escalado automático del clúster de Amazon ECS.

```
aws ecs create-capacity-provider \
    --name "MyCapacityProvider" \
    --auto-scaling-group-provider "autoScalingGroupArn=arn:aws:autoscaling:us-
east-1:123456789012:autoScalingGroup:57ffcb94-11f0-4d6d-
bf60-3bac5EXAMPLE:autoScalingGroupName/
MyASG,managedScaling={status=ENABLED,targetCapacity=100},managedTerminationProtection=ENABLE
```

Salida:

```
{
    "capacityProvider": {
    "capacityProviderArn": "arn:aws:ecs:us-east-1:123456789012:capacity-provider/
MyCapacityProvider",
    "name": "MyCapacityProvider",
    "status": "ACTIVE",
    "autoScalingGroupProvider": {
        "autoScalingGroupArn": "arn:aws:autoscaling:us-
east-1:132456789012:autoScalingGroup:57ffcb94-11f0-4d6d-
bf60-3bac5EXAMPLE:autoScalingGroupName/MyASG",
        "managedScaling": {
            "status": "ENABLED",
            "targetCapacity": 100,
            "minimumScalingStepSize": 1,
```

```
            "maximumScalingStepSize": 10000,
            "instanceWarmupPeriod": 300
        },
        "managedTerminationProtection": "ENABLED"
    },
    "tags": []
}
```

Para obtener más información, consulte Administración automática de la capacidad de Amazon ECS con el escalado automático de clústeres en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte CreateCapacityProvider en la Referencia de comandos de la AWS CLI.

`create-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-cluster`.

AWS CLI

Ejemplo 1: creación de un clúster nuevo

En el siguiente ejemplo de `create-cluster`, se crea un clúster denominado `MyCluster` y habilita información de contenedores de CloudWatch con observabilidad mejorada.

```
aws ecs create-cluster \
    --cluster-name MyCluster \
    --settings name=containerInsights,value=enhanced
```

Salida:

```
{
    "cluster": {
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster",
        "clusterName": "MyCluster",
        "status": "ACTIVE",
        "registeredContainerInstancesCount": 0,
        "pendingTasksCount": 0,
        "runningTasksCount": 0,
        "activeServicesCount": 0,
        "statistics": [],
        "settings": [
            {
```

```
                "name": "containerInsights",
                "value": "enhanced"
            }
        ],
        "tags": []
    }
}
```

Para obtener más información, consulte Creación de un clúster en la Guía para desarrolladores de Amazon ECS.

Ejemplo 2: creación de un clúster nuevo con proveedores de capacidad

En el siguiente ejemplo de `create-cluster` se crea un clúster y se le asocian dos proveedores de capacidad existentes. El comando `create-capacity-provider` se utiliza para crear un proveedor de capacidad. La especificación de una estrategia predeterminada de proveedor de capacidad es opcional, pero se recomienda. En este ejemplo, creamos un clúster denominado `MyCluster` y le asociamos los proveedores de capacidad `MyCapacityProvider1` y `MyCapacityProvider2`. Se especifica una estrategia predeterminada de proveedor de capacidad que distribuye las tareas de manera uniforme entre ambos proveedores de capacidad.

```
aws ecs create-cluster \
    --cluster-name MyCluster \
    --capacity-providers MyCapacityProvider1 MyCapacityProvider2 \
    --default-capacity-provider-
strategy capacityProvider=MyCapacityProvider1,weight=1 capacityProvider=MyCapacityProvider2,
```

Salida:

```
{
    "cluster": {
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster",
        "clusterName": "MyCluster",
        "status": "PROVISIONING",
        "registeredContainerInstancesCount": 0,
        "pendingTasksCount": 0,
        "runningTasksCount": 0,
        "activeServicesCount": 0,
        "statistics": [],
        "settings": [
            {
                "name": "containerInsights",
```

```
                "value": "enabled"
            }
        ],
        "capacityProviders": [
            "MyCapacityProvider1",
            "MyCapacityProvider2"
        ],
        "defaultCapacityProviderStrategy": [
            {
                "capacityProvider": "MyCapacityProvider1",
                "weight": 1,
                "base": 0
            },
            {
                "capacityProvider": "MyCapacityProvider2",
                "weight": 1,
                "base": 0
            }
        ],
        "attachments": [
           {
               "id": "0fb0c8f4-6edd-4de1-9b09-17e470ee1918",
               "type": "asp",
               "status": "PRECREATED",
               "details": [
                   {
                       "name": "capacityProviderName",
                       "value": "MyCapacityProvider1"
                   },
                   {
                       "name": "scalingPlanName",
                       "value": "ECSManagedAutoScalingPlan-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
                   }
               ]
            },
            {
                "id": "ae592060-2382-4663-9476-b015c685593c",
                "type": "asp",
                "status": "PRECREATED",
                "details": [
                    {
                        "name": "capacityProviderName",
                        "value": "MyCapacityProvider2"
```

```
                    },
                    {
                        "name": "scalingPlanName",
                        "value": "ECSManagedAutoScalingPlan-a1b2c3d4-5678-90ab-cdef-
EXAMPLE22222"
                    }
                ]
            }
        ],
        "attachmentsStatus": "UPDATE_IN_PROGRESS"
    }
}
```

Para obtener más información, consulte Proveedores de capacidad de clúster en la Guía para desarrolladores de Amazon ECS.

Ejemplo 3: creación de un clúster nuevo con varias etiquetas

En el siguiente ejemplo de `create-cluster` se crea un clúster con varias etiquetas. Para obtener más información sobre cómo añadir etiquetas mediante la sintaxis abreviada, consulte Uso de sintaxis abreviada con la interfaz de línea de comandos de AWS en la Guía del usuario de AWS CLI.

```
aws ecs create-cluster \
    --cluster-name MyCluster \
    --tags key=key1,value=value1 key=key2,value=value2
```

Salida:

```
{
    "cluster": {
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster",
        "clusterName": "MyCluster",
        "status": "ACTIVE",
        "registeredContainerInstancesCount": 0,
        "pendingTasksCount": 0,
        "runningTasksCount": 0,
        "activeServicesCount": 0,
        "statistics": [],
        "tags": [
            {
                "key": "key1",
```

```
                "value": "value1"
            },
            {
                "key": "key2",
                "value": "value2"
            }
        ]
    }
}
```

Para obtener más información, consulte Creación de un clúster en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte CreateCluster en la Referencia de comandos de la AWS CLI.

`create-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-service`.

AWS CLI

Ejemplo 1: creación de un servicio con una tarea de Fargate

En el siguiente ejemplo de `create-service` se muestra cómo crear un servicio mediante una tarea de Fargate.

```
aws ecs create-service \
    --cluster MyCluster \
    --service-name MyService \
    --task-definition sample-fargate:1 \
    --desired-count 2 \
    --launch-type FARGATE \
    --platform-version LATEST \
    --network-configuration
 'awsvpcConfiguration={subnets=[subnet-12344321],securityGroups=[sg-12344321],assignPublicIp
 \
    --tags key=key1,value=value1 key=key2,value=value2 key=key3,value=value3
```

Salida:

```
{
    "service": {
```

```
        "serviceArn": "arn:aws:ecs:us-west-2:123456789012:service/MyCluster/
MyService",
        "serviceName": "MyService",
          "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster",
        "loadBalancers": [],
        "serviceRegistries": [],
        "status": "ACTIVE",
        "desiredCount": 2,
        "runningCount": 0,
        "pendingCount": 0,
        "launchType": "FARGATE",
        "platformVersion": "LATEST",
        "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-definition/
sample-fargate:1",
        "deploymentConfiguration": {
            "maximumPercent": 200,
            "minimumHealthyPercent": 100
        },
        "deployments": [
            {
                "id": "ecs-svc/1234567890123456789",
                "status": "PRIMARY",
                "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-
definition/sample-fargate:1",
                "desiredCount": 2,
                "pendingCount": 0,
                "runningCount": 0,
                "createdAt": 1557119253.821,
                "updatedAt": 1557119253.821,
                "launchType": "FARGATE",
                "platformVersion": "1.3.0",
                "networkConfiguration": {
                    "awsvpcConfiguration": {
                        "subnets": [
                            "subnet-12344321"
                        ],
                        "securityGroups": [
                            "sg-12344321"
                        ],
                        "assignPublicIp": "ENABLED"
                    }
                }
            }
        ],
```

```
        "roleArn": "arn:aws:iam::123456789012:role/aws-service-role/
ecs.amazonaws.com/AWSServiceRoleForECS",
        "events": [],
        "createdAt": 1557119253.821,
        "placementConstraints": [],
        "placementStrategy": [],
        "networkConfiguration": {
            "awsvpcConfiguration": {
                "subnets": [
                    "subnet-12344321"
                ],
                "securityGroups": [
                    "sg-12344321"
                ],
                "assignPublicIp": "ENABLED"
            }
        },
        "schedulingStrategy": "REPLICA",
        "tags": [
            {
                "key": "key1",
                "value": "value1"
            },
            {
                "key": "key2",
                "value": "value2"
            },
            {
                "key": "key3",
                "value": "value3"
            }
        ],
        "enableECSManagedTags": false,
        "propagateTags": "NONE"
    }
}
```

Para obtener más información, consulte Creación de un servicio en la Guía para desarrolladores de Amazon ECS.

Ejemplo 2: creación de un servicio mediante el tipo de lanzamiento EC

En el siguiente ejemplo de `create-service` se muestra cómo crear un servicio llamado `ecs-simple-service` con una tarea que utiliza el tipo de lanzamiento de EC2. El servicio utiliza la definición de la tarea `sleep360` y mantiene 1 instancia de la tarea.

```
aws ecs create-service \
    --cluster MyCluster \
    --service-name ecs-simple-service \
    --task-definition sleep360:2 \
    --desired-count 1
```

Salida:

```
{
    "service": {
        "serviceArn": "arn:aws:ecs:us-west-2:123456789012:service/MyCluster/ecs-
simple-service",
        "serviceName": "ecs-simple-service",
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster",
        "loadBalancers": [],
        "serviceRegistries": [],
        "status": "ACTIVE",
        "desiredCount": 1,
        "runningCount": 0,
        "pendingCount": 0,
        "launchType": "EC2",
        "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-definition/
sleep360:2",
        "deploymentConfiguration": {
            "maximumPercent": 200,
            "minimumHealthyPercent": 100
        },
        "deployments": [
            {
                "id": "ecs-svc/1234567890123456789",
                "status": "PRIMARY",
                "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-
definition/sleep360:2",
                "desiredCount": 1,
                "pendingCount": 0,
                "runningCount": 0,
                "createdAt": 1557206498.798,
                "updatedAt": 1557206498.798,
                "launchType": "EC2"
```

```
            }
        ],
        "events": [],
        "createdAt": 1557206498.798,
        "placementConstraints": [],
        "placementStrategy": [],
        "schedulingStrategy": "REPLICA",
        "enableECSManagedTags": false,
        "propagateTags": "NONE"
    }
}
```

Para obtener más información, consulte Creación de un servicio en la Guía para desarrolladores de Amazon ECS.

Ejemplo 3: creación de un servicio que utilice un controlador de implementación externo

En el siguiente ejemplo de `create-service` se crea un servicio que utiliza un controlador de implementación externo.

```
aws ecs create-service \
    --cluster MyCluster \
    --service-name MyService \
    --deployment-controller type=EXTERNAL \
    --desired-count 1
```

Salida:

```
{
    "service": {
        "serviceArn": "arn:aws:ecs:us-west-2:123456789012:service/MyCluster/
MyService",
        "serviceName": "MyService",
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster",
        "loadBalancers": [],
        "serviceRegistries": [],
        "status": "ACTIVE",
        "desiredCount": 1,
        "runningCount": 0,
        "pendingCount": 0,
        "launchType": "EC2",
        "deploymentConfiguration": {
```

```
            "maximumPercent": 200,
            "minimumHealthyPercent": 100
        },
        "taskSets": [],
        "deployments": [],
        "roleArn": "arn:aws:iam::123456789012:role/aws-service-role/
ecs.amazonaws.com/AWSServiceRoleForECS",
        "events": [],
        "createdAt": 1557128207.101,
        "placementConstraints": [],
        "placementStrategy": [],
        "schedulingStrategy": "REPLICA",
        "deploymentController": {
            "type": "EXTERNAL"
        },
        "enableECSManagedTags": false,
        "propagateTags": "NONE"
    }
}
```

Para obtener más información, consulte Creación de un servicio en la Guía para desarrolladores de Amazon ECS.

Ejemplo 4: creación de un nuevo servicio detrás de un equilibrador de carga

En el siguiente ejemplo de `create-service` se muestra cómo crear un servicio que se encuentra detrás de un equilibrador de carga. Debe tener un equilibrador de carga configurado en la misma región que la instancia de contenedor. En este ejemplo se utiliza la opción `--cli-input-json` y un archivo de entrada JSON llamado `ecs-simple-service-elb.json` con el siguiente contenido.

```
aws ecs create-service \
    --cluster MyCluster \
    --service-name ecs-simple-service-elb \
    --cli-input-json file://ecs-simple-service-elb.json
```

Contenido de `ecs-simple-service-elb.json`:

```
 {
    "serviceName": "ecs-simple-service-elb",
    "taskDefinition": "ecs-demo",
    "loadBalancers": [
```

```
        {
            "loadBalancerName": "EC2Contai-EcsElast-123456789012",
            "containerName": "simple-demo",
            "containerPort": 80
        }
    ],
    "desiredCount": 10,
    "role": "ecsServiceRole"
}
```

Salida:

```
{
    "service": {
        "status": "ACTIVE",
        "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-definition/ecs-
demo:1",
        "pendingCount": 0,
        "loadBalancers": [
            {
                "containerName": "ecs-demo",
                "containerPort": 80,
                "loadBalancerName": "EC2Contai-EcsElast-123456789012"
            }
        ],
        "roleArn": "arn:aws:iam::123456789012:role/ecsServiceRole",
        "desiredCount": 10,
        "serviceName": "ecs-simple-service-elb",
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster",
        "serviceArn": "arn:aws:ecs:us-west-2:123456789012:service/ecs-simple-
service-elb",
        "deployments": [
            {
                "status": "PRIMARY",
                "pendingCount": 0,
                "createdAt": 1428100239.123,
                "desiredCount": 10,
                "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-
definition/ecs-demo:1",
                "updatedAt": 1428100239.123,
                "id": "ecs-svc/1234567890123456789",
                "runningCount": 0
            }
```

```
        ],
        "events": [],
        "runningCount": 0
    }
}
```

Para obtener más información, consulte Uso del equilibrio de carga para distribuir el tráfico de servicios de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

Ejemplo 5: configuración de los volúmenes de Amazon EBS al crear servicios

En el siguiente ejemplo de `create-service` se muestra cómo configurar los volúmenes de Amazon EBS para cada tarea administrada por el servicio. Debe tener configurado un rol de infraestructura de Amazon ECS con la política administrada por `AmazonECSInfrastructureRolePolicyForVolumes` asociada. Debe especificar una definición de tarea con el mismo nombre de volumen que en la solicitud de `create-service`. En este ejemplo se utiliza la opción `--cli-input-json` y un archivo de entrada JSON llamado `ecs-simple-service-ebs.json` con el siguiente contenido.

```
aws ecs create-service \
    --cli-input-json file://ecs-simple-service-ebs.json
```

Contenido de `ecs-simple-service-ebs.json`:

```
{
    "cluster": "mycluster",
    "taskDefinition": "mytaskdef",
    "serviceName": "ecs-simple-service-ebs",
    "desiredCount": 2,
    "launchType": "FARGATE",
    "networkConfiguration":{
        "awsvpcConfiguration":{
            "assignPublicIp": "ENABLED",
            "securityGroups": ["sg-12344321"],
            "subnets":["subnet-12344321"]
        }
    },
    "volumeConfigurations": [
        {
            "name": "myEbsVolume",
            "managedEBSVolume": {
```

```
                "roleArn":"arn:aws:iam::123456789012:role/ecsInfrastructureRole",
                "volumeType": "gp3",
                "sizeInGiB": 100,
                "iops": 3000,
                "throughput": 125,
                "filesystemType": "ext4"
            }
        }
   ]
}
```

Salida:

```
{
    "service": {
        "serviceArn": "arn:aws:ecs:us-west-2:123456789012:service/mycluster/ecs-
simple-service-ebs",
        "serviceName": "ecs-simple-service-ebs",
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/mycluster",
        "loadBalancers": [],
        "serviceRegistries": [],
        "status": "ACTIVE",
        "desiredCount": 2,
        "runningCount": 0,
        "pendingCount": 0,
        "launchType": "EC2",
        "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-definition/
mytaskdef:3",
        "deploymentConfiguration": {
            "deploymentCircuitBreaker": {
                "enable": false,
                "rollback": false
            },
            "maximumPercent": 200,
            "minimumHealthyPercent": 100
        },
        "deployments": [
            {
                "id": "ecs-svc/7851020056849183687",
                "status": "PRIMARY",
                "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-
definition/mytaskdef:3",
                "desiredCount": 0,
```

```
                "pendingCount": 0,
                "runningCount": 0,
                "failedTasks": 0,
                "createdAt": "2025-01-21T11:32:38.034000-06:00",
                "updatedAt": "2025-01-21T11:32:38.034000-06:00",
                "launchType": "EC2",
                "networkConfiguration": {
                    "awsvpcConfiguration": {
                        "subnets": [
                            "subnet-12344321"
                        ],
                        "securityGroups": [
                            "sg-12344321"
                        ],
                        "assignPublicIp": "DISABLED"
                    }
                },
                "rolloutState": "IN_PROGRESS",
                "rolloutStateReason": "ECS deployment ecs-svc/7851020056849183687 in
 progress.",
                "volumeConfigurations": [
                    {
                        "name": "myEBSVolume",
                        "managedEBSVolume": {
                            "volumeType": "gp3",
                            "sizeInGiB": 100,
                            "iops": 3000,
                            "throughput": 125,
                            "roleArn": "arn:aws:iam::123456789012:role/
ecsInfrastructureRole",
                            "filesystemType": "ext4"
                        }
                    }
                ]
            }
        ],
        "roleArn": "arn:aws:iam::123456789012:role/aws-service-role/
ecs.amazonaws.com/AWSServiceRoleForECS",
        "events": [],
        "createdAt": "2025-01-21T11:32:38.034000-06:00",
        "placementConstraints": [],
        "placementStrategy": [],
        "networkConfiguration": {
            "awsvpcConfiguration": {
```

```
                "subnets": [
                    "subnet-12344321"
                ],
                "securityGroups": [
                    "sg-12344321"
                ],
                "assignPublicIp": "DISABLED"
            }
        },
        "healthCheckGracePeriodSeconds": 0,
        "schedulingStrategy": "REPLICA",
        "deploymentController": {
            "type": "ECS"
        },
        "createdBy": "arn:aws:iam::123456789012:user/AIDACKCEVSQ6C2EXAMPLE",
        "enableECSManagedTags": false,
        "propagateTags": "NONE",
        "enableExecuteCommand": false,
        "availabilityZoneRebalancing": "DISABLED"
    }
}
```

Para obtener más información, consulte Uso de volúmenes de Amazon EBS con Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte CreateService en la Referencia de comandos de la AWS CLI.

`create-task-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-task-set`.

AWS CLI

Para crear un conjunto de tareas

En el siguiente ejemplo de `create-task-set`, se crea un conjunto de tareas de un servicio que utiliza un controlador de implementación externo.

```
aws ecs create-task-set \
    --cluster MyCluster \
    --service MyService \
    --task-definition MyTaskDefinition:2 \
```

```
    --network-
configuration "awsvpcConfiguration={subnets=[subnet-12344321],securityGroups=[sg-12344321]}"
```

Salida:

```
{
    "taskSet": {
        "id": "ecs-svc/1234567890123456789",
        "taskSetArn": "arn:aws:ecs:us-west-2:123456789012:task-set/MyCluster/
MyService/ecs-svc/1234567890123456789",
        "status": "ACTIVE",
        "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-definition/
MyTaskDefinition:2",
        "computedDesiredCount": 0,
        "pendingCount": 0,
        "runningCount": 0,
        "createdAt": 1557128360.711,
        "updatedAt": 1557128360.711,
        "launchType": "EC2",
        "networkConfiguration": {
            "awsvpcConfiguration": {
                "subnets": [
                    "subnet-12344321"
                ],
                "securityGroups": [
                    "sg-12344321"
                ],
                "assignPublicIp": "DISABLED"
            }
        },
        "loadBalancers": [],
        "serviceRegistries": [],
        "scale": {
            "value": 0.0,
            "unit": "PERCENT"
        },
        "stabilityStatus": "STABILIZING",
        "stabilityStatusAt": 1557128360.711
    }
}
```

- Para obtener información sobre la API, consulte CreateTaskSet en la Referencia de comandos de la AWS CLI.

`delete-account-setting`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-account-setting`.

AWS CLI

Para eliminar la configuración de cuenta de un usuario o rol de IAM específico

En el siguiente ejemplo de `delete-account-setting`, se elimina la configuración de cuenta del usuario o rol de IAM específico.

```
aws ecs delete-account-setting \
    --name serviceLongArnFormat \
    --principal-arn arn:aws:iam::123456789012:user/MyUser
```

Salida:

```
{
    "setting": {
        "name": "serviceLongArnFormat",
        "value": "enabled",
        "principalArn": "arn:aws:iam::123456789012:user/MyUser"
    }
}
```

Para obtener más información, consulte Amazon Resource Names (ARNs) and IDs en la Guía para desarrolladores de ECS.

- Para obtener información sobre la API, consulte DeleteAccountSetting en la Referencia de comandos de la AWS CLI.

`delete-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-attributes`.

AWS CLI

Para eliminar uno o varios atributos personalizados de un recurso de Amazon ECS

En el siguiente ejemplo de `delete-attributes`, se elimina un atributo con el nombre `stack` de una instancia de contenedor.

```
aws ecs delete-attributes \
    --attributes name=stack,targetId=arn:aws:ecs:us-west-2:130757420319:container-
instance/1c3be8ed-df30-47b4-8f1e-6e68ebd01f34
```

Salida:

```
{
    "attributes": [
        {
            "name": "stack",
            "targetId": "arn:aws:ecs:us-west-2:130757420319:container-
instance/1c3be8ed-df30-47b4-8f1e-6e68ebd01f34",
            "value": "production"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DeleteAttributes en la Referencia de comandos de la AWS CLI.

`delete-capacity-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-capacity-provider`.

AWS CLI

Ejemplo 1: eliminación de un proveedor de capacidad mediante el nombre de recurso de Amazon (ARN)

En el siguiente ejemplo de `delete-capacity-provider`, se elimina un proveedor de capacidad especificando el nombre de recurso de Amazon (ARN) del proveedor de capacidad. El ARN y el estado de eliminación del proveedor de capacidad se pueden recuperar mediante el comando `describe-capacity-providers`.

```
aws ecs delete-capacity-provider \
    --capacity-provider arn:aws:ecs:us-west-2:123456789012:capacity-provider/
ExampleCapacityProvider
```

Salida:

```
{
    "capacityProvider": {
        "capacityProviderArn": "arn:aws:ecs:us-west-2:123456789012:capacity-
provider/ExampleCapacityProvider",
        "name": "ExampleCapacityProvider",
        "status": "ACTIVE",
        "autoScalingGroupProvider": {
            "autoScalingGroupArn": "arn:aws:autoscaling:us-
west-2:123456789012:autoScalingGroup:a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111:autoScalingGroupName/MyAutoScalingGroup",
            "managedScaling": {
                "status": "ENABLED",
                "targetCapacity": 100,
                "minimumScalingStepSize": 1,
                "maximumScalingStepSize": 10000
            },
            "managedTerminationProtection": "DISABLED"
        },
        "updateStatus": "DELETE_IN_PROGRESS",
        "tags": []
    }
}
```

Para obtener más información, consulte Proveedores de capacidad de clúster en la Guía para desarrolladores de Amazon ECS.

Ejemplo 2: eliminación de un proveedor de capacidad mediante el nombre

En el siguiente ejemplo de `delete-capacity-provider`, se elimina un proveedor de capacidad especificando el nombre corto del proveedor de capacidad. El nombre corto y el estado de eliminación del proveedor de capacidad se pueden recuperar mediante el comando `describe-capacity-providers`.

```
aws ecs delete-capacity-provider \
    --capacity-provider ExampleCapacityProvider
```

Salida:

```
{
    "capacityProvider": {
        "capacityProviderArn": "arn:aws:ecs:us-west-2:123456789012:capacity-
provider/ExampleCapacityProvider",
```

```
        "name": "ExampleCapacityProvider",
        "status": "ACTIVE",
        "autoScalingGroupProvider": {
            "autoScalingGroupArn": "arn:aws:autoscaling:us-
west-2:123456789012:autoScalingGroup:a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111:autoScalingGroupName/MyAutoScalingGroup",
            "managedScaling": {
                "status": "ENABLED",
                "targetCapacity": 100,
                "minimumScalingStepSize": 1,
                "maximumScalingStepSize": 10000
            },
            "managedTerminationProtection": "DISABLED"
        },
        "updateStatus": "DELETE_IN_PROGRESS",
        "tags": []
    }
}
```

Para obtener más información, consulte Proveedores de capacidad de clúster en la Guía para desarrolladores de Amazon ECS.

- Para obtener detalles sobre la API, consulte DeleteCapacityProvider en la Referencia de comandos de la AWS CLI.

`delete-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-cluster`.

AWS CLI

Para eliminar un clúster vacío

En el siguiente ejemplo de `delete-cluster` se elimina el clúster vacío especificado.

```
aws ecs delete-cluster --cluster MyCluster
```

Salida:

```
{
    "cluster": {
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster",
```

```
        "status": "INACTIVE",
        "clusterName": "MyCluster",
        "registeredContainerInstancesCount": 0,
        "pendingTasksCount": 0,
        "runningTasksCount": 0,
        "activeServicesCount": 0
        "statistics": [],
        "tags": []
    }
}
```

Para obtener más información, consulte Eliminación de un clúster en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte DeleteCluster en la Referencia de comandos de la AWS CLI.

`delete-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-service`.

AWS CLI

Para eliminar un servicio

En el siguiente ejemplo de `ecs delete-service` se elimina el servicio especificado de un clúster. Puede incluir el parámetro `--force` para eliminar un servicio aunque no se haya escalado a cero tareas.

```
aws ecs delete-service --cluster MyCluster --service MyService1 --force
```

Para obtener más información, consulte Eliminación de un servicio en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte DeleteService en la Referencia de comandos de la AWS CLI.

`delete-task-definitions`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-task-definitions`.

AWS CLI

Para eliminar una definición de tarea

En el siguiente ejemplo de `delete-task-definitions`, se elimina una definición de tarea INACTIVE.

```
aws ecs delete-task-definitions \
    --task-definition curltest:1
```

Salida:

```
{
"taskDefinitions": [
    {
        "taskDefinitionArn": "arn:aws:ecs:us-east-1:123456789012:task-definition/
curltest:1",
        "containerDefinitions": [
            {
                "name": "ctest",
                "image": "mreferre/eksutils",
                "cpu": 0,
                "portMappings": [],
                "essential": true,
                "entryPoint": [
                    "sh",
                    "-c"
                ],
                "command": [
                    "curl ${ECS_CONTAINER_METADATA_URI_V4}/task"
                ],
                "environment": [],
                "mountPoints": [],
                "volumesFrom": [],
                "logConfiguration": {
                    "logDriver": "awslogs",
                    "options": {
                        "awslogs-create-group": "true",
                        "awslogs-group": "/ecs/curltest",
                        "awslogs-region": "us-east-1",
                        "awslogs-stream-prefix": "ecs"
                    }
                }
```

```
            }
        ],
        "family": "curltest",
        "taskRoleArn": "arn:aws:iam::123456789012:role/ecsTaskExecutionRole",
        "executionRoleArn": "arn:aws:iam::123456789012:role/ecsTaskExecutionRole",
        "networkMode": "awsvpc",
        "revision": 1,
        "volumes": [],
        "status": "DELETE_IN_PROGRESS",
        "compatibilities": [
            "EC2",
            "FARGATE"
        ],
        "requiresCompatibilities": [
            "FARGATE"
        ],
        "cpu": "256",
        "memory": "512",
        "registeredAt": "2021-09-10T12:56:24.704000+00:00",
        "deregisteredAt": "2023-03-14T15:20:59.419000+00:00",
        "registeredBy": "arn:aws:sts::123456789012:assumed-role/Admin/jdoe"
        }
    ],
    "failures": []
}
```

Para obtener más información, consulte Definiciones de tareas de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte DeleteTaskDefinitions en la Referencia de comandos de la AWS CLI.

`delete-task-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-task-set`.

AWS CLI

Para eliminar un conjunto de tareas

En el siguiente ejemplo de `delete-task-set`, se muestra cómo se elimina un conjunto de tareas. Puede incluir el parámetro `--force` para eliminar una tarea aunque no se haya escalado a cero.

```
aws ecs delete-task-set \
    --cluster MyCluster \
    --service MyService \
    --task-set arn:aws:ecs:us-west-2:123456789012:task-set/MyCluster/MyService/ecs-svc/1234567890123456789 \
    --force
```

Salida:

```
{
    "taskSet": {
        "id": "ecs-svc/1234567890123456789",
        "taskSetArn": "arn:aws:ecs:us-west-2:123456789012:task-set/MyCluster/
MyService/ecs-svc/1234567890123456789",
        "status": "DRAINING",
        "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-definition/
sample-fargate:2",
        "computedDesiredCount": 0,
        "pendingCount": 0,
        "runningCount": 0,
        "createdAt": 1557130260.276,
        "updatedAt": 1557130290.707,
        "launchType": "EC2",
        "networkConfiguration": {
            "awsvpcConfiguration": {
                "subnets": [
                    "subnet-12345678"
                ],
                "securityGroups": [
                    "sg-12345678"
                ],
                "assignPublicIp": "DISABLED"
            }
        },
        "loadBalancers": [],
        "serviceRegistries": [],
        "scale": {
            "value": 0.0,
            "unit": "PERCENT"
        },
        "stabilityStatus": "STABILIZING",
        "stabilityStatusAt": 1557130290.707
    }
```

```
}
```

- Para obtener información sobre la API, consulte DeleteTaskSet en la Referencia de comandos de la AWS CLI.

`deregister-container-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-container-instance`.

AWS CLI

Para anular el registro de una instancia de contenedor de un clúster

En el siguiente ejemplo de `deregister-container-instance`, se anula el registro de la instancia de contenedor del clúster especificado. Si aún hay tareas en ejecución en la instancia de contenedor, debe detenerlas antes de anular el registro, o bien usar la opción `--force`.

```
aws ecs deregister-container-instance \
    --cluster arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster \
    --container-instance arn:aws:ecs:us-west-2:123456789012:container-instance/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --force
```

Salida:

```
{
    "containerInstance": {
        "remainingResources": [
            {
                "integerValue": 1024,
                "doubleValue": 0.0,
                "type": "INTEGER",
                "longValue": 0,
                "name": "CPU"
            },
            {
                "integerValue": 985,
                "doubleValue": 0.0,
                "type": "INTEGER",
                "longValue": 0,
                "name": "MEMORY"
            },
```

```
            {
                "type": "STRINGSET",
                "integerValue": 0,
                "name": "PORTS",
                "stringSetValue": [
                    "22",
                    "2376",
                    "2375",
                    "51678",
                    "51679"
                ],
                "longValue": 0,
                "doubleValue": 0.0
            },
            {
                "type": "STRINGSET",
                "integerValue": 0,
                "name": "PORTS_UDP",
                "stringSetValue": [],
                "longValue": 0,
                "doubleValue": 0.0
            }
        ],
        "agentConnected": true,
        "attributes": [
            {
                "name": "ecs.capability.secrets.asm.environment-variables"
            },
            {
                "name": "com.amazonaws.ecs.capability.logging-driver.syslog"
            },
            {
                "value": "ami-01a82c3fce2c3ba58",
                "name": "ecs.ami-id"
            },
            {
                "name": "ecs.capability.secrets.asm.bootstrap.log-driver"
            },
            {
                "name": "com.amazonaws.ecs.capability.logging-driver.none"
            },
            {
                "name": "ecs.capability.ecr-endpoint"
            },
```

```
            {
                "name": "com.amazonaws.ecs.capability.logging-driver.json-file"
            },
            {
                "value": "vpc-1234567890123467",
                "name": "ecs.vpc-id"
            },
            {
                "name": "ecs.capability.execution-role-awslogs"
            },
            {
                "name": "com.amazonaws.ecs.capability.docker-remote-api.1.17"
            },
            {
                "name": "com.amazonaws.ecs.capability.docker-remote-api.1.18"
            },
            {
                "name": "com.amazonaws.ecs.capability.docker-remote-api.1.19"
            },
            {
                "name": "ecs.capability.docker-plugin.local"
            },
            {
                "name": "ecs.capability.task-eni"
            },
            {
                "name": "ecs.capability.task-cpu-mem-limit"
            },
            {
                "name": "ecs.capability.secrets.ssm.bootstrap.log-driver"
            },
            {
                "name": "com.amazonaws.ecs.capability.docker-remote-api.1.30"
            },
            {
                "name": "com.amazonaws.ecs.capability.docker-remote-api.1.31"
            },
            {
                "name": "com.amazonaws.ecs.capability.docker-remote-api.1.32"
            },
            {
                "name": "ecs.capability.execution-role-ecr-pull"
            },
            {
```

```
            "name": "ecs.capability.container-health-check"
        },
        {
            "value": "subnet-1234567890123467",
            "name": "ecs.subnet-id"
        },
        {
            "value": "us-west-2a",
            "name": "ecs.availability-zone"
        },
        {
            "value": "t2.micro",
            "name": "ecs.instance-type"
        },
        {
            "name": "com.amazonaws.ecs.capability.task-iam-role-network-host"
        },
        {
            "name": "ecs.capability.aws-appmesh"
        },
        {
            "name": "com.amazonaws.ecs.capability.logging-driver.awslogs"
        },
        {
            "name": "com.amazonaws.ecs.capability.docker-remote-api.1.24"
        },
        {
            "name": "com.amazonaws.ecs.capability.docker-remote-api.1.25"
        },
        {
            "name": "com.amazonaws.ecs.capability.docker-remote-api.1.26"
        },
        {
            "name": "com.amazonaws.ecs.capability.docker-remote-api.1.27"
        },
        {
            "name": "com.amazonaws.ecs.capability.privileged-container"
        },
        {
            "name": "ecs.capability.container-ordering"
        },
        {
            "name": "com.amazonaws.ecs.capability.docker-remote-api.1.28"
        },
```

```
            {
                "name": "com.amazonaws.ecs.capability.docker-remote-api.1.29"
            },
            {
                "value": "x86_64",
                "name": "ecs.cpu-architecture"
            },
            {
                "value": "93f43776-2018.10.0",
                "name": "ecs.capability.cni-plugin-version"
            },
            {
                "name": "ecs.capability.secrets.ssm.environment-variables"
            },
            {
                "name": "ecs.capability.pid-ipc-namespace-sharing"
            },
            {
                "name": "com.amazonaws.ecs.capability.ecr-auth"
            },
            {
                "value": "linux",
                "name": "ecs.os-type"
            },
            {
                "name": "com.amazonaws.ecs.capability.docker-remote-api.1.20"
            },
            {
                "name": "com.amazonaws.ecs.capability.docker-remote-api.1.21"
            },
            {
                "name": "com.amazonaws.ecs.capability.docker-remote-api.1.22"
            },
            {
                "name": "ecs.capability.task-eia"
            },
            {
                "name": "ecs.capability.private-registry-
authentication.secretsmanager"
            },
            {
                "name": "com.amazonaws.ecs.capability.task-iam-role"
            },
            {
```

```
                "name": "com.amazonaws.ecs.capability.docker-remote-api.1.23"
            }
        ],
        "pendingTasksCount": 0,
        "tags": [],
        "containerInstanceArn": "arn:aws:ecs:us-west-2:123456789012:container-
instance/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
        "registeredResources": [
            {
                "integerValue": 1024,
                "doubleValue": 0.0,
                "type": "INTEGER",
                "longValue": 0,
                "name": "CPU"
            },
            {
                "integerValue": 985,
                "doubleValue": 0.0,
                "type": "INTEGER",
                "longValue": 0,
                "name": "MEMORY"
            },
            {
                "type": "STRINGSET",
                "integerValue": 0,
                "name": "PORTS",
                "stringSetValue": [
                    "22",
                    "2376",
                    "2375",
                    "51678",
                    "51679"
                ],
                "longValue": 0,
                "doubleValue": 0.0
            },
            {
                "type": "STRINGSET",
                "integerValue": 0,
                "name": "PORTS_UDP",
                "stringSetValue": [],
                "longValue": 0,
                "doubleValue": 0.0
            }
```

```
        ],
        "status": "INACTIVE",
        "registeredAt": 1557768075.681,
        "version": 4,
        "versionInfo": {
            "agentVersion": "1.27.0",
            "agentHash": "aabe65ee",
            "dockerVersion": "DockerVersion: 18.06.1-ce"
        },
        "attachments": [],
        "runningTasksCount": 0,
        "ec2InstanceId": "i-12345678901234678"
    }
}
```

Para obtener más información, consulte Anulación del registro de una instancia de contenedor en la Guía para desarrolladores de ECS.

- Para obtener información sobre la API, consulte DeregisterContainerInstance en la Referencia de comandos de la AWS CLI.

`deregister-task-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-task-definition`.

AWS CLI

Para anular el registro de una definición de tareas

En el siguiente ejemplo de `deregister-task-definition`, se anula el registro de la primera revisión de la definición de tarea `curler` en la región predeterminada.

```
aws ecs deregister-task-definition --task-definition curler:1
```

Tenga en cuenta que, en el resultado obtenido, el estado de la definición de tarea `INACTIVE` indica:

```
{
    "taskDefinition": {
        "status": "INACTIVE",
        "family": "curler",
        "volumes": [],
```

```
        "taskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/
curler:1",
        "containerDefinitions": [
            {
                "environment": [],
                "name": "curler",
                "mountPoints": [],
                "image": "curl:latest",
                "cpu": 100,
                "portMappings": [],
                "entryPoint": [],
                "memory": 256,
                "command": [
                    "curl -v http://example.com/"
                ],
                "essential": true,
                "volumesFrom": []
            }
        ],
        "revision": 1
    }
}
```

Para obtener más información, consulte Definiciones de tareas de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte DeregisterTaskDefinition en la Referencia de comandos de la AWS CLI.

`describe-capacity-providers`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-capacity-providers`.

AWS CLI

Ejemplo 1: descripción de todos los proveedores de capacidad

En el siguiente ejemplo de `describe-capacity-providers`, se recuperan los detalles de todos los proveedores de capacidad.

```
aws ecs describe-capacity-providers
```

Salida:

```
{
    "capacityProviders": [
        {
            "capacityProviderArn": "arn:aws:ecs:us-west-2:123456789012:capacity-
provider/MyCapacityProvider",
            "name": "MyCapacityProvider",
            "status": "ACTIVE",
            "autoScalingGroupProvider": {
                "autoScalingGroupArn": "arn:aws:autoscaling:us-
west-2:123456789012:autoScalingGroup:a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111:autoScalingGroupName/MyAutoScalingGroup",
                "managedScaling": {
                    "status": "ENABLED",
                    "targetCapacity": 100,
                    "minimumScalingStepSize": 1,
                    "maximumScalingStepSize": 1000
                },
                "managedTerminationProtection": "ENABLED"
            },
            "tags": []
        },
        {
            "capacityProviderArn": "arn:aws:ecs:us-west-2:123456789012:capacity-
provider/FARGATE",
            "name": "FARGATE",
            "status": "ACTIVE",
            "tags": []
        },
        {
            "capacityProviderArn": "arn:aws:ecs:us-west-2:123456789012:capacity-
provider/FARGATE_SPOT",
            "name": "FARGATE_SPOT",
            "status": "ACTIVE",
            "tags": []
        }
    ]
}
```

Para obtener más información, consulte Proveedores de capacidad de clúster en la Guía para desarrolladores de Amazon ECS.

Ejemplo 2: descripción de un proveedor de capacidad específico

En el siguiente ejemplo de `describe-capacity-providers`, se recuperan los detalles sobre un proveedor de capacidad específico. Si se utiliza el parámetro `--include TAGS`, se añadirán a la salida las etiquetas asociadas al proveedor de capacidad.

```
aws ecs describe-capacity-providers \
    --capacity-providers MyCapacityProvider \
    --include TAGS
```

Salida:

```
{
    "capacityProviders": [
        {
            "capacityProviderArn": "arn:aws:ecs:us-west-2:123456789012:capacity-
provider/MyCapacityProvider",
            "name": "MyCapacityProvider",
            "status": "ACTIVE",
            "autoScalingGroupProvider": {
                "autoScalingGroupArn": "arn:aws:autoscaling:us-
west-2:123456789012:autoScalingGroup:a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111:autoScalingGroupName/MyAutoScalingGroup",
                "managedScaling": {
                    "status": "ENABLED",
                    "targetCapacity": 100,
                    "minimumScalingStepSize": 1,
                    "maximumScalingStepSize": 1000
                },
                "managedTerminationProtection": "ENABLED"
            },
            "tags": [
                {
                    "key": "environment",
                    "value": "production"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Proveedores de capacidad de clúster en la Guía para desarrolladores de Amazon ECS.

- Para obtener detalles sobre la API, consulte DescribeCapacityProviders en la Referencia de comandos de la AWS CLI.

`describe-clusters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-clusters`.

AWS CLI

Ejemplo 1: Descripción de un clúster

En el siguiente ejemplo de `describe-clusters` se recuperan los detalles sobre el clúster especificado.

```
aws ecs describe-clusters \
    --cluster default
```

Salida:

```
{
    "clusters": [
        {
            "status": "ACTIVE",
            "clusterName": "default",
            "registeredContainerInstancesCount": 0,
            "pendingTasksCount": 0,
            "runningTasksCount": 0,
            "activeServicesCount": 1,
            "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/default"
        }
    ],
    "failures": []
}
```

Para obtener más información, consulte Clústeres de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

Ejemplo 2: descripción de un clúster con la opción de asociar

En el siguiente ejemplo de `describe-clusters` se especifica la opción ARCHIVOS ADJUNTOS. Recupera detalles sobre el clúster especificado y una lista de los recursos adjuntos al clúster en forma de archivos adjuntos. Cuando se utiliza un proveedor de capacidad con un

clúster, los recursos, ya sean planes de AutoScaling o políticas de escalado, se representarán como ARCHIVOS ADJUNTOS asp o as_policy.

```
aws ecs describe-clusters \
    --include ATTACHMENTS \
    --clusters sampleCluster
```

Salida:

```
{
    "clusters": [
        {
            "clusterArn": "arn:aws:ecs:af-south-1:123456789222:cluster/
sampleCluster",
            "clusterName": "sampleCluster",
            "status": "ACTIVE",
            "registeredContainerInstancesCount": 0,
            "runningTasksCount": 0,
            "pendingTasksCount": 0,
            "activeServicesCount": 0,
            "statistics": [],
            "tags": [],
            "settings": [],
            "capacityProviders": [
                "sampleCapacityProvider"
            ],
            "defaultCapacityProviderStrategy": [],
            "attachments": [
                {
                    "id": "a1b2c3d4-5678-901b-cdef-EXAMPLE22222",
                    "type": "as_policy",
                    "status": "CREATED",
                    "details": [
                        {
                            "name": "capacityProviderName",
                            "value": "sampleCapacityProvider"
                        },
                        {
                            "name": "scalingPolicyName",
                            "value": "ECSManagedAutoScalingPolicy-3048e262-
fe39-4eaf-826d-6f975d303188"
                        }
                    ]
```

```
                }
            ],
            "attachmentsStatus": "UPDATE_COMPLETE"
        }
    ],
    "failures": []
}
```

Para obtener más información, consulte Clústeres de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte DescribeClusters en la Referencia de comandos de la AWS CLI.

`describe-container-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-container-instances`.

AWS CLI

Para describir la instancia de contenedor

En el siguiente ejemplo de `describe-container-instances`, se recuperan los detalles de una instancia de contenedor del clúster `update` mediante el uso del UUID de la instancia de contenedor como identificador.

```
aws ecs describe-container-instances \
    --cluster update \
    --container-instances a1b2c3d4-5678-90ab-cdef-11111EXAMPLE
```

Salida:

```
{
    "failures": [],
    "containerInstances": [
        {
            "status": "ACTIVE",
            "registeredResources": [
                {
                    "integerValue": 2048,
                    "longValue": 0,
                    "type": "INTEGER",
```

```
                    "name": "CPU",
                    "doubleValue": 0.0
                },
                {
                    "integerValue": 3955,
                    "longValue": 0,
                    "type": "INTEGER",
                    "name": "MEMORY",
                    "doubleValue": 0.0
                },
                {
                    "name": "PORTS",
                    "longValue": 0,
                    "doubleValue": 0.0,
                    "stringSetValue": [
                        "22",
                        "2376",
                        "2375",
                        "51678"
                    ],
                    "type": "STRINGSET",
                    "integerValue": 0
                }
            ],
            "ec2InstanceId": "i-A1B2C3D4",
            "agentConnected": true,
            "containerInstanceArn": "arn:aws:ecs:us-west-2:123456789012:container-
instance/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "pendingTasksCount": 0,
            "remainingResources": [
                {
                    "integerValue": 2048,
                    "longValue": 0,
                    "type": "INTEGER",
                    "name": "CPU",
                    "doubleValue": 0.0
                },
                {
                    "integerValue": 3955,
                    "longValue": 0,
                    "type": "INTEGER",
                    "name": "MEMORY",
                    "doubleValue": 0.0
                },
```

```
                {
                    "name": "PORTS",
                    "longValue": 0,
                    "doubleValue": 0.0,
                    "stringSetValue": [
                        "22",
                        "2376",
                        "2375",
                        "51678"
                    ],
                    "type": "STRINGSET",
                    "integerValue": 0
                }
            ],
            "runningTasksCount": 0,
            "versionInfo": {
                "agentVersion": "1.0.0",
                "agentHash": "4023248",
                "dockerVersion": "DockerVersion: 1.5.0"
            }
        }
    ]
}
```

Para obtener más información, consulte Instancias de contenedor de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte DescribeContainerInstances en la Referencia de comandos de la AWS CLI.

`describe-service-deployments`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-service-deployments`.

AWS CLI

Descripción de los detalles de la implementación del servicio

En el siguiente ejemplo de `describe-service-deployments`, se devuelven los detalles de la implementación del servicio con el ARN `arn:aws:ecs:us-east-1:123456789012:service-deployment/example-cluster/example-service/ejGvqq2ilnbKT9qj0vLJe`.

```
aws ecs describe-service-deployments \
    --service-deployment-arn arn:aws:ecs:us-east-1:123456789012:service-deployment/
example-cluster/example-service/ejGvqq2ilnbKT9qj0vLJe
```

Salida:

```
{
    "serviceDeployments": [
        {
            "serviceDeploymentArn": "arn:aws:ecs:us-east-1:123456789012:service-
deployment/example-cluster/example-service/ejGvqq2ilnbKT9qj0vLJe",
            "serviceArn": "arn:aws:ecs:us-east-1:123456789012:service/example-
cluster/example-service",
            "clusterArn": "arn:aws:ecs:us-east-1:123456789012:cluster/example-
cluster",
            "createdAt": "2024-10-31T08:03:30.917000-04:00",
            "startedAt": "2024-10-31T08:03:32.510000-04:00",
            "finishedAt": "2024-10-31T08:05:04.527000-04:00",
            "updatedAt": "2024-10-31T08:05:04.527000-04:00",
            "sourceServiceRevisions": [],
            "targetServiceRevision": {
                "arn": "arn:aws:ecs:us-east-1:123456789012:service-revision/example-
cluster/example-service/1485800978477494678",
                "requestedTaskCount": 1,
                "runningTaskCount": 1,
                "pendingTaskCount": 0
            },
            "status": "SUCCESSFUL",
            "deploymentConfiguration": {
                "deploymentCircuitBreaker": {
                    "enable": true,
                    "rollback": true
                },
                "maximumPercent": 200,
                "minimumHealthyPercent": 100,
                "alarms": {
                    "alarmNames": [],
                    "rollback": false,
                    "enable": false
                }
            },
            "deploymentCircuitBreaker": {
                "status": "MONITORING_COMPLETE",
```

```
                "failureCount": 0,
                "threshold": 3
            },
            "alarms": {
                "status": "DISABLED"
            }
        }
    ],
    "failures": []
}
```

Para obtener más información, consulte Visualización del historial de servicios mediante las implementaciones de servicios de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte DescribeServiceDeployments en la Referencia de comandos de la AWS CLI.

`describe-service-revisions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-service-revisions`.

AWS CLI

Descripción de los detalles de la revisión del servicio

En el siguiente ejemplo de `describe-service-revisions`, se devuelven los detalles de la revisión del servicio con el ARN `arn:aws:ecs:us-east-1:123456789012:service-revision/example-cluster/example-service/1485800978477494678`.

```
aws ecs describe-service-revisions \
    --service-revision-arns arn:aws:ecs:us-east-1:123456789012:service-revision/
example-cluster/example-service/1485800978477494678
```

Salida:

```
{
    "serviceRevisions": [
        {
            "serviceRevisionArn": "arn:aws:ecs:us-east-1:123456789012:service-
revision/example-cluster/example-service/1485800978477494678",
```

```
            "serviceArn": "arn:aws:ecs:us-east-1:123456789012:service/example-
cluster/example-service",
            "clusterArn": "arn:aws:ecs:us-east-1:123456789012:cluster/example-
cluster",
            "taskDefinition": "arn:aws:ecs:us-east-1:123456789012:task-definition/
webserver:5",
            "capacityProviderStrategy": [
                {
                    "capacityProvider": "FARGATE",
                    "weight": 1,
                    "base": 0
                }
            ],
            "platformVersion": "1.4.0",
            "platformFamily": "Linux",
            "networkConfiguration": {
                "awsvpcConfiguration": {
                    "subnets": [
                        "subnet-0d0eab1bb38d5ca64",
                        "subnet-0db5010045995c2d5"
                    ],
                    "securityGroups": [
                        "sg-02556bf85a191f59a"
                    ],
                    "assignPublicIp": "ENABLED"
                }
            },
            "containerImages": [
                {
                    "containerName": "aws-otel-collector",
                    "imageDigest":
 "sha256:7a1b3560655071bcacd66902c20ebe9a69470d5691fe3bd36baace7c2f3c4640",
                    "image": "public.ecr.aws/aws-observability/aws-otel-
collector:v0.32.0"
                },
                {
                    "containerName": "web",
                    "imageDigest":
 "sha256:28402db69fec7c17e179ea87882667f1e054391138f77ffaf0c3eb388efc3ffb",
                    "image": "nginx"
                }
            ],
            "guardDutyEnabled": false,
            "serviceConnectConfiguration": {
```

```
                "enabled": false
            },
            "createdAt": "2024-10-31T08:03:29.302000-04:00"
        }
    ],
    "failures": []
}
```

Para obtener más información, consulte Revisiones de servicio de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte DescribeServiceRevisions en la Referencia de comandos de la AWS CLI.

`describe-services`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-services`.

AWS CLI

Para describir un servicio

En el siguiente ejemplo de `describe-services`, se recuperan los detalles del servicio `my-http-service` en el clúster predeterminado.

```
aws ecs describe-services --services my-http-service
```

Salida:

```
{
    "services": [
        {
            "status": "ACTIVE",
            "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-definition/
amazon-ecs-sample:1",
            "pendingCount": 0,
            "loadBalancers": [],
            "desiredCount": 10,
            "createdAt": 1466801808.595,
            "serviceName": "my-http-service",
            "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/default",
            "serviceArn": "arn:aws:ecs:us-west-2:123456789012:service/my-http-
service",
```

```
            "deployments": [
                {
                    "status": "PRIMARY",
                    "pendingCount": 0,
                    "createdAt": 1466801808.595,
                    "desiredCount": 10,
                    "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-
definition/amazon-ecs-sample:1",
                    "updatedAt": 1428326312.703,
                    "id": "ecs-svc/1234567890123456789",
                    "runningCount": 10
                }
            ],
            "events": [
                {
                    "message": "(service my-http-service) has reached a steady
 state.",
                    "id": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
                    "createdAt": 1466801812.435
                }
            ],
            "runningCount": 10
        }
    ],
    "failures": []
}
```

Para obtener más información, consulte Servicios en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte DescribeServices en la Referencia de comandos de la AWS CLI.

`describe-task-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-task-definition`.

AWS CLI

Para describir una definición de tarea

En el siguiente ejemplo de `describe-task-definition`, se recuperan los detalles de una definición de tarea.

```
aws ecs describe-task-definition \
    --task-definition hello_world:8
```

Salida:

```
{
    "taskDefinition": {
        "taskDefinitionArn": "arn:aws:ecs:us-east-1:012345678910:task-definition/
hello_world:8",
        "containerDefinitions": [
            {
                "cpu": 10,
                "environment": [],
                "essential": true,
                "image": "wordpress",
                "links": [
                    "mysql"
                ] ,
                "memory": 500,
                "mountPoints": [],
                "name": "wordpress",
                "portMappings": [
                    {
                        "containerPort": 80,
                        "hostPort": 80
                    }
                ],
                "volumesFrom": []
            },
            {
                "cpu": 10,
                "environment": [
                    {
                        "name": "MYSQL_ROOT_PASSWORD",
                        "value": "password"
                    }
                ],
                "essential": true,
                "image": "mysql",
                "memory": 500,
                "mountPoints": [],
                "name": "mysql",
                "portMappings": [],
```

```
                "volumesFrom": []
            }
        ],
    "family": "hello_world",
    "revision": 8,
    "volumes": [],
    "status": "ACTIVE",
    "placementConstraints": [],
    "compatibilities": [
        "EXTERNAL",
        "EC2"
    ],
    "registeredAt": "2024-06-21T11:15:12.669000-05:00",
    "registeredBy": "arn:aws:sts::012345678910:assumed-role/demo-role/jane-doe"
    },
    "tags": []
}
```

Para obtener más información, consulte Definiciones de tareas de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte DescribeTaskDefinition en la Referencia de comandos de la AWS CLI.

`describe-task-sets`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-task-sets`.

AWS CLI

Para describir un conjunto de tareas

En el siguiente ejemplo de `describe-task-sets`, se describe un conjunto de tareas de un servicio que utiliza un implementador externo.

```
aws ecs describe-task-sets \
    --cluster MyCluster \
    --service MyService \
    --task-sets arn:aws:ecs:us-west-2:123456789012:task-set/MyCluster/MyService/ecs-svc/1234567890123456789
```

Salida:

```
{
    "taskSets": [
        {
            "id": "ecs-svc/1234567890123456789",
            "taskSetArn": "arn:aws:ecs:us-west-2:123456789012:task-set/MyCluster/
MyService/ecs-svc/1234567890123456789",
            "status": "ACTIVE",
            "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-definition/
sample-fargate:2",
            "computedDesiredCount": 0,
            "pendingCount": 0,
            "runningCount": 0,
            "createdAt": 1557207715.195,
            "updatedAt": 1557207740.014,
            "launchType": "EC2",
            "networkConfiguration": {
                "awsvpcConfiguration": {
                    "subnets": [
                        "subnet-12344321"
                    ],
                    "securityGroups": [
                        "sg-1234431"
                    ],
                    "assignPublicIp": "DISABLED"
                }
            },
            "loadBalancers": [],
            "serviceRegistries": [],
            "scale": {
                "value": 0.0,
                "unit": "PERCENT"
            },
            "stabilityStatus": "STEADY_STATE",
            "stabilityStatusAt": 1557207740.014
        }
    ],
    "failures": []
}
```

- Para obtener información sobre la API, consulte DescribeTaskSets en la Referencia de comandos de la AWS CLI.

describe-tasks

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-tasks`.

AWS CLI

Ejemplo 1: Descripción de una sola tarea

En el siguiente ejemplo de `describe-tasks` se recuperan los detalles de una tarea de un clúster. Puede especificar la tarea mediante el ID o el ARN completo de la tarea. En este ejemplo, se utiliza el ARN completo de la tarea.

```
aws ecs describe-tasks \
    --cluster MyCluster \
    --tasks arn:aws:ecs:us-east-1:123456789012:task/
MyCluster/4d590253bb114126b7afa7b58EXAMPLE
```

Salida:

```
{
    "tasks": [
        {
            "attachments": [],
            "attributes": [
                {
                    "name": "ecs.cpu-architecture",
                    "value": "x86_64"
                }
            ],
            "availabilityZone": "us-east-1b",
            "clusterArn": "arn:aws:ecs:us-east-1:123456789012:cluster/MyCluster",
            "connectivity": "CONNECTED",
            "connectivityAt": "2021-08-11T12:21:26.681000-04:00",
            "containerInstanceArn": "arn:aws:ecs:us-east-1:123456789012:container-
instance/test/025c7e2c5e054a6790a29fc1fEXAMPLE",
            "containers": [
                {
                    "containerArn": "arn:aws:ecs:us-east-1:123456789012:container/
MyCluster/4d590253bb114126b7afa7b58eea9221/a992d1cc-ea46-474a-b6e8-24688EXAMPLE",
                    "taskArn": "arn:aws:ecs:us-east-1:123456789012:task/
MyCluster/4d590253bb114126b7afa7b58EXAMPLE",
                    "name": "simple-app",
                    "image": "httpd:2.4",
```

```
                    "runtimeId":
 "91251eed27db90006ad67b1a08187290869f216557717dd5c39b37c94EXAMPLE",
                    "lastStatus": "RUNNING",
                    "networkBindings": [
                        {
                            "bindIP": "0.0.0.0",
                            "containerPort": 80,
                            "hostPort": 80,
                            "protocol": "tcp"
                        }
                    ],
                    "networkInterfaces": [],
                    "healthStatus": "UNKNOWN",
                    "cpu": "10",
                    "memory": "300"
                }
            ],
            "cpu": "10",
            "createdAt": "2021-08-11T12:21:26.681000-04:00",
            "desiredStatus": "RUNNING",
            "enableExecuteCommand": false,
            "group": "service:testupdate",
            "healthStatus": "UNKNOWN",
            "lastStatus": "RUNNING",
            "launchType": "EC2",
            "memory": "300",
            "overrides": {
                "containerOverrides": [
                    {
                        "name": "simple-app"
                    }
                ],
                "inferenceAcceleratorOverrides": []
            },
            "pullStartedAt": "2021-08-11T12:21:28.234000-04:00",
            "pullStoppedAt": "2021-08-11T12:21:33.793000-04:00",
            "startedAt": "2021-08-11T12:21:34.945000-04:00",
            "startedBy": "ecs-svc/968695068243EXAMPLE",
            "tags": [],
            "taskArn": "arn:aws:ecs:us-east-1:123456789012:task/
MyCluster/4d590253bb114126b7afa7b58eea9221",
            "taskDefinitionArn": "arn:aws:ecs:us-east-1:123456789012:task-
definition/console-sample-app-static2:1",
            "version": 2
```

```
        }
    ],
    "failures": []
}
```

Para obtener más información, consulte Definiciones de tareas de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

Ejemplo 2: Descripción de varias tareas

En el siguiente ejemplo de `describe-tasks` se recuperan los detalles de varias tareas de un clúster. Puede especificar la tarea mediante el ID o el ARN completo de la tarea. En este ejemplo se utilizan los ID completos de las tareas.

```
aws ecs describe-tasks \
    --cluster MyCluster \
    --tasks "74de0355a10a4f979ac495c14EXAMPLE" "d789e94343414c25b9f6bd59eEXAMPLE"
```

Salida:

```
{
    "tasks": [
        {
            "attachments": [
                {
                    "id": "d9e7735a-16aa-4128-bc7a-b2d51EXAMPLE",
                    "type": "ElasticNetworkInterface",
                    "status": "ATTACHED",
                    "details": [
                        {
                            "name": "subnetId",
                            "value": "subnet-0d0eab1bb3EXAMPLE"
                        },
                        {
                            "name": "networkInterfaceId",
                            "value": "eni-0fa40520aeEXAMPLE"
                        },
                        {
                            "name": "macAddress",
                            "value": "0e:89:76:28:07:b3"
                        },
                        {
                            "name": "privateDnsName",
```

```
                            "value": "ip-10-0-1-184.ec2.internal"
                        },
                        {
                            "name": "privateIPv4Address",
                            "value": "10.0.1.184"
                        }
                    ]
                }
            ],
            "attributes": [
                {
                    "name": "ecs.cpu-architecture",
                    "value": "x86_64"
                }
            ],
            "availabilityZone": "us-east-1b",
            "clusterArn": "arn:aws:ecs:us-east-1:123456789012:cluster/MyCluster",
            "connectivity": "CONNECTED",
            "connectivityAt": "2021-12-20T12:13:37.875000-05:00",
            "containers": [
                {
                    "containerArn": "arn:aws:ecs:us-east-1:123456789012:container/
MyCluster/74de0355a10a4f979ac495c14EXAMPLE/aad3ba00-83b3-4dac-84d4-11f8cEXAMPLE",
                    "taskArn": "arn:aws:ecs:us-east-1:123456789012:task/
MyCluster/74de0355a10a4f979ac495c14EXAMPLE",
                    "name": "web",
                    "image": "nginx",
                    "runtimeId": "74de0355a10a4f979ac495c14EXAMPLE-265927825",
                    "lastStatus": "RUNNING",
                    "networkBindings": [],
                    "networkInterfaces": [
                        {
                            "attachmentId": "d9e7735a-16aa-4128-bc7a-b2d51EXAMPLE",
                            "privateIpv4Address": "10.0.1.184"
                        }
                    ],
                    "healthStatus": "UNKNOWN",
                    "cpu": "99",
                    "memory": "100"
                }
            ],
            "cpu": "256",
            "createdAt": "2021-12-20T12:13:20.226000-05:00",
            "desiredStatus": "RUNNING",
```

```
            "enableExecuteCommand": false,
            "group": "service:tdsevicetag",
            "healthStatus": "UNKNOWN",
            "lastStatus": "RUNNING",
            "launchType": "FARGATE",
            "memory": "512",
            "overrides": {
                "containerOverrides": [
                    {
                        "name": "web"
                    }
                ],
                "inferenceAcceleratorOverrides": []
            },
            "platformVersion": "1.4.0",
            "platformFamily": "Linux",
            "pullStartedAt": "2021-12-20T12:13:42.665000-05:00",
            "pullStoppedAt": "2021-12-20T12:13:46.543000-05:00",
            "startedAt": "2021-12-20T12:13:48.086000-05:00",
            "startedBy": "ecs-svc/988401040018EXAMPLE",
            "tags": [],
            "taskArn": "arn:aws:ecs:us-east-1:123456789012:task/
MyCluster/74de0355a10a4f979ac495c14EXAMPLE",
            "taskDefinitionArn": "arn:aws:ecs:us-east-1:123456789012:task-
definition/webserver:2",
            "version": 3,
            "ephemeralStorage": {
            "sizeInGiB": 20
            }
        },
        {
            "attachments": [
                {
                    "id": "214eb5a9-45cd-4bf8-87bc-57fefEXAMPLE",
                    "type": "ElasticNetworkInterface",
                    "status": "ATTACHED",
                    "details": [
                        {
                            "name": "subnetId",
                            "value": "subnet-0d0eab1bb3EXAMPLE"
                        },
                        {
                            "name": "networkInterfaceId",
                            "value": "eni-064c7766daEXAMPLE"
```

```
                        },
                        {
                            "name": "macAddress",
                            "value": "0e:76:83:01:17:a9"
                        },
                        {
                            "name": "privateDnsName",
                            "value": "ip-10-0-1-41.ec2.internal"
                        },
                        {
                            "name": "privateIPv4Address",
                            "value": "10.0.1.41"
                        }
                    ]
                }
            ],
            "attributes": [
                {
                    "name": "ecs.cpu-architecture",
                    "value": "x86_64"
                }
            ],
            "availabilityZone": "us-east-1b",
            "clusterArn": "arn:aws:ecs:us-east-1:123456789012:cluster/MyCluster",
            "connectivity": "CONNECTED",
            "connectivityAt": "2021-12-20T12:13:35.243000-05:00",
            "containers": [
                {
                    "containerArn": "arn:aws:ecs:us-east-1:123456789012:container/
MyCluster/d789e94343414c25b9f6bd59eEXAMPLE/9afef792-609b-43a5-bb6a-3efdbEXAMPLE",
                    "taskArn": "arn:aws:ecs:us-east-1:123456789012:task/MyCluster/
d789e94343414c25b9f6bd59eEXAMPLE",
                    "name": "web",
                    "image": "nginx",
                    "runtimeId": "d789e94343414c25b9f6bd59eEXAMPLE-265927825",
                    "lastStatus": "RUNNING",
                    "networkBindings": [],
                    "networkInterfaces": [
                        {
                            "attachmentId": "214eb5a9-45cd-4bf8-87bc-57fefEXAMPLE",
                            "privateIpv4Address": "10.0.1.41"
                        }
                    ],
                    "healthStatus": "UNKNOWN",
```

```
                    "cpu": "99",
                    "memory": "100"
                }
            ],
            "cpu": "256",
            "createdAt": "2021-12-20T12:13:20.226000-05:00",
            "desiredStatus": "RUNNING",
            "enableExecuteCommand": false,
            "group": "service:tdsevicetag",
            "healthStatus": "UNKNOWN",
            "lastStatus": "RUNNING",
            "launchType": "FARGATE",
            "memory": "512",
            "overrides": {
                "containerOverrides": [
                    {
                        "name": "web"
                    }
                ],
                "inferenceAcceleratorOverrides": []
            },
            "platformVersion": "1.4.0",
            "platformFamily": "Linux",
            "pullStartedAt": "2021-12-20T12:13:44.611000-05:00",
            "pullStoppedAt": "2021-12-20T12:13:48.251000-05:00",
            "startedAt": "2021-12-20T12:13:49.326000-05:00",
            "startedBy": "ecs-svc/988401040018EXAMPLE",
            "tags": [],
            "taskArn": "arn:aws:ecs:us-east-1:123456789012:task/MyCluster/
d789e94343414c25b9f6bd59eEXAMPLE",
            "taskDefinitionArn": "arn:aws:ecs:us-east-1:123456789012:task-
definition/webserver:2",
            "version": 3,
            "ephemeralStorage": {
                "sizeInGiB": 20
            }
        }
    ],
    "failures": []
}
```


Para obtener más información, consulte Definiciones de tareas de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información de la API, consulte DescribeTasks en la Referencia de comandos de la AWS CLI.

`execute-command`

En el siguiente ejemplo de código, se muestra cómo utilizar `execute-command`.

AWS CLI

Para ejecutar un comando /bin/sh interactivo

En el siguiente ejemplo de `execute-command`, se ejecuta un comando /bin/sh interactivo contra un contenedor llamado MyContainer para una tarea con el id `arn:aws:ecs:us-east-1:123456789012:task/MyCluster/d789e94343414c25b9f6bd59eEXAMPLE`.

```
aws ecs execute-command \
    --cluster MyCluster \
    --task arn:aws:ecs:us-east-1:123456789012:task/MyCluster/
d789e94343414c25b9f6bd59eEXAMPLE \
    --container MyContainer \
    --interactive \
    --command "/bin/sh"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Using Amazon ECS Exec for debugging en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte ExecuteCommand en la Referencia de comandos de la AWS CLI.

`get-task-protection`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-task-protection`.

AWS CLI

Recuperación del estado de protección de la tarea en el servicio de ECS

El siguiente `get-task-protection` proporciona el estado de protección de las tareas de ECS que pertenecen al servicio de Amazon ECS.

```
aws ecs get-task-protection \
    --cluster ECS-project-update-cluster \
    --tasks c43ed3b1331041f289316f958adb6a24
```

Salida:

```
{
    "protectedTasks": [
        {
            "taskArn": "arn:aws:ecs:us-west-2:123456789012:task/
c43ed3b1331041f289316f958adb6a24",
            "protectionEnabled": false
        }
    ],
    "failures": []
}
```

Para obtener más información sobre la protección de tareas, consulte Proteger las tareas de Amazon ECS para que no finalicen por eventos de reducción horizontal en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte GetTaskProtection en la Referencia de comandos de la AWS CLI.

`list-account-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-account-settings`.

AWS CLI

Ejemplo 1: visualización de la configuración de una cuenta

En el siguiente ejemplo de `list-account-settings`, se muestra la configuración de cuenta en vigor de una cuenta.

```
aws ecs list-account-settings --effective-settings
```

Salida:

```
{
    "settings": [
```

```
        {
            "name": "containerInstanceLongArnFormat",
            "value": "enabled",
            "principalArn": "arn:aws:iam::123456789012:root"
        },
        {
            "name": "serviceLongArnFormat",
            "value": "enabled",
            "principalArn": "arn:aws:iam::123456789012:root"
        },
        {
            "name": "taskLongArnFormat",
            "value": "enabled",
            "principalArn": "arn:aws:iam::123456789012:root"
        }
    ]
}
```

Ejemplo 2: visualización de la configuración de cuenta de un usuario o rol de IAM específico

En el siguiente ejemplo de `list-account-settings`, se muestra la configuración de cuenta del usuario o rol de IAM especificado.

```
aws ecs list-account-settings --principal-arn arn:aws:iam::123456789012:user/MyUser
```

Salida:

```
{
    "settings": [
        {
            "name": "serviceLongArnFormat",
            "value": "enabled",
            "principalArn": "arn:aws:iam::123456789012:user/MyUser"
        }
    ]
}
```

Para obtener más información, consulte Amazon Resource Names (ARNs) and IDs en la Guía para desarrolladores de ECS.

- Para obtener información sobre la API, consulte ListAccountSettings en la Referencia de comandos de la AWS CLI.

`list-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-attributes`.

AWS CLI

Para enumerar las instancias de contenedor que contienen un atributo específico

En el siguiente ejemplo, se enumeran los atributos de las instancias de contenedor que tienen el atributo `stack=production` en el clúster predeterminado.

```
aws ecs list-attributes \
    --target-type container-instance \
    --attribute-name stack \
    --attribute-value production \
    --cluster default
```

Salida:

```
{
    "attributes": [
        {
            "name": "stack",
            "targetId": "arn:aws:ecs:us-west-2:130757420319:container-
instance/1c3be8ed-df30-47b4-8f1e-6e68ebd01f34",
            "value": "production"
        }
    ]
}
```

Para obtener más información, consulte Configuración del agente de contenedor de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte ListAttributes en la Referencia de comandos de la AWS CLI.

`list-clusters`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-clusters`.

AWS CLI

Para crear una lista de los clústeres disponibles

En el siguiente ejemplo de `list-clusters` se enumeran todos los clústeres disponibles.

```
aws ecs list-clusters
```

Salida:

```
{
    "clusterArns": [
        "arn:aws:ecs:us-west-2:123456789012:cluster/MyECSCluster1",
        "arn:aws:ecs:us-west-2:123456789012:cluster/AnotherECSCluster"
    ]
}
```

Para obtener más información, consulte Clústeres de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte ListClusters en la Referencia de comandos de la AWS CLI.

`list-container-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-container-instances`.

AWS CLI

Para enumerar las instancias de contenedor de un clúster

En el siguiente ejemplo de `list-container-instances`, se enumeran todas las instancias de contenedor disponibles en un clúster.

```
aws ecs list-container-instances --cluster MyCluster
```

Salida:

```
{
    "containerInstanceArns": [
        "arn:aws:ecs:us-west-2:123456789012:container-instance/MyCluster/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
        "arn:aws:ecs:us-west-2:123456789012:container-instance/MyCluster/
a1b2c3d4-5678-90ab-cdef-22222EXAMPLE"
```

```
    ]
}
```

Para obtener más información, consulte Instancias de contenedor de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte ListContainerInstances en la Referencia de comandos de la AWS CLI.

`list-service-deployments`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-service-deployments`.

AWS CLI

Muestra de las implementaciones de servicios

En el siguiente ejemplo de `list-service-deployments`, se recuperan las implementaciones de servicios del servicio denominado `example-service`.

```
aws ecs list-service-deployments \
    --service arn:aws:ecs:us-east-1:123456789012:service/example-cluster/example-service
```

Salida:

```
{
    "serviceDeployments": [
        {
            "serviceDeploymentArn": "arn:aws:ecs:us-east-1:123456789012:service-deployment/example-cluster/example-service/ejGvqq2ilnbKT9qj0vLJe",
            "serviceArn": "arn:aws:ecs:us-east-1:123456789012:service/example-cluster/example-service",
            "clusterArn": "arn:aws:ecs:us-east-1:123456789012:cluster/example-cluster",
            "startedAt": "2024-10-31T08:03:32.510000-04:00",
            "createdAt": "2024-10-31T08:03:30.917000-04:00",
            "finishedAt": "2024-10-31T08:05:04.527000-04:00",
            "targetServiceRevisionArn": "arn:aws:ecs:us-east-1:123456789012:service-revision/example-cluster/example-service/1485800978477494678",
            "status": "SUCCESSFUL"
```

```
        }
    ]
}
```

Para obtener más información, consulte Visualización del historial de servicios mediante las implementaciones de servicios de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte ListServiceDeployments en la Referencia de comandos de la AWS CLI.

`list-services-by-namespace`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-services-by-namespace`.

AWS CLI

Para enumerar los servicios de un espacio de nombres

En el siguiente ejemplo de `list-services-by-namespace`, se enumeran todos los servicios configurados para el espacio de nombres especificado en la región predeterminada.

```
aws ecs list-services-by-namespace \
    --namespace service-connect
```

Salida:

```
{
    "serviceArns": [
        "arn:aws:ecs:us-west-2:123456789012:service/MyCluster/MyService",
        "arn:aws:ecs:us-west-2:123456789012:service/tutorial/service-connect-nginx-
service"
    ]
}
```

Para obtener más información, consulte Service Connect en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte ListServicesByNamespace en la Referencia de comandos de la AWS CLI.

`list-services`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-services`.

AWS CLI

Para crear una lista de los servicios de un clúster

En el siguiente ejemplo de `list-services` se muestra cómo enumerar los servicios que se ejecutan en un clúster.

```
aws ecs list-services --cluster MyCluster
```

Salida:

```
 {
     "serviceArns": [
         "arn:aws:ecs:us-west-2:123456789012:service/MyCluster/MyService"
     ]
}
```

Para obtener más información, consulte Servicios en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte ListServices en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran las etiquetas de un clúster específico.

```
aws ecs list-tags-for-resource \
    --resource-arn arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster
```

Salida:

```
{
    "tags": [
        {
            "key": "key1",
            "value": "value1"
        },
        {
            "key": "key2",
            "value": "value2"
        },
        {
            "key": "key3",
            "value": "value3"
        }
    ]
}
```

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-task-definition-families`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-task-definition-families`.

AWS CLI

Ejemplo 1: enumeración de las familias de definiciones de tareas registradas

En el siguiente ejemplo de `list-task-definition-families`, se enumeran todas las familias de definiciones de tareas registradas.

```
aws ecs list-task-definition-families
```

Salida:

```
{
    "families": [
        "node-js-app",
        "web-timer",
        "hpcc",
        "hpcc-c4-8xlarge"
```

```
    ]
}
```

Ejemplo 2: filtrado de las familias de definiciones de tareas registradas

En el siguiente ejemplo de `list-task-definition-families`, se enumeran las revisiones de definiciones de tareas que comienzan por hpcc.

```
aws ecs list-task-definition-families --family-prefix hpcc
```

Salida:

```
{
    "families": [
        "hpcc",
        "hpcc-c4-8xlarge"
    ]
}
```

Para obtener más información, consulte Parámetros de definición de tareas en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte ListTaskDefinitionFamilies en la Referencia de comandos de la AWS CLI.

`list-task-definitions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-task-definitions`.

AWS CLI

Ejemplo 1: enumeración de las definiciones de tareas registradas

En el siguiente ejemplo de `list-task-definitions`, se enumeran todas las definiciones de tareas registradas.

```
aws ecs list-task-definitions
```

Salida:

```
{
```

```
    "taskDefinitionArns": [
        "arn:aws:ecs:us-west-2:123456789012:task-definition/sleep300:2",
        "arn:aws:ecs:us-west-2:123456789012:task-definition/sleep360:1",
        "arn:aws:ecs:us-west-2:123456789012:task-definition/wordpress:3",
        "arn:aws:ecs:us-west-2:123456789012:task-definition/wordpress:4",
        "arn:aws:ecs:us-west-2:123456789012:task-definition/wordpress:5",
        "arn:aws:ecs:us-west-2:123456789012:task-definition/wordpress:6"
    ]
}
```

Ejemplo 2: enumeración de las definiciones de tareas registradas en una familia

En el siguiente ejemplo de list-task-definitions, se enumeran las revisiones de las definiciones de tareas de la familia especificada.

```
aws ecs list-task-definitions --family-prefix wordpress
```

Salida:

```
{
    "taskDefinitionArns": [
        "arn:aws:ecs:us-west-2:123456789012:task-definition/wordpress:3",
        "arn:aws:ecs:us-west-2:123456789012:task-definition/wordpress:4",
        "arn:aws:ecs:us-west-2:123456789012:task-definition/wordpress:5",
        "arn:aws:ecs:us-west-2:123456789012:task-definition/wordpress:6"
    ]
}
```

Para obtener más información, consulte Definiciones de tareas de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte ListTaskDefinitions en la Referencia de comandos de la AWS CLI.

`list-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tasks`.

AWS CLI

Ejemplo 1: Creación de una lista de las tareas de un clúster

En el siguiente ejemplo de `list-tasks` se muestran todas las tareas de un clúster.

```
aws ecs list-tasks --cluster default
```

Salida:

```
{
    "taskArns": [
        "arn:aws:ecs:us-west-2:123456789012:task/a1b2c3d4-5678-90ab-
cdef-11111EXAMPLE",
        "arn:aws:ecs:us-west-2:123456789012:task/a1b2c3d4-5678-90ab-
cdef-22222EXAMPLE"
    ]
}
```

Ejemplo 2: creación de una lista de las tareas de una instancia de contenedor concreta

En el siguiente ejemplo de `list-tasks` se enumeran las tareas de una instancia de contenedor, utilizando el UUID de la instancia de contenedor como filtro.

```
aws ecs list-tasks --cluster default --container-instance a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE
```

Salida:

```
{
    "taskArns": [
        "arn:aws:ecs:us-west-2:123456789012:task/a1b2c3d4-5678-90ab-
cdef-44444EXAMPLE"
    ]
}
```

Para obtener más información, consulte Definiciones de tareas de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte ListTasks en la Referencia de comandos de la AWS CLI.

`put-account-setting-default`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-account-setting-default`.

AWS CLI

Para modificar la configuración de cuenta predeterminada

En el siguiente ejemplo de `put-account-setting-default`, se modifica la configuración de cuenta predeterminada para todos los usuarios o roles de IAM de la cuenta. Estos cambios se aplican a toda la cuenta de AWS, a menos que un usuario o rol de IAM invalide explícitamente esta configuración para sí mismo.

```
aws ecs put-account-setting-default --name serviceLongArnFormat --value enabled
```

Salida:

```
{
    "setting": {
        "name": "serviceLongArnFormat",
        "value": "enabled",
        "principalArn": "arn:aws:iam::123456789012:root"
    }
}
```

Para obtener más información, consulte Amazon Resource Names (ARNs) and IDs en la Guía para desarrolladores de ECS.

- Para obtener información sobre la API, consulte PutAccountSettingDefault en la Referencia de comandos de la AWS CLI.

`put-account-setting`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-account-setting`.

AWS CLI

Para modificar la configuración de cuenta para su cuenta de usuario de IAM

En el siguiente ejemplo de `put-account-setting`, se establece la configuración de cuenta de `containerInsights` en `enhanced` para la cuenta de usuario de IAM. Esto activa información de contenedores con observabilidad mejorada.

```
aws ecs put-account-setting \
    --name containerInsights \
```

```
    --value enhanced
```

Salida:

```
{
    "setting": {
        "name": "containerInsights",
        "value": "enhanced",
        "principalArn": "arn:aws:iam::123456789012:user/johndoe",
        "type": "user"
    }
}
```

Para obtener más información, consulte Modificación de la configuración de la cuenta en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte PutAccountSetting en la Referencia de comandos de la AWS CLI.

`put-account-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-account-settings`.

AWS CLI

Para modificar la configuración de cuenta de un usuario o rol de IAM

En el siguiente ejemplo de `put-account-setting`, se modifica la configuración de cuenta del usuario o rol de IAM especificado.

```
aws ecs put-account-setting \
    --name serviceLongArnFormat \
    --value enabled \
    --principal-arn arn:aws:iam::123456789012:user/MyUser
```

Salida:

```
{
    "setting": {
        "name": "serviceLongArnFormat",
        "value": "enabled",
```

```
        "principalArn": "arn:aws:iam::123456789012:user/MyUser"
    }
}
```

- Para obtener información sobre la API, consulte PutAccountSettings en la Referencia de comandos de la AWS CLI.

`put-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-attributes`.

AWS CLI

Para crear un atributo y su asociación a un recurso de Amazon ECS

En el siguiente ejemplo de `put-attributes`, se aplica a una instancia de contenedor un atributo con la pila de nombres y la producción de valores.

```
aws ecs put-attributes \
    --attributes name=stack,value=production,targetId=arn:aws:ecs:us-
west-2:130757420319:container-instance/1c3be8ed-df30-47b4-8f1e-6e68ebd01f34
```

Salida:

```
{
    "attributes": [
        {
            "name": "stack",
            "targetId": "arn:aws:ecs:us-west-2:130757420319:container-
instance/1c3be8ed-df30-47b4-8f1e-6e68ebd01f34",
            "value": "production"
        }
    ]
}
```

- Para obtener información acerca de la API, consulte PutAttributes en la Referencia de comandos de la AWS CLI.

`put-cluster-capacity-providers`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-cluster-capacity-providers`.

AWS CLI

Ejemplo 1: adición de un proveedor de capacidad existente a un clúster

En el siguiente ejemplo de `put-cluster-capacity-providers`, se agrega un proveedor de capacidad existente a un clúster. El comando `create-capacity-provider` se utiliza para crear un proveedor de capacidad. El comando `describe-clusters` se utiliza para describir los proveedores de capacidad actuales y la estrategia de estos predeterminada asociada a un clúster. Al agregar un nuevo proveedor de capacidad a un clúster, debe especificar todos los proveedores de capacidad existentes además del nuevo que desee asociar al clúster. También debe especificar la estrategia de proveedor de capacidad predeterminada que se va a asociar al clúster. En este ejemplo, el clúster `MyCluster` tiene asociado el proveedor de capacidad `MyCapacityProvider1` y se desea agregar e incluir el proveedor de capacidad `MyCapacityProvider2` en la estrategia de proveedor de capacidad predeterminada para que las tareas se distribuyan de manera uniforme entre ambos.

```
aws ecs put-cluster-capacity-providers \
    --cluster MyCluster \
    --capacity-providers MyCapacityProvider1 MyCapacityProvider2 \
    --default-capacity-provider-
strategy capacityProvider=MyCapacityProvider1,weight=1 capacityProvider=MyCapacityProvider2,
```

Salida:

```
{
    "cluster": {
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster",
        "clusterName": "MyCluster",
        "status": "ACTIVE",
        "registeredContainerInstancesCount": 0,
        "runningTasksCount": 0,
        "pendingTasksCount": 0,
        "activeServicesCount": 0,
        "statistics": [],
        "tags": [],
        "settings": [
            {
                "name": "containerInsights",
                "value": "enabled"
            }
        ],
```

```
        "capacityProviders": [
            "MyCapacityProvider1",
            "MyCapacityProvider2"
        ],
        "defaultCapacityProviderStrategy": [
            {
                "capacityProvider": "MyCapacityProvider1",
                "weight": 1,
                "base": 0
            },
            {
                "capacityProvider": "MyCapacityProvider2",
                "weight": 1,
                "base": 0
            }
        ],
        "attachments": [
           {
                "id": "0fb0c8f4-6edd-4de1-9b09-17e470ee1918",
                "type": "as_policy",
                "status": "ACTIVE",
                "details": [
                    {
                        "name": "capacityProviderName",
                        "value": "MyCapacityProvider1"
                    },
                    {
                        "name": "scalingPolicyName",
                        "value": "ECSManagedAutoScalingPolicy-a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
                    }
                ]
            },
            {
                "id": "ae592060-2382-4663-9476-b015c685593c",
                "type": "as_policy",
                "status": "ACTIVE",
                "details": [
                    {
                        "name": "capacityProviderName",
                        "value": "MyCapacityProvider2"
                    },
                    {
                        "name": "scalingPolicyName",
```

```
                        "value": "ECSManagedAutoScalingPolicy-a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"
                    }
                ]
            }
        ],
        "attachmentsStatus": "UPDATE_IN_PROGRESS"
    }
}
```

Para obtener más información, consulte Proveedores de capacidad de clúster en la Guía para desarrolladores de Amazon ECS.

Ejemplo 2: eliminación de un proveedor de capacidad de un clúster

En el siguiente ejemplo de `put-cluster-capacity-providers`, se elimina a un proveedor de capacidad de un clúster. El comando `describe-clusters` se utiliza para describir los proveedores de capacidad actuales asociados a un clúster. Al eliminar un proveedor de capacidad de un clúster, es preciso especificar los proveedores de capacidad que se desea que permanezcan asociados al clúster, así como la estrategia predeterminada de proveedor de capacidad que debe asociarse al clúster. En este ejemplo, el clúster tiene asociados los proveedores de capacidad `MyCapacityProvider1` y `MyCapacityProvider2` y se desea eliminar el proveedor de capacidad `MyCapacityProvider2`; por ello, solamente se especifica `MyCapacityProvider1` en el comando junto con la estrategia predeterminada y actualizada de proveedor de capacidad.

```
aws ecs put-cluster-capacity-providers \
    --cluster MyCluster \
    --capacity-providers MyCapacityProvider1 \
    --default-capacity-provider-
strategy capacityProvider=MyCapacityProvider1,weight=1,base=0
```

Salida:

```
{
    "cluster": {
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster",
        "clusterName": "MyCluster",
        "status": "ACTIVE",
        "registeredContainerInstancesCount": 0,
        "runningTasksCount": 0,
```

```
        "pendingTasksCount": 0,
        "activeServicesCount": 0,
        "statistics": [],
        "tags": [],
        "settings": [
            {
                "name": "containerInsights",
                "value": "enabled"
            }
        ],
        "capacityProviders": [
            "MyCapacityProvider1"
        ],
        "defaultCapacityProviderStrategy": [
            "capacityProvider": "MyCapacityProvider1",
            "weight": 1,
            "base": 0
        ],
        "attachments": [
           {
                "id": "0fb0c8f4-6edd-4de1-9b09-17e470ee1918",
                "type": "as_policy",
                "status": "ACTIVE",
                "details": [
                    {
                        "name": "capacityProviderName",
                        "value": "MyCapacityProvider1"
                    },
                    {
                        "name": "scalingPolicyName",
                        "value": "ECSManagedAutoScalingPolicy-a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
                    }
                ]
            },
            {
                "id": "ae592060-2382-4663-9476-b015c685593c",
                "type": "as_policy",
                "status": "DELETING",
                "details": [
                    {
                        "name": "capacityProviderName",
                        "value": "MyCapacityProvider2"
                    },
```

```
                    {
                        "name": "scalingPolicyName",
                        "value": "ECSManagedAutoScalingPolicy-a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"
                    }
                ]
            }
        ],
        "attachmentsStatus": "UPDATE_IN_PROGRESS"
    }
}
```

Para obtener más información, consulte Proveedores de capacidad de clúster en la Guía para desarrolladores de Amazon ECS.

Ejemplo 3: eliminación de todos los proveedores de capacidad de un clúster

En el siguiente ejemplo de `put-cluster-capacity-providers`, se eliminan todos los proveedores de capacidad existentes del clúster especificado.

```
aws ecs put-cluster-capacity-providers \
    --cluster MyCluster \
    --capacity-providers [] \
    --default-capacity-provider-strategy []
```

Salida:

```
{
    "cluster": {
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster",
        "clusterName": "MyCluster",
        "status": "ACTIVE",
        "registeredContainerInstancesCount": 0,
        "runningTasksCount": 0,
        "pendingTasksCount": 0,
        "activeServicesCount": 0,
        "statistics": [],
        "tags": [],
        "settings": [
            {
                "name": "containerInsights",
                "value": "enabled"
            }
```

```
        ],
        "capacityProviders": [],
        "defaultCapacityProviderStrategy": [],
        "attachments": [
           {
                "id": "0fb0c8f4-6edd-4de1-9b09-17e470ee1918",
                "type": "as_policy",
                "status": "DELETING",
                "details": [
                    {
                        "name": "capacityProviderName",
                        "value": "MyCapacityProvider1"
                    },
                    {
                        "name": "scalingPolicyName",
                        "value": "ECSManagedAutoScalingPolicy-a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
                    }
                ]
            },
            {
                "id": "ae592060-2382-4663-9476-b015c685593c",
                "type": "as_policy",
                "status": "DELETING",
                "details": [
                    {
                        "name": "capacityProviderName",
                        "value": "MyCapacityProvider2"
                    },
                    {
                        "name": "scalingPolicyName",
                        "value": "ECSManagedAutoScalingPolicy-a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"
                    }
                ]
            }
        ],
        "attachmentsStatus": "UPDATE_IN_PROGRESS"
    }
}
```

Para obtener más información, consulte Proveedores de capacidad de clúster en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte PutClusterCapacityProviders en la Referencia de comandos de la AWS CLI.

`register-task-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-task-definition`.

AWS CLI

Ejemplo 1: registro de una definición de tarea con un archivo JSON

En el siguiente ejemplo de `register-task-definition`, se registra una definición de tarea en la familia especificada. Las definiciones de contenedor se guardan en formato JSON en la ubicación de archivo especificada.

```
aws ecs register-task-definition \
    --cli-input-json file://<path_to_json_file>/sleep360.json
```

Contenido de `sleep360.json`:

```
{
    "containerDefinitions": [
        {
            "name": "sleep",
            "image": "busybox",
            "cpu": 10,
            "command": [
                "sleep",
                "360"
            ],
            "memory": 10,
            "essential": true
        }
    ],
    "family": "sleep360"
}
```

Salida:

```
{
    "taskDefinition": {
        "status": "ACTIVE",
```

```
        "family": "sleep360",
        "placementConstraints": [],
        "compatibilities": [
                "EXTERNAL",
                "EC2"
        ],
        "volumes": [],
        "taskDefinitionArn": "arn:aws:ecs:us-east-1:123456789012:task-definition/
sleep360:1",
        "containerDefinitions": [
            {
                "environment": [],
                "name": "sleep",
                "mountPoints": [],
                "image": "busybox",
                "cpu": 10,
                "portMappings": [],
                "command": [
                    "sleep",
                    "360"
                ],
        "memory": 10,
        "essential": true,
        "volumesFrom": []
        }
    ],
        "revision": 1
    }
}
```

Para obtener más información, consulte Ejemplo de definiciones de tareas en la Guía para desarrolladores de Amazon ECS.

Ejemplo 2: registro de una definición de tarea con un parámetro de cadena JSON

En el siguiente ejemplo de `register-task-definition`, se registra una definición de tarea mediante las definiciones de contenedor proporcionadas como un parámetro de cadena JSON con comillas dobles con caracteres de escape.

```
aws ecs register-task-definition \
    --family sleep360 \
    --container-definitions "[{\"name\":\"sleep\",\"image\":\"busybox\",\"cpu\":10,
\"command\":[\"sleep\",\"360\"],\"memory\":10,\"essential\":true}]"
```

Se obtiene la misma salida que en el ejemplo anterior.

Para obtener más información, consulte Creación de una definición de tareas en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte RegisterTaskDefinition en la Referencia de comandos de la AWS CLI.

`run-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `run-task`.

AWS CLI

Ejemplo 1: ejecución de una tarea en el clúster predeterminado

En el siguiente ejemplo de `run-task`, se ejecuta una tarea en el clúster predeterminado y se utiliza un token de cliente.

```
aws ecs run-task \
    --cluster default \
    --task-definition sleep360:1 \
    --client-token 550e8400-e29b-41d4-a716-446655440000
```

Salida:

```
{
    "tasks": [
        {
            "attachments": [],
            "attributes": [
                {
                    "name": "ecs.cpu-architecture",
                    "value": "x86_64"
                }
            ],
            "availabilityZone": "us-east-1b",
            "capacityProviderName": "example-capacity-provider",
            "clusterArn": "arn:aws:ecs:us-east-1:123456789012:cluster/default",
            "containerInstanceArn": "arn:aws:ecs:us-east-1:123456789012:container-
instance/default/bc4d2ec611d04bb7bb97e83ceEXAMPLE",
            "containers": [
                {
```

```
                    "containerArn": "arn:aws:ecs:us-east-1:123456789012:container/
default/d6f51cc5bbc94a47969c92035e9f66f8/75853d2d-711e-458a-8362-0f0aEXAMPLE",
                    "taskArn": "arn:aws:ecs:us-east-1:123456789012:task/default/
d6f51cc5bbc94a47969c9203EXAMPLE",
                    "name": "sleep",
                    "image": "busybox",
                    "lastStatus": "PENDING",
                    "networkInterfaces": [],
                    "cpu": "10",
                    "memory": "10"
                }
            ],
            "cpu": "10",
            "createdAt": "2023-11-21T16:59:34.403000-05:00",
            "desiredStatus": "RUNNING",
            "enableExecuteCommand": false,
            "group": "family:sleep360",
            "lastStatus": "PENDING",
            "launchType": "EC2",
            "memory": "10",
            "overrides": {
                "containerOverrides": [
                    {
                        "name": "sleep"
                    }
                ],
                "inferenceAcceleratorOverrides": []
            },
            "tags": [],
            "taskArn": "arn:aws:ecs:us-east-1:123456789012:task/default/
d6f51cc5bbc94a47969c9203EXAMPLE",
            "taskDefinitionArn": "arn:aws:ecs:us-east-1:123456789012:task-
definition/sleep360:1",
            "version": 1
        }
    ],
    "failures": []
}
```


Para obtener más información, consulte Ejecución de una aplicación como una tarea independiente en la Guía para desarrolladores de Amazon ECS.

Ejemplo 2: configuración de un volumen de Amazon EBS para una tarea independiente

En el siguiente ejemplo de `run-task` se configura un volumen de Amazon EBS cifrado para una tarea Fargate en el clúster predeterminado. Debe tener configurado un rol de infraestructura de Amazon ECS con la política administrada por `AmazonECSInfrastructureRolePolicyForVolumes` asociada. Debe especificar una definición de tarea con el mismo nombre de volumen que en la solicitud de `run-task`. En este ejemplo se utiliza la opción `--cli-input-json` y un archivo de entrada JSON llamado `ebs.json`.

```
aws ecs run-task \
    --cli-input-json file://ebs.json
```

Contenido de `ebs.json`:

```
{
   "cluster": "default",
   "taskDefinition": "mytaskdef",
   "launchType": "FARGATE",
   "networkConfiguration":{
        "awsvpcConfiguration":{
            "assignPublicIp": "ENABLED",
            "securityGroups": ["sg-12344321"],
            "subnets":["subnet-12344321"]
        }
    },
   "volumeConfigurations": [
        {
            "name": "myEBSVolume",
            "managedEBSVolume": {
                "volumeType": "gp3",
                "sizeInGiB": 100,
                "roleArn":"arn:aws:iam::1111222333:role/ecsInfrastructureRole",
                "encrypted": true,
                "kmsKeyId":
 "arn:aws:kms:region:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
            }
        }
    ]
}
```

Salida:

```
{
    "tasks": [
        {
            "attachments": [
                {
                    "id": "ce868693-15ca-4083-91ac-f782f64000c9",
                    "type": "ElasticNetworkInterface",
                    "status": "PRECREATED",
                    "details": [
                        {
                        "name": "subnetId",
                        "value": "subnet-070982705451dad82"
                        }
                    ]
                },
                {
                    "id": "a17ed863-786c-4372-b5b3-b23e53f37877",
                    "type": "AmazonElasticBlockStorage",
                    "status": "CREATED",
                    "details": [
                        {
                            "name": "roleArn",
                            "value": "arn:aws:iam::123456789012:role/
ecsInfrastructureRole"
                        },
                        {
                            "name": "volumeName",
                            "value": "myEBSVolume"
                        },
                        {
                            "name": "deleteOnTermination",
                            "value": "true"
                        }
                    ]
                }
            ],
            "attributes": [
                {
                    "name": "ecs.cpu-architecture",
                    "value": "x86_64"
                }
            ],
            "availabilityZone": "us-west-2b",
```

```
            "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/default",
            "containers": [
                {
                    "containerArn": "arn:aws:ecs:us-west-2:123456789012:container/
default/7f1fbd3629434cc4b82d72d2f09b67c9/e21962a2-f328-4699-98a3-5161ac2c186a",
                    "taskArn": "arn:aws:ecs:us-west-2:123456789012:task/
default/7f1fbd3629434cc4b82d72d2f09b67c9",
                    "name": "container-using-ebs",
                    "image": "amazonlinux:2",
                    "lastStatus": "PENDING",
                    "networkInterfaces": [],
                    "cpu": "0"
                }
            ],
            "cpu": "1024",
            "createdAt": "2025-01-23T10:29:46.650000-06:00",
            "desiredStatus": "RUNNING",
            "enableExecuteCommand": false,
            "group": "family:mytaskdef",
            "lastStatus": "PROVISIONING",
            "launchType": "FARGATE",
            "memory": "3072",
            "overrides": {
                "containerOverrides": [
                    {
                        "name": "container-using-ebs"
                    }
                ],
                "inferenceAcceleratorOverrides": []
            },
            "platformVersion": "1.4.0",
            "platformFamily": "Linux",
            "tags": [],
            "taskArn": "arn:aws:ecs:us-west-2:123456789012:task/
default/7f1fbd3629434cc4b82d72d2f09b67c9",
            "taskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-
definition/mytaskdef:4",
            "version": 1,
            "ephemeralStorage": {
                "sizeInGiB": 20
            },
            "fargateEphemeralStorage": {
                "sizeInGiB": 20
            }
```

```
        }
    ],
    "failures": []
}
```

Para obtener más información, consulte Uso de volúmenes de Amazon EBS con Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte RunTask en la Referencia de comandos de la AWS CLI.

`start-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-task`.

AWS CLI

Ejemplo 1: inicio de una nueva tarea

En el siguiente ejemplo de `start-task`, se inicia una tarea con la última revisión de la definición de tarea `sleep360` en la instancia de contenedor especificada en el clúster predeterminado.

```
aws ecs start-task \
    --task-definition sleep360 \
    --container-instances 765936fadbdd46b5991a4bd70c2a43d4
```

Salida:

```
{
    "tasks": [
        {
            "taskArn": "arn:aws:ecs:us-west-2:123456789012:task/
default/666fdccc2e2d4b6894dd422f4eeee8f8",
            "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/default",
            "taskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-
definition/sleep360:3",
            "containerInstanceArn": "arn:aws:ecs:us-west-2:123456789012:container-
instance/default/765936fadbdd46b5991a4bd70c2a43d4",
            "overrides": {
                "containerOverrides": [
                    {
                        "name": "sleep"
                    }
```

```
                ]
            },
            "lastStatus": "PENDING",
            "desiredStatus": "RUNNING",
            "cpu": "128",
            "memory": "128",
            "containers": [
                {
                    "containerArn": "arn:aws:ecs:us-
west-2:123456789012:container/75f11ed4-8a3d-4f26-a33b-ad1db9e02d41",
                    "taskArn": "arn:aws:ecs:us-west-2:123456789012:task/
default/666fdccc2e2d4b6894dd422f4eeee8f8",
                    "name": "sleep",
                    "lastStatus": "PENDING",
                    "networkInterfaces": [],
                    "cpu": "10",
                    "memory": "10"
                }
            ],
            "version": 1,
            "createdAt": 1563421494.186,
            "group": "family:sleep360",
            "launchType": "EC2",
            "attachments": [],
            "tags": []
        }
    ],
    "failures": []
}
```

Para obtener más información, consulte Programación de los contenedores en Amazon ECS en la Guía para desarrolladores de Amazon ECS.

Ejemplo 2: configuración de un volumen de Amazon EBS al inicio de la tarea

En el siguiente ejemplo de `start-task` se configura un volumen de Amazon EBS cifrado para una tarea en la instancia de contenedor especificada. Debe tener configurado un rol de infraestructura de Amazon ECS con la política administrada por `AmazonECSInfrastructureRolePolicyForVolumes` asociada. Debe especificar una definición de tarea con el mismo nombre de volumen que en la solicitud de `start-task`. En este ejemplo se utiliza la opción `--cli-input-json` y un archivo de entrada JSON llamado `ebs.json` con el siguiente contenido.

```
aws ecs start-task \
    --cli-input-json file://ebs.json \
    --container-instances 765936fadbdd46b5991a4bd70c2a43d4
```

Contenido de `ebs.json`:

```
{
   "cluster": "default",
   "taskDefinition": "mytaskdef",
   "networkConfiguration":{
        "awsvpcConfiguration":{
            "assignPublicIp": "ENABLED",
            "securityGroups": ["sg-12344321"],
            "subnets":["subnet-12344321"]
        }
    },
   "volumeConfigurations": [
        {
            "name": "myEBSVolume",
            "managedEBSVolume": {
                "volumeType": "gp3",
                "sizeInGiB": 100,
                "roleArn":"arn:aws:iam::123456789012:role/ecsInfrastructureRole",
                "encrypted": true,
                "kmsKeyId":
 "arn:aws:kms:region:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
            }
        }
    ]
}
```

Salida:

```
{
    "tasks": [
        {
            "attachments": [
                {
                    "id": "aea29489-9dcd-49f1-8164-4d91566e1113",
                    "type": "ElasticNetworkInterface",
                    "status": "PRECREATED",
                    "details": [
```

```
                        {
                            "name": "subnetId",
                            "value": "subnet-12344321"
                        }
                    ]
                },
                {
                    "id": "f29e1222-9a1e-410f-b499-a12a7cd6d42e",
                    "type": "AmazonElasticBlockStorage",
                    "status": "CREATED",
                    "details": [
                        {
                            "name": "roleArn",
                            "value": "arn:aws:iam::123456789012:role/
ecsInfrastructureRole"
                        },
                        {
                            "name": "volumeName",
                            "value": "myEBSVolume"
                        },
                        {
                            "name": "deleteOnTermination",
                            "value": "true"
                        }
                    ]
                }
            ],
            "attributes": [
                {
                    "name": "ecs.cpu-architecture",
                    "value": "arm64"
                }
            ],
            "availabilityZone": "us-west-2c",
            "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/default",
            "containerInstanceArn": "arn:aws:ecs:us-west-2:123456789012:container-
instance/default/765936fadbdd46b5991a4bd70c2a43d4",
            "containers": [
                {
                    "containerArn": "arn:aws:ecs:us-west-2:123456789012:container/
default/bb122ace3ed84add92c00a351a03c69e/a4a9ed10-51c7-4567-9653-50e71b94f867",
                    "taskArn": "arn:aws:ecs:us-west-2:123456789012:task/default/
bb122ace3ed84add92c00a351a03c69e",
                    "name": "container-using-ebs",
```

```
                    "image": "amazonlinux:2",
                    "lastStatus": "PENDING",
                    "networkInterfaces": [],
                    "cpu": "0"
                }
            ],
            "cpu": "1024",
            "createdAt": "2025-01-23T14:51:05.191000-06:00",
            "desiredStatus": "RUNNING",
            "enableExecuteCommand": false,
            "group": "family:mytaskdef",
            "lastStatus": "PROVISIONING",
            "launchType": "EC2",
            "memory": "3072",
            "overrides": {
                "containerOverrides": [
                    {
                        "name": "container-using-ebs"
                    }
                ],
                "inferenceAcceleratorOverrides": []
            },
             "tags": [],
            "taskArn": "arn:aws:ecs:us-west-2:123456789012:task/default/
bb122ace3ed84add92c00a351a03c69e",
            "taskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-
definition/mytaskdef:4",
            "version": 1
        }
    ],
    "failures": []
}
```

Para obtener más información, consulte Uso de volúmenes de Amazon EBS con Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener más información sobre la API, consulte StartTask en Referencia de comandos de la AWS CLI.

`stop-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-task`.

AWS CLI

Para detener una tarea

En el siguiente ejemplo de `stop-task`, se detiene la ejecución de la tarea especificada en el clúster predeterminado.

```
aws ecs stop-task \
    --task 666fdccc2e2d4b6894dd422f4eeee8f8
```

Salida:

```
{
    "task": {
        "taskArn": "arn:aws:ecs:us-west-2:130757420319:task/
default/666fdccc2e2d4b6894dd422f4eeee8f8",
        "clusterArn": "arn:aws:ecs:us-west-2:130757420319:cluster/default",
        "taskDefinitionArn": "arn:aws:ecs:us-west-2:130757420319:task-definition/
sleep360:3",
        "containerInstanceArn": "arn:aws:ecs:us-west-2:130757420319:container-
instance/default/765936fadbdd46b5991a4bd70c2a43d4",
        "overrides": {
            "containerOverrides": []
        },
        "lastStatus": "STOPPED",
        "desiredStatus": "STOPPED",
        "cpu": "128",
        "memory": "128",
        "containers": [],
        "version": 2,
        "stoppedReason": "Taskfailedtostart",
        "stopCode": "TaskFailedToStart",
        "connectivity": "CONNECTED",
        "connectivityAt": 1563421494.186,
        "pullStartedAt": 1563421494.252,
        "pullStoppedAt": 1563421496.252,
        "executionStoppedAt": 1563421497,
        "createdAt": 1563421494.186,
        "stoppingAt": 1563421497.252,
        "stoppedAt": 1563421497.252,
        "group": "family:sleep360",
        "launchType": "EC2",
        "attachments": [],
```

```
        "tags": []
    }
}
```

- Para obtener información sobre la API, consulte StopTask en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para etiquetar un recurso

En el siguiente ejemplo de `tag-resource`, se agrega una etiqueta única al recurso especificado.

```
aws ecs tag-resource \
    --resource-arn arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster
    --tags key=key1,value=value1
```

Este comando no genera ninguna salida.

Para agregar varias etiquetas a un recurso

En el siguiente ejemplo de `tag-resource`, se agregan varias etiquetas al recurso especificado.

```
aws ecs tag-resource \
--resource-arn arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster \
--tags key=key1,value=value1 key=key2,value=value2 key=key3,value=value3
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar una etiqueta de un recurso

En el siguiente ejemplo de `untag-resource`, se eliminan la etiquetas enumeradas del recurso especificado.

```
aws ecs untag-resource \
    --resource-arn arn:aws:ecs:us-west-2:123456789012:cluster/MyCluster \
    --tag-keys key1,key2
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-cluster-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-cluster-settings`.

AWS CLI

Para modificar la configuración del clúster

En el siguiente ejemplo de `update-cluster-settings`, se habilita información de contenedores de CloudWatch con observabilidad mejorada para el clúster de `MyCluster`.

```
aws ecs update-cluster-settings \
    --cluster MyCluster \
    --settings name=containerInsights,value=enhanced
```

Salida:

```
{
    "cluster": {
        "clusterArn": "arn:aws:ecs:us-esat-1:123456789012:cluster/MyCluster",
        "clusterName": "default",
        "status": "ACTIVE",
        "registeredContainerInstancesCount": 0,
        "runningTasksCount": 0,
        "pendingTasksCount": 0,
        "activeServicesCount": 0,
        "statistics": [],
```

```
        "tags": [],
        "settings": [
            {
                "name": "containerInsights",
                "value": "enhanced"
            }
        ]
    }
}
```

Para obtener más información, consulte Modificación de la configuración de la cuenta en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte UpdateClusterSettings en la Referencia de comandos de la AWS CLI.

`update-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-cluster`.

AWS CLI

Ejemplo 1: actualización del clúster de ECS mediante la habilitación de containerInsights

El siguiente `update-cluster` actualiza el valor de containerInsights a `enabled` en un clúster ya creado. De forma predeterminada, está desactivado.

```
aws ecs update-cluster \
    --cluster ECS-project-update-cluster \
    --settings name=containerInsights,value=enabled
```

Salida:

```
"cluster": {
    "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/ECS-project-update-
cluster",
    "clusterName": "ECS-project-update-cluster",
    "status": "ACTIVE",
    "registeredContainerInstancesCount": 0,
    "runningTasksCount": 0,
    "pendingTasksCount": 0,
    "activeServicesCount": 0,
    "statistics": [],
```

```
    "tags": [],
    "settings": [
        {
            "name": "containerInsights",
            "value": "enabled"
        }
    ],
    "capacityProviders": [
        "Infra-ECS-Cluster-ECS-project-update-cluster-d6bb6d5b-
EC2CapacityProvider-3fIpdkLywwFt"
    ],
    "defaultCapacityProviderStrategy": [
        {
            "capacityProvider": "Infra-ECS-Cluster-ECS-project-update-cluster-
d6bb6d5b-EC2CapacityProvider-3fIpdkLywwFt",
            "weight": 1,
            "base": 0
        }
    ],
    "attachments": [
        {
            "id": "069d002b-7634-42e4-b1d4-544f4c8f6380",
            "type": "as_policy",
            "status": "CREATED",
            "details": [
                {
                    "name": "capacityProviderName",
                    "value": "Infra-ECS-Cluster-ECS-project-update-cluster-d6bb6d5b-
EC2CapacityProvider-3fIpdkLywwFt"
                },
                {
                    "name": "scalingPolicyName",
                    "value": "ECSManagedAutoScalingPolicy-152363a6-8c65-484c-
b721-42c3e070ae93"
                }
            ]
        },
        {
            "id": "08b5b6ca-45e9-4209-a65d-e962a27c490a",
            "type": "managed_draining",
            "status": "CREATED",
            "details": [
                {
                    "name": "capacityProviderName",
```

```
                    "value": "Infra-ECS-Cluster-ECS-project-update-cluster-d6bb6d5b-
EC2CapacityProvider-3fIpdkLywwFt"
                },
                {
                    "name": "autoScalingLifecycleHookName",
                    "value": "ecs-managed-draining-termination-hook"
                }
            ]
        },
        {
            "id": "45d0b36f-8cff-46b6-9380-1288744802ab",
            "type": "sc",
            "status": "ATTACHED",
            "details": []
        }
    ],
    "attachmentsStatus": "UPDATE_COMPLETE",
    "serviceConnectDefaults": {
        "namespace": "arn:aws:servicediscovery:us-west-2:123456789012:namespace/ns-
igwrsylmy3kwvcdx"
    }
}
```

Ejemplo 2: actualización del clúster de ECS para establecer un espacio de nombres predeterminado de Service Connect

El siguiente `update-cluster` actualiza el clúster de ECS mediante la configuración de un espacio de nombres de Service Connect predeterminado.

```
aws ecs update-cluster \
    --cluster ECS-project-update-cluster \
    --service-connect-defaults namespace=test
```

Salida:

```
 {
     "cluster": {
         "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/ECS-project-
update-cluster",
         "clusterName": "ECS-project-update-cluster",
         "status": "ACTIVE",
         "registeredContainerInstancesCount": 0,
         "runningTasksCount": 0,
```

```
        "pendingTasksCount": 0,
        "activeServicesCount": 0,
        "statistics": [],
        "tags": [],
        "settings": [
            {
                "name": "containerInsights",
                "value": "enabled"
            }
        ],
        "capacityProviders": [
            "Infra-ECS-Cluster-ECS-project-update-cluster-d6bb6d5b-
EC2CapacityProvider-3fIpdkLywwFt"
        ],
        "defaultCapacityProviderStrategy": [
            {
                "capacityProvider": "Infra-ECS-Cluster-ECS-project-update-cluster-
d6bb6d5b-EC2CapacityProvider-3fIpdkLywwFt",
                "weight": 1,
                "base": 0
            }
        ],
        "attachments": [
            {
                "id": "069d002b-7634-42e4-b1d4-544f4c8f6380",
                "type": "as_policy",
                "status": "CREATED",
                "details": [
                    {
                        "name": "capacityProviderName",
                        "value": "Infra-ECS-Cluster-ECS-project-update-cluster-
d6bb6d5b-EC2CapacityProvider-3fIpdkLywwFt"
                    },
                    {
                        "name": "scalingPolicyName",
                        "value": "ECSManagedAutoScalingPolicy-152363a6-8c65-484c-
b721-42c3e070ae93"
                    }
                ]
            },
            {
                "id": "08b5b6ca-45e9-4209-a65d-e962a27c490a",
                "type": "managed_draining",
                "status": "CREATED",
```

```
                "details": [
                    {
                        "name": "capacityProviderName",
                        "value": "Infra-ECS-Cluster-ECS-project-update-cluster-
d6bb6d5b-EC2CapacityProvider-3fIpdkLywwFt"
                    },
                    {
                        "name": "autoScalingLifecycleHookName",
                        "value": "ecs-managed-draining-termination-hook"
                    }
                ]
            },
            {
                "id": "45d0b36f-8cff-46b6-9380-1288744802ab",
                "type": "sc",
                "status": "DELETED",
                "details": []
            },
            {
                "id": "3e6890c3-609c-4832-91de-d6ca891b3ef1",
                "type": "sc",
                "status": "ATTACHED",
                "details": []
            },
            {
                "id": "961b8ec1-c2f1-4070-8495-e669b7668e90",
                "type": "sc",
                "status": "DELETED",
                "details": []
            }
        ],
        "attachmentsStatus": "UPDATE_COMPLETE",
        "serviceConnectDefaults": {
            "namespace": "arn:aws:servicediscovery:us-
west-2:123456789012:namespace/ns-dtjmxqpfi46ht7dr"
        }
    }
}
```


Para obtener más información sobre Service Connect, consulte Uso de Service Connect para conectar los servicios de Amazon ECS con nombres abreviados en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte UpdateCluster en la Referencia de comandos de la AWS CLI.

`update-container-agent`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-container-agent`.

AWS CLI

Para actualizar el agente de contenedor de una instancia de contenedor de Amazon ECS

En el siguiente ejemplo de `update-container-agent`, se actualiza el agente de contenedor de la instancia de contenedor especificada en el clúster predeterminado.

```
aws ecs update-container-agent --cluster default --container-
instance a1b2c3d4-5678-90ab-cdef-11111EXAMPLE
```

Salida:

```
{
    "containerInstance": {
        "status": "ACTIVE",
...
        "agentUpdateStatus": "PENDING",
        "versionInfo": {
            "agentVersion": "1.0.0",
            "agentHash": "4023248",
            "dockerVersion": "DockerVersion: 1.5.0"
        }
    }
}
```

Para obtener más información, consulte Actualización del agente de contenedor de Amazon ECS en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte UpdateContainerAgent en la Referencia de comandos de la AWS CLI.

update-container-instances-state

En el siguiente ejemplo de código, se muestra cómo utilizar update-container-instances-state.

AWS CLI

Para actualizar el estado de una instancia de contenedor

En el siguiente ejemplo de update-container-instances-state, se actualiza el estado de la instancia de contenedor especificada a DRAINING, lo que la elimina del clúster en el que está registrada.

```
aws ecs update-container-instances-state \
    --container-instances 765936fadbdd46b5991a4bd70c2a43d4 \
    --status DRAINING
```

Salida:

```
{
    "containerInstances": [
        {
            "containerInstanceArn": "arn:aws:ecs:us-west-2:130757420319:container-
instance/default/765936fadbdd46b5991a4bd70c2a43d4",
            "ec2InstanceId": "i-013d87ffbb4d513bf",
            "version": 4390,
            "versionInfo": {
                "agentVersion": "1.29.0",
                "agentHash": "a190a73f",
                "dockerVersion": "DockerVersion:18.06.1-ce"
            },
            "remainingResources": [
                {
                    "name": "CPU",
                    "type": "INTEGER",
                    "doubleValue": 0,
                    "longValue": 0,
                    "integerValue": 1536
                },
                {
                    "name": "MEMORY",
                    "type": "INTEGER",
                    "doubleValue": 0,
```

```
                    "longValue": 0,
                    "integerValue": 2681
                },
                {
                    "name": "PORTS",
                    "type": "STRINGSET",
                    "doubleValue": 0,
                    "longValue": 0,
                    "integerValue": 0,
                    "stringSetValue": [
                        "22",
                        "2376",
                        "2375",
                        "51678",
                        "51679"
                    ]
                },
                {
                    "name": "PORTS_UDP",
                    "type": "STRINGSET",
                    "doubleValue": 0,
                    "longValue": 0,
                    "integerValue": 0,
                    "stringSetValue": []
                }
            ],
            "registeredResources": [
                {
                    "name": "CPU",
                    "type": "INTEGER",
                    "doubleValue": 0,
                    "longValue": 0,
                    "integerValue": 2048
                },
                {
                    "name": "MEMORY",
                    "type": "INTEGER",
                    "doubleValue": 0,
                    "longValue": 0,
                    "integerValue": 3705
                },
                {
                    "name": "PORTS",
                    "type": "STRINGSET",
```

```
                    "doubleValue": 0,
                    "longValue": 0,
                    "integerValue": 0,
                    "stringSetValue": [
                        "22",
                        "2376",
                        "2375",
                        "51678",
                        "51679"
                    ]
                },
                {
                    "name": "PORTS_UDP",
                    "type": "STRINGSET",
                    "doubleValue": 0,
                    "longValue": 0,
                    "integerValue": 0,
                    "stringSetValue": []
                }
            ],
            "status": "DRAINING",
            "agentConnected": true,
            "runningTasksCount": 2,
            "pendingTasksCount": 0,
            "attributes": [
                {
                    "name": "ecs.capability.secrets.asm.environment-variables"
                },
                {
                    "name": "ecs.capability.branch-cni-plugin-version",
                    "value": "e0703516-"
                },
                {
                    "name": "ecs.ami-id",
                    "value": "ami-00e0090ac21971297"
                },
                {
                    "name": "ecs.capability.secrets.asm.bootstrap.log-driver"
                },
                {
                    "name": "com.amazonaws.ecs.capability.logging-driver.none"
                },
                {
                    "name": "ecs.capability.ecr-endpoint"
```

```
                },
                {
                    "name": "ecs.capability.docker-plugin.local"
                },
                {
                    "name": "ecs.capability.task-cpu-mem-limit"
                },
                {
                    "name": "ecs.capability.secrets.ssm.bootstrap.log-driver"
                },
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.30"
                },
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.31"
                },
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.32"
                },
                {
                    "name": "ecs.availability-zone",
                    "value": "us-west-2c"
                },
                {
                    "name": "ecs.capability.aws-appmesh"
                },
                {
                    "name": "com.amazonaws.ecs.capability.logging-driver.awslogs"
                },
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.24"
                },
                {
                    "name": "ecs.capability.task-eni-trunking"
                },
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.25"
                },
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.26"
                },
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.27"
                },
```

```
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.28"
                },
                {
                    "name": "com.amazonaws.ecs.capability.privileged-container"
                },
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.29"
                },
                {
                    "name": "ecs.cpu-architecture",
                    "value": "x86_64"
                },
                {
                    "name": "com.amazonaws.ecs.capability.ecr-auth"
                },
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.20"
                },
                {
                    "name": "ecs.os-type",
                    "value": "linux"
                },
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.21"
                },
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.22"
                },
                {
                    "name": "ecs.capability.task-eia"
                },
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.23"
                },
                {
                    "name": "ecs.capability.private-registry-
authentication.secretsmanager"
                },
                {
                    "name": "com.amazonaws.ecs.capability.logging-driver.syslog"
                },
                {
                    "name": "com.amazonaws.ecs.capability.logging-driver.json-file"
```

```
                },
                {
                    "name": "ecs.capability.execution-role-awslogs"
                },
                {
                    "name": "ecs.vpc-id",
                    "value": "vpc-1234"
                },
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.17"
                },
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.18"
                },
                {
                    "name": "com.amazonaws.ecs.capability.docker-remote-api.1.19"
                },
                {
                    "name": "ecs.capability.task-eni"
                },
                {
                    "name": "ecs.capability.execution-role-ecr-pull"
                },
                {
                    "name": "ecs.capability.container-health-check"
                },
                {
                    "name": "ecs.subnet-id",
                    "value": "subnet-1234"
                },
                {
                    "name": "ecs.instance-type",
                    "value": "c5.large"
                },
                {
                    "name": "com.amazonaws.ecs.capability.task-iam-role-network-
host"
                },
                {
                    "name": "ecs.capability.container-ordering"
                },
                {
                    "name": "ecs.capability.cni-plugin-version",
                    "value": "91ccefc8-2019.06.0"
```

```
                },
                {
                    "name": "ecs.capability.pid-ipc-namespace-sharing"
                },
                {
                    "name": "ecs.capability.secrets.ssm.environment-variables"
                },
                {
                    "name": "com.amazonaws.ecs.capability.task-iam-role"
                }
            ],
            "registeredAt": 1560788724.507,
            "attachments": [],
            "tags": []
        }
    ],
    "failures": []
}
```

- Para obtener más información sobre la API, consulte UpdateContainerInstancesState en la Referencia de comandos de la AWS CLI.

update-service-primary-task-set

En el siguiente ejemplo de código, se muestra cómo utilizar `update-service-primary-task-set`.

AWS CLI

Para actualizar el conjunto de tareas principal de un servicio

En el siguiente ejemplo de `update-service-primary-task-set`, se actualiza el conjunto de tareas principal del servicio especificado.

```
aws ecs update-service-primary-task-set \
    --cluster MyCluster \
    --service MyService \
    --primary-task-set arn:aws:ecs:us-west-2:123456789012:task-set/MyCluster/
MyService/ecs-svc/1234567890123456789
```

Salida:

```
{
    "taskSet": {
        "id": "ecs-svc/1234567890123456789",
        "taskSetArn": "arn:aws:ecs:us-west-2:123456789012:task-set/MyCluster/
MyService/ecs-svc/1234567890123456789",
        "status": "PRIMARY",
        "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-definition/
sample-fargate:2",
        "computedDesiredCount": 1,
        "pendingCount": 0,
        "runningCount": 0,
        "createdAt": 1557128360.711,
        "updatedAt": 1557129412.653,
        "launchType": "EC2",
        "networkConfiguration": {
            "awsvpcConfiguration": {
                "subnets": [
                    "subnet-12344321"
                ],
                "securityGroups": [
                    "sg-12344312"
                ],
                "assignPublicIp": "DISABLED"
            }
        },
        "loadBalancers": [],
        "serviceRegistries": [],
        "scale": {
            "value": 50.0,
            "unit": "PERCENT"
        },
        "stabilityStatus": "STABILIZING",
        "stabilityStatusAt": 1557129279.914
    }
}
```

- Para obtener información sobre la API, consulte UpdateServicePrimaryTaskSet en la Referencia de comandos de la AWS CLI.

`update-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-service`.

AWS CLI

Ejemplo 1: Cambio de la definición de tarea utilizada en un servicio

En el siguiente ejemplo de `update-service` se actualiza el servicio `my-http-service` para usar la definición de la tarea `amazon-ecs-sample`.

```
aws ecs update-service \
    --cluster test \
    --service my-http-service \
    --task-definition amazon-ecs-sample
```

Salida:

```
{
    "service": {
        "serviceArn": "arn:aws:ecs:us-west-2:123456789012:service/test/my-http-
service",
        "serviceName": "my-http-service",
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/test",
        "loadBalancers": [],
        "serviceRegistries": [],
        "status": "ACTIVE",
        "desiredCount": 2,
        "runningCount": 2,
        "pendingCount": 0,
        "launchType": "FARGATE",
        "platformVersion": "1.4.0",
        "platformFamily": "Linux",
        "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-definition/
amazon-ecs-sample:2",
        "deploymentConfiguration": {
            "deploymentCircuitBreaker": {
                "enable": true,
                "rollback": true
            },
            "maximumPercent": 200,
            "minimumHealthyPercent": 100,
            "alarms": {
                "alarmNames": [],
                "rollback": false,
                "enable": false
            }
```

```
        },
        "deployments": [
            {
                "id": "ecs-svc/7419115625193919142",
                "status": "PRIMARY",
                "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-
definition/amazon-ecs-sample:2",
                "desiredCount": 0,
                "pendingCount": 0,
                "runningCount": 0,
                "failedTasks": 0,
                "createdAt": "2025-02-21T13:26:02.734000-06:00",
                "updatedAt": "2025-02-21T13:26:02.734000-06:00",
                "launchType": "FARGATE",
                "platformVersion": "1.4.0",
                "platformFamily": "Linux",
                "networkConfiguration": {
                    "awsvpcConfiguration": {
                        "subnets": [
                            "subnet-12344321"
                        ],
                        "securityGroups": [
                            "sg-12344321"
                        ],
                        "assignPublicIp": "ENABLED"
                    }
                },
                "rolloutState": "IN_PROGRESS",
                "rolloutStateReason": "ECS deployment ecs-svc/7419115625193919142 in
 progress."
            },
            {
                "id": "ecs-svc/1709597507655421668",
                "status": "ACTIVE",
                "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-
definition/old-amazon-ecs-sample:4",
                "desiredCount": 2,
                "pendingCount": 0,
                "runningCount": 2,
                "failedTasks": 0,
                "createdAt": "2025-01-24T11:13:07.621000-06:00",
                "updatedAt": "2025-02-02T16:11:30.838000-06:00",
                "launchType": "FARGATE",
                "platformVersion": "1.4.0",
```

```
                "platformFamily": "Linux",
                "networkConfiguration": {
                    "awsvpcConfiguration": {
                        "subnets": [
                            "subnet-12344321"
                        ],
                        "securityGroups": [
                             "sg-12344321"
                        ],
                        "assignPublicIp": "ENABLED"
                    }
                },
                "rolloutState": "COMPLETED",
                "rolloutStateReason": "ECS deployment ecs-svc/1709597507655421668
 completed."
            }
        ],
        "roleArn": "arn:aws:iam::123456789012:role/aws-service-role/
ecs.amazonaws.com/AWSServiceRoleForECS",
        "events": [
            {
                "id": "e40b4d1c-80d9-4834-aaf3-6a268e530e17",
                "createdAt": "2025-02-21T10:31:26.037000-06:00",
                "message": "(my-http-service) has reached a steady state."
            },
            {
                "id": "6ac069ad-fc8b-4e49-a35d-b5574a964c8e",
                "createdAt": "2025-02-21T04:31:22.703000-06:00",
                "message": "(my-http-service) has reached a steady state."
            },
            {
                "id": "265f7d37-dfd1-4880-a846-ec486f341919",
                "createdAt": "2025-02-20T22:31:22.514000-06:00",
                "message": "(my-http-service) has reached a steady state."
            }
        ],
        "createdAt": "2024-10-30T17:12:43.218000-05:00",
        "placementConstraints": [],
        "placementStrategy": [],
        "networkConfiguration": {
            "awsvpcConfiguration": {
                "subnets": [
                    "subnet-12344321",
                ],
```

```
                "securityGroups": [
                    "sg-12344321"
                ],
                "assignPublicIp": "ENABLED"
            }
        },
        "healthCheckGracePeriodSeconds": 0,
        "schedulingStrategy": "REPLICA",
        "deploymentController": {
            "type": "ECS"
        },
        "createdBy": "arn:aws:iam::123456789012:role/AIDACKCEVSQ6C2EXAMPLE",
        "enableECSManagedTags": true,
        "propagateTags": "NONE",
        "enableExecuteCommand": false,
        "availabilityZoneRebalancing": "DISABLED"
    }
}
```

Para obtener más información, consulte Actualización de un servicio de Amazon ECS con la consola en la Guía para desarrolladores de Amazon ECS.

Ejemplo 2: cambio del número de tareas de un servicio

En el siguiente ejemplo de `update-service`, se actualiza el recuento de tareas deseado del servicio `my-http-service` desde 2.

```
aws ecs update-service \
    --cluster MyCluster \
    --service my-http-service \
    --desired-count 2
```

Salida:

```
{
    "service": {
        "serviceArn": "arn:aws:ecs:us-east-1:123456789012:service/MyCluster/my-http-
service",
        "serviceName": "my-http-service",
        "clusterArn": "arn:aws:ecs:us-east-1:123456789012:cluster/MyCluster",
        "loadBalancers": [],
        "serviceRegistries": [],
        "status": "ACTIVE",
```

```
        "desiredCount": 2,
        "runningCount": 1,
        "pendingCount": 0,
        "capacityProviderStrategy": [
            {
                "capacityProvider": "FARGATE",
                "weight": 1,
                "base": 0
            }
        ],
        "platformVersion": "LATEST",
        "platformFamily": "Linux",
        "taskDefinition": "arn:aws:ecs:us-east-1:123456789012:task-definition/
MyTaskDefinition",
        "deploymentConfiguration": {
            "deploymentCircuitBreaker": {
                "enable": true,
                "rollback": true
            },
            "maximumPercent": 200,
            "minimumHealthyPercent": 100,
            "alarms": {
                "alarmNames": [],
                "rollback": false,
                "enable": false
            }
        },
        "deployments": [
            {
                "id": "ecs-svc/1976744184940610707",
                "status": "PRIMARY",
                "taskkDefinition": "arn:aws:ecs:us-east-1:123456789012:task-
definition/MyTaskDefinition",
                "desiredCount": 1,
                "pendingCount": 0,
                "runningCount": 1,
                "failedTasks": 0,
                "createdAt": "2024-12-03T16:24:25.225000-05:00",
                "updatedAt": "2024-12-03T16:25:15.837000-05:00",
                "capacityProviderStrategy": [
                    {
                        "capacityProvider": "FARGATE",
                        "weight": 1,
                        "base": 0
```

```
                    }
                ],
                "platformVersion": "1.4.0",
                "platformFamily": "Linux",
                "networkConfiguration": {
                    "awsvpcConfiguration": {
                        "subnets": [
                            "subnet-0d0eab1bb38d5ca64",
                            "subnet-0db5010045995c2d5"
                        ],
                        "securityGroups": [
                            "sg-02556bf85a191f59a"
                        ],
                        "assignPublicIp": "ENABLED"
                    }
                },
                "rolloutState": "COMPLETED",
                "rolloutStateReason": "ECS deployment ecs-svc/1976744184940610707
 completed."
            }
        ],
        "roleArn": "arn:aws:iam::123456789012:role/aws-service-role/
ecs.amazonaws.com/AWSServiceRoleForECS",
        "events": [
            {
                "id": "f27350b9-4b2a-4e2e-b72e-a4b68380de45",
                "createdAt": "2024-12-30T13:24:07.345000-05:00",
                "message": "(service my-http-service) has reached a steady state."
            },
            {
                "id": "e764ec63-f53f-45e3-9af2-d99f922d2957",
                "createdAt": "2024-12-30T12:32:21.600000-05:00",
                "message": "(service my-http-service) has reached a steady state."
            },
            {
                "id": "28444756-c2fa-47f8-bd60-93a8e05f3991",
                "createdAt": "2024-12-08T19:26:10.367000-05:00",
                "message": "(service my-http-service) has reached a steady state."
            }
        ],
        "createdAt": "2024-12-03T16:24:25.225000-05:00",
        "placementConstraints": [],
        "placementStrategy": [],
        "networkConfiguration": {
```

```
            "awsvpcConfiguration": {
                "subnets": [
                    "subnet-0d0eab1bb38d5ca64",
                    "subnet-0db5010045995c2d5"
                ],
                "securityGroups": [
                    "sg-02556bf85a191f59a"
                ],
                "assignPublicIp": "ENABLED"
            }
        },
        "healthCheckGracePeriodSeconds": 0,
        "schedulingStrategy": "REPLICA",
        "deploymentController": {
            "type": "ECS"
        },
        "createdBy": "arn:aws:iam::123456789012:role/Admin",
        "enableECSManagedTags": true,
        "propagateTags": "NONE",
        "enableExecuteCommand": false,
        "availabilityZoneRebalancing": "ENABLED"
    }
}
```

Para obtener más información, consulte Actualización de un servicio de Amazon ECS con la consola en la Guía para desarrolladores de Amazon ECS.

Ejemplo 3: configuración de los volúmenes de Amazon EBS para adjuntarlos en la actualización del servicio

En el siguiente ejemplo de `update-service` se actualiza el servicio `my-http-service` para utilizar los volúmenes de Amazon EBS. Debe tener configurado un rol de infraestructura de Amazon ECS con la política administrada por `AmazonECSInfrastructureRolePolicyForVolumes` asociada. También debe especificar una definición de tarea con el mismo nombre de volumen que en la solicitud de `update-service` y con `configuredAtLaunch` establecido en `true`. En este ejemplo se utiliza la opción `--cli-input-json` y un archivo de entrada JSON llamado `ebs.json`.

```
aws ecs update-service \
    --cli-input-json file://ebs.json
```

Contenido de `ebs.json`:

```
{
   "cluster": "mycluster",
   "taskDefinition": "mytaskdef",
   "service": "my-http-service",
   "desiredCount": 2,
   "volumeConfigurations": [
        {
            "name": "myEbsVolume",
            "managedEBSVolume": {
                "roleArn":"arn:aws:iam::123456789012:role/ecsInfrastructureRole",
                "volumeType": "gp3",
                "sizeInGiB": 100,
                "iops": 3000,
                "throughput": 125,
                "filesystemType": "ext4"
            }
        }
   ]
}
```

Salida:

```
{
    "service": {
        "serviceArn": "arn:aws:ecs:us-west-2:123456789012:service/mycluster/my-http-
service",
        "serviceName": "my-http-service",
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/mycluster",
        "loadBalancers": [],
        "serviceRegistries": [],
        "status": "ACTIVE",
        "desiredCount": 2,
        "runningCount": 2,
        "pendingCount": 0,
        "launchType": "FARGATE",
        "platformVersion": "LATEST",
        "platformFamily": "Linux",
        "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-definition/
mytaskdef:1",
        "deploymentConfiguration": {
            "deploymentCircuitBreaker": {
                "enable": true,
                "rollback": true
```

```
            },
            "maximumPercent": 200,
            "minimumHealthyPercent": 100,
            "alarms": {
                "alarmNames": [],
                "rollback": false,
                "enable": false
            }
        },
        "deployments": [
            {
                "id": "ecs-svc/2420458347226626275",
                "status": "PRIMARY",
                "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-
definition/mytaskdef:1",
                "desiredCount": 0,
                "pendingCount": 0,
                "runningCount": 0,
                "failedTasks": 0,
                "createdAt": "2025-02-21T15:07:20.519000-06:00",
                "updatedAt": "2025-02-21T15:07:20.519000-06:00",
                "launchType": "FARGATE",
                "platformVersion": "1.4.0",
                "platformFamily": "Linux",
                "networkConfiguration": {
                    "awsvpcConfiguration": {
                        "subnets": [
                            "subnet-12344321",
                        ],
                        "securityGroups": [
                            "sg-12344321"
                        ],
                        "assignPublicIp": "ENABLED"
                    }
                },
                "rolloutState": "IN_PROGRESS",
                "rolloutStateReason": "ECS deployment ecs-svc/2420458347226626275 in
 progress.",
                "volumeConfigurations": [
                    {
                        "name": "ebs-volume",
                        "managedEBSVolume": {
                            "volumeType": "gp3",
                            "sizeInGiB": 100,
```

```
                            "iops": 3000,
                            "throughput": 125,
                            "roleArn": "arn:aws:iam::123456789012:role/
ecsInfrastructureRole",
                            "filesystemType": "ext4"
                        }
                    }
                ]
            },
            {
                "id": "ecs-svc/5191625155316533644",
                "status": "ACTIVE",
                "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-
definition/mytaskdef:2",
                "desiredCount": 2,
                "pendingCount": 0,
                "runningCount": 2,
                "failedTasks": 0,
                "createdAt": "2025-02-21T14:54:48.862000-06:00",
                "updatedAt": "2025-02-21T14:57:22.502000-06:00",
                "launchType": "FARGATE",
                "platformVersion": "1.4.0",
                "platformFamily": "Linux",
                "networkConfiguration": {
                    "awsvpcConfiguration": {
                        "subnets": [
                            "subnet-12344321"
                        ],
                        "securityGroups": [
                            "sg-12344321"
                        ],
                        "assignPublicIp": "ENABLED"
                    }
                },
                "rolloutState": "COMPLETED",
                "rolloutStateReason": "ECS deployment ecs-svc/5191625155316533644
 completed."
            }
        ],
        "roleArn": "arn:aws:iam::123456789012:role/aws-service-role/
ecs.amazonaws.com/AWSServiceRoleForECS",
        "events": [
            {
                "id": "b5823113-c2c5-458e-9649-8c2ed38f23a5",
```

```
                "createdAt": "2025-02-21T14:57:22.508000-06:00",
                "message": "(service my-http-service) has reached a steady state."
            },
            {
                "id": "b05a48e8-da35-4074-80aa-37ceb3167357",
                "createdAt": "2025-02-21T14:57:22.507000-06:00",
                "message": "(service my-http-service) (deployment ecs-
svc/5191625155316533644) deployment completed."
            },
            {
                "id": "a10cd55d-4ba6-4cea-a655-5a5d32ada8a0",
                "createdAt": "2025-02-21T14:55:32.833000-06:00",
                "message": "(service my-http-service) has started 1 tasks: (task
 fb9c8df512684aec92f3c57dc3f22361)."
            },
        ],
        "createdAt": "2025-02-21T14:54:48.862000-06:00",
        "placementConstraints": [],
        "placementStrategy": [],
        "networkConfiguration": {
            "awsvpcConfiguration": {
                "subnets": [
                    "subnet-12344321"
                ],
                "securityGroups": [
                    "sg-12344321"
                ],
                "assignPublicIp": "ENABLED"
            }
        },
        "healthCheckGracePeriodSeconds": 0,
        "schedulingStrategy": "REPLICA",
        "deploymentController": {
            "type": "ECS"
        },
        "createdBy": "arn:aws:iam::123456789012:role/AIDACKCEVSQ6C2EXAMPLE",
        "enableECSManagedTags": true,
        "propagateTags": "NONE",
        "enableExecuteCommand": false,
        "availabilityZoneRebalancing": "ENABLED"
    }
}
```

Para obtener más información, consulte Uso de volúmenes de Amazon EBS con Amazon ECS en la Guía para desarrolladores de Amazon ECS.

Ejemplo 4: actualización de un servicio para que deje de utilizar los volúmenes de Amazon EBS

En el siguiente ejemplo de `update-service` se actualiza el servicio `my-http-service` para dejar de utilizar los volúmenes de Amazon EBS. Debe especificar una revisión de definición de tarea con el parámetro `configuredAtLaunch` establecido en `false`.

```
aws ecs update-service \
    --cluster mycluster \
    --task-definition mytaskdef \
    --service my-http-service \
    --desired-count 2 \
    --volume-configurations "[]"
```

Salida:

```
{
    "service": {
        "serviceArn": "arn:aws:ecs:us-west-2:123456789012:service/mycluster/my-http-
service",
        "serviceName": "my-http-service",
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/mycluster",
        "loadBalancers": [],
        "serviceRegistries": [],
        "status": "ACTIVE",
        "desiredCount": 2,
        "runningCount": 2,
        "pendingCount": 0,
        "launchType": "FARGATE",
        "platformVersion": "LATEST",
        "platformFamily": "Linux",
        "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-definition/
mytaskdef:3",
        "deploymentConfiguration": {
            "deploymentCircuitBreaker": {
                "enable": true,
                "rollback": true
            },
            "maximumPercent": 200,
            "minimumHealthyPercent": 100,
            "alarms": {
```

```
                "alarmNames": [],
                "rollback": false,
                "enable": false
            }
        },
        "deployments": [
            {
                "id": "ecs-svc/7522791612543716777",
                "status": "PRIMARY",
                "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-
definition/mytaskdef:3",
                "desiredCount": 0,
                "pendingCount": 0,
                "runningCount": 0,
                "failedTasks": 0,
                "createdAt": "2025-02-21T15:25:38.598000-06:00",
                "updatedAt": "2025-02-21T15:25:38.598000-06:00",
                    "launchType": "FARGATE",
                "platformVersion": "1.4.0",
                "platformFamily": "Linux",
                "networkConfiguration": {
                    "awsvpcConfiguration": {
                        "subnets": [
                            "subnet-12344321"
                        ],
                        "securityGroups": [
                            "sg-12344321"
                        ],
                        "assignPublicIp": "ENABLED"
                    }
                },
                "rolloutState": "IN_PROGRESS",
                "rolloutStateReason": "ECS deployment ecs-svc/7522791612543716777 in
 progress."
            },
            {
                "id": "ecs-svc/2420458347226626275",
                "status": "ACTIVE",
                "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-
definition/myoldtaskdef:1",
                "desiredCount": 2,
                "pendingCount": 0,
                "runningCount": 2,
                "failedTasks": 0,
```

```
                "createdAt": "2025-02-21T15:07:20.519000-06:00",
                "updatedAt": "2025-02-21T15:10:59.955000-06:00",
                "launchType": "FARGATE",
                "platformVersion": "1.4.0",
                "platformFamily": "Linux",
                "networkConfiguration": {
                    "awsvpcConfiguration": {
                        "subnets": [
                            "subnet-12344321"
                        ],
                        "securityGroups": [
                            "sg-12344321"
                        ],
                        "assignPublicIp": "ENABLED"
                    }
                },
                "rolloutState": "COMPLETED",
                "rolloutStateReason": "ECS deployment ecs-svc/2420458347226626275
 completed.",
                "volumeConfigurations": [
                    {
                        "name": "ebs-volume",
                        "managedEBSVolume": {
                            "volumeType": "gp3",
                            "sizeInGiB": 100,
                            "iops": 3000,
                            "throughput": 125,
                            "roleArn": "arn:aws:iam::123456789012:role/
ecsInfrastructureRole",
                            "filesystemType": "ext4"
                        }
                    }
                ]
            }
        ],
        "roleArn": "arn:aws:iam::123456789012:role/aws-service-role/
ecs.amazonaws.com/AWSServiceRoleForECS",
        "events": [
            {
                "id": "4f2c3ca1-7800-4048-ba57-bba210ada2ad",
                "createdAt": "2025-02-21T15:10:59.959000-06:00",
                "message": "(service my-http-service) has reached a steady state."
            },
            {
```

```
                "id": "4b36a593-2d40-4ed6-8be8-b9b699eb6198",
                "createdAt": "2025-02-21T15:10:59.958000-06:00",
                "message": "(service my-http-service) (deployment ecs-
svc/2420458347226626275) deployment completed."
            },
            {
                "id": "88380089-14e2-4ef0-8dbb-a33991683371",
                "createdAt": "2025-02-21T15:09:39.055000-06:00",
                "message": "(service my-http-service) has stopped 1 running tasks:
 (task fb9c8df512684aec92f3c57dc3f22361)."
            },
            {
                "id": "97d84243-d52f-4255-89bb-9311391c61f6",
                "createdAt": "2025-02-21T15:08:57.653000-06:00",
                "message": "(service my-http-service) has stopped 1 running tasks:
 (task 33eff090ad2c40539daa837e6503a9bc)."
            },
            {
                "id": "672ece6c-e2d0-4021-b5da-eefb14001687",
                "createdAt": "2025-02-21T15:08:15.631000-06:00",
                "message": "(service my-http-service) has started 1 tasks: (task
 996c02a66ff24f3190a4a8e0c841740f)."
            },
            {
                "id": "a3cf9bea-9be6-4175-ac28-4c68360986eb",
                "createdAt": "2025-02-21T15:07:36.931000-06:00",
                "message": "(service my-http-service) has started 1 tasks: (task
 d5d23c39f89e46cf9a647b9cc6572feb)."
            },
            {
                "id": "b5823113-c2c5-458e-9649-8c2ed38f23a5",
                "createdAt": "2025-02-21T14:57:22.508000-06:00",
                "message": "(service my-http-service) has reached a steady state."
            },
            {
                "id": "b05a48e8-da35-4074-80aa-37ceb3167357",
                "createdAt": "2025-02-21T14:57:22.507000-06:00",
                "message": "(service my-http-service) (deployment ecs-
svc/5191625155316533644) deployment completed."
            },
            {
                "id": "a10cd55d-4ba6-4cea-a655-5a5d32ada8a0",
                "createdAt": "2025-02-21T14:55:32.833000-06:00",
```

```
                "message": "(service my-http-service) has started 1 tasks: (task
 fb9c8df512684aec92f3c57dc3f22361)."
            },
            {
                "id": "42da91fa-e26d-42ef-88c3-bb5965c56b2f",
                "createdAt": "2025-02-21T14:55:02.703000-06:00",
                "message": "(service my-http-service) has started 1 tasks: (task
 33eff090ad2c40539daa837e6503a9bc)."
            }
        ],
        "createdAt": "2025-02-21T14:54:48.862000-06:00",
        "placementConstraints": [],
        "placementStrategy": [],
        "networkConfiguration": {
            "awsvpcConfiguration": {
                "subnets": [
                    "subnet-12344321"
                ],
                "securityGroups": [
                    "sg-12344321"
                ],
                "assignPublicIp": "ENABLED"
            }
        },
        "healthCheckGracePeriodSeconds": 0,
        "schedulingStrategy": "REPLICA",
        "deploymentController": {
            "type": "ECS"
        },
        "createdBy": "arn:aws:iam::123456789012:role/AIDACKCEVSQ6C2EXAMPLE",
        "enableECSManagedTags": true,
        "propagateTags": "NONE",
        "enableExecuteCommand": false,
        "availabilityZoneRebalancing": "ENABLED"
    }
}
```

Para obtener más información, consulte Uso de volúmenes de Amazon EBS con Amazon ECS en la Guía para desarrolladores de Amazon ECS.

Ejemplo 5: activación del reequilibrado de zonas de disponibilidad para un servicio

En el siguiente ejemplo de `update-service`, se activa el reequilibrado de zonas de disponibilidad para el servicio `my-http-service`.

```
aws ecs update-service \
    --cluster MyCluster \
    --service my-http-service \
    --availability-zone-rebalancing ENABLED
```

Salida:

```
{
    "service": {
        "serviceArn": "arn:aws:ecs:us-east-1:123456789012:service/MyCluster/my-http-
service",
        "serviceName": "my-http-service",
        "clusterArn": "arn:aws:ecs:us-east-1:123456789012:cluster/MyCluster",
        "loadBalancers": [],
        "serviceRegistries": [],
        "status": "ACTIVE",
        "desiredCount": 2,
        "runningCount": 1,
        "pendingCount": 0,
        "capacityProviderStrategy": [
            {
                "capacityProvider": "FARGATE",
                "weight": 1,
                "base": 0
            }
        ],
        "platformVersion": "LATEST",
        "platformFamily": "Linux",
        "taskDefinition": "arn:aws:ecs:us-east-1:123456789012:task-definition/
MyTaskDefinition",
        "deploymentConfiguration": {
            "deploymentCircuitBreaker": {
                "enable": true,
                "rollback": true
            },
            "maximumPercent": 200,
            "minimumHealthyPercent": 100,
            "alarms": {
                "alarmNames": [],
                "rollback": false,
```

```
                "enable": false
            }
        },
        "deployments": [
            {
                "id": "ecs-svc/1976744184940610707",
                "status": "PRIMARY",
                "taskkDefinition": "arn:aws:ecs:us-east-1:123456789012:task-
definition/MyTaskDefinition",
                "desiredCount": 1,
                "pendingCount": 0,
                "runningCount": 1,
                "failedTasks": 0,
                "createdAt": "2024-12-03T16:24:25.225000-05:00",
                "updatedAt": "2024-12-03T16:25:15.837000-05:00",
                "capacityProviderStrategy": [
                    {
                        "capacityProvider": "FARGATE",
                        "weight": 1,
                        "base": 0
                    }
                ],
                "platformVersion": "1.4.0",
                "platformFamily": "Linux",
                "networkConfiguration": {
                    "awsvpcConfiguration": {
                        "subnets": [
                            "subnet-0d0eab1bb38d5ca64",
                            "subnet-0db5010045995c2d5"
                        ],
                        "securityGroups": [
                            "sg-02556bf85a191f59a"
                        ],
                        "assignPublicIp": "ENABLED"
                    }
                },
                "rolloutState": "COMPLETED",
                "rolloutStateReason": "ECS deployment ecs-svc/1976744184940610707
 completed."
            }
        ],
        "roleArn": "arn:aws:iam::123456789012:role/aws-service-role/
ecs.amazonaws.com/AWSServiceRoleForECS",
        "events": [],
```

```
        "createdAt": "2024-12-03T16:24:25.225000-05:00",
        "placementConstraints": [],
        "placementStrategy": [],
        "networkConfiguration": {
            "awsvpcConfiguration": {
                "subnets": [
                    "subnet-0d0eab1bb38d5ca64",
                    "subnet-0db5010045995c2d5"
                ],
                "securityGroups": [
                    "sg-02556bf85a191f59a"
                ],
                "assignPublicIp": "ENABLED"
            }
        },
        "healthCheckGracePeriodSeconds": 0,
        "schedulingStrategy": "REPLICA",
        "deploymentController": {
            "type": "ECS"
        },
        "createdBy": "arn:aws:iam::123456789012:role/Admin",
        "enableECSManagedTags": true,
        "propagateTags": "NONE",
        "enableExecuteCommand": false,
        "availabilityZoneRebalancing": "ENABLED"
    }
}
```

Para obtener más información, consulte Actualización de un servicio de Amazon ECS con la consola en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte UpdateService en la Referencia de comandos de la AWS CLI.

`update-task-protection`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-task-protection`.

AWS CLI

Ejemplo 1: habilitación de la protección de tareas para las tareas de ECS

El siguiente `update-task-protection` protege la tarea de ECS de la finalización durante la reducción horizontal desde implementaciones o escalado automático de servicios. Puede especificar un periodo de caducidad personalizado para la protección de tareas, de 1 a 2880 minutos (48 horas). Si no especifica el periodo de caducidad, el tiempo predeterminado para habilitar la protección de tareas es de 2 horas.

```
aws ecs update-task-protection \
    --cluster ECS-project-update-cluster \
    --tasks c43ed3b1331041f289316f958adb6a24 \
    --protection-enabled \
    --expires-in-minutes 300
```

Salida:

```
{
"protectedTasks": [
    {
        "taskArn": "arn:aws:ecs:us-west-2:123456789012:task/
c43ed3b1331041f289316f958adb6a24",
        "protectionEnabled": true,
        "expirationDate": "2024-09-14T19:53:36.687000-05:00"
    }
],
"failures": []
}
```

Ejemplo 2: desactivación de la protección de tareas para las tareas de ECS

El siguiente `update-task-protection` desactiva las tareas protegidas de la reducción horizontal desde implementaciones o Service AutoScaling.

```
aws ecs update-task-protection \
    --cluster ECS-project-update-cluster \
    --tasks c43ed3b1331041f289316f958adb6a24 \
    --no-protection-enabled
```

Salida:

```
{
    "protectedTasks": [
```

```
        {
            "taskArn": "arn:aws:ecs:us-west-2:123456789012:task/
c43ed3b1331041f289316f958adb6a24",
            "protectionEnabled": false
        }
    ],
    "failures": []
}
```

Para obtener más información sobre la protección de tareas, consulte Proteger las tareas de Amazon ECS para que no finalicen por eventos de reducción horizontal en la Guía para desarrolladores de Amazon ECS.

- Para obtener información sobre la API, consulte UpdateTaskProtection en la Referencia de comandos de AWS CLI.

`update-task-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-task-set`.

AWS CLI

Para actualizar un conjunto de tareas

En el siguiente ejemplo de `update-task-set`, se actualiza un conjunto de tareas para ajustar la escala.

```
aws ecs update-task-set \
    --cluster MyCluster \
    --service MyService \
    --task-set arn:aws:ecs:us-west-2:123456789012:task-set/MyCluster/MyService/ecs-
svc/1234567890123456789 \
    --scale value=50,unit=PERCENT
```

Salida:

```
{
    "taskSet": {
        "id": "ecs-svc/1234567890123456789",
        "taskSetArn": "arn:aws:ecs:us-west-2:123456789012:task-set/MyCluster/
MyService/ecs-svc/1234567890123456789",
```

```
        "status": "ACTIVE",
        "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-definition/
sample-fargate:2",
        "computedDesiredCount": 0,
        "pendingCount": 0,
        "runningCount": 0,
        "createdAt": 1557128360.711,
        "updatedAt": 1557129279.914,
        "launchType": "EC2",
        "networkConfiguration": {
            "awsvpcConfiguration": {
                "subnets": [
                    "subnet-12344321"
                ],
                "securityGroups": [
                    "sg-12344321"
                ],
                "assignPublicIp": "DISABLED"
            }
        },
        "loadBalancers": [],
        "serviceRegistries": [],
        "scale": {
            "value": 50.0,
            "unit": "PERCENT"
        },
        "stabilityStatus": "STABILIZING",
        "stabilityStatusAt": 1557129279.914
    }
}
```

- Para obtener información sobre la API, consulte UpdateTaskSet en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon EFS que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante el uso de la AWS Command Line Interface con Amazon EFS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-file-system`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-file-system`.

AWS CLI

Para crear un sistema de archivos cifrado

En el siguiente ejemplo de `create-file-system`, se crea un sistema de archivos cifrado con la CMK predeterminada. También se agrega la etiqueta `Name=my-file-system`.

```
aws efs create-file-system \
    --performance-mode generalPurpose \
    --throughput-mode bursting \
    --encrypted \
    --tags Key=Name,Value=my-file-system
```

Salida:

```
{
    "OwnerId": "123456789012",
    "CreationToken": "console-d7f56c5f-e433-41ca-8307-9d9c0example",
    "FileSystemId": "fs-c7a0456e",
    "FileSystemArn": "arn:aws:elasticfilesystem:us-west-2:123456789012:file-system/
fs-48499b4d",
    "CreationTime": 1595286880.0,
    "LifeCycleState": "creating",
    "Name": "my-file-system",
    "NumberOfMountTargets": 0,
    "SizeInBytes": {
        "Value": 0,
        "ValueInIA": 0,
        "ValueInStandard": 0
    },
```

```
    "PerformanceMode": "generalPurpose",
    "Encrypted": true,
    "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/a59b3472-e62c-42e4-
adcf-30d92example",
    "ThroughputMode": "bursting",
    "Tags": [
        {
            "Key": "Name",
            "Value": "my-file-system"
        }
    ]
}
```

Para obtener más información, consulte Creating Amazon EFS file systems en la Guía del usuario de Amazon Elastic File System.

- Para obtener información sobre la API, consulte CreateFileSystem en la Referencia de comandos de la AWS CLI.

`create-mount-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-mount-target`.

AWS CLI

Para crear un destino de montaje

En el siguiente ejemplo de `create-mount-target`, se crea un destino de montaje para el sistema de archivos especificado.

```
aws efs create-mount-target \
    --file-system-id fs-c7a0456e \
    --subnet-id subnet-02bf4c428bexample \
    --security-groups sg-068f739363example
```

Salida:

```
{
    "OwnerId": "123456789012",
    "MountTargetId": "fsmt-f9a14450",
    "FileSystemId": "fs-c7a0456e",
    "SubnetId": "subnet-02bf4c428bexample",
    "LifeCycleState": "creating",
```

```
    "IpAddress": "10.0.1.24",
    "NetworkInterfaceId": "eni-02d542216aexample",
    "AvailabilityZoneId": "use2-az2",
    "AvailabilityZoneName": "us-east-2b",
    "VpcId": "vpc-0123456789abcdef0"
}
```

Para obtener más información, consulte Creating mount targets en la Guía del usuario de Amazon Elastic File System.

- Para obtener información sobre la API, consulte CreateMountTarget en la Referencia de comandos de la AWS CLI.

`delete-file-system`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-file-system`.

AWS CLI

Para eliminar un sistema de archivos

En el siguiente ejemplo de `delete-file-system`, se elimina el sistema de archivos especificado.

```
aws efs delete-file-system \
    --file-system-id fs-c7a0456e
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting an Amazon EFS file system en la Guía del usuario de Amazon Elastic File System.

- Para obtener información sobre la API, consulte DeleteFileSystem en la Referencia de comandos de la AWS CLI.

`delete-mount-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-mount-target`.

AWS CLI

Para eliminar un destino de montaje

En el siguiente ejemplo de `delete-mount-target`, se elimina el destino de montaje especificado.

```
aws efs delete-mount-target \
    --mount-target-id fsmt-f9a14450
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creating mount targets en la Guía del usuario de Amazon Elastic File System.

- Para obtener información sobre la API, consulte DeleteMountTarget en la Referencia de comandos de la AWS CLI.

`describe-file-systems`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-file-systems`.

AWS CLI

Para describir un sistema de archivos

En el siguiente ejemplo de `describe-file-systems`, se describe el sistema de archivos especificado.

```
aws efs describe-file-systems \
    --file-system-id fs-c7a0456e
```

Salida:

```
{
    "FileSystems": [
        {
            "OwnerId": "123456789012",
            "CreationToken": "console-d7f56c5f-e433-41ca-8307-9d9c0example",
            "FileSystemId": "fs-c7a0456e",
            "FileSystemArn": "arn:aws:elasticfilesystem:us-west-2:123456789012:file-
system/fs-48499b4d",
            "CreationTime": 1595286880.0,
            "LifeCycleState": "available",
            "Name": "my-file-system",
            "NumberOfMountTargets": 3,
```

```
            "SizeInBytes": {
                "Value": 6144,
                "Timestamp": 1600991437.0,
                "ValueInIA": 0,
                "ValueInStandard": 6144
            },
            "PerformanceMode": "generalPurpose",
            "Encrypted": true,
            "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/a59b3472-e62c-42e4-
adcf-30d92example",
            "ThroughputMode": "bursting",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "my-file-system"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Managing Amazon EFS file systems en la Guía del usuario de Amazon Elastic File System.

- Para obtener información sobre la API, consulte DescribeFileSystems en la Referencia de comandos de la AWS CLI.

`describe-mount-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-mount-targets`.

AWS CLI

Para describir un destino de montaje

En el siguiente ejemplo de `describe-mount-targets`, se describe el destino de montaje especificado.

```
aws efs describe-mount-targets \
    --mount-target-id fsmt-f9a14450
```

Salida:

```
{
    "MountTargets": [
        {
            "OwnerId": "123456789012",
            "MountTargetId": "fsmt-f9a14450",
            "FileSystemId": "fs-c7a0456e",
            "SubnetId": "subnet-02bf4c428bexample",
            "LifeCycleState": "creating",
            "IpAddress": "10.0.1.24",
            "NetworkInterfaceId": "eni-02d542216aexample",
            "AvailabilityZoneId": "use2-az2",
            "AvailabilityZoneName": "us-east-2b",
            "VpcId": "vpc-0123456789abcdef0"
        }
    ]
}
```

Para obtener más información, consulte Creating mount targets en la Guía del usuario de Amazon Elastic File System.

- Para obtener información sobre la API, consulte DescribeMountTargets en la Referencia de comandos de la AWS CLI.

`describe-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-tags`.

AWS CLI

Para describir las etiquetas de un sistema de archivos

En el siguiente ejemplo de `describe-tags`, se describen las etiquetas del sistema de archivos especificado.

```
aws efs describe-tags \
    --file-system-id fs-c7a0456e
```

Salida:

```
{
    "Tags": [
        {
```

```
            "Key": "Name",
            "Value": "my-file-system"
        },
        {
            "Key": "Department",
            "Value": "Business Intelligence"
        }
    ]
}
```

Para obtener más información, consulte Managing file system tags en la Guía del usuario de Amazon Elastic File System.

- Para obtener detalles sobre la API, consulte DescribeTags en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para recuperar las etiquetas de un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se recuperan las etiquetas asociadas al sistema de archivos especificado.

```
aws efs list-tags-for-resource \
    --resource-id fs-c7a0456e
```

Salida:

```
{
    "Tags": [
        {
            "Key": "Name",
            "Value": "my-file-system"
        },
        {
            "Key": "Department",
            "Value": "Business Intelligence"
        }
```

```
    ]
}
```

Para obtener más información, consulte Managing file system tags en la Guía del usuario de Amazon Elastic File System.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para etiquetar un recurso

En el siguiente ejemplo de `tag-resource`, se agrega la etiqueta `Department=Business Intelligence` al sistema de archivos especificado.

```
aws efs tag-resource \
    --resource-id fs-c7a0456e \
    --tags Key=Department,Value="Business Intelligence"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing file system tags en la Guía del usuario de Amazon Elastic File System.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar una etiqueta de un recurso

En el siguiente ejemplo de `untag-resource`, se elimina la etiqueta con la clave de etiqueta `Department` del sistema de archivos especificado.

```
aws efs untag-resource \
    --resource-id fs-c7a0456e \
    --tag-keys Department
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing file system tags en la Guía del usuario de Amazon Elastic File System.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon EKS que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante el uso de la AWS Command Line Interface con Amazon EKS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-access-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-access-policy`.

AWS CLI

Asociación de una política de acceso y su ámbito de aplicación a la entrada de acceso del clúster

En el siguiente ejemplo de `associate-access-policy` se asocia una política de acceso y su ámbito a la entrada de acceso del clúster especificado.

```
aws eks associate-access-policy \
```

```
    --cluster-name eks-customer \
    --principal-arn arn:aws:iam::111122223333:role/Admin \
    --policy-arn arn:aws:eks::aws:cluster-access-policy/AmazonEKSEditPolicy \
    --access-scope type=namespace,namespaces=default
```

Salida:

```
{
    "clusterName": "eks-customer",
    "principalArn": "arn:aws:iam::111122223333:role/Admin",
    "associatedAccessPolicy": {
        "policyArn": "arn:aws:eks::aws:cluster-access-policy/AmazonEKSEditPolicy",
        "accessScope": {
            "type": "namespace",
            "namespaces": [
                "default"
            ]
        },
        "associatedAt": "2025-05-24T15:59:51.981000-05:00",
        "modifiedAt": "2025-05-24T15:59:51.981000-05:00"
    }
}
```

Para obtener más información, consulte Asociación de políticas de acceso con entradas de acceso en la Guía del usuario de Amazon EKS.

- Para obtener detalles sobre la API, consulte AssociateAccessPolicy en la Referencia de comandos de la AWS CLI.

`associate-encryption-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-encryption-config`.

AWS CLI

Para asociar una configuración de cifrado a un clúster existente

En el siguiente ejemplo de `associate-encryption-config` se habilita el cifrado en un clúster de EKS existente que aún no tiene habilitado el cifrado.

```
aws eks associate-encryption-config \
    --cluster-name my-eks-cluster \
```

```
    --encryption-config '[{"resources":["secrets"],"provider":
{"keyArn":"arn:aws:kms:region-code:account:key/key"}}]'
```

Salida:

```
{
    "update": {
        "id": "3141b835-8103-423a-8e68-12c2521ffa4d",
        "status": "InProgress",
        "type": "AssociateEncryptionConfig",
        "params": [
            {
                "type": "EncryptionConfig",
                "value": "[{\"resources\":[\"secrets\"],\"provider\":{\"keyArn\":
\"arn:aws:kms:region-code:account:key/key\"}}]"
            }
        ],
        "createdAt": "2024-03-14T11:01:26.297000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Cifrado de los secretos de Kubernetes con AWS KMS en los clústeres existentes en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte AssociateEncryptionConfig en la Referencia de comandos de la AWS CLI.

`associate-identity-provider-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-identity-provider-config`.

AWS CLI

Asociación del proveedor de identidad al clúster de Amazon EKS

En el siguiente ejemplo de `associate-identity-provider-config` se asocia un proveedor de identidad a su clúster de Amazon EKS.

```
aws eks associate-identity-provider-config \
    --cluster-name my-eks-cluster \
```

```
    --oidc 'identityProviderConfigName=my-identity-provider,issuerUrl=https://
oidc.eks.us-east-2.amazonaws.com/
id/38D6A4619A0A69E342B113ED7F1A7652,clientId=kubernetes,usernameClaim=email,usernamePrefix=m
username-prefix,groupsClaim=my-claim,groupsPrefix=my-groups-
prefix,requiredClaims={Claim1=value1,Claim2=value2}' \
    --tags env=dev
```

Salida:

```
{
    "update": {
        "id": "8c6c1bef-61fe-42ac-a242-89412387b8e7",
        "status": "InProgress",
        "type": "AssociateIdentityProviderConfig",
        "params": [
            {
                "type": "IdentityProviderConfig",
                "value": "[{\"type\":\"oidc\",\"name\":\"my-identity-provider\"}]"
            }
        ],
        "createdAt": "2024-04-11T13:46:49.648000-04:00",
        "errors": []
    },
    "tags": {
        "env": "dev"
    }
}
```

Para obtener más información, consulte Concesión de acceso a los usuarios a Kubernetes con un proveedor de OIDC externo. Asociación de un proveedor de identidad OIDC en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte AssociateIdentityProviderConfig en la Referencia de comandos de la AWS CLI.

`create-access-entry`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-access-entry`.

AWS CLI

Ejemplo 1: creación de la entrada de acceso para el clúster de EKS

En el siguiente ejemplo de `create-access-entry` se crea una entrada de acceso que permite a una entidad principal de IAM acceder al clúster de EKS.

```
aws eks create-access-entry \
    --cluster-name eks-customer \
    --principal-arn arn:aws:iam::111122223333:user/eks-user
```

Salida:

```
{
    "accessEntry": {
        "clusterName": "eks-customer",
        "principalArn": "arn:aws:iam::111122223333:user/eks-user",
        "kubernetesGroups": [],
        "accessEntryArn": "arn:aws:eks:us-west-2:111122223333:access-entry/eks-
customer/user/111122223333/eks-user/a1b2c3d4-5678-90ab-cdef-a6506e3d36p0",
        "createdAt": "2025-04-14T22:45:48.097000-05:00",
        "modifiedAt": "2025-04-14T22:45:48.097000-05:00",
        "tags": {},
        "username": "arn:aws:iam::111122223333:user/eks-user",
        "type": "STANDARD"
    }
}
```

Para obtener más información, consulte Creación de entradas de acceso en la Guía del usuario de Amazon EKS.

Ejemplo 2: creación de la entrada de acceso para el clúster de EKS mediante la especificación del tipo de entrada de acceso

En el siguiente ejemplo de `create-access-entry` se crea una entrada de acceso de tipo `EC2_LINUX` en el clúster de EKS. De forma predeterminada, se crea una entrada de acceso de tipo `STANDARD`. Aparte del valor predeterminado, si especificamos cualquier otro tipo de entrada de acceso, es necesario pasar un ARN de rol de IAM en la CLI.

```
aws eks create-access-entry \
    --cluster-name eks-customer \
    --principal-arn arn:aws:iam::111122223333:role/admin-test-ip \
    --type EC2_LINUX
```

Salida:

```
{
    "accessEntry": {
        "clusterName": "eks-customer",
        "principalArn": "arn:aws:iam::111122223333:role/admin-test-ip",
        "kubernetesGroups": [
            "system:nodes"
        ],
        "accessEntryArn": "arn:aws:eks:us-west-2:111122223333:access-entry/eks-
customer/role/111122223333/admin-test-ip/accb5418-f493-f390-3e6e-c3f19f725fcp",
        "createdAt": "2025-05-06T19:42:45.453000-05:00",
        "modifiedAt": "2025-05-06T19:42:45.453000-05:00",
        "tags": {},
        "username": "system:node:{{EC2PrivateDNSName}}",
        "type": "EC2_LINUX"
    }
}
```

Para obtener más información, consulte Creación de entradas de acceso en la Guía del usuario de Amazon EKS.

- Para obtener detalles de la API, consulte CreateAccessEntry en la Referencia de comandos de AWS CLI.

`create-addon`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-addon`.

AWS CLI

Ejemplo 1: creación de un complemento de Amazon EKS con una versión compatible predeterminada para la versión del clúster de EKS correspondiente

En el siguiente ejemplo del comando `create-addon` se crea un complemento de Amazon EKS con una versión compatible predeterminada para la versión del clúster de EKS correspondiente.

```
aws eks create-addon \
    --cluster-name my-eks-cluster \
    --addon-name my-eks-addon \
    --service-account-role-arn arn:aws:iam::111122223333:role/role-name
```

Salida:

```
{
    "addon": {
        "addonName": "my-eks-addon",
        "clusterName": "my-eks-cluster",
        "status": "CREATING",
        "addonVersion": "v1.15.1-eksbuild.1",
        "health": {
            "issues": []
        },
        "addonArn": "arn:aws:eks:us-east-2:111122223333:addon/my-eks-cluster/my-eks-
addon/1ec71ee1-b9c2-8915-4e17-e8be0a55a149",
        "createdAt": "2024-03-14T12:20:03.264000-04:00",
        "modifiedAt": "2024-03-14T12:20:03.283000-04:00",
        "serviceAccountRoleArn": "arn:aws:iam::111122223333:role/role-name",
        "tags": {}
    }
}
```

Para obtener más información, consulte Managing Amazon EKS add-ons - Creating an add-on en la Guía del usuario de Amazon EKS.

Ejemplo 2: creación de un complemento de Amazon EKS con una versión del complemento específica

En el siguiente ejemplo del comando `create-addon` se crea un complemento de Amazon EKS con una versión del complemento específica.

```
aws eks create-addon \
    --cluster-name my-eks-cluster \
    --addon-name my-eks-addon \
    --service-account-role-arn arn:aws:iam::111122223333:role/role-name \
    --addon-version v1.16.4-eksbuild.2
```

Salida:

```
{
    "addon": {
        "addonName": "my-eks-addon",
        "clusterName": "my-eks-cluster",
        "status": "CREATING",
        "addonVersion": "v1.16.4-eksbuild.2",
        "health": {
```

```
            "issues": []
        },
        "addonArn": "arn:aws:eks:us-east-2:111122223333:addon/my-eks-cluster/my-eks-
addon/34c71ee6-7738-6c8b-c6bd-3921a176b5ff",
        "createdAt": "2024-03-14T12:30:24.507000-04:00",
        "modifiedAt": "2024-03-14T12:30:24.521000-04:00",
        "serviceAccountRoleArn": "arn:aws:iam::111122223333:role/role-name",
        "tags": {}
    }
}
```

Para obtener más información, consulte Managing Amazon EKS add-ons - Creating an add-on en la Guía del usuario de Amazon EKS.

Ejemplo 3: creación de un complemento de Amazon EKS con valores de configuración personalizados y datos de resolución de conflictos

En el siguiente ejemplo del comando `create-addon` se crea un complemento de Amazon EKS con valores de configuración personalizados y datos de resolución de conflictos.

```
aws eks create-addon \
    --cluster-name my-eks-cluster \
    --addon-name my-eks-addon \
    --service-account-role-arn arn:aws:iam::111122223333:role/role-name \
    --addon-version v1.16.4-eksbuild.2 \
    --configuration-values '{"resources":{"limits":{"cpu":"100m"}}}' \
    --resolve-conflicts OVERWRITE
```

Salida:

```
{
    "addon": {
        "addonName": "my-eks-addon",
        "clusterName": "my-eks-cluster",
        "status": "CREATING",
        "addonVersion": "v1.16.4-eksbuild.2",
        "health": {
            "issues": []
        },
        "addonArn": "arn:aws:eks:us-east-2:111122223333:addon/my-eks-cluster/my-eks-
addon/a6c71ee9-0304-9237-1be8-25af1b0f1ffb",
        "createdAt": "2024-03-14T12:35:58.313000-04:00",
        "modifiedAt": "2024-03-14T12:35:58.327000-04:00",
```

```
        "serviceAccountRoleArn": "arn:aws:iam::111122223333:role/role-name",
        "tags": {},
        "configurationValues": "{\"resources\":{\"limits\":{\"cpu\":\"100m\"}}}"
    }
}
```

Para obtener más información, consulte Managing Amazon EKS add-ons - Creating an add-on en la Guía del usuario de Amazon EKS.

Ejemplo 4: creación de un complemento de Amazon EKS con un archivo de JSON de valores de configuración personalizados

En el siguiente ejemplo del comando `create-addon` se crea un complemento de Amazon EKS con valores de configuración personalizados y datos de resolución de conflictos.

```
aws eks create-addon \
    --cluster-name my-eks-cluster \
    --addon-name my-eks-addon \
    --service-account-role-arn arn:aws:iam::111122223333:role/role-name \
    --addon-version v1.16.4-eksbuild.2 \
    --configuration-values 'file://configuration-values.json' \
    --resolve-conflicts OVERWRITE \
    --tags '{"eks-addon-key-1": "value-1" , "eks-addon-key-2": "value-2"}'
```

Contenido de `configuration-values.json`:

```
{
    "resources": {
        "limits": {
            "cpu": "150m"
        }
    },
    "env": {
        "AWS_VPC_K8S_CNI_LOGLEVEL": "ERROR"
    }
}
```

Salida:

```
{
    "addon": {
        "addonName": "my-eks-addon",
```

```
        "clusterName": "my-eks-cluster",
        "status": "CREATING",
        "addonVersion": "v1.16.4-eksbuild.2",
        "health": {
            "issues": []
        },
        "addonArn": "arn:aws:eks:us-east-2:111122223333:addon/my-eks-cluster/my-eks-
addon/d8c71ef8-fbd8-07d0-fb32-6a7be19ececd",
        "createdAt": "2024-03-14T13:10:51.763000-04:00",
        "modifiedAt": "2024-03-14T13:10:51.777000-04:00",
        "serviceAccountRoleArn": "arn:aws:iam::111122223333:role/role-name",
        "tags": {
            "eks-addon-key-1": "value-1",
            "eks-addon-key-2": "value-2"
        },
        "configurationValues": "{\n    \"resources\": {\n        \"limits\":
 {\n            \"cpu\": \"150m\"\n        }\n    },\n    \"env\": {\n
 \"AWS_VPC_K8S_CNI_LOGLEVEL\": \"ERROR\"\n    }\n}"
    }
}
```

Para obtener más información, consulte Managing Amazon EKS add-ons - Creating an add-on en la Guía del usuario de Amazon EKS.

Ejemplo 5: creación de un complemento de Amazon EKS con un archivo de YAML de valores de configuración personalizados

En el siguiente ejemplo del comando `create-addon` se crea un complemento de Amazon EKS con valores de configuración personalizados y datos de resolución de conflictos.

```
aws eks create-addon \
    --cluster-name my-eks-cluster \
    --addon-name my-eks-addon \
    --service-account-role-arn arn:aws:iam::111122223333:role/role-name \
    --addon-version v1.16.4-eksbuild.2 \
    --configuration-values 'file://configuration-values.yaml' \
    --resolve-conflicts OVERWRITE \
    --tags '{"eks-addon-key-1": "value-1" , "eks-addon-key-2": "value-2"}'
```

Contenido de `configuration-values.yaml`:

```
resources:
```

```
    limits:
        cpu: '100m'
env:
    AWS_VPC_K8S_CNI_LOGLEVEL: 'DEBUG'
```

Salida:

```
{
    "addon": {
        "addonName": "my-eks-addon",
        "clusterName": "my-eks-cluster",
        "status": "CREATING",
        "addonVersion": "v1.16.4-eksbuild.2",
        "health": {
            "issues": []
        },
        "addonArn": "arn:aws:eks:us-east-2:111122223333:addon/my-eks-cluster/my-eks-
addon/d4c71efb-3909-6f36-a548-402cd4b5d59e",
        "createdAt": "2024-03-14T13:15:45.220000-04:00",
        "modifiedAt": "2024-03-14T13:15:45.237000-04:00",
        "serviceAccountRoleArn": "arn:aws:iam::111122223333:role/role-name",
        "tags": {
            "eks-addon-key-3": "value-3",
            "eks-addon-key-4": "value-4"
        },
        "configurationValues": "resources:\n    limits:\n        cpu: '100m'\nenv:\n
    AWS_VPC_K8S_CNI_LOGLEVEL: 'INFO'"
    }
}
```

Para obtener más información, consulte Managing Amazon EKS add-ons - Creating an add-on en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte CreateAddon en la Referencia de comandos de la AWS CLI.

`create-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-cluster`.

AWS CLI

Creación de un nuevo clúster

Este comando de ejemplo crea un clúster denominado `prod` en la región predeterminada.

Comando:

```
aws eks create-cluster --name prod \
--role-arn arn:aws:iam::012345678910:role/eks-service-role-
AWSServiceRoleForAmazonEKS-J7ONKE3BQ4PI \
--resources-vpc-config subnetIds=subnet-6782e71e,subnet-
e7e761ac,securityGroupIds=sg-6979fe18
```

Salida:

```
{
    "cluster": {
        "name": "prod",
        "arn": "arn:aws:eks:us-west-2:012345678910:cluster/prod",
        "createdAt": 1527808069.147,
        "version": "1.10",
        "roleArn": "arn:aws:iam::012345678910:role/eks-service-role-
AWSServiceRoleForAmazonEKS-J7ONKE3BQ4PI",
        "resourcesVpcConfig": {
            "subnetIds": [
                "subnet-6782e71e",
                "subnet-e7e761ac"
            ],
            "securityGroupIds": [
                "sg-6979fe18"
            ],
            "vpcId": "vpc-950809ec"
        },
        "status": "CREATING",
        "certificateAuthority": {}
    }
}
```

Creación de un clúster nuevo con acceso privado al punto de conexión y el registro activados

Este comando de ejemplo crea un clúster denominado `example` de la región predeterminada con acceso público al punto de conexión desactivado, acceso privado al punto de conexión activado y todos los tipos de registro activados.

Comando:

```
aws eks create-cluster --name example --kubernetes-version 1.12 \
--role-arn arn:aws:iam::012345678910:role/example-cluster-ServiceRole-1XWBQWYSFRE2Q
 \
--resources-vpc-
config subnetIds=subnet-0a188dccd2f9a632f,subnet-09290d93da4278664,subnet-0f21dd86e0e91134a,
 \
--logging '{"clusterLogging":[{"types":
["api","audit","authenticator","controllerManager","scheduler"],"enabled":true}]}'
```

Salida:

```
{
    "cluster": {
        "name": "example",
        "arn": "arn:aws:eks:us-west-2:012345678910:cluster/example",
        "createdAt": 1565804921.901,
        "version": "1.12",
        "roleArn": "arn:aws:iam::012345678910:role/example-cluster-
ServiceRole-1XWBQWYSFRE2Q",
        "resourcesVpcConfig": {
            "subnetIds": [
                "subnet-0a188dccd2f9a632f",
                "subnet-09290d93da4278664",
                "subnet-0f21dd86e0e91134a",
                "subnet-0173dead68481a583",
                "subnet-051f70a57ed6fcab6",
                "subnet-01322339c5c7de9b4"
            ],
            "securityGroupIds": [
                "sg-0c5b580845a031c10"
            ],
            "vpcId": "vpc-0f622c01f68d4afec",
            "endpointPublicAccess": false,
            "endpointPrivateAccess": true
        },
        "logging": {
            "clusterLogging": [
                {
                    "types": [
                        "api",
                        "audit",
                        "authenticator",
                        "controllerManager",
```

```
                        "scheduler"
                    ],
                    "enabled": true
                }
            ]
        },
        "status": "CREATING",
        "certificateAuthority": {},
        "platformVersion": "eks.3"
    }
}
```

- Para obtener información sobre la API, consulte CreateCluster en la Referencia de comandos de la AWS CLI.

`create-fargate-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-fargate-profile`.

AWS CLI

Ejemplo 1: creación de un perfil de Fargate de EKS para un selector con un espacio de nombres

En el siguiente ejemplo de `create-fargate-profile` se crea de un perfil de Fargate de EKS para un selector con un espacio de nombres.

```
aws eks create-fargate-profile \
    --cluster-name my-eks-cluster \
    --pod-execution-role-arn arn:aws:iam::111122223333:role/role-name \
    --fargate-profile-name my-fargate-profile \
    --selectors '[{"namespace": "default"}]'
```

Salida:

```
{
    "fargateProfile": {
        "fargateProfileName": "my-fargate-profile",
        "fargateProfileArn": "arn:aws:eks:us-east-2:111122223333:fargateprofile/my-
eks-cluster/my-fargate-profile/a2c72bca-318e-abe8-8ed1-27c6d4892e9e",
        "clusterName": "my-eks-cluster",
        "createdAt": "2024-03-19T12:38:47.368000-04:00",
        "podExecutionRoleArn": "arn:aws:iam::111122223333:role/role-name",
```

```
        "subnets": [
            "subnet-09d912bb63ef21b9a",
            "subnet-04ad87f71c6e5ab4d",
            "subnet-0e2907431c9988b72"
        ],
        "selectors": [
            {
                "namespace": "default"
            }
        ],
        "status": "CREATING",
        "tags": {}
    }
}
```

Para obtener más información, consulte AWS Fargate profile - Creating a Fargate profile en la Guía del usuario de Amazon EKS.

Ejemplo 2: creación de un perfil de Fargate de EKS para un selector con un espacio de nombres y etiquetas

En el siguiente ejemplo de `create-fargate-profile` se crea de un perfil de Fargate de EKS para un selector con un espacio de nombres y etiquetas.

```
aws eks create-fargate-profile \
    --cluster-name my-eks-cluster \
    --pod-execution-role-arn arn:aws:iam::111122223333:role/role-name \
    --fargate-profile-name my-fargate-profile \
    --selectors '[{"namespace": "default", "labels": {"labelname1":
 "labelvalue1"}}]'
```

Salida:

```
{
    "fargateProfile": {
        "fargateProfileName": "my-fargate-profile",
        "fargateProfileArn": "arn:aws:eks:us-east-2:111122223333:fargateprofile/my-
eks-cluster/my-fargate-profile/88c72bc7-e8a4-fa34-44e4-2f1397224bb3",
        "clusterName": "my-eks-cluster",
        "createdAt": "2024-03-19T12:33:48.125000-04:00",
        "podExecutionRoleArn": "arn:aws:iam::111122223333:role/role-name",
        "subnets": [
            "subnet-09d912bb63ef21b9a",
```

```
            "subnet-04ad87f71c6e5ab4d",
            "subnet-0e2907431c9988b72"
        ],
        "selectors": [
            {
                "namespace": "default",
                "labels": {
                    "labelname1": "labelvalue1"
                }
            }
        ],
        "status": "CREATING",
        "tags": {}
    }
}
```

Para obtener más información, consulte AWS Fargate profile - Creating a Fargate profile en la Guía del usuario de Amazon EKS.

Ejemplo 3: creación de un perfil de Fargate de EKS para un selector con un espacio de nombres y etiquetas, así como los ID de las subredes en las que lanzar un pod.

En el siguiente ejemplo de `create-fargate-profile` se crea un perfil de Fargate de EKS para un selector con un espacio de nombres y etiquetas, así como los ID de las subredes en las que lanzar un pod.

```
aws eks create-fargate-profile \
    --cluster-name my-eks-cluster \
    --pod-execution-role-arn arn:aws:iam::111122223333:role/role-name \
    --fargate-profile-name my-fargate-profile \
    --selectors '[{"namespace": "default", "labels": {"labelname1":
 "labelvalue1"}}]' \
    --subnets '["subnet-09d912bb63ef21b9a", "subnet-04ad87f71c6e5ab4d",
 "subnet-0e2907431c9988b72"]'
```

Salida:

```
{
    "fargateProfile": {
        "fargateProfileName": "my-fargate-profile",
        "fargateProfileArn": "arn:aws:eks:us-east-2:111122223333:fargateprofile/my-
eks-cluster/my-fargate-profile/e8c72bc8-e87b-5eb6-57cb-ed4fe57577e3",
```

```
        "clusterName": "my-eks-cluster",
        "createdAt": "2024-03-19T12:35:58.640000-04:00",
        "podExecutionRoleArn": "arn:aws:iam::111122223333:role/role-name",
        "subnets": [
            "subnet-09d912bb63ef21b9a",
            "subnet-04ad87f71c6e5ab4d",
            "subnet-0e2907431c9988b72"
        ],
        "selectors": [
            {
                "namespace": "default",
                "labels": {
                    "labelname1": "labelvalue1"
                }
            }
        ],
        "status": "CREATING",
        "tags": {}
    }
}
```

Para obtener más información, consulte AWS Fargate profile - Creating a Fargate profile en la Guía del usuario de Amazon EKS.

Ejemplo 4: creación de un perfil de Fargate de EKS para un selector con varios espacios de nombres y etiquetas, así como los ID de las subredes en las que lanzar un pod

En el siguiente ejemplo de `create-fargate-profile` se crea un perfil de Fargate de EKS para un selector con varios espacios de nombres y etiquetas, así como los ID de las subredes en las que lanzar un pod.

```
aws eks create-fargate-profile \
    --cluster-name my-eks-cluster \
    --pod-execution-role-arn arn:aws:iam::111122223333:role/role-name \
    --fargate-profile-name my-fargate-profile \
    --selectors '[{"namespace": "default1", "labels": {"labelname1": "labelvalue1",
 "labelname2": "labelvalue2"}}, {"namespace": "default2", "labels": {"labelname1":
 "labelvalue1", "labelname2": "labelvalue2"}}]' \
    --subnets '["subnet-09d912bb63ef21b9a", "subnet-04ad87f71c6e5ab4d",
 "subnet-0e2907431c9988b72"]' \
    --tags '{"eks-fargate-profile-key-1": "value-1" , "eks-fargate-profile-key-2":
 "value-2"}'
```

Salida:

```
{
    "fargateProfile": {
        "fargateProfileName": "my-fargate-profile",
        "fargateProfileArn": "arn:aws:eks:us-east-2:111122223333:fargateprofile/my-
eks-cluster/my-fargate-profile/4cc72bbf-b766-8ee6-8d29-e62748feb3cd",
        "clusterName": "my-eks-cluster",
        "createdAt": "2024-03-19T12:15:55.271000-04:00",
        "podExecutionRoleArn": "arn:aws:iam::111122223333:role/role-name",
        "subnets": [
            "subnet-09d912bb63ef21b9a",
            "subnet-04ad87f71c6e5ab4d",
            "subnet-0e2907431c9988b72"
        ],
        "selectors": [
            {
                "namespace": "default1",
                "labels": {
                    "labelname2": "labelvalue2",
                    "labelname1": "labelvalue1"
                }
            },
            {
                "namespace": "default2",
                "labels": {
                    "labelname2": "labelvalue2",
                    "labelname1": "labelvalue1"
                }
            }
        ],
        "status": "CREATING",
        "tags": {
            "eks-fargate-profile-key-2": "value-2",
            "eks-fargate-profile-key-1": "value-1"
        }
    }
}
```

Para obtener más información, consulte AWS Fargate profile - Creating a Fargate profile en la Guía del usuario de Amazon EKS.

Ejemplo 5: creación de un perfil de Fargate de EKS para un selector de comodín de espacios de nombres y etiquetas, así como los ID de las subredes en las que lanzar un pod

En el siguiente ejemplo de `create-fargate-profile` se crea un perfil de Fargate de EKS para un selector con varios espacios de nombres y etiquetas, así como los ID de las subredes en las que lanzar un pod.

```
aws eks create-fargate-profile \
    --cluster-name my-eks-cluster \
    --pod-execution-role-arn arn:aws:iam::111122223333:role/role-name \
    --fargate-profile-name my-fargate-profile \
    --selectors '[{"namespace": "prod*", "labels": {"labelname*?": "*value1"}},
 {"namespace": "*dev*", "labels": {"labelname*?": "*value*"}}]' \
    --subnets '["subnet-09d912bb63ef21b9a", "subnet-04ad87f71c6e5ab4d",
 "subnet-0e2907431c9988b72"]' \
    --tags '{"eks-fargate-profile-key-1": "value-1" , "eks-fargate-profile-key-2":
 "value-2"}'
```

Salida:

```
{
    "fargateProfile": {
        "fargateProfileName": "my-fargate-profile",
        "fargateProfileArn": "arn:aws:eks:us-east-2:111122223333:fargateprofile/my-
eks-cluster/my-fargate-profile/e8c72bd6-5966-0bfe-b77b-1802893e5a6f",
        "clusterName": "my-eks-cluster",
        "createdAt": "2024-03-19T13:05:20.550000-04:00",
        "podExecutionRoleArn": "arn:aws:iam::111122223333:role/role-name",
        "subnets": [
            "subnet-09d912bb63ef21b9a",
            "subnet-04ad87f71c6e5ab4d",
            "subnet-0e2907431c9988b72"
        ],
        "selectors": [
            {
                "namespace": "prod*",
                "labels": {
                    "labelname*?": "*value1"
                }
            },
            {
                "namespace": "*dev*",
                "labels": {
```

```
                    "labelname*?": "*value*"
                }
            }
        ],
        "status": "CREATING",
        "tags": {
            "eks-fargate-profile-key-2": "value-2",
            "eks-fargate-profile-key-1": "value-1"
        }
    }
}
```

Para obtener más información, consulte AWS Fargate profile - Creating a Fargate profile en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte CreateFargateProfile en la Referencia de comandos de la AWS CLI.

`create-nodegroup`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-nodegroup`.

AWS CLI

Ejemplo 1: creación de un grupo de nodos administrados para un clúster de Amazon EKS

En el siguiente ejemplo de `create-nodegroup` se crea un grupo de nodos administrados para un clúster de Amazon EKS.

```
aws eks create-nodegroup \
    --cluster-name my-eks-cluster \
    --nodegroup-name my-eks-nodegroup \
    --node-role arn:aws:iam::111122223333:role/role-name \
    --
subnets "subnet-0e2907431c9988b72" "subnet-04ad87f71c6e5ab4d" "subnet-09d912bb63ef21b9a"
 \
    --scaling-config minSize=1,maxSize=3,desiredSize=1 \
    --region us-east-2
```

Salida:

```
{
    "nodegroup": {
```

```
        "nodegroupName": "my-eks-nodegroup",
        "nodegroupArn": "arn:aws:eks:us-east-2:111122223333:nodegroup/my-eks-
cluster/my-eks-nodegroup/bac7550f-b8b8-5fbb-4f3e-7502a931119e",
        "clusterName": "my-eks-cluster",
        "version": "1.26",
        "releaseVersion": "1.26.12-20240329",
        "createdAt": "2024-04-04T13:19:32.260000-04:00",
        "modifiedAt": "2024-04-04T13:19:32.260000-04:00",
        "status": "CREATING",
        "capacityType": "ON_DEMAND",
        "scalingConfig": {
            "minSize": 1,
            "maxSize": 3,
            "desiredSize": 1
        },
        "instanceTypes": [
            "t3.medium"
        ],
        "subnets": [
            "subnet-0e2907431c9988b72, subnet-04ad87f71c6e5ab4d,
 subnet-09d912bb63ef21b9a"
        ],
        "amiType": "AL2_x86_64",
        "nodeRole": "arn:aws:iam::111122223333:role/role-name",
        "diskSize": 20,
        "health": {
            "issues": []
        },
        "updateConfig": {
            "maxUnavailable": 1
        },
        "tags": {}
    }
}
```

Para obtener más información, consulte Creación de un grupo de nodos administrados para un clúster en la Guía del usuario de Amazon EKS.

Ejemplo 2: creación de un grupo de nodos administrados para un clúster de Amazon EKS con valores personalizados de instance-types y disk-size

En el siguiente ejemplo de `create-nodegroup` se crea un grupo de nodos administrados para un clúster de Amazon EKS con valores personalizados de instance-types y disk-size.

```
aws eks create-nodegroup \
    --cluster-name my-eks-cluster \
    --nodegroup-name my-eks-nodegroup \
    --node-role arn:aws:iam::111122223333:role/role-name \
    --
subnets "subnet-0e2907431c9988b72" "subnet-04ad87f71c6e5ab4d" "subnet-09d912bb63ef21b9a"
 \
    --scaling-config minSize=1,maxSize=3,desiredSize=1 \
    --capacity-type ON_DEMAND \
    --instance-types 'm5.large' \
    --disk-size 50 \
    --region us-east-2
```

Salida:

```
{
    "nodegroup": {
        "nodegroupName": "my-eks-nodegroup",
        "nodegroupArn": "arn:aws:eks:us-east-2:111122223333:nodegroup/my-eks-
cluster/my-eks-nodegroup/c0c7551b-e4f9-73d9-992c-a450fdb82322",
        "clusterName": "my-eks-cluster",
        "version": "1.26",
        "releaseVersion": "1.26.12-20240329",
        "createdAt": "2024-04-04T13:46:07.595000-04:00",
        "modifiedAt": "2024-04-04T13:46:07.595000-04:00",
        "status": "CREATING",
        "capacityType": "ON_DEMAND",
        "scalingConfig": {
            "minSize": 1,
            "maxSize": 3,
            "desiredSize": 1
        },
        "instanceTypes": [
            "m5.large"
        ],
        "subnets": [
            "subnet-0e2907431c9988b72",
            "subnet-04ad87f71c6e5ab4d",
            "subnet-09d912bb63ef21b9a"
        ],
        "amiType": "AL2_x86_64",
        "nodeRole": "arn:aws:iam::111122223333:role/role-name",
        "diskSize": 50,
```

```
        "health": {
            "issues": []
        },
        "updateConfig": {
            "maxUnavailable": 1
        },
        "tags": {}
    }
}
```

Para obtener más información, consulte Creación de un grupo de nodos administrados para un clúster en la Guía del usuario de Amazon EKS.

Ejemplo 3: creación de un grupo de nodos administrados para un clúster de Amazon EKS con valores personalizados de instance-types, disk-size, ami-type, capacity-type, update-config, labels, taints y tags.

En el siguiente ejemplo de `create-nodegroup` se crea un grupo de nodos administrados para un clúster de Amazon EKS con valores personalizados de instance-types, disk-size, ami-type, capacity-type, update-config, labels, taints y tags.

```
aws eks create-nodegroup  \
    --cluster-name my-eks-cluster \
    --nodegroup-name my-eks-nodegroup \
    --node-role arn:aws:iam::111122223333:role/role-name \
    --
subnets "subnet-0e2907431c9988b72" "subnet-04ad87f71c6e5ab4d" "subnet-09d912bb63ef21b9a"
 \
    --scaling-config minSize=1,maxSize=5,desiredSize=4 \
    --instance-types 't3.large' \
    --disk-size 50 \
    --ami-type AL2_x86_64 \
    --capacity-type SPOT \
    --update-config maxUnavailable=2 \
    --labels '{"my-eks-nodegroup-label-1": "value-1" , "my-eks-nodegroup-label-2":
 "value-2"}' \
    --taints '{"key": "taint-key-1" , "value": "taint-value-1", "effect":
 "NO_EXECUTE"}' \
    --tags '{"my-eks-nodegroup-key-1": "value-1" , "my-eks-nodegroup-key-2":
 "value-2"}'
```

Salida:

```
{
    "nodegroup": {
        "nodegroupName": "my-eks-nodegroup",
        "nodegroupArn": "arn:aws:eks:us-east-2:111122223333:nodegroup/my-eks-
cluster/my-eks-nodegroup/88c75524-97af-0cb9-a9c5-7c0423ab5314",
        "clusterName": "my-eks-cluster",
        "version": "1.26",
        "releaseVersion": "1.26.12-20240329",
        "createdAt": "2024-04-04T14:05:07.940000-04:00",
        "modifiedAt": "2024-04-04T14:05:07.940000-04:00",
        "status": "CREATING",
        "capacityType": "SPOT",
        "scalingConfig": {
            "minSize": 1,
            "maxSize": 5,
            "desiredSize": 4
        },
        "instanceTypes": [
            "t3.large"
        ],
        "subnets": [
            "subnet-0e2907431c9988b72",
            "subnet-04ad87f71c6e5ab4d",
            "subnet-09d912bb63ef21b9a"
        ],
        "amiType": "AL2_x86_64",
        "nodeRole": "arn:aws:iam::111122223333:role/role-name",
        "labels": {
            "my-eks-nodegroup-label-2": "value-2",
            "my-eks-nodegroup-label-1": "value-1"
        },
        "taints": [
            {
                "key": "taint-key-1",
                "value": "taint-value-1",
                "effect": "NO_EXECUTE"
            }
        ],
        "diskSize": 50,
        "health": {
            "issues": []
        },
        "updateConfig": {
```

```
            "maxUnavailable": 2
        },
        "tags": {
            "my-eks-nodegroup-key-1": "value-1",
            "my-eks-nodegroup-key-2": "value-2"
        }
    }
}
```

Para obtener más información, consulte Creación de un grupo de nodos administrados para un clúster en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte CreateNodegroup en la Referencia de comandos de la AWS CLI.

`create-pod-identity-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-pod-identity-association`.

AWS CLI

Ejemplo 1: creación de una asociación de Pod Identity de EKS en el clúster de EKS

En el siguiente ejemplo de `create-pod-identity-association` se crea una asociación de Pod Identity de EKS entre una cuenta de servicio del clúster de EKS y un rol de IAM.

```
aws eks create-pod-identity-association \
    --cluster-name eks-customer \
    --namespace default \
    --service-account default \
    --role-arn arn:aws:iam::111122223333:role/my-role
```

Salida:

```
{
    "association": {
        "clusterName": "eks-customer",
        "namespace": "default",
        "serviceAccount": "default",
        "roleArn": "arn:aws:iam::111122223333:role/my-role",
```

```
        "associationArn": "arn:aws:eks:us-
west-2:111122223333:podidentityassociation/eks-customer/a-8mvwvh57cu74mgcst",
        "associationId": "a-8mvwvh57cu74mgcst",
        "tags": {},
        "createdAt": "2025-05-24T19:40:13.961000-05:00",
        "modifiedAt": "2025-05-24T19:40:13.961000-05:00"
    }
}
```

Para obtener más información, consulte Información sobre cómo Pod Identity de EKS concede a los pods acceso a los servicios de AWS en la Guía del usuario de Amazon EKS.

Ejemplo 2: creación de una asociación de Pod Identity de EKS en el clúster de EKS con etiquetas

En el siguiente ejemplo de `create-pod-identity-association` se crea una asociación de Pod Identity de EKS entre una cuenta de servicio y un rol de IAM en el clúster de EKS con etiquetas.

```
aws eks create-pod-identity-association \
    --cluster-name eks-customer \
    --namespace default \
    --service-account default \
    --role-arn arn:aws:iam::111122223333:role/my-role \
    --tags Key1=value1,Key2=value2
```

Salida:

```
{
    "association": {
        "clusterName": "eks-customer",
        "namespace": "default",
        "serviceAccount": "default",
        "roleArn": "arn:aws:iam::111122223333:role/my-role",
        "associationArn": "arn:aws:eks:us-
west-2:111122223333:podidentityassociation/eks-customer/a-9njjin9gfghecgoda",
        "associationId": "a-9njjin9gfghecgoda",
        "tags": {
            "Key2": "value2",
            "Key1": "value1"
        },
        "createdAt": "2025-05-24T19:52:14.135000-05:00",
        "modifiedAt": "2025-05-24T19:52:14.135000-05:00"
    }
```

```
}
```

Para obtener más información, consulte Información sobre cómo Pod Identity de EKS concede a los pods acceso a los servicios de AWS en la Guía del usuario de Amazon EKS.

- Para obtener detalles de la API, consulte CreatePodIdentityAssociation en la Referencia de comandos de AWS CLI.

`delete-access-entry`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-access-entry`.

AWS CLI

Eliminación de una entrada de acceso asociada al clúster

En el siguiente ejemplo de `delete-access-entry` se elimina una entrada de acceso asociada al clúster de EKS denominada `eks-customer`.

```
aws eks delete-access-entry \
    --cluster-name eks-customer \
    --principal-arn arn:aws:iam::111122223333:role/Admin
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de entradas de acceso en la Guía del usuario de Amazon EKS.

- Para obtener detalles de la API, consulte DeleteAccessEntry en la Referencia de comandos de AWS CLI.

`delete-addon`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-addon`.

AWS CLI

Ejemplo 1. Para eliminar un complemento de Amazon EKS, pero conservar el software del complemento en el clúster de EKS

En el siguiente ejemplo de `delete-addon` se elimina un complemento de Amazon EKS, pero se conserva el software del complemento en el clúster de EKS.

```
aws eks delete-addon \
    --cluster-name my-eks-cluster \
    --addon-name my-eks-addon \
    --preserve
```

Salida:

```
{
    "addon": {
        "addonName": "my-eks-addon",
        "clusterName": "my-eks-cluster",
        "status": "DELETING",
        "addonVersion": "v1.9.3-eksbuild.7",
        "health": {
            "issues": []
        },
        "addonArn": "arn:aws:eks:us-east-2:111122223333:addon/my-eks-cluster/my-eks-
addon/a8c71ed3-944e-898b-9167-c763856af4b8",
        "createdAt": "2024-03-14T11:49:09.009000-04:00",
        "modifiedAt": "2024-03-14T12:03:49.776000-04:00",
        "tags": {}
    }
}
```

Para obtener más información, consulte Managing Amazon EKS add-ons - Deleting an add-on en la Guía del usuario de Amazon EKS.

Ejemplo 2. Para eliminar un complemento de Amazon EKS y también el software del complemento del clúster de EKS

En el siguiente ejemplo de `delete-addon` se elimina un complemento de Amazon EKS y también el software del complemento del clúster de EKS.

```
aws eks delete-addon \
    --cluster-name my-eks-cluster \
    --addon-name my-eks-addon
```

Salida:

```
{
    "addon": {
        "addonName": "my-eks-addon",
```

```
        "clusterName": "my-eks-cluster",
        "status": "DELETING",
        "addonVersion": "v1.15.1-eksbuild.1",
        "health": {
            "issues": []
        },
        "addonArn": "arn:aws:eks:us-east-2:111122223333:addon/my-eks-cluster/my-eks-
addon/bac71ed1-ec43-3bb6-88ea-f243cdb58954",
        "createdAt": "2024-03-14T11:45:31.983000-04:00",
        "modifiedAt": "2024-03-14T11:58:40.136000-04:00",
        "serviceAccountRoleArn": "arn:aws:iam::111122223333:role/role-name",
        "tags": {}
    }
}
```

Para obtener más información, consulte Managing Amazon EKS add-ons - Deleting an add-on en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte DeleteAddon en la Referencia de comandos de la AWS CLI.

`delete-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-cluster`.

AWS CLI

Eliminación de un plano de control del clúster de EKS

En el siguiente ejemplo de `delete-cluster` se elimina un plano de control de clúster de Amazon EKS.

```
aws eks delete-cluster \
    --name my-eks-cluster
```

Salida:

```
{
    "cluster": {
        "name": "my-eks-cluster",
        "arn": "arn:aws:eks:us-east-2:111122223333:cluster/my-eks-cluster",
        "createdAt": "2024-03-14T11:31:44.348000-04:00",
        "version": "1.27",
```

```
        "endpoint": "https://DALSJ343KE23J3RN45653DSKJTT647TYD.yl4.us-
east-2.eks.amazonaws.com",
        "roleArn": "arn:aws:iam::111122223333:role/eksctl-my-eks-cluster-cluster-
ServiceRole-zMF6CBakwwbW",
        "resourcesVpcConfig": {
            "subnetIds": [
                "subnet-0fb75d2d8401716e7",
                "subnet-02184492f67a3d0f9",
                "subnet-04098063527aab776",
                "subnet-0e2907431c9988b72",
                "subnet-04ad87f71c6e5ab4d",
                "subnet-09d912bb63ef21b9a"
            ],
            "securityGroupIds": [
                "sg-0c1327f6270afbb36"
            ],
            "clusterSecurityGroupId": "sg-01c84d09d70f39a7f",
            "vpcId": "vpc-0012b8e1cc0abb17d",
            "endpointPublicAccess": true,
            "endpointPrivateAccess": true,
            "publicAccessCidrs": [
                "0.0.0.0/0"
            ]
        },
        "kubernetesNetworkConfig": {
            "serviceIpv4Cidr": "10.100.0.0/16",
            "ipFamily": "ipv4"
        },
        "logging": {
            "clusterLogging": [
                {
                    "types": [
                        "api",
                        "audit",
                        "authenticator",
                        "controllerManager",
                        "scheduler"
                    ],
                    "enabled": true
                }
            ]
        },
        "identity": {
            "oidc": {
```

```
                "issuer": "https://oidc.eks.us-east-2.amazonaws.com/id/
DALSJ343KE23J3RN45653DSKJTT647TYD"
            }
        },
        "status": "DELETING",
        "certificateAuthority": {
            "data": "XXX_CA_DATA_XXX"
        },
        "platformVersion": "eks.16",
        "tags": {
            "aws:cloudformation:stack-name": "eksctl-my-eks-cluster-cluster",
            "alpha.eksctl.io/cluster-name": "my-eks-cluster",
            "karpenter.sh/discovery": "my-eks-cluster",
            "aws:cloudformation:stack-id": "arn:aws:cloudformation:us-
east-2:111122223333:stack/eksctl-my-eks-cluster-cluster/e752ea00-e217-11ee-
beae-0a9599c8c7ed",
            "auto-delete": "no",
            "eksctl.cluster.k8s.io/v1alpha1/cluster-name": "my-eks-cluster",
            "EKS-Cluster-Name": "my-eks-cluster",
            "alpha.eksctl.io/cluster-oidc-enabled": "true",
            "aws:cloudformation:logical-id": "ControlPlane",
            "alpha.eksctl.io/eksctl-version": "0.173.0-dev
+a7ee89342.2024-03-01T03:40:57Z",
            "Name": "eksctl-my-eks-cluster-cluster/ControlPlane"
        },
        "accessConfig": {
            "authenticationMode": "API_AND_CONFIG_MAP"
        }
    }
}
```

Para obtener más información, consulte Eliminar un clúster en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte DeleteCluster en la Referencia de comandos de la AWS CLI.

`delete-fargate-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-fargate-profile`.

AWS CLI

Ejemplo 1: creación de un perfil de Fargate de EKS para un selector con un espacio de nombres

En el siguiente ejemplo de `delete-fargate-profile` se crea de un perfil de Fargate de EKS para un selector con un espacio de nombres.

```
aws eks delete-fargate-profile \
    --cluster-name my-eks-cluster \
    --fargate-profile-name my-fargate-profile
```

Salida:

```
{
    "fargateProfile": {
        "fargateProfileName": "my-fargate-profile",
        "fargateProfileArn": "arn:aws:eks:us-east-2:111122223333:fargateprofile/my-
eks-cluster/my-fargate-profile/1ac72bb3-3fc6-2631-f1e1-98bff53bed62",
        "clusterName": "my-eks-cluster",
        "createdAt": "2024-03-19T11:48:39.975000-04:00",
        "podExecutionRoleArn": "arn:aws:iam::111122223333:role/role-name",
        "subnets": [
            "subnet-09d912bb63ef21b9a",
            "subnet-04ad87f71c6e5ab4d",
            "subnet-0e2907431c9988b72"
        ],
        "selectors": [
            {
                "namespace": "default",
                "labels": {
                    "foo": "bar"
                }
            }
        ],
        "status": "DELETING",
        "tags": {}
    }
}
```

Para obtener más información, consulte AWS Fargate profile - Deleting a Fargate en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte DeleteFargateProfile en la Referencia de comandos de la AWS CLI.

`delete-nodegroup`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-nodegroup`.

AWS CLI

Ejemplo 1: eliminación de un grupo de nodos administrados para un clúster de Amazon EKS

En el siguiente ejemplo de `delete-nodegroup` se elimina un grupo de nodos administrados para un clúster de Amazon EKS.

```
aws eks delete-nodegroup \
    --cluster-name my-eks-cluster \
    --nodegroup-name my-eks-nodegroup
```

Salida:

```
{
    "nodegroup": {
        "nodegroupName": "my-eks-nodegroup",
        "nodegroupArn": "arn:aws:eks:us-east-2:111122223333:nodegroup/my-eks-
cluster/my-eks-nodegroup/1ec75f5f-0e21-dcc0-b46e-f9c442685cd8",
        "clusterName": "my-eks-cluster",
        "version": "1.26",
        "releaseVersion": "1.26.12-20240329",
        "createdAt": "2024-04-08T13:25:15.033000-04:00",
        "modifiedAt": "2024-04-08T13:25:31.252000-04:00",
        "status": "DELETING",
        "capacityType": "SPOT",
        "scalingConfig": {
            "minSize": 1,
            "maxSize": 5,
            "desiredSize": 4
        },
        "instanceTypes": [
            "t3.large"
        ],
        "subnets": [
            "subnet-0e2907431c9988b72",
```

```
            "subnet-04ad87f71c6e5ab4d",
            "subnet-09d912bb63ef21b9a"
        ],
        "amiType": "AL2_x86_64",
        "nodeRole": "arn:aws:iam::111122223333:role/role-name",
        "labels": {
            "my-eks-nodegroup-label-2": "value-2",
            "my-eks-nodegroup-label-1": "value-1"
        },
        "taints": [
            {
                "key": "taint-key-1",
                "value": "taint-value-1",
                "effect": "NO_EXECUTE"
            }
        ],
        "diskSize": 50,
        "health": {
            "issues": []
        },
        "updateConfig": {
            "maxUnavailable": 2
        },
        "tags": {
            "my-eks-nodegroup-key-1": "value-1",
            "my-eks-nodegroup-key-2": "value-2"
        }
    }
}
```

- Para obtener información sobre la API, consulte DeleteNodegroup en la Referencia de comandos de la AWS CLI.

`delete-pod-identity-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-pod-identity-association`.

AWS CLI

Eliminación de la asociación de Pod Identity de EKS

En el siguiente ejemplo de `delete-pod-identity-association` se elimina la asociación de Pod Identity de EKS con el ID de asociación `a-9njjin9gfghecgocd` del clúster de EKS denominado `eks-customer`.

```
aws eks delete-pod-identity-association \
    --cluster-name eks-customer \
    --association-id a-9njjin9gfghecgocd
```

Salida:

```
{
    "association": {
        "clusterName": "eks-customer",
        "namespace": "default",
        "serviceAccount": "default",
        "roleArn": "arn:aws:iam::111122223333:role/s3-role",
        "associationArn": "arn:aws:eks:us-
west-2:111122223333:podidentityassociation/eks-customer/a-9njjin9gfghecgocd",
        "associationId": "a-9njjin9gfghecgocd",
        "tags": {
            "Key2": "value2",
            "Key1": "value1"
        },
        "createdAt": "2025-05-24T19:52:14.135000-05:00",
        "modifiedAt": "2025-05-25T21:10:56.923000-05:00"
    }
}
```

Para obtener más información, consulte Información sobre cómo Pod Identity de EKS concede a los pods acceso a los servicios de AWS en la Guía del usuario de Amazon EKS.

- Para obtener detalles de la API, consulte DeletePodIdentityAssociation en la Referencia de comandos de AWS CLI.

`deregister-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-cluster`.

AWS CLI

Para anular el registro de un clúster conectado y eliminarlo del plano de control de Amazon EKS

En el siguiente ejemplo de `deregister-cluster` se anula el registro de un clúster conectado y se elimina del plano de control de Amazon EKS.

```
aws eks deregister-cluster \
    --name my-eks-anywhere-cluster
```

Salida:

```
{
    "cluster": {
        "name": "my-eks-anywhere-cluster",
        "arn": "arn:aws:eks:us-east-2:111122223333:cluster/my-eks-anywhere-cluster",
        "createdAt": "2024-04-12T12:38:37.561000-04:00",
        "status": "DELETING",
        "tags": {},
        "connectorConfig": {
            "activationId": "dfb5ad28-13c3-4e26-8a19-5b2457638c74",
            "activationExpiry": "2024-04-15T12:38:37.082000-04:00",
            "provider": "EKS_ANYWHERE",
            "roleArn": "arn:aws:iam::111122223333:role/AmazonEKSConnectorAgentRole"
        }
    }
}
```

Para obtener más información, consulte Anulación del registro de un clúster en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte DeregisterCluster en la Referencia de comandos de la AWS CLI.

`describe-access-entry`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-access-entry`.

AWS CLI

Descripción de la entrada de acceso al clúster de EKS

En el siguiente ejemplo de `describe-access-entry` se describe una entrada de acceso para el clúster de EKS.

```
aws eks describe-access-entry \
```

```
    --cluster-name eks-customer \
    --principal-arn arn:aws:iam::111122223333:user/eks-admin-user
```

Salida:

```
{
    "accessEntry": {
        "clusterName": "eks-customer",
        "principalArn": "arn:aws:iam::111122223333:user/eks-admin-user",
        "kubernetesGroups": [],
        "accessEntryArn": "arn:aws:eks:us-west-2:111122223333:access-entry/eks-
customer/user/111122223333/eks-admin-user/0acb1bc6-cb0a-ede6-11ae-a6506e3d36p0",
        "createdAt": "2025-04-14T22:45:48.097000-05:00",
        "modifiedAt": "2025-04-14T22:45:48.097000-05:00",
        "tags": {},
        "username": "arn:aws:iam::111122223333:user/eks-admin-user",
        "type": "STANDARD"
    }
}
```

Para obtener más información, consulte Concesión de acceso a Kubernetes a los usuarios de IAM con entradas de acceso de EKS en la Guía del usuario de Amazon EKS.

- Para obtener detalles de la API, consulte DescribeAccessEntry en la Referencia de comandos de AWS CLI.

`describe-addon-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-addon-configuration`.

AWS CLI

Ejemplo 1: opciones de configuración disponibles al crear o actualizar complementos vpc-cni de Amazon

En el siguiente ejemplo de `describe-addon-configuration` se devuelve todo el esquema de configuración disponible que se utiliza cuando se crea o actualiza un complemento para el complemento vpc-cni con la versión correspondiente.

```
aws eks describe-addon-configuration \
    --addon-name vpc-cni \
    --addon-version v1.15.1-eksbuild.1
```

Salida:


```
{
    "addonName": "vpc-cni",
    "addonVersion": "v1.15.1-eksbuild.1",
    "configurationSchema": "{\"$ref\":\"#/definitions/VpcCni\",\"$schema\":\"http://
json-schema.org/draft-06/schema#\",\"definitions\":{\"Affinity\":{\"type\":
[\"object\",\"null\"]},\"EniConfig\":{\"additionalProperties\":false,\"properties
\":{\"create\":{\"type\":\"boolean\"},\"region\":{\"type\":\"string\"},\"subnets\":
{\"additionalProperties\":{\"additionalProperties\":false,\"properties\":{\"id\":
{\"type\":\"string\"},\"securityGroups\":{\"items\":{\"type\":\"string\"},\"type\":
\"array\"}},\"required\":[\"id\"],\"type\":\"object\"},\"minProperties\":1,\"type
\":\"object\"}},\"required\":[\"create\",\"region\",\"subnets\"],\"type\":\"object
\"},\"Env\":{\"additionalProperties\":false,\"properties\":{\"ADDITIONAL_ENI_TAGS
\":{\"type\":\"string\"},\"ANNOTATE_POD_IP\":{\"format\":\"boolean\",\"type\":
\"string\"},\"AWS_EC2_ENDPOINT\":{\"type\":\"string\"},\"AWS_EXTERNAL_SERVICE_CIDRS
\":{\"type\":\"string\"},\"AWS_MANAGE_ENIS_NON_SCHEDULABLE\":{\"format\":\"boolean
\",\"type\":\"string\"},\"AWS_VPC_CNI_NODE_PORT_SUPPORT\":{\"format\":\"boolean
\",\"type\":\"string\"},\"AWS_VPC_ENI_MTU\":{\"format\":\"integer\",\"type\":
\"string\"},\"AWS_VPC_K8S_CNI_CUSTOM_NETWORK_CFG\":{\"format\":\"boolean\",\"type
\":\"string\"},\"AWS_VPC_K8S_CNI_EXCLUDE_SNAT_CIDRS\":{\"type\":\"string\"},
\"AWS_VPC_K8S_CNI_EXTERNALSNAT\":{\"format\":\"boolean\",\"type\":\"string\"},
\"AWS_VPC_K8S_CNI_LOGLEVEL\":{\"type\":\"string\"},\"AWS_VPC_K8S_CNI_LOG_FILE\":
{\"type\":\"string\"},\"AWS_VPC_K8S_CNI_RANDOMIZESNAT\":{\"type\":\"string\"},
\"AWS_VPC_K8S_CNI_VETHPREFIX\":{\"type\":\"string\"},\"AWS_VPC_K8S_PLUGIN_LOG_FILE
\":{\"type\":\"string\"},\"AWS_VPC_K8S_PLUGIN_LOG_LEVEL\":{\"type\":\"string
\"},\"CLUSTER_ENDPOINT\":{\"type\":\"string\"},\"DISABLE_INTROSPECTION\":
{\"format\":\"boolean\",\"type\":\"string\"},\"DISABLE_LEAKED_ENI_CLEANUP\":
{\"format\":\"boolean\",\"type\":\"string\"},\"DISABLE_METRICS\":{\"format
\":\"boolean\",\"type\":\"string\"},\"DISABLE_NETWORK_RESOURCE_PROVISIONING
\":{\"format\":\"boolean\",\"type\":\"string\"},\"DISABLE_POD_V6\":{\"format
\":\"boolean\",\"type\":\"string\"},\"ENABLE_BANDWIDTH_PLUGIN\":{\"format\":
\"boolean\",\"type\":\"string\"},\"ENABLE_POD_ENI\":{\"format\":\"boolean\",
\"type\":\"string\"},\"ENABLE_PREFIX_DELEGATION\":{\"format\":\"boolean\",
\"type\":\"string\"},\"ENABLE_V4_EGRESS\":{\"format\":\"boolean\",\"type\":
\"string\"},\"ENABLE_V6_EGRESS\":{\"format\":\"boolean\",\"type\":\"string\"},
\"ENI_CONFIG_ANNOTATION_DEF\":{\"type\":\"string\"},\"ENI_CONFIG_LABEL_DEF\":
{\"type\":\"string\"},\"INTROSPECTION_BIND_ADDRESS\":{\"type\":\"string\"},
\"IP_COOLDOWN_PERIOD\":{\"format\":\"integer\",\"type\":\"string\"},\"MAX_ENI
\":{\"format\":\"integer\",\"type\":\"string\"},\"MINIMUM_IP_TARGET\":{\"format
\":\"integer\",\"type\":\"string\"},\"POD_SECURITY_GROUP_ENFORCING_MODE\":
{\"type\":\"string\"},\"WARM_ENI_TARGET\":{\"format\":\"integer\",\"type\":
\"string\"},\"WARM_IP_TARGET\":{\"format\":\"integer\",\"type\":\"string\"},
\"WARM_PREFIX_TARGET\":{\"format\":\"integer\",\"type\":\"string\"}},\"title
```

```
\":\"Env\",\"type\":\"object\"},\"Init\":{\"additionalProperties\":false,
\"properties\":{\"env\":{\"$ref\":\"#/definitions/InitEnv\"}},\"title\":\"Init
\",\"type\":\"object\"},\"InitEnv\":{\"additionalProperties\":false,\"properties
\":{\"DISABLE_TCP_EARLY_DEMUX\":{\"format\":\"boolean\",\"type\":\"string\"},
\"ENABLE_V6_EGRESS\":{\"format\":\"boolean\",\"type\":\"string\"}},\"title\":
\"InitEnv\",\"type\":\"object\"},\"Limits\":{\"additionalProperties\":false,
\"properties\":{\"cpu\":{\"type\":\"string\"},\"memory\":{\"type\":\"string\"}},
\"title\":\"Limits\",\"type\":\"object\"},\"NodeAgent\":{\"additionalProperties
\":false,\"properties\":{\"enableCloudWatchLogs\":{\"format\":\"boolean\",
\"type\":\"string\"},\"enablePolicyEventLogs\":{\"format\":\"boolean\",\"type\":
\"string\"},\"healthProbeBindAddr\":{\"format\":\"integer\",\"type\":\"string
\"},\"metricsBindAddr\":{\"format\":\"integer\",\"type\":\"string\"}},\"title\":
\"NodeAgent\",\"type\":\"object\"},\"Resources\":{\"additionalProperties\":false,
\"properties\":{\"limits\":{\"$ref\":\"#/definitions/Limits\"},\"requests\":
{\"$ref\":\"#/definitions/Limits\"}},\"title\":\"Resources\",\"type\":\"object
\"},\"Tolerations\":{\"additionalProperties\":false,\"items\":{\"type\":\"object
\"},\"type\":\"array\"},\"VpcCni\":{\"additionalProperties\":false,\"properties
\":{\"affinity\":{\"$ref\":\"#/definitions/Affinity\"},\"enableNetworkPolicy\":
{\"format\":\"boolean\",\"type\":\"string\"},\"enableWindowsIpam\":{\"format\":
\"boolean\",\"type\":\"string\"},\"eniConfig\":{\"$ref\":\"#/definitions/EniConfig
\"},\"env\":{\"$ref\":\"#/definitions/Env\"},\"init\":{\"$ref\":\"#/definitions/Init
\"},\"livenessProbeTimeoutSeconds\":{\"type\":\"integer\"},\"nodeAgent\":{\"$ref\":
\"#/definitions/NodeAgent\"},\"readinessProbeTimeoutSeconds\":{\"type\":\"integer
\"},\"resources\":{\"$ref\":\"#/definitions/Resources\"},\"tolerations\":{\"$ref
\":\"#/definitions/Tolerations\"}},\"title\":\"VpcCni\",\"type\":\"object\"}},
\"description\":\"vpc-cni\"}"
}
```


Ejemplo 2: opciones de configuración disponibles al crear o actualizar complementos coredns de Amazon

En el siguiente ejemplo de `describe-addon-configuration` se devuelve todo el esquema de configuración disponible que se utiliza cuando se crea o actualiza un complemento para el complemento coredns con la versión correspondiente.

```
aws eks describe-addon-configuration \
    --addon-name coredns \
    --addon-version v1.8.7-eksbuild.4
```

Salida:


```
{
```

```
    "addonName": "coredns",
    "addonVersion": "v1.8.7-eksbuild.4",
    "configurationSchema": "{\"$ref\":\"#/definitions/Coredns\",\"$schema
\":\"http://json-schema.org/draft-06/schema#\",\"definitions\":{\"Coredns\":
{\"additionalProperties\":false,\"properties\":{\"computeType\":{\"type\":
\"string\"},\"corefile\":{\"description\":\"Entire corefile contents to use with
 installation\",\"type\":\"string\"},\"nodeSelector\":{\"additionalProperties\":
{\"type\":\"string\"},\"type\":\"object\"},\"replicaCount\":{\"type\":\"integer
\"},\"resources\":{\"$ref\":\"#/definitions/Resources\"}},\"title\":\"Coredns\",
\"type\":\"object\"},\"Limits\":{\"additionalProperties\":false,\"properties\":
{\"cpu\":{\"type\":\"string\"},\"memory\":{\"type\":\"string\"}},\"title\":\"Limits
\",\"type\":\"object\"},\"Resources\":{\"additionalProperties\":false,\"properties
\":{\"limits\":{\"$ref\":\"#/definitions/Limits\"},\"requests\":{\"$ref\":\"#/
definitions/Limits\"}},\"title\":\"Resources\",\"type\":\"object\"}}}"
}
```

Para obtener más información, consulte Conexión de kubectl a un clúster de EKS mediante la creación de un archivo kubeconfig en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte DescribeAddonConfiguration en la Referencia de comandos de la AWS CLI.

`describe-addon-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-addon-versions`.

AWS CLI

Ejemplo 1: enumeración de todos los complementos disponibles para un clúster de EKS

En el siguiente ejemplo de `describe-addon-versions` se enumeran todos los complementos de AWS disponibles.

```
aws eks describe-addon-versions  \
    --query 'sort_by(addons  &owner)[].{publisher: publisher, owner: owner,
 addonName: addonName, type: type}' \
    --output table
```

Salida:

```
-------------------------------------------------------------------------------------------
|                                          DescribeAddonVersions
                                |
```

```
+-------------------------------------------+-----------------
+----------------------+-------------------------+
|                  addonName                |      owner       |       publisher
     |          type           |
+-------------------------------------------+-----------------
+----------------------+-------------------------+
|  vpc-cni                                  |  aws             |  eks
     |  networking             |
|  snapshot-controller                      |  aws             |  eks
     |  storage                |
|  kube-proxy                               |  aws             |  eks
     |  networking             |
|  eks-pod-identity-agent                   |  aws             |  eks
     |  security               |
|  coredns                                  |  aws             |  eks
     |  networking             |
|  aws-mountpoint-s3-csi-driver             |  aws             |  s3
     |  storage                |
|  aws-guardduty-agent                      |  aws             |  eks
     |  security               |
|  aws-efs-csi-driver                       |  aws             |  eks
     |  storage                |
|  aws-ebs-csi-driver                       |  aws             |  eks
     |  storage                |
|  amazon-cloudwatch-observability          |  aws             |  eks
     |  observability          |
|  adot                                     |  aws             |  eks
     |  observability          |
|  upwind-security_upwind-operator          |  aws-marketplace |  Upwind Security
     |  security               |
|  upbound_universal-crossplane             |  aws-marketplace |  upbound
     |  infra-management       |
|  tetrate-io_istio-distro                  |  aws-marketplace |  tetrate-io
     |  policy-management      |
|  teleport_teleport                        |  aws-marketplace |  teleport
     |  policy-management      |
|  stormforge_optimize-live                 |  aws-marketplace |  StormForge
     |  cost-management        |
|  splunk_splunk-otel-collector-chart       |  aws-marketplace |  Splunk
     |  monitoring             |
|  solo-io_istio-distro                     |  aws-marketplace |  Solo.io
     |  service-mesh           |
|  rafay-systems_rafay-operator             |  aws-marketplace |  rafay-systems
     |  kubernetes-management  |
```

```
|  new-relic_kubernetes-operator              |  aws-marketplace |  New Relic
     |  observability          |
|  netapp_trident-operator                    |  aws-marketplace |  NetApp Inc.
     |  storage                |
|  leaksignal_leakagent                       |  aws-marketplace |  leaksignal
     |  monitoring             |
|  kubecost_kubecost                          |  aws-marketplace |  kubecost
     |  cost-management        |
|  kong_konnect-ri                            |  aws-marketplace |  kong
     |  ingress-service-type   |
|  kasten_k10                                 |  aws-marketplace |  Kasten by Veeam
     |  data-protection        |
|  haproxy-technologies_kubernetes-ingress-ee |  aws-marketplace |  HAProxy
 Technologies |  ingress-controller     |
|  groundcover_agent                          |  aws-marketplace |  groundcover
     |  monitoring             |
|  grafana-labs_kubernetes-monitoring         |  aws-marketplace |  Grafana Labs
     |  monitoring             |
|  factorhouse_kpow                           |  aws-marketplace |  factorhouse
     |  monitoring             |
|  dynatrace_dynatrace-operator               |  aws-marketplace |  dynatrace
     |  monitoring             |
|  datree_engine-pro                          |  aws-marketplace |  datree
     |  policy-management      |
|  datadog_operator                           |  aws-marketplace |  Datadog
     |  monitoring             |
|  cribl_cribledge                            |  aws-marketplace |  Cribl
     |  observability          |
|  calyptia_fluent-bit                        |  aws-marketplace |  Calyptia Inc
     |  observability          |
|  accuknox_kubearmor                         |  aws-marketplace |  AccuKnox
     |  security               |
+---------------------------------------------+------------------
+----------------------+-------------------------+
```

Para obtener más información, consulte Managing Amazon EKS add-ons - Creating an add-on en la Guía del usuario de Amazon EKS.

Ejemplo 2: enumeración de todos los complementos disponibles para la versión especificada de Kubernetes compatible con EKS

En el siguiente ejemplo de `describe-addon-versions` se enumeran todos los complementos disponibles para la versión especificada de Kubernetes compatible con EKS.

```
aws eks describe-addon-versions  \
    --kubernetes-version=1.26 \
    --query 'sort_by(addons  &owner)[].{publisher: publisher, owner: owner,
 addonName: addonName, type: type}' \
    --output table
```

Salida:

```
-------------------------------------------------------------------------------------------------
|                                                DescribeAddonVersions
                                |
+-----------------------------------------------+------------------
+-----------------------+-------------------------+
|                   addonName                   |      owner       |       publisher
     |          type           |
+-----------------------------------------------+------------------
+-----------------------+-------------------------+
|  vpc-cni                                      |  aws             |  eks
     |  networking             |
|  snapshot-controller                          |  aws             |  eks
     |  storage                |
|  kube-proxy                                   |  aws             |  eks
     |  networking             |
|  eks-pod-identity-agent                       |  aws             |  eks
     |  security               |
|  coredns                                      |  aws             |  eks
     |  networking             |
|  aws-mountpoint-s3-csi-driver                 |  aws             |  s3
     |  storage                |
|  aws-guardduty-agent                          |  aws             |  eks
     |  security               |
|  aws-efs-csi-driver                           |  aws             |  eks
     |  storage                |
|  aws-ebs-csi-driver                           |  aws             |  eks
     |  storage                |
|  amazon-cloudwatch-observability              |  aws             |  eks
     |  observability          |
|  adot                                         |  aws             |  eks
     |  observability          |
|  upwind-security_upwind-operator              |  aws-marketplace |  Upwind Security
     |  security               |
|  tetrate-io_istio-distro                      |  aws-marketplace |  tetrate-io
     |  policy-management      |
```

```
|  stormforge_optimize-live                    |  aws-marketplace |  StormForge
     |  cost-management        |
|  splunk_splunk-otel-collector-chart          |  aws-marketplace |  Splunk
     |  monitoring             |
|  solo-io_istio-distro                        |  aws-marketplace |  Solo.io
     |  service-mesh           |
|  rafay-systems_rafay-operator                |  aws-marketplace |  rafay-systems
     |  kubernetes-management  |
|  new-relic_kubernetes-operator               |  aws-marketplace |  New Relic
     |  observability          |
|  netapp_trident-operator                     |  aws-marketplace |  NetApp Inc.
     |  storage                |
|  leaksignal_leakagent                        |  aws-marketplace |  leaksignal
     |  monitoring             |
|  kubecost_kubecost                           |  aws-marketplace |  kubecost
     |  cost-management        |
|  kong_konnect-ri                             |  aws-marketplace |  kong
     |  ingress-service-type   |
|  haproxy-technologies_kubernetes-ingress-ee |  aws-marketplace |  HAProxy
 Technologies |  ingress-controller     |
|  groundcover_agent                           |  aws-marketplace |  groundcover
     |  monitoring             |
|  grafana-labs_kubernetes-monitoring          |  aws-marketplace |  Grafana Labs
     |  monitoring             |
|  dynatrace_dynatrace-operator                |  aws-marketplace |  dynatrace
     |  monitoring             |
|  datadog_operator                            |  aws-marketplace |  Datadog
     |  monitoring             |
|  cribl_cribledge                             |  aws-marketplace |  Cribl
     |  observability          |
|  calyptia_fluent-bit                         |  aws-marketplace |  Calyptia Inc
     |  observability          |
|  accuknox_kubearmor                          |  aws-marketplace |  AccuKnox
     |  security               |
+----------------------------------------------+------------------
+----------------------+-------------------------+
```

Para obtener más información, consulte Managing Amazon EKS add-ons - Creating an add-on en la Guía del usuario de Amazon EKS.

Ejemplo 3: enumeración de todos los complementos vpc-cni disponibles para la versión especificada de Kubernetes compatible con EKS

En el siguiente ejemplo de `describe-addon-versions` se enumeran todos los complementos vpc-cni disponibles para la versión especificada de Kubernetes compatible con EKS.

```
aws eks describe-addon-versions \
    --kubernetes-version=1.26 \
    --addon-name=vpc-cni \
    --query='addons[].addonVersions[].addonVersion'
```

Salida:

```
[
    "v1.18.0-eksbuild.1",
    "v1.17.1-eksbuild.1",
    "v1.16.4-eksbuild.2",
    "v1.16.3-eksbuild.2",
    "v1.16.2-eksbuild.1",
    "v1.16.0-eksbuild.1",
    "v1.15.5-eksbuild.1",
    "v1.15.4-eksbuild.1",
    "v1.15.3-eksbuild.1",
    "v1.15.1-eksbuild.1",
    "v1.15.0-eksbuild.2",
    "v1.14.1-eksbuild.1",
    "v1.14.0-eksbuild.3",
    "v1.13.4-eksbuild.1",
    "v1.13.3-eksbuild.1",
    "v1.13.2-eksbuild.1",
    "v1.13.0-eksbuild.1",
    "v1.12.6-eksbuild.2",
    "v1.12.6-eksbuild.1",
    "v1.12.5-eksbuild.2",
    "v1.12.0-eksbuild.2"
]
```

Para obtener más información, consulte Managing Amazon EKS add-ons - Creating an add-on en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte DescribeAddonVersions en la Referencia de comandos de la AWS CLI.

`describe-addon`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-addon`.

AWS CLI

Descripción de la ejecución activa del complemento de EKS en su clúster de Amazon EKS

En el siguiente ejemplo de `describe-addon` se describe la ejecución activa del complemento de EKS en su clúster de Amazon EKS.

```
aws eks describe-addon \
    --cluster-name my-eks-cluster \
    --addon-name vpc-cni
```

Salida:

```
{
    "addon": {
        "addonName": "vpc-cni",
        "clusterName": "my-eks-cluster",
        "status": "ACTIVE",
        "addonVersion": "v1.16.4-eksbuild.2",
        "health": {
            "issues": []
        },
        "addonArn": "arn:aws:eks:us-east-2:111122223333:addon/my-eks-cluster/vpc-
cni/0ec71efc-98dd-3203-60b0-4b939b2a5e5f",
        "createdAt": "2024-03-14T13:18:45.417000-04:00",
        "modifiedAt": "2024-03-14T13:18:49.557000-04:00",
        "serviceAccountRoleArn": "arn:aws:iam::111122223333:role/eksctl-my-eks-
cluster-addon-vpc-cni-Role1-YfakrqOC1UTm",
        "tags": {
            "eks-addon-key-3": "value-3",
            "eks-addon-key-4": "value-4"
        },
        "configurationValues": "resources:\n    limits:\n        cpu: '100m'\nenv:\n
    AWS_VPC_K8S_CNI_LOGLEVEL: 'DEBUG'"
    }
}
```

- Para obtener información sobre la API, consulte DescribeAddon en la Referencia de comandos de la AWS CLI.

describe-cluster

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cluster`.

AWS CLI

Descripción de la ejecución activa del complemento de EKS en su clúster de Amazon EKS

En el siguiente ejemplo de `describe-cluster` se describe la ejecución activa del complemento de EKS en su clúster de Amazon EKS.

```
aws eks describe-cluster \
    --name my-eks-cluster
```

Salida:

```
{
    "cluster": {
        "name": "my-eks-cluster",
        "arn": "arn:aws:eks:us-east-2:111122223333:cluster/my-eks-cluster",
        "createdAt": "2024-03-14T11:31:44.348000-04:00",
        "version": "1.26",
        "endpoint": "https://JSA79429HJDASKJDJ8223829MNDNASW.yl4.us-
east-2.eks.amazonaws.com",
        "roleArn": "arn:aws:iam::111122223333:role/eksctl-my-eks-cluster-cluster-
ServiceRole-zMF6CBakwwbW",
        "resourcesVpcConfig": {
            "subnetIds": [
                "subnet-0fb75d2d8401716e7",
                "subnet-02184492f67a3d0f9",
                "subnet-04098063527aab776",
                "subnet-0e2907431c9988b72",
                "subnet-04ad87f71c6e5ab4d",
                "subnet-09d912bb63ef21b9a"
            ],
            "securityGroupIds": [
                "sg-0c1327f6270afbb36"
            ],
            "clusterSecurityGroupId": "sg-01c84d09d70f39a7f",
            "vpcId": "vpc-0012b8e1cc0abb17d",
            "endpointPublicAccess": true,
            "endpointPrivateAccess": true,
            "publicAccessCidrs": [
```

```
                "22.19.18.2/32"
            ]
        },
        "kubernetesNetworkConfig": {
            "serviceIpv4Cidr": "10.100.0.0/16",
            "ipFamily": "ipv4"
        },
        "logging": {
            "clusterLogging": [
                {
                    "types": [
                        "api",
                        "audit",
                        "authenticator",
                        "controllerManager",
                        "scheduler"
                    ],
                    "enabled": true
                }
            ]
        },
        "identity": {
            "oidc": {
                "issuer": "https://oidc.eks.us-east-2.amazonaws.com/id/
JSA79429HJDASKJDJ8223829MNDNASW"
            }
        },
        "status": "ACTIVE",
        "certificateAuthority": {
            "data": "CA_DATA_STRING..."
        },
        "platformVersion": "eks.14",
        "tags": {
            "aws:cloudformation:stack-name": "eksctl-my-eks-cluster-cluster",
            "alpha.eksctl.io/cluster-name": "my-eks-cluster",
            "karpenter.sh/discovery": "my-eks-cluster",
            "aws:cloudformation:stack-id": "arn:aws:cloudformation:us-
east-2:111122223333:stack/eksctl-my-eks-cluster-cluster/e752ea00-e217-11ee-
beae-0a9599c8c7ed",
            "auto-delete": "no",
            "eksctl.cluster.k8s.io/v1alpha1/cluster-name": "my-eks-cluster",
            "EKS-Cluster-Name": "my-eks-cluster",
            "alpha.eksctl.io/cluster-oidc-enabled": "true",
            "aws:cloudformation:logical-id": "ControlPlane",
```

```
            "alpha.eksctl.io/eksctl-version": "0.173.0-dev
+a7ee89342.2024-03-01T03:40:57Z",
            "Name": "eksctl-my-eks-cluster-cluster/ControlPlane"
        },
        "health": {
            "issues": []
        },
        "accessConfig": {
            "authenticationMode": "API_AND_CONFIG_MAP"
        }
    }
}
```

- Para obtener información sobre la API, consulte DescribeCluster en la Referencia de comandos de la AWS CLI.

`describe-fargate-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fargate-profile`.

AWS CLI

Descripción de un perfil de Fargate

En el siguiente ejemplo de `describe-fargate-profile` se describe un perfil de Fargate.

```
aws eks describe-fargate-profile \
    --cluster-name my-eks-cluster \
    --fargate-profile-name my-fargate-profile
```

Salida:

```
{
    "fargateProfile": {
        "fargateProfileName": "my-fargate-profile",
        "fargateProfileArn": "arn:aws:eks:us-east-2:111122223333:fargateprofile/my-
eks-cluster/my-fargate-profile/96c766ce-43d2-f9c9-954c-647334391198",
        "clusterName": "my-eks-cluster",
        "createdAt": "2024-04-11T10:42:52.486000-04:00",
        "podExecutionRoleArn": "arn:aws:iam::111122223333:role/eksctl-my-eks-
cluster-farga-FargatePodExecutionRole-1htfAaJdJUEO",
```

```
        "subnets": [
            "subnet-09d912bb63ef21b9a",
            "subnet-04ad87f71c6e5ab4d",
            "subnet-0e2907431c9988b72"
        ],
        "selectors": [
            {
                "namespace": "prod*",
                "labels": {
                    "labelname*?": "*value1"
                }
            },
            {
                "namespace": "*dev*",
                "labels": {
                    "labelname*?": "*value*"
                }
            }
        ],
        "status": "ACTIVE",
        "tags": {
            "eks-fargate-profile-key-2": "value-2",
            "eks-fargate-profile-key-1": "value-1"
        }
    }
}
```

- Para obtener información sobre la API, consulte DescribeFargateProfile en la Referencia de comandos de la AWS CLI.

`describe-identity-provider-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-identity-provider-config`.

AWS CLI

Descripción de una configuración de proveedor de identidad asociada a su clúster de Amazon EKS

En el siguiente ejemplo de `describe-identity-provider-config` se describe una configuración de proveedor de identidad asociada a su clúster de Amazon EKS.

```
aws eks describe-identity-provider-config \
    --cluster-name my-eks-cluster \
    --identity-provider-config type=oidc,name=my-identity-provider
```

Salida:

```
{
    "identityProviderConfig": {
        "oidc": {
            "identityProviderConfigName": "my-identity-provider",
            "identityProviderConfigArn": "arn:aws:eks:us-
east-2:111122223333:identityproviderconfig/my-eks-cluster/oidc/my-identity-
provider/8ac76722-78e4-cec1-ed76-d49eea058622",
            "clusterName": "my-eks-cluster",
            "issuerUrl": "https://oidc.eks.us-east-2.amazonaws.com/
id/38D6A4619A0A69E342B113ED7F1A7652",
            "clientId": "kubernetes",
            "usernameClaim": "email",
            "usernamePrefix": "my-username-prefix",
            "groupsClaim": "my-claim",
            "groupsPrefix": "my-groups-prefix",
            "requiredClaims": {
                "Claim1": "value1",
                "Claim2": "value2"
            },
            "tags": {
                "env": "dev"
            },
            "status": "ACTIVE"
        }
    }
}
```

Para obtener más información, consulte Concesión de acceso a los usuarios a Kubernetes con un proveedor de OIDC externo en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte DescribeIdentityProviderConfig en la Referencia de comandos de la AWS CLI.

`describe-insight`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-insight`.

AWS CLI

Obtención de los detalles de una información de un clúster de EKS mediante su ID

En el siguiente ejemplo de `describe-insight` se devuelven los detalles sobre la información especificada mediante el nombre del clúster y el ID de la información.

```
aws eks describe-insight \
    --cluster-name eks-customer \
    --id 38ea7a64-a14f-4e0e-95c7-8dbcab3c3623
```

Salida:

```
{
    "insight": {
        "id": "38ea7a64-a14f-4e0e-95c7-8dbcab3c3623",
        "name": "Kubelet version skew",
        "category": "UPGRADE_READINESS",
        "kubernetesVersion": "1.33",
        "lastRefreshTime": "2025-05-24T11:22:50-05:00",
        "lastTransitionTime": "2025-05-24T11:22:50-05:00",
        "description": "Checks for kubelet versions of worker nodes in the cluster
 to see if upgrade would cause noncompliance with supported Kubernetes kubelet
 version skew policy.",
        "insightStatus": {
            "status": "PASSING",
            "reason": "Node kubelet versions match the cluster control plane
 version."
        },
        "recommendation": "Upgrade your worker nodes to match the Kubernetes version
 of your cluster control plane.",
        "additionalInfo": {
            "Kubelet version skew policy": "https://kubernetes.io/releases/version-
skew-policy/#kubelet",
            "Updating a managed node group": "https://docs.aws.amazon.com/eks/
latest/userguide/update-managed-node-group.html"
        },
        "resources": [],
        "categorySpecificSummary": {
            "deprecationDetails": []
        }
    }
}
```

Para obtener más información, consulte Visualización de la información del clúster en la Guía del usuario de Amazon EKS.

- Para obtener detalles de la API, consulte DescribeInsight en la Referencia de comandos de la AWS CLI.

`describe-nodegroup`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-nodegroup`.

AWS CLI

Descripción de un grupo de nodos administrados para un clúster de Amazon EKS

En el siguiente ejemplo de `describe-nodegroup` se describe un grupo de nodos administrados para un clúster de Amazon EKS.

```
aws eks describe-nodegroup \
    --cluster-name my-eks-cluster \
    --nodegroup-name my-eks-nodegroup
```

Salida:

```
{
    "nodegroup": {
        "nodegroupName": "my-eks-nodegroup",
        "nodegroupArn": "arn:aws:eks:us-east-2:111122223333:nodegroup/my-eks-
cluster/my-eks-nodegroup/a8c75f2f-df78-a72f-4063-4b69af3de5b1",
        "clusterName": "my-eks-cluster",
        "version": "1.26",
        "releaseVersion": "1.26.12-20240329",
        "createdAt": "2024-04-08T11:42:10.555000-04:00",
        "modifiedAt": "2024-04-08T11:44:12.402000-04:00",
        "status": "ACTIVE",
        "capacityType": "ON_DEMAND",
        "scalingConfig": {
            "minSize": 1,
            "maxSize": 3,
            "desiredSize": 1
        },
        "instanceTypes": [
            "t3.medium"
        ],
```

```
        "subnets": [
            "subnet-0e2907431c9988b72",
            "subnet-04ad87f71c6e5ab4d",
            "subnet-09d912bb63ef21b9a"
        ],
        "amiType": "AL2_x86_64",
        "nodeRole": "arn:aws:iam::111122223333:role/role-name",
        "labels": {},
        "resources": {
            "autoScalingGroups": [
                {
                    "name": "eks-my-eks-nodegroup-a8c75f2f-df78-
a72f-4063-4b69af3de5b1"
                }
            ]
        },
        "diskSize": 20,
        "health": {
            "issues": []
        },
        "updateConfig": {
            "maxUnavailable": 1
        },
        "tags": {}
    }
}
```

- Para obtener información sobre la API, consulte DescribeNodegroup en la Referencia de comandos de la AWS CLI.

`describe-pod-identity-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-pod-identity-association`.

AWS CLI

Suministro de detalles sobre la asociación de Pod Identity

En el siguiente ejemplo de `describe-pod-identity-association` se describe una asociación de Pod Identity en el clúster de EKS.

```
aws eks describe-pod-identity-association \
```

```
    --cluster-name eks-customer \
    --association-id a-9njjin9gfghecgocd
```

Salida:

```
{
    "association": {
        "clusterName": "eks-customer",
        "namespace": "default",
        "serviceAccount": "default",
        "roleArn": "arn:aws:iam::111122223333:role/my-role",
        "associationArn": "arn:aws:eks:us-
west-2:111122223333:podidentityassociation/eks-customer/a-9njjin9gfghecgocd",
        "associationId": "a-9njjin9gfghecgocd",
        "tags": {
            "Key2": "value2",
            "Key1": "value1"
        },
        "createdAt": "2025-05-24T19:52:14.135000-05:00",
        "modifiedAt": "2025-05-24T19:52:14.135000-05:00"
    }
}
```

Para obtener más información, consulte Información sobre cómo Pod Identity de EKS concede a los pods acceso a los servicios de AWS en la Guía del usuario de Amazon EKS.

- Para obtener detalles de la API, consulte DescribePodIdentityAssociation en la Referencia de comandos de AWS CLI.

`describe-update`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-update`.

AWS CLI

Ejemplo 1: descripción de una actualización de un clúster

En el siguiente ejemplo de `describe-update` se describe una actualización para un clúster con nombre.

```
aws eks describe-update \
    --name my-eks-cluster \
```

```
    --update-id 10bddb13-a71b-425a-b0a6-71cd03e59161
```

Salida:

```
{
    "update": {
        "id": "10bddb13-a71b-425a-b0a6-71cd03e59161",
        "status": "Successful",
        "type": "EndpointAccessUpdate",
        "params": [
            {
                "type": "EndpointPublicAccess",
                "value": "false"
            },
            {
                "type": "EndpointPrivateAccess",
                "value": "true"
            }
        ],
        "createdAt": "2024-03-14T10:01:26.297000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Actualización del clúster existente a la nueva versión de Kubernetes en la Guía del usuario de Amazon EKS.

Ejemplo 2: descripción de una actualización de un clúster

En el siguiente ejemplo de `describe-update` se describe una actualización para un clúster con nombre.

```
aws eks describe-update \
    --name my-eks-cluster \
    --update-id e4994991-4c0f-475a-a040-427e6da52966
```

Salida:

```
{
    "update": {
        "id": "e4994991-4c0f-475a-a040-427e6da52966",
        "status": "Successful",
```

```
        "type": "AssociateEncryptionConfig",
        "params": [
            {
                "type": "EncryptionConfig",
                "value": "[{\"resources\":[\"secrets\"],\"provider\":{\"keyArn\":
\"arn:aws:kms:region-code:account:key/key\"}}]"
            }
        ],
        "createdAt": "2024-03-14T11:01:26.297000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Actualización del clúster existente a la nueva versión de Kubernetes en la Guía del usuario de Amazon EKS.

Ejemplo 3: descripción de una actualización de un clúster

En el siguiente ejemplo de `describe-update` se describe una actualización para un clúster con nombre.

```
aws eks describe-update \
    --name my-eks-cluster \
    --update-id b5f0ba18-9a87-4450-b5a0-825e6e84496f
```

Salida:

```
{
    "update": {
        "id": "b5f0ba18-9a87-4450-b5a0-825e6e84496f",
        "status": "Successful",
        "type": "VersionUpdate",
        "params": [
            {
                "type": "Version",
                "value": "1.29"
            },
            {
                "type": "PlatformVersion",
                "value": "eks.1"
            }
        ],
        "createdAt": "2024-03-14T12:05:26.297000-04:00",
```

```
        "errors": []
    }
}
```

Para obtener más información, consulte Actualización del clúster existente a la nueva versión de Kubernetes en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte DescribeUpdate en la Referencia de comandos de la AWS CLI.

`disassociate-access-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-access-policy`.

AWS CLI

Desasociación de la política de acceso de una entrada de acceso

En el siguiente ejemplo de `disassociate-access-policy` se elimina la política de acceso asociada a la entrada de acceso.

```
aws eks disassociate-access-policy \
    --cluster-name eks-customer \
    --principal-arn arn:aws:iam::111122223333:role/Admin \
    --policy-arn arn:aws:eks::aws:cluster-access-policy/AmazonEKSEditPolicy
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Asociación de políticas de acceso con entradas de acceso en la Guía del usuario de Amazon EKS.

- Para obtener detalles de la API, consulte DisassociateAccessPolicy en la Referencia de comandos de AWS CLI.

`disassociate-identity-provider-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-identity-provider-config`.

AWS CLI

Desasociación del proveedor de identidad del clúster de Amazon EKS

En el siguiente ejemplo de `disassociate-identity-provider-config` se desasocia un proveedor de identidad de su clúster de Amazon EKS.

```
aws eks disassociate-identity-provider-config \
    --cluster-name my-eks-cluster \
    --identity-provider-config 'type=oidc,name=my-identity-provider'
```

Salida:

```
{
    "update": {
        "id": "5f78d14e-c57b-4857-a3e4-cf664ae20949",
        "status": "InProgress",
        "type": "DisassociateIdentityProviderConfig",
        "params": [
            {
                "type": "IdentityProviderConfig",
                "value": "[]"
            }
        ],
        "createdAt": "2024-04-11T13:53:43.314000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Concesión de acceso a los usuarios a Kubernetes con un proveedor de OIDC externo. Cómo desasociar un proveedor de identidad OIDC del clúster en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte DisassociateIdentityProviderConfig en la Referencia de comandos de la AWS CLI.

`get-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-token`.

AWS CLI

Ejemplo 1: obtención de un token de autenticación para un clúster de Amazon EKS denominado my-eks-cluster`

En el siguiente ejemplo de `get-token` se obtiene un token de autenticación para un clúster de Amazon EKS denominado my-eks-cluster.

```
aws eks get-token \
    --cluster-name my-eks-cluster
```

Salida:

```
{
    "kind": "ExecCredential",
    "apiVersion": "client.authentication.k8s.io/v1beta1",
    "spec": {},
    "status": {
        "expirationTimestamp": "2024-04-11T20:59:56Z",
        "token": "k8s-aws-v1.EXAMPLE_TOKEN_DATA_STRING..."
    }
}
```

Ejemplo 2: obtención de un token de autenticación para un clúster de Amazon EKS denominado my-eks-cluster tomando el ARN del rol para las credenciales al firmar con el token

En el siguiente ejemplo de `get-token` se obtiene un token de autenticación para un clúster de Amazon EKS denominado my-eks-cluster tomando el ARN del rol para las credenciales al firmar con el token.

```
aws eks get-token \
    --cluster-name my-eks-cluster \
    --role-arn arn:aws:iam::111122223333:role/eksctl-EKS-Linux-Cluster-v1-24-cluster-ServiceRole-j1k7AfTIQtnM
```

Salida:

```
{
    "kind": "ExecCredential",
    "apiVersion": "client.authentication.k8s.io/v1beta1",
    "spec": {},
    "status": {
        "expirationTimestamp": "2024-04-11T21:05:26Z",
        "token": "k8s-aws-v1.EXAMPLE_TOKEN_DATA_STRING..."
    }
}
```

- Para obtener información sobre la API, consulte GetToken en la Referencia de comandos de la AWS CLI.

`list-access-entries`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-access-entries`.

AWS CLI

Enumeración de las entradas de acceso de un clúster de EKS

En el siguiente ejemplo de `list-access-entries` se devuelve la lista de entradas de acceso asociadas al clúster de EKS `eks-customer`.

```
aws eks list-access-entries \
    --cluster-name eks-customer
```

Salida:

```
{
    "accessEntries": [
        "arn:aws:iam::111122223333:role/Admin",
        "arn:aws:iam::111122223333:role/admin-test-ip",
        "arn:aws:iam::111122223333:role/assume-worker-node-role",
        "arn:aws:iam::111122223333:user/eks-admin-user"
    ]
}
```

Para obtener más información, consulte Concesión de acceso a Kubernetes a los usuarios de IAM con entradas de acceso de EKS en la Guía del usuario de Amazon EKS.

- Para obtener detalles de la API, consulte ListAccessEntries en la Referencia de comandos de AWS CLI.

`list-access-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-access-policies`.

AWS CLI

Enumeración de todas las políticas de acceso disponibles

En este ejemplo de `list-access-policies` se devuelve la lista de todas las políticas de acceso disponibles.

```
aws eks list-access-policies
```

Salida:

```
{
    "accessPolicies": [
        {
            "name": "AmazonEKSAdminPolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/AmazonEKSAdminPolicy"
        },
        {
            "name": "AmazonEKSAdminViewPolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/AmazonEKSAdminViewPolicy"
        },
        {
            "name": "AmazonEKSAutoNodePolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/AmazonEKSAutoNodePolicy"
        },
        {
            "name": "AmazonEKSBlockStorageClusterPolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSBlockStorageClusterPolicy"
        },
        {
            "name": "AmazonEKSBlockStoragePolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSBlockStoragePolicy"
        },
        {
            "name": "AmazonEKSClusterAdminPolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSClusterAdminPolicy"
        },
        {
            "name": "AmazonEKSComputeClusterPolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSComputeClusterPolicy"
        },
        {
            "name": "AmazonEKSComputePolicy",
```

```
            "arn": "arn:aws:eks::aws:cluster-access-policy/AmazonEKSComputePolicy"
        },
        {
            "name": "AmazonEKSEditPolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/AmazonEKSEditPolicy"
        },
        {
            "name": "AmazonEKSHybridPolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/AmazonEKSHybridPolicy"
        },
        {
            "name": "AmazonEKSLoadBalancingClusterPolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSLoadBalancingClusterPolicy"
        },
        {
            "name": "AmazonEKSLoadBalancingPolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSLoadBalancingPolicy"
        },
        {
            "name": "AmazonEKSNetworkingClusterPolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSNetworkingClusterPolicy"
        },
        {
            "name": "AmazonEKSNetworkingPolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSNetworkingPolicy"
        },
        {
            "name": "AmazonEKSViewPolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/AmazonEKSViewPolicy"
        },
        {
            "name": "AmazonEMRJobPolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/AmazonEMRJobPolicy"
        },
        {
            "name": "AmazonSagemakerHyperpodClusterPolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/
AmazonSagemakerHyperpodClusterPolicy"
        },
        {
```

```
            "name": "AmazonSagemakerHyperpodControllerPolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/
AmazonSagemakerHyperpodControllerPolicy"
        },
        {
            "name": "AmazonSagemakerHyperpodSystemNamespacePolicy",
            "arn": "arn:aws:eks::aws:cluster-access-policy/
AmazonSagemakerHyperpodSystemNamespacePolicy"
        }
    ]
}
```

Para obtener más información, consulte Asociación de políticas de acceso con entradas de acceso en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte ListAccessPolicies en la Referencia de comandos de la AWS CLI.

`list-addons`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-addons`.

AWS CLI

Para enumerar todos los complementos instalados en su clúster de Amazon EKS denominado my-eks-cluster`

En el siguiente ejemplo de `list-addons` se enumeran todos los complementos instalados en su clúster de Amazon EKS denominado my-eks-cluster.

```
aws eks list-addons \
    --cluster-name my-eks-cluster
```

Salida:

```
{
    "addons": [
        "kube-proxy",
        "vpc-cni"
    ]
}
```

- Para obtener información sobre la API, consulte ListAddons en la Referencia de comandos de la AWS CLI.

`list-associated-access-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-associated-access-policies`.

AWS CLI

Enumeración de las políticas de acceso asociadas a una entrada de acceso

En el siguiente ejemplo de `list-associated-access-policies` se devuelve la lista de políticas de acceso asociadas a una entrada de acceso en el clúster de EKS.

```
aws eks list-associated-access-policies \
    --cluster-name eks-customer \
    --principal-arn arn:aws:iam::111122223333:role/Admin
```

Salida:

```
{
    "associatedAccessPolicies": [
        {
            "policyArn": "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSAdminPolicy",
            "accessScope": {
                "type": "cluster",
                "namespaces": []
            },
            "associatedAt": "2025-05-24T17:26:22.935000-05:00",
            "modifiedAt": "2025-05-24T17:26:22.935000-05:00"
        }
    ],
    "clusterName": "eks-customer",
    "principalArn": "arn:aws:iam::111122223333:role/Admin"
}
```

Para obtener más información, consulte Concesión de acceso a Kubernetes a los usuarios de IAM con entradas de acceso de EKS en la Guía del usuario de Amazon EKS.

- Para obtener detalles de la API, consulte ListAssociatedAccessPolicies en la Referencia de comandos de AWS CLI.

`list-clusters`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-clusters`.

AWS CLI

Para enumerar todos los complementos instalados en su clúster de Amazon EKS denominado my-eks-cluster`

En el siguiente ejemplo de `list-clusters` se enumeran todos los complementos instalados en su clúster de Amazon EKS denominado my-eks-cluster.

```
aws eks list-clusters
```

Salida:

```
{
    "clusters": [
        "prod",
        "qa",
        "stage",
        "my-eks-cluster"
    ]
}
```

- Para obtener información sobre la API, consulte ListClusters en la Referencia de comandos de la AWS CLI.

`list-fargate-profiles`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-fargate-profiles`.

AWS CLI

Para enumerar todos los perfiles de Fargate de su clúster de Amazon EKS denominado my-eks-cluster`

En el siguiente ejemplo de `list-fargate-profiles` se enumeran todos los perfiles de Fargate de su clúster de Amazon EKS denominado my-eks-cluster.

```
aws eks list-fargate-profiles \
    --cluster-name my-eks-cluster
```

Salida:

```
{
    "fargateProfileNames": [
        "my-fargate-profile"
    ]
}
```

- Para obtener información sobre la API, consulte ListFargateProfiles en la Referencia de comandos de la AWS CLI.

`list-identity-provider-configs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-identity-provider-configs`.

AWS CLI

Para enumerar los proveedores de identidad asociados a un clúster de Amazon EKS

En el siguiente ejemplo de `list-identity-provider-configs` se enumeran los proveedores de identidad asociados a un clúster de Amazon EKS.

```
aws eks list-identity-provider-configs \
    --cluster-name my-eks-cluster
```

Salida:

```
{
    "identityProviderConfigs": [
        {
            "type": "oidc",
            "name": "my-identity-provider"
        }
    ]
}
```

Para obtener más información, consulte Concesión de acceso a los usuarios a Kubernetes con un proveedor de OIDC externo en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte ListIdentityProviderConfigs en la Referencia de comandos de la AWS CLI.

`list-insights`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-insights`.

AWS CLI

Enumeración de toda la información del clúster especificado

En el siguiente ejemplo de `list-insights` se devuelve la lista de toda la información verificada según el clúster especificado.

```
aws eks list-insights \
--cluster-name eks-customer
```

Salida:

```
{
    "insights": [
        {
            "id": "38ea7a64-a14f-4e0e-95c7-8dbcab3c3616",
            "name": "Kubelet version skew",
            "category": "UPGRADE_READINESS",
            "kubernetesVersion": "1.33",
            "lastRefreshTime": "2025-05-24T11:22:50-05:00",
            "lastTransitionTime": "2025-05-24T11:22:50-05:00",
            "description": "Checks for kubelet versions of worker nodes in the
 cluster to see if upgrade would cause noncompliance with supported Kubernetes
 kubelet version skew policy.",
            "insightStatus": {
                "status": "PASSING",
                "reason": "Node kubelet versions match the cluster control plane
 version."
            }
        },
        {
            "id": "9cd91472-f99c-45a9-b7d7-54d4900dee23",
            "name": "EKS add-on version compatibility",
```

```
            "category": "UPGRADE_READINESS",
            "kubernetesVersion": "1.33",
            "lastRefreshTime": "2025-05-24T11:22:59-05:00",
            "lastTransitionTime": "2025-05-24T11:22:50-05:00",
            "description": "Checks version of installed EKS add-ons to ensure they
are compatible with the next version of Kubernetes. ",
            "insightStatus": {
                "status": "PASSING",
                "reason": "All installed EKS add-on versions are compatible with
next Kubernetes version."
            }
        },
        {
            "id": "0deb269d-b1e1-458c-a2b4-7a57f940c875",
            "name": "Cluster health issues",
            "category": "UPGRADE_READINESS",
            "kubernetesVersion": "1.33",
            "lastRefreshTime": "2025-05-24T11:22:59-05:00",
            "lastTransitionTime": "2025-05-24T11:22:50-05:00",
            "description": "Checks for any cluster health issues that prevent
successful upgrade to the next Kubernetes version on EKS.",
            "insightStatus": {
                "status": "PASSING",
                "reason": "No cluster health issues detected."
            }
        },
        {
            "id": "214fa274-344f-420b-812a-5049ce72c9ww",
            "name": "kube-proxy version skew",
            "category": "UPGRADE_READINESS",
            "kubernetesVersion": "1.33",
            "lastRefreshTime": "2025-05-24T11:22:50-05:00",
            "lastTransitionTime": "2025-05-24T11:22:50-05:00",
            "description": "Checks version of kube-proxy in cluster to see if
upgrade would cause noncompliance with supported Kubernetes kube-proxy version skew
policy.",
            "insightStatus": {
                "status": "PASSING",
                "reason": "kube-proxy versions match the cluster control plane
version."
            }
        }
    ]
```

```
}
```

Para obtener más información, consulte Visualización de la información del clúster en la Guía del usuario de Amazon EKS.

- Para obtener detalles de la API, consulte ListInsights en la Referencia de comandos de AWS CLI.

`list-nodegroups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-nodegroups`.

AWS CLI

Para enumerar todos los grupos de nodos de un clúster de Amazon EKS

En el siguiente ejemplo de `list-nodegroups` se enumeran todos los grupos de nodos de un clúster de Amazon EKS.

```
aws eks list-nodegroups \
    --cluster-name my-eks-cluster
```

Salida:

```
{
    "nodegroups": [
        "my-eks-managed-node-group",
        "my-eks-nodegroup"
    ]
}
```

- Para obtener información sobre la API, consulte ListNodegroups en la Referencia de comandos de la AWS CLI.

`list-pod-identity-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-pod-identity-associations`.

AWS CLI

Ejemplo 1: enumeración de las asociaciones de Pod Identity en un clúster de EKS

En el siguiente ejemplo de `list-pod-identity-associations` se devuelve la lista de asociaciones de Pod Identity asociadas al clúster de EKS denominadas `eks-customer` en todos los espacios de nombres y cuentas de servicio.

```
aws eks list-pod-identity-associations \
    --cluster-name eks-customer
```

Salida:

```
{
    "associations": [
        {
            "clusterName": "eks-customer",
            "namespace": "default",
            "serviceAccount": "default",
            "associationArn": "arn:aws:eks:us-
west-2:111122223333:podidentityassociation/eks-customer/a-9njjin9gfghecgocd",
            "associationId": "a-9njjin9gfghecgocd"
        },
        {
            "clusterName": "eks-customer",
            "namespace": "kube-system",
            "serviceAccount": "eks-customer",
            "associationArn": "arn:aws:eks:us-
west-2:111122223333:podidentityassociation/eks-customer/a-dvtacahdvjn01ffbc",
            "associationId": "a-dvtacahdvjn01ffbc"
        },
        {
            "clusterName": "eks-customer",
            "namespace": "kube-system",
            "serviceAccount": "coredns",
            "associationArn": "arn:aws:eks:us-
west-2:111122223333:podidentityassociation/eks-customer/a-yrpsdroc4ei7k6xps",
            "associationId": "a-yrpsdroc4ei7k6xps"
        }
    ]
}
```

Para obtener más información, consulte Información sobre cómo Pod Identity de EKS concede a los pods acceso a los servicios de AWS en la Guía del usuario de Amazon EKS.

Ejemplo 2: enumeración de las asociaciones de Pod Identity en un clúster de EKS en función del espacio de nombres y la cuenta de servicio

En el siguiente ejemplo de `list-pod-identity-associations` se devuelve la lista de asociaciones de Pod Identity en el clúster de EKS en función del espacio de nombres y la cuenta de servicio.

```
aws eks list-pod-identity-associations \
    --cluster-name eks-customer \
    --namespace kube-system \
    --service-account eks-customer
```

Salida:

```
{
    "associations": [
        {
            "clusterName": "eks-customer",
            "namespace": "kube-system",
            "serviceAccount": "eks-customer",
            "associationArn": "arn:aws:eks:us-
west-2:111122223333:podidentityassociation/eks-customer/a-dvtacahdvjn01ffbc",
            "associationId": "a-dvtacahdvjn01ffbc"
        }
    ]
}
```

Para obtener más información, consulte Información sobre cómo Pod Identity de EKS concede a los pods acceso a los servicios de AWS en la Guía del usuario de Amazon EKS.

- Para obtener detalles de la API, consulte ListPodIdentityAssociations en la Referencia de comandos de AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Ejemplo 1: enumeración de todas las etiquetas de un ARN de un clúster de Amazon EKS

En el siguiente ejemplo de `list-tags-for-resource` se enumeran todas las etiquetas del ARN de un clúster de Amazon EKS.

```
aws eks list-tags-for-resource \
    --resource-arn arn:aws:eks:us-east-2:111122223333:cluster/my-eks-cluster
```

Salida:

```
{
    "tags": {
        "aws:cloudformation:stack-name": "eksctl-my-eks-cluster-cluster",
        "alpha.eksctl.io/cluster-name": "my-eks-cluster",
        "karpenter.sh/discovery": "my-eks-cluster",
        "aws:cloudformation:stack-id": "arn:aws:cloudformation:us-
east-2:111122223333:stack/eksctl-my-eks-cluster-cluster/e752ea00-e217-11ee-
beae-0a9599c8c7ed",
        "auto-delete": "no",
        "eksctl.cluster.k8s.io/v1alpha1/cluster-name": "my-eks-cluster",
        "EKS-Cluster-Name": "my-eks-cluster",
        "alpha.eksctl.io/cluster-oidc-enabled": "true",
        "aws:cloudformation:logical-id": "ControlPlane",
        "alpha.eksctl.io/eksctl-version": "0.173.0-dev
+a7ee89342.2024-03-01T03:40:57Z",
        "Name": "eksctl-my-eks-cluster-cluster/ControlPlane"
    }
}
```

Ejemplo 2: enumeración de todas las etiquetas de un ARN de un grupo de nodos de Amazon EKS

En el siguiente ejemplo de `list-tags-for-resource` se enumeran todas las etiquetas del ARN de un grupo de nodos de Amazon EKS.

```
aws eks list-tags-for-resource \
    --resource-arn arn:aws:eks:us-east-2:111122223333:nodegroup/my-eks-cluster/my-
eks-managed-node-group/60c71ed2-2cfb-020f-a5f4-ad32477f198c
```

Salida:

```
{
    "tags": {
```

```
        "aws:cloudformation:stack-name": "eksctl-my-eks-cluster-nodegroup-my-eks-
managed-node-group",
        "aws:cloudformation:stack-id": "arn:aws:cloudformation:us-
east-2:111122223333:stack/eksctl-my-eks-cluster-nodegroup-my-eks-managed-node-group/
eaa20310-e219-11ee-b851-0ab9ad8228ff",
        "eksctl.cluster.k8s.io/v1alpha1/cluster-name": "my-eks-cluster",
        "EKS-Cluster-Name": "my-eks-cluster",
        "alpha.eksctl.io/nodegroup-type": "managed",
        "NodeGroup Name 1": "my-eks-managed-node-group",
        "k8s.io/cluster-autoscaler/enabled": "true",
        "nodegroup-role": "worker",
        "alpha.eksctl.io/cluster-name": "my-eks-cluster",
        "alpha.eksctl.io/nodegroup-name": "my-eks-managed-node-group",
        "karpenter.sh/discovery": "my-eks-cluster",
        "NodeGroup Name 2": "AmazonLinux-Linux-Managed-NG-v1-26-v1",
        "auto-delete": "no",
        "k8s.io/cluster-autoscaler/my-eks-cluster": "owned",
        "aws:cloudformation:logical-id": "ManagedNodeGroup",
        "alpha.eksctl.io/eksctl-version": "0.173.0-dev
+a7ee89342.2024-03-01T03:40:57Z"
    }
}
```

Ejemplo 3: enumeración de todas las etiquetas de un ARNe de perfil de Amazon EKS Fargate

En el siguiente ejemplo de `list-tags-for-resource` se enumeran todas las etiquetas del ARN de un perfil de Fargate de Amazon EKS.

```
aws eks list-tags-for-resource  \
    --resource-arn arn:aws:eks:us-east-2:111122223333:fargateprofile/my-eks-cluster/
my-fargate-profile/d6c76780-e541-0725-c816-36754cab734b
```

Salida:

```
{
    "tags": {
        "eks-fargate-profile-key-2": "value-2",
        "eks-fargate-profile-key-1": "value-1"
    }
}
```

Ejemplo 4: enumeración de todas las etiquetas de un ARN del complemento de Amazon EKS

En el siguiente ejemplo de `list-tags-for-resource` se enumeran todas las etiquetas del ARN de un complemento de Amazon EKS.

```
aws eks list-tags-for-resource \
    --resource-arn arn:aws:eks:us-east-2:111122223333:addon/my-eks-cluster/vpc-cni/0ec71efc-98dd-3203-60b0-4b939b2a5e5f
```

Salida:

```
{
    "tags": {
        "eks-addon-key-2": "value-2",
        "eks-addon-key-1": "value-1"
    }
}
```

Ejemplo 5: enumeración de todas las etiquetas de un ARN de proveedor de identidad de OIDC de Amazon EKS

En el siguiente ejemplo de `list-tags-for-resource` se enumeran todas las etiquetas del ARN de un proveedor de identidad de OIDC de Amazon EKS.

```
aws eks list-tags-for-resource \
    --resource-arn arn:aws:eks:us-east-2:111122223333:identityproviderconfig/my-eks-cluster/oidc/my-identity-provider/8ac76722-78e4-cec1-ed76-d49eea058622
```

Salida:

```
{
    "tags": {
        "my-identity-provider": "test"
    }
}
```

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-update`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-update`.

AWS CLI

Ejemplo 1: enumeración de las actualizaciones asociadas a un nombre de clúster de Amazon EKS

En el siguiente ejemplo de `list-updates` se enumeran todos los ID de actualización del nombre de un clúster de Amazon EKS.

```
aws eks list-updates \
    --name my-eks-cluster
```

Salida:

```
{
    "updateIds": [
        "5f78d14e-c57b-4857-a3e4-cf664ae20949",
        "760e5a3f-adad-48c7-88d3-7ac283c09c26",
        "cd4ec863-bc55-47d5-a377-3971502f529b",
        "f12657ce-e869-4f17-b158-a82ab8b7d937"
    ]
}
```

Ejemplo 2: enumeración de todos los ID de actualización de un grupo de nodos de Amazon EKS

En el siguiente ejemplo de `list-updates` se enumeran todos los ID de actualización de un grupo de nodos de Amazon EKS.

```
aws eks list-updates \
    --name my-eks-cluster \
    --nodegroup-name my-eks-managed-node-group
```

Salida:

```
{
    "updateIds": [
        "8c6c1bef-61fe-42ac-a242-89412387b8e7"
    ]
}
```

Ejemplo 3: enumeración de todos los ID de actualización de un complemento de Amazon EKS

En el siguiente ejemplo de `list-updates` se enumeran todos los ID de actualización de un complemento de Amazon EKS.

```
aws eks list-updates \
    --name my-eks-cluster \
    --addon-name vpc-cni
```

Salida:

```
{
    "updateIds": [
        "9cdba8d4-79fb-3c83-afe8-00b508d33268"
    ]
}
```

- Para obtener información sobre la API, consulte ListUpdate en la Referencia de comandos de la AWS CLI.

`list-updates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-updates`.

AWS CLI

Para enumerar las actualizaciones de un clúster

En este ejemplo de comando se enumeran las actualizaciones actuales de un clúster denominado `example` de su región predeterminada.

Comando:

```
aws eks list-updates --name example
```

Salida:

```
{
    "updateIds": [
        "10bddb13-a71b-425a-b0a6-71cd03e59161"
    ]
```

```
}
```

- Para obtener información sobre la API, consulte ListUpdates en la Referencia de comandos de la AWS CLI.

`register-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-cluster`.

AWS CLI

Ejemplo 1: registro de un clúster EKS_ANYWHERE externo de Kubernetes en Amazon EKS

En el siguiente ejemplo de `register-cluster` se registra un clúster EKS_ANYWHERE externo de Kubernetes en Amazon EKS.

```
aws eks register-cluster \
    --name my-eks-anywhere-cluster \
    --connector-config 'roleArn=arn:aws:iam::111122223333:role/
AmazonEKSConnectorAgentRole,provider=EKS_ANYWHERE'
```

Salida:

```
{
    "cluster": {
        "name": "my-eks-anywhere-cluster",
        "arn": "arn:aws:eks:us-east-2:111122223333:cluster/my-eks-anywhere-cluster",
        "createdAt": "2024-04-12T12:38:37.561000-04:00",
        "status": "PENDING",
        "tags": {},
        "connectorConfig": {
            "activationId": "xxxxxxxxACTIVATION_IDxxxxxxxx",
            "activationCode": "xxxxxxxxACTIVATION_CODExxxxxxxx",
            "activationExpiry": "2024-04-15T12:38:37.082000-04:00",
            "provider": "EKS_ANYWHERE",
            "roleArn": "arn:aws:iam::111122223333:role/AmazonEKSConnectorAgentRole"
        }
    }
}
```

Para obtener más información, consulte Conexión de un clúster externo en la Guía del usuario de Amazon EKS.

Ejemplo 2: registro de cualquier clúster externo de Kubernetes en Amazon EKS

En el siguiente ejemplo de `register-cluster` se registra un clúster EKS_ANYWHERE externo de Kubernetes en Amazon EKS.

```
aws eks register-cluster \
    --name my-eks-anywhere-cluster \
    --connector-config 'roleArn=arn:aws:iam::111122223333:role/
AmazonEKSConnectorAgentRole,provider=OTHER'
```

Salida:

```
{
    "cluster": {
        "name": "my-onprem-k8s-cluster",
        "arn": "arn:aws:eks:us-east-2:111122223333:cluster/my-onprem-k8s-cluster",
        "createdAt": "2024-04-12T12:42:10.861000-04:00",
        "status": "PENDING",
        "tags": {},
        "connectorConfig": {
            "activationId": "xxxxxxxxACTIVATION_IDxxxxxxxx",
            "activationCode": "xxxxxxxxACTIVATION_CODExxxxxxxx",
            "activationExpiry": "2024-04-15T12:42:10.339000-04:00",
            "provider": "OTHER",
            "roleArn": "arn:aws:iam::111122223333:role/AmazonEKSConnectorAgentRole"
        }
    }
}
```

Para obtener más información, consulte Conexión de un clúster externo en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte RegisterCluster en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Ejemplo 1: adición de las etiquetas especificadas a un clúster de Amazon EKS

En el siguiente ejemplo de `tag-resource` se agregan las etiquetas especificadas a un clúster de Amazon EKS.

```
aws eks tag-resource \
    --resource-arn arn:aws:eks:us-east-2:111122223333:cluster/my-eks-cluster \
    --tag 'my-eks-cluster-test-1=test-value-1,my-eks-cluster-dev-1=dev-value-2'
```

Este comando no genera ninguna salida.

Ejemplo 2: adición de las etiquetas especificadas a un grupo de nodos de Amazon EKS

En el siguiente ejemplo de `tag-resource` se agregan las etiquetas especificadas a un grupo de nodos de Amazon EKS.

```
aws eks tag-resource \
    --resource-arn arn:aws:eks:us-east-2:111122223333:nodegroup/my-eks-cluster/my-eks-managed-node-group/60c71ed2-2cfb-020f-a5f4-ad32477f198c \
    --tag 'my-eks-nodegroup-test-1=test-value-1,my-eks-nodegroup-dev-1=dev-value-2'
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Ejemplo 1: eliminación de las etiquetas especificadas de un clúster de Amazon EKS

En el siguiente ejemplo de `untag-resource` se eliminan las etiquetas especificadas de un clúster de Amazon EKS.

```
aws eks untag-resource \
    --resource-arn arn:aws:eks:us-east-2:111122223333:cluster/my-eks-cluster \
    --tag-keys "my-eks-cluster-test-1" "my-eks-cluster-dev-1"
```

Este comando no genera ninguna salida.

Ejemplo 2: eliminación de las etiquetas especificadas de un grupo de nodos de Amazon EKS

En el siguiente ejemplo de `untag-resource` se eliminan las etiquetas especificadas de un grupo de nodos de Amazon EKS.

```
aws eks untag-resource \
    --resource-arn arn:aws:eks:us-east-2:111122223333:nodegroup/my-eks-cluster/my-eks-managed-node-group/60c71ed2-2cfb-020f-a5f4-ad32477f198c \
    --tag-keys "my-eks-nodegroup-test-1" "my-eks-nodegroup-dev-1"
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-access-entry`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-access-entry`.

AWS CLI

Actualización de una entrada de acceso para un clúster de EKS

En el siguiente ejemplo de `update-access-entry` se actualiza una entrada de acceso para el clúster de EKS mediante la adición del grupo de Kubernetes `tester`.

```
aws eks update-access-entry \
    --cluster-name eks-customer \
    --principal-arn arn:aws:iam::111122223333:role/Admin \
    --kubernetes-groups tester
```

Salida:

```
{
    "accessEntry": {
        "clusterName": "eks-customer",
        "principalArn": "arn:aws:iam::111122223333:role/Admin",
        "kubernetesGroups": [
            "tester"
        ],
        "accessEntryArn": "arn:aws:eks:us-west-2:111122223333:access-entry/eks-customer/role/111122223333/Admin/d2cb8183-d6ec-b82a-d967-eca21902a4b4",
```

```
        "createdAt": "2025-05-24T11:02:04.432000-05:00",
        "modifiedAt": "2025-05-24T17:08:01.608000-05:00",
        "tags": {},
        "username": "arn:aws:sts::111122223333:assumed-role/Admin/{{SessionName}}",
        "type": "STANDARD"
    }
}
```

Para obtener más información, consulte Actualización de entradas de acceso en la Guía del usuario de Amazon EKS.

- Para obtener detalles de la API, consulte UpdateAccessEntry en la Referencia de comandos de AWS CLI.

`update-addon`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-addon`.

AWS CLI

Ejemplo 1. Para actualizar un complemento de Amazon EKS con el ARN de rol de cuenta de servicio

En el siguiente ejemplo del comando `update-addon` se actualiza un complemento de Amazon EKS con el ARN de rol de cuenta de servicio.

```
aws eks update-addon \
    --cluster-name my-eks-cluster \
    --addon-name vpc-cni \
    --service-account-role-arn arn:aws:iam::111122223333:role/eksctl-my-eks-cluster-addon-vpc-cni-Role1-YfakrqOC1UTm
```

Salida:

```
{
    "update": {
        "id": "c00d2de2-c2e4-3d30-929e-46b8edec2ce4",
        "status": "InProgress",
        "type": "AddonUpdate",
        "params": [
            {
                "type": "ServiceAccountRoleArn",
```

```
                "value": "arn:aws:iam::111122223333:role/eksctl-my-eks-cluster-
addon-vpc-cni-Role1-YfakrqOC1UTm"
            }
        ],
        "updatedAt": "2024-04-12T16:04:55.614000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Managing Amazon EKS add-ons - Updating an add-on en la Guía del usuario de Amazon EKS.

Ejemplo 2. Para actualizar un complemento de Amazon EKS con una versión del complemento específica

En el siguiente ejemplo del comando `update-addon` se actualiza un complemento de Amazon EKS con una versión del complemento específica.

```
aws eks update-addon \
    --cluster-name my-eks-cluster \
    --addon-name vpc-cni \
    --service-account-role-arn arn:aws:iam::111122223333:role/eksctl-my-eks-cluster-
addon-vpc-cni-Role1-YfakrqOC1UTm \
    --addon-version v1.16.4-eksbuild.2
```

Salida:

```
{
    "update": {
        "id": "f58dc0b0-2b18-34bd-bc6a-e4abc0011f36",
        "status": "InProgress",
        "type": "AddonUpdate",
        "params": [
            {
                "type": "AddonVersion",
                "value": "v1.16.4-eksbuild.2"
            },
            {
                "type": "ServiceAccountRoleArn",
                "value": "arn:aws:iam::111122223333:role/eksctl-my-eks-cluster-
addon-vpc-cni-Role1-YfakrqOC1UTm"
            }
```

```
        ],
        "createdAt": "2024-04-12T16:07:16.550000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Managing Amazon EKS add-ons - Updating an add-on en la Guía del usuario de Amazon EKS.

Ejemplo 3. Para actualizar un complemento de Amazon EKS con valores de configuración personalizados y datos de resolución de conflictos

En el siguiente ejemplo del comando `update-addon` se actualiza un complemento de Amazon EKS con valores de configuración personalizados y datos de resolución de conflictos.

```
aws eks update-addon \
    --cluster-name my-eks-cluster \
    --addon-name vpc-cni \
    --service-account-role-arn arn:aws:iam::111122223333:role/eksctl-my-eks-cluster-addon-vpc-cni-Role1-YfakrqOC1UTm \
    --addon-version v1.16.4-eksbuild.2 \
    --configuration-values '{"resources": {"limits":{"cpu":"100m"}, "requests": {"cpu":"50m"}}}' \
    --resolve-conflicts PRESERVE
```

Salida:

```
{
    "update": {
        "id": "cd9f2173-a8d8-3004-a90f-032f14326520",
        "status": "InProgress",
        "type": "AddonUpdate",
        "params": [
            {
                "type": "AddonVersion",
                "value": "v1.16.4-eksbuild.2"
            },
            {
                "type": "ServiceAccountRoleArn",
                "value": "arn:aws:iam::111122223333:role/eksctl-my-eks-cluster-addon-vpc-cni-Role1-YfakrqOC1UTm"
            },
```

```
            {
                "type": "ResolveConflicts",
                "value": "PRESERVE"
            },
            {
                "type": "ConfigurationValues",
                "value": "{\"resources\": {\"limits\":{\"cpu\":\"100m\"}, \"requests
\":{\"cpu\":\"50m\"}}}"
            }
        ],
        "createdAt": "2024-04-12T16:16:27.363000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Managing Amazon EKS add-ons - Updating an add-on en la Guía del usuario de Amazon EKS.

Ejemplo 4. Para actualizar un complemento de Amazon EKS con un archivo de JSON de valores de configuración personalizados

En el siguiente ejemplo del comando `update-addon` se actualiza un complemento de Amazon EKS con valores de configuración personalizados y datos de resolución de conflictos de JSON.

```
aws eks update-addon \
    --cluster-name my-eks-cluster \
    --addon-name vpc-cni \
    --service-account-role-arn arn:aws:iam::111122223333:role/eksctl-my-eks-cluster-
addon-vpc-cni-Role1-YfakrqOC1UTm \
    --addon-version v1.17.1-eksbuild.1 \
    --configuration-values 'file://configuration-values.json' \
    --resolve-conflicts PRESERVE
```

Contenido de `configuration-values.json`:

```
{
    "resources": {
        "limits": {
            "cpu": "100m"
        },
        "requests": {
            "cpu": "50m"
```

```
        }
    },
    "env": {
        "AWS_VPC_K8S_CNI_LOGLEVEL": "ERROR"
    }
}
```

Salida:

```
{
    "update": {
        "id": "6881a437-174f-346b-9a63-6e91763507cc",
        "status": "InProgress",
        "type": "AddonUpdate",
        "params": [
            {
                "type": "AddonVersion",
                "value": "v1.17.1-eksbuild.1"
            },
            {
                "type": "ServiceAccountRoleArn",
                "value": "arn:aws:iam::111122223333:role/eksctl-my-eks-cluster-
addon-vpc-cni-Role1-YfakrqOC1UTm"
            },
            {
                "type": "ResolveConflicts",
                "value": "PRESERVE"
            },
            {
                "type": "ConfigurationValues",
                "value": "{\n    \"resources\": {\n        \"limits\": {\n
  \"cpu\": \"100m\"\n        },\n        \"requests\": {\n            \"cpu\": \"50m
\"\n        }\n    },\n    \"env\": {\n        \"AWS_VPC_K8S_CNI_LOGLEVEL\": \"ERROR
\"\n    }\n}"
            }
        ],
        "createdAt": "2024-04-12T16:22:55.519000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Managing Amazon EKS add-ons - Updating an add-on en la Guía del usuario de Amazon EKS.

Ejemplo 5. Para actualizar un complemento de Amazon EKS con un archivo de YAML de valores de configuración personalizados

En el siguiente ejemplo del comando `update-addon` se actualiza un complemento de Amazon EKS con valores de configuración personalizados y datos de resolución de conflictos de YAML.

```
aws eks update-addon \
    --cluster-name my-eks-cluster \
    --addon-name vpc-cni \
    --service-account-role-arn arn:aws:iam::111122223333:role/eksctl-my-eks-cluster-addon-vpc-cni-Role1-YfakrqOC1UTm \
    --addon-version v1.18.0-eksbuild.1 \
    --configuration-values 'file://configuration-values.yaml' \
    --resolve-conflicts PRESERVE
```

Contenido de `configuration-values.yaml`:

```
resources:
    limits:
        cpu: '100m'
    requests:
        cpu: '50m'
env:
    AWS_VPC_K8S_CNI_LOGLEVEL: 'DEBUG'
```

Salida:

```
{
    "update": {
        "id": "a067a4c9-69d0-3769-ace9-d235c5b16701",
        "status": "InProgress",
        "type": "AddonUpdate",
        "params": [
            {
                "type": "AddonVersion",
                "value": "v1.18.0-eksbuild.1"
            },
            {
                "type": "ServiceAccountRoleArn",
                "value": "arn:aws:iam::111122223333:role/eksctl-my-eks-cluster-addon-vpc-cni-Role1-YfakrqOC1UTm"
            },
```

```
            {
                "type": "ResolveConflicts",
                "value": "PRESERVE"
            },
            {
                "type": "ConfigurationValues",
                "value": "resources:\n    limits:\n        cpu: '100m'\n
 requests:\n        cpu: '50m'\nenv:\n    AWS_VPC_K8S_CNI_LOGLEVEL: 'DEBUG'"
            }
        ],
        "createdAt": "2024-04-12T16:25:07.212000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Managing Amazon EKS add-ons - Updating an add-on en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte UpdateAddon en la Referencia de comandos de la AWS CLI.

`update-cluster-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-cluster-config`.

AWS CLI

Para actualizar el acceso al punto de conexión del clúster

En este ejemplo de comando se actualiza un clúster para deshabilitar el acceso público a los puntos de conexión y habilitar el acceso privado a los puntos de conexión.

Comando:

```
aws eks update-cluster-config --name example \
--resources-vpc-config endpointPublicAccess=false,endpointPrivateAccess=true
```

Salida:

```
{
    "update": {
```

```
        "id": "ec883c93-2e9e-407c-a22f-8f6fa6e67d4f",
        "status": "InProgress",
        "type": "EndpointAccessUpdate",
        "params": [
            {
                "type": "EndpointPublicAccess",
                "value": "false"
            },
            {
                "type": "EndpointPrivateAccess",
                "value": "true"
            }
        ],
        "createdAt": 1565806986.506,
        "errors": []
    }
}
```

Para habilitar el registro en un clúster

En este ejemplo de comando se habilitan todos los tipos de registro del plano de control del clúster para un clúster denominado `example`.

Comando:

```
aws eks update-cluster-config --name example \
--logging '{"clusterLogging":[{"types":
["api","audit","authenticator","controllerManager","scheduler"],"enabled":true}]}'
```

Salida:

```
{
    "update": {
        "id": "7551c64b-1d27-4b1e-9f8e-c45f056eb6fd",
        "status": "InProgress",
        "type": "LoggingUpdate",
        "params": [
            {
                "type": "ClusterLogging",
                "value": "{\"clusterLogging\":[{\"types\":[\"api\",\"audit\",
\"authenticator\",\"controllerManager\",\"scheduler\"],\"enabled\":true}]}"
            }
```

```
        ],
        "createdAt": 1565807210.37,
        "errors": []
    }
}
```

- Para obtener información sobre la API, consulte UpdateClusterConfig en la Referencia de comandos de la AWS CLI.

`update-cluster-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-cluster-version`.

AWS CLI

Para actualizar un clúster de Amazon EKS denominado my-eks-cluster a la versión de Kubernetes especificada

En el siguiente ejemplo de `update-cluster-version` se actualiza un clúster de Amazon EKS a la versión de Kubernetes especificada.

```
aws eks update-cluster-version \
    --name my-eks-cluster \
    --kubernetes-version 1.27
```

Salida:

```
{
    "update": {
        "id": "e4091a28-ea14-48fd-a8c7-975aeb469e8a",
        "status": "InProgress",
        "type": "VersionUpdate",
        "params": [
            {
                "type": "Version",
                "value": "1.27"
            },
            {
                "type": "PlatformVersion",
                "value": "eks.16"
            }
```

```
        ],
        "createdAt": "2024-04-12T16:56:01.082000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Actualización del clúster existente a la nueva versión de Kubernetes en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte UpdateClusterVersion en la Referencia de comandos de la AWS CLI.

`update-kubeconfig`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-kubeconfig`.

AWS CLI

Ejemplo 1: configuración de su kubectl creando o actualizando el kubeconfig para que pueda conectarse a un clúster de Amazon EKS denominado my-eks-cluster`

En el siguiente ejemplo de `update-kubeconfig` se configura su kubectl mediante la creación o actualización del archivo kubeconfig para que pueda conectarse a un clúster de Amazon EKS denominado my-eks-cluster.

```
aws eks update-kubeconfig \
    --name my-eks-cluster
```

Salida:

```
Updated context arn:aws:eks:us-east-2:111122223333:cluster/my-eks-cluster in /Users/
xxx/.kube/config
```

Para obtener más información, consulte Conexión de kubectl a un clúster de EKS mediante la creación de un archivo kubeconfig en la Guía del usuario de Amazon EKS.

Ejemplo 2: configuración de su kubectl mediante la creación o actualización del archivo kubeconfig (con la opción role-arn para asumir un rol de autenticación de clúster) para que pueda conectarse a un clúster de Amazon EKS denominado my-eks-cluster`

En el siguiente ejemplo de `update-kubeconfig` se configura su kubectl mediante la creación o actualización del archivo kubeconfig (con la opción role-arn para asumir un rol de autenticación de clúster) para que pueda conectarse a un clúster de Amazon EKS denominado my-eks-cluster.

```
aws eks update-kubeconfig \
    --name my-eks-cluster \
    --role-arn arn:aws:iam::111122223333:role/eksctl-EKS-Linux-Cluster-v1-24-cluster-ServiceRole-j1k7AfTIQtnM
```

Salida:

```
Updated context arn:aws:eks:us-east-2:111122223333:cluster/my-eks-cluster in /Users/xxx/.kube/config
```

Para obtener más información, consulte Conexión de kubectl a un clúster de EKS mediante la creación de un archivo kubeconfig en la Guía del usuario de Amazon EKS.

Ejemplo 3: configuración de su kubectl mediante la creación o actualización del archivo kubeconfig (con la opción role-arn para asumir un rol de autenticación de clúster, así como un alias de clúster y un alias de usuario personalizados) para que pueda conectarse a un clúster de Amazon EKS denominado my-eks-cluster`

En el siguiente ejemplo de `update-kubeconfig` se configura su kubectl mediante la creación o actualización del archivo kubeconfig (con la opción role-arn para asumir un rol de autenticación de clúster, así como un alias de clúster y un alias de usuario personalizados) para que pueda conectarse a un clúster de Amazon EKS denominado my-eks-cluster.

```
aws eks update-kubeconfig \
    --name my-eks-cluster \
    --role-arn arn:aws:iam::111122223333:role/eksctl-EKS-Linux-Cluster-v1-24-cluster-ServiceRole-j1k7AfTIQtnM \
    --alias stage-eks-cluster \
    --user-alias john
```

Salida:

```
Updated context stage-eks-cluster in /Users/dubaria/.kube/config
```

Para obtener más información, consulte Conexión de kubectl a un clúster de EKS mediante la creación de un archivo kubeconfig en la Guía del usuario de Amazon EKS.

Ejemplo 4: impresión de las entradas del archivo kubeconfig para su revisión y configuración de su kubectl para que pueda conectarse a un clúster de Amazon EKS denominado my-eks-cluster`

En el siguiente ejemplo de `update-kubeconfig` se configura su kubectl mediante la creación o actualización del archivo kubeconfig (con la opción role-arn para asumir un rol de autenticación de clúster, así como un alias de clúster y un alias de usuario personalizados) para que pueda conectarse a un clúster de Amazon EKS denominado my-eks-cluster.

```
aws eks update-kubeconfig \
    --name my-eks-cluster \
    --role-arn arn:aws:iam::111122223333:role/eksctl-EKS-Linux-Cluster-v1-24-cluster-ServiceRole-j1k7AfTIQtnM \
    --alias stage-eks-cluster \
    --user-alias john \
    --verbose
```

Salida:

```
Updated context stage-eks-cluster in /Users/dubaria/.kube/config
Entries:

context:
cluster: arn:aws:eks:us-east-2:111122223333:cluster/my-eks-cluster
user: john
name: stage-eks-cluster

name: john
user:
exec:
    apiVersion: client.authentication.k8s.io/v1beta1
    args:
    - --region
    - us-east-2
    - eks
    - get-token
    - --cluster-name
    - my-eks-cluster
    - --output
    - json
    - --role
    - arn:aws:iam::111122223333:role/eksctl-EKS-Linux-Cluster-v1-24-cluster-ServiceRole-j1k7AfTIQtnM
```

```
    command: aws

cluster:
certificate-authority-data: xxx_CA_DATA_xxx
server: https://DALSJ343KE23J3RN45653DSKJTT647TYD.yl4.us-east-2.eks.amazonaws.com
name: arn:aws:eks:us-east-2:111122223333:cluster/my-eks-cluster
```

Para obtener más información, consulte Conexión de kubectl a un clúster de EKS mediante la creación de un archivo kubeconfig en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte UpdateKubeconfig en la Referencia de comandos de la AWS CLI.

`update-nodegroup-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-nodegroup-config`.

AWS CLI

Ejemplo 1: actualización de un grupo de nodos administrados para agregar nuevas etiquetas y taint al nodo de trabajo de EKS de un clúster de Amazon EKS

En el siguiente ejemplo de `update-nodegroup-config` se actualiza un grupo de nodos administrados para agregar nuevas etiquetas y taint al nodo de trabajo de EKS de un clúster de Amazon EKS.

```
aws eks update-nodegroup-config \
    --cluster-name my-eks-cluster \
    --nodegroup-name my-eks-nodegroup \
    --labels 'addOrUpdateLabels={my-eks-nodegroup-label-1=value-1,my-eks-nodegroup-label-2=value-2}' \
    --taints 'addOrUpdateTaints=[{key=taint-key-1,value=taint-value-1,effect=NO_EXECUTE}]'
```

Salida:

```
{
    "update": {
        "id": "e66d21d3-bd8b-3ad1-a5aa-b196dc08c7c1",
        "status": "InProgress",
        "type": "ConfigUpdate",
        "params": [
```

```
            {
                "type": "LabelsToAdd",
                "value": "{\"my-eks-nodegroup-label-2\":\"value-2\",\"my-eks-
nodegroup-label-1\":\"value-1\"}"
            },
            {
                "type": "TaintsToAdd",
                "value": "[{\"effect\":\"NO_EXECUTE\",\"value\":\"taint-value-1\",
\"key\":\"taint-key-1\"}]"
            }
        ],
        "createdAt": "2024-04-08T12:05:19.161000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Actualización de un grupo de nodos administrados para un clúster en la Guía del usuario de Amazon EKS.

Ejemplo 2: actualización de un grupo de nodos administrados para quitar etiquetas y taint del nodo de trabajo de EKS de un clúster de Amazon EKS

En el siguiente ejemplo de `update-nodegroup-config` se actualiza un grupo de nodos administrados para quitar etiquetas y taint del nodo de trabajo de EKS de un clúster de Amazon EKS.

```
aws eks update-nodegroup-config \
    --cluster-name my-eks-cluster \
    --nodegroup-name my-eks-nodegroup \
    --labels 'removeLabels=my-eks-nodegroup-label-1, my-eks-nodegroup-label-2' \
    --taints 'removeTaints=[{key=taint-key-1,value=taint-
value-1,effect=NO_EXECUTE}]'
```

Salida:

```
{
    "update": {
        "id": "67a08692-9e59-3ace-a916-13929f44cec3",
        "status": "InProgress",
        "type": "ConfigUpdate",
        "params": [
            {
```

```
                "type": "LabelsToRemove",
                "value": "[\"my-eks-nodegroup-label-1\",\"my-eks-nodegroup-
label-2\"]"
            },
            {
                "type": "TaintsToRemove",
                "value": "[{\"effect\":\"NO_EXECUTE\",\"value\":\"taint-value-1\",
\"key\":\"taint-key-1\"}]"
            }
        ],
        "createdAt": "2024-04-08T12:17:31.817000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Actualización de un grupo de nodos administrados para un clúster en la Guía del usuario de Amazon EKS.

Ejemplo 3: actualización de un grupo de nodos administrados para quitar y agregar etiquetas y taint del nodo de trabajo de EKS de un clúster de Amazon EKS

En el siguiente ejemplo de `update-nodegroup-config` se actualiza un grupo de nodos administrados para quitar y agregar etiquetas y taint del nodo de trabajo de EKS de un clúster de Amazon EKS.

```
aws eks update-nodegroup-config \
    --cluster-name my-eks-cluster \
    --nodegroup-name my-eks-nodegroup \
    --labels 'addOrUpdateLabels={my-eks-nodegroup-new-label-1=new-value-1,my-eks-
nodegroup-new-label-2=new-value-2},removeLabels=my-eks-nodegroup-label-1, my-eks-
nodegroup-label-2' \
    --taints 'addOrUpdateTaints=[{key=taint-new-key-1,value=taint-new-
value-1,effect=PREFER_NO_SCHEDULE}],removeTaints=[{key=taint-key-1,value=taint-
value-1,effect=NO_EXECUTE}]'
```

Salida:

```
{
    "update": {
        "id": "4a9c8c45-6ac7-3115-be71-d6412a2339b7",
        "status": "InProgress",
        "type": "ConfigUpdate",
```

```
        "params": [
            {
                "type": "LabelsToAdd",
                "value": "{\"my-eks-nodegroup-new-label-1\":\"new-value-1\",\"my-
eks-nodegroup-new-label-2\":\"new-value-2\"}"
            },
            {
                "type": "LabelsToRemove",
                "value": "[\"my-eks-nodegroup-label-1\",\"my-eks-nodegroup-
label-2\"]"
            },
            {
                "type": "TaintsToAdd",
                "value": "[{\"effect\":\"PREFER_NO_SCHEDULE\",\"value\":\"taint-new-
value-1\",\"key\":\"taint-new-key-1\"}]"
            },
            {
                "type": "TaintsToRemove",
                "value": "[{\"effect\":\"NO_EXECUTE\",\"value\":\"taint-value-1\",
\"key\":\"taint-key-1\"}]"
            }
        ],
        "createdAt": "2024-04-08T12:30:55.486000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Actualización de un grupo de nodos administrados para un clúster en la Guía del usuario de Amazon EKS.

Ejemplo 4: actualización de un grupo de nodos administrados para actualizar scaling-config y update-config para el nodo de trabajo de EKS de un clúster de Amazon EKS

En el siguiente ejemplo de `update-nodegroup-config` se actualiza un grupo de nodos administrados para actualizar scaling-config y update-config para el nodo de trabajo de EKS de un clúster de Amazon EKS.

```
aws eks update-nodegroup-config \
    --cluster-name my-eks-cluster \
    --nodegroup-name my-eks-nodegroup \
    --scaling-config minSize=1,maxSize=5,desiredSize=2 \
    --update-config maxUnavailable=2
```

Salida:

```
{
    "update": {
        "id": "a977160f-59bf-3023-805d-c9826e460aea",
        "status": "InProgress",
        "type": "ConfigUpdate",
        "params": [
            {
                "type": "MinSize",
                "value": "1"
            },
            {
                "type": "MaxSize",
                "value": "5"
            },
            {
                "type": "DesiredSize",
                "value": "2"
            },
            {
                "type": "MaxUnavailable",
                "value": "2"
            }
        ],
        "createdAt": "2024-04-08T12:35:17.036000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Actualización de un grupo de nodos administrados para un clúster en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte UpdateNodegroupConfig en la Referencia de comandos de la AWS CLI.

`update-nodegroup-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-nodegroup-version`.

AWS CLI

Ejemplo 1: actualización de la versión de Kubernetes o la versión de AMI de un grupo de nodos administrados de Amazon EKS

En el siguiente ejemplo de `update-nodegroup-version` se actualiza la versión de Kubernetes o la versión de AMI de un grupo de nodos administrados de Amazon EKS a la última versión disponible para su clúster de Kubernetes.

```
aws eks update-nodegroup-version \
    --cluster-name my-eks-cluster \
    --nodegroup-name my-eks-nodegroup \
    --no-force
```

Salida:

```
{
    "update": {
        "id": "a94ebfc3-6bf8-307a-89e6-7dbaa36421f7",
        "status": "InProgress",
        "type": "VersionUpdate",
        "params": [
            {
                "type": "Version",
                "value": "1.26"
            },
            {
                "type": "ReleaseVersion",
                "value": "1.26.12-20240329"
            }
        ],
        "createdAt": "2024-04-08T13:16:00.724000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Actualización de un grupo de nodos administrados para un clúster en la Guía del usuario de Amazon EKS.

Ejemplo 2: actualización de la versión de Kubernetes o la versión de AMI de un grupo de nodos administrados de Amazon EKS

En el siguiente ejemplo de `update-nodegroup-version` se actualiza la versión de Kubernetes o la versión de AMI de un grupo de nodos administrados de Amazon EKS a la versión de lanzamiento de la AMI especificada.

```
aws eks update-nodegroup-version \
    --cluster-name my-eks-cluster \
    --nodegroup-name my-eks-nodegroup \
    --kubernetes-version '1.26' \
    --release-version '1.26.12-20240307' \
    --no-force
```

Salida:

```
{
    "update": {
        "id": "4db06fe1-088d-336b-bdcd-3fdb94995fb7",
        "status": "InProgress",
        "type": "VersionUpdate",
        "params": [
            {
                "type": "Version",
                "value": "1.26"
            },
            {
                "type": "ReleaseVersion",
                "value": "1.26.12-20240307"
            }
        ],
        "createdAt": "2024-04-08T13:13:58.595000-04:00",
        "errors": []
    }
}
```

Para obtener más información, consulte Actualización de un grupo de nodos administrados para un clúster <https://docs.aws.amazon.com/eks/latest/userguide/update-managed-node-group.html> en la Guía del usuario de Amazon EKS.

- Para obtener información sobre la API, consulte UpdateNodegroupVersion en la Referencia de comandos de la AWS CLI.

update-pod-identity-association

En el siguiente ejemplo de código, se muestra cómo utilizar `update-pod-identity-association`.

AWS CLI

Actualización de la asociación de Pod Identity de EKS

En el siguiente ejemplo de `update-pod-identity-association` se actualiza una asociación de Pod Identity de EKS a través del cambio del rol de IAM asociado de `arn:aws:iam::111122223333:role/my-role` a `arn:aws:iam::111122223333:role/s3-role` correspondiente al ID de asociación `a-9njjin9gfghecgocd`. Esta API solo permite actualizar el rol de IAM asociado.

```
aws eks update-pod-identity-association \
    --cluster-name eks-customer \
    --association-id a-9njjin9gfghecgocd \
    --role-arn arn:aws:iam::111122223333:role/s3-role
```

Salida:

```
{
    "association": {
        "clusterName": "eks-customer",
        "namespace": "default",
        "serviceAccount": "default",
        "roleArn": "arn:aws:iam::111122223333:role/s3-role",
        "associationArn": "arn:aws:eks:us-
west-2:111122223333:podidentityassociation/eks-customer/a-9njjin9gfghecgocd",
        "associationId": "a-9njjin9gfghecgocd",
        "tags": {
            "Key2": "value2",
            "Key1": "value1"
        },
        "createdAt": "2025-05-24T19:52:14.135000-05:00",
        "modifiedAt": "2025-05-25T21:01:53.120000-05:00"
    }
}
```

Para obtener más información, consulte Información sobre cómo Pod Identity de EKS concede a los pods acceso a los servicios de AWS en la Guía del usuario de Amazon EKS.

- Para obtener detalles de la API, consulte UpdatePodIdentityAssociation en la Referencia de comandos de AWS CLI.

Ejemplos de Elastic Beanstalk que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante el uso de la AWS Command Line Interface con Elastic Beanstalk.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`abort-environment-update`

En el siguiente ejemplo de código, se muestra cómo utilizar `abort-environment-update`.

AWS CLI

Para anular una implementación

En el siguiente comando, se anula la implementación de la versión de una aplicación en ejecución en un entorno denominado `my-env`:

```
aws elasticbeanstalk abort-environment-update --environment-name my-env
```

- Para obtener información sobre la API, consulte AbortEnvironmentUpdate en la Referencia de comandos de la AWS CLI.

`check-dns-availability`

En el siguiente ejemplo de código, se muestra cómo utilizar `check-dns-availability`.

AWS CLI

Para comprobar la disponibilidad de un CNAME

En el siguiente comando, se comprueba la disponibilidad del subdominio `my-cname.elasticbeanstalk.com`:

```
aws elasticbeanstalk check-dns-availability --cname-prefix my-cname
```

Salida:

```
{
    "Available": true,
    "FullyQualifiedCNAME": "my-cname.elasticbeanstalk.com"
}
```

- Para obtener información sobre la API, consulte CheckDnsAvailability en la Referencia de comandos de la AWS CLI.

`create-application-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-application-version`.

AWS CLI

Para crear una nueva versión de la aplicación

En el siguiente comando, se crea una nueva versión, v1, de una aplicación denominada MyApp:

```
aws elasticbeanstalk create-application-version --application-name MyApp --
version-label v1 --description MyAppv1 --source-bundle S3Bucket="amzn-s3-demo-
bucket",S3Key="sample.war" --auto-create-application
```

La aplicación se creará automáticamente si aún no existe, gracias a la opción auto-create-application. El paquete de código fuente es un archivo .war almacenado en un bucket de S3 denominado “amzn-s3-demo-bucket” que contiene el ejemplo de aplicación de Apache Tomcat.

Salida:

```
{
  "ApplicationVersion": {
```

```
      "ApplicationName": "MyApp",
      "VersionLabel": "v1",
      "Description": "MyAppv1",
      "DateCreated": "2015-02-03T23:01:25.412Z",
      "DateUpdated": "2015-02-03T23:01:25.412Z",
      "SourceBundle": {
          "S3Bucket": "amzn-s3-demo-bucket",
          "S3Key": "sample.war"
      }
  }
}
```

- Para obtener información sobre la API, consulte CreateApplicationVersion en la Referencia de comandos de la AWS CLI.

`create-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-application`.

AWS CLI

Para crear una nueva aplicación

En el siguiente comando, se crea una nueva versión denominada MyApp:

```
aws elasticbeanstalk create-application --application-name MyApp --description "my
 application"
```

En el comando `create-application` solo se configuran el nombre y la descripción de la aplicación. Para cargar el código fuente de la aplicación, cree una versión inicial de la aplicación mediante `create-application-version`. `create-application-version` también cuenta con la opción `auto-create-application` que permite crear la aplicación y la versión de la aplicación en un mismo paso.

Salida:

```
{
  "Application": {
      "ApplicationName": "MyApp",
      "ConfigurationTemplates": [],
      "DateUpdated": "2015-02-12T18:32:21.181Z",
      "Description": "my application",
```

```
        "DateCreated": "2015-02-12T18:32:21.181Z"
    }
}
```

- Para obtener información sobre la API, consulte CreateApplication en la Referencia de comandos de la AWS CLI.

`create-configuration-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-configuration-template`.

AWS CLI

Para crear una plantilla de configuración

En el siguiente comando, se crea una plantilla de configuración denominada `my-app-v1` a partir de la configuración aplicada a un entorno cuyo id es `e-rpqsewtp2j`:

```
aws elasticbeanstalk create-configuration-template --application-name my-app --
template-name my-app-v1 --environment-id e-rpqsewtp2j
```

Salida:

```
{
    "ApplicationName": "my-app",
    "TemplateName": "my-app-v1",
    "DateCreated": "2015-08-12T18:40:39Z",
    "DateUpdated": "2015-08-12T18:40:39Z",
    "SolutionStackName": "64bit Amazon Linux 2015.03 v2.0.0 running Tomcat 8 Java 8"
}
```

- Para obtener información sobre la API, consulte CreateConfigurationTemplate en la Referencia de comandos de la AWS CLI.

`create-environment`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-environment`.

AWS CLI

Para crear un nuevo entorno para una aplicación

En el siguiente comando, se crea un nuevo entorno para la versión v1 de una aplicación de Java denominada my-app:

```
aws elasticbeanstalk create-environment --application-name my-app --environment-
name my-env --cname-prefix my-app --version-label v1 --solution-stack-name "64bit
 Amazon Linux 2015.03 v2.0.0 running Tomcat 8 Java 8"
```

Salida:

```
{
  "ApplicationName": "my-app",
  "EnvironmentName": "my-env",
  "VersionLabel": "v1",
  "Status": "Launching",
  "EnvironmentId": "e-izqpassy4h",
  "SolutionStackName": "64bit Amazon Linux 2015.03 v2.0.0 running Tomcat 8 Java 8",
  "CNAME": "my-app.elasticbeanstalk.com",
  "Health": "Grey",
  "Tier": {
      "Type": "Standard",
      "Name": "WebServer",
      "Version": " "
  },
  "DateUpdated": "2015-02-03T23:04:54.479Z",
  "DateCreated": "2015-02-03T23:04:54.479Z"
}
```

v1 es la etiqueta de una versión de la aplicación cargada anteriormente mediante create-application-version.

Para especificar un archivo de JSON a fin de definir las opciones de configuración del entorno

En el siguiente comando `create-environment`, se especifica que se debe usar un archivo de JSON con el nombre `myoptions.json` para anular los valores obtenidos del conjunto de soluciones o de la plantilla de configuración:

```
aws elasticbeanstalk create-environment --environment-name sample-env --application-
name sampleapp --option-settings file://myoptions.json
```

`myoptions.json` es un objeto de JSON que define varios ajustes:

```
[
```

```
  {
    "Namespace": "aws:elb:healthcheck",
    "OptionName": "Interval",
    "Value": "15"
  },
  {
    "Namespace": "aws:elb:healthcheck",
    "OptionName": "Timeout",
    "Value": "8"
  },
  {
    "Namespace": "aws:elb:healthcheck",
    "OptionName": "HealthyThreshold",
    "Value": "2"
  },
  {
    "Namespace": "aws:elb:healthcheck",
    "OptionName": "UnhealthyThreshold",
    "Value": "3"
  }
]
```

Para obtener más información, consulte Option Values en la Guía para desarrolladores de AWS Elastic Beanstalk.

- Para obtener información sobre la API, consulte CreateEnvironment en la Referencia de comandos de la AWS CLI.

`create-storage-location`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-storage-location`.

AWS CLI

Para crear una ubicación de almacenamiento

En el siguiente comando, se crea una ubicación de almacenamiento de Amazon S3.

```
aws elasticbeanstalk create-storage-location
```

Salida:

```
{
```

```
    "S3Bucket": "elasticbeanstalk-us-west-2-0123456789012"
}
```

- Para obtener información sobre la API, consulte CreateStorageLocation en la Referencia de comandos de la AWS CLI.

`delete-application-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-application-version`.

AWS CLI

Para eliminar una versión de la aplicación

En el siguiente comando, se elimina una versión de la aplicación denominada `22a0-stage-150819_182129` de una aplicación denominada `my-app`:

```
aws elasticbeanstalk delete-application-version --version-label 22a0-stage-150819_182129 --application-name my-app
```

- Para obtener información sobre la API, consulte DeleteApplicationVersion en la Referencia de comandos de la AWS CLI.

`delete-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-application`.

AWS CLI

Para eliminar una aplicación de

En el siguiente comando, se elimina una aplicación denominada `my-app`:

```
aws elasticbeanstalk delete-application --application-name my-app
```

- Para obtener información sobre la API, consulte DeleteApplication en la Referencia de comandos de la AWS CLI.

`delete-configuration-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-configuration-template`.

AWS CLI

Para eliminar una plantilla de configuración

En el siguiente comando, se elimina una plantilla de configuración denominada `my-template` de una aplicación denominada `my-app`:

```
aws elasticbeanstalk delete-configuration-template --template-name my-template --
application-name my-app
```

- Para obtener información sobre la API, consulte DeleteConfigurationTemplate en la Referencia de comandos de la AWS CLI.

`delete-environment-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-environment-configuration`.

AWS CLI

Para eliminar una configuración provisional

En el siguiente comando, se elimina una configuración provisional de un entorno denominado `my-env`:

```
aws elasticbeanstalk delete-environment-configuration --environment-name my-env --
application-name my-app
```

- Para obtener información sobre la API, consulte DeleteEnvironmentConfiguration en la Referencia de comandos de la AWS CLI.

`describe-application-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-application-versions`.

AWS CLI

Para ver información sobre la versión de una aplicación

En el siguiente comando, se recupera información sobre una versión de la aplicación con la etiqueta `v2`:

```
aws elasticbeanstalk describe-application-versions --application-name my-app --
version-label "v2"
```

Salida:

```
{
    "ApplicationVersions": [
        {
            "ApplicationName": "my-app",
            "VersionLabel": "v2",
            "Description": "update cover page",
            "DateCreated": "2015-07-23T01:32:26.079Z",
            "DateUpdated": "2015-07-23T01:32:26.079Z",
            "SourceBundle": {
                "S3Bucket": "elasticbeanstalk-us-west-2-015321684451",
                "S3Key": "my-app/5026-stage-150723_224258.war"
            }
        },
      {
          "ApplicationName": "my-app",
          "VersionLabel": "v1",
          "Description": "initial version",
          "DateCreated": "2015-07-23T22:26:10.816Z",
          "DateUpdated": "2015-07-23T22:26:10.816Z",
          "SourceBundle": {
              "S3Bucket": "elasticbeanstalk-us-west-2-015321684451",
              "S3Key": "my-app/5026-stage-150723_222618.war"
          }
      }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeApplicationVersions en la Referencia de comandos de la AWS CLI.

`describe-applications`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-applications`.

AWS CLI

Para ver una lista de aplicaciones

En el siguiente comando, se recupera información sobre las aplicaciones de la región actual:

```
aws elasticbeanstalk describe-applications
```

Salida:

```
{
    "Applications": [
        {
            "ApplicationName": "ruby",
            "ConfigurationTemplates": [],
            "DateUpdated": "2015-08-13T21:05:44.376Z",
            "Versions": [
                "Sample Application"
            ],
            "DateCreated": "2015-08-13T21:05:44.376Z"
        },
        {
            "ApplicationName": "pythonsample",
            "Description": "Application created from the EB CLI using \"eb init\"",
            "Versions": [
                "Sample Application"
            ],
            "DateCreated": "2015-08-13T19:05:43.637Z",
            "ConfigurationTemplates": [],
            "DateUpdated": "2015-08-13T19:05:43.637Z"
        },
        {
            "ApplicationName": "nodejs-example",
            "ConfigurationTemplates": [],
            "DateUpdated": "2015-08-06T17:50:02.486Z",
            "Versions": [
                "add elasticache",
                "First Release"
            ],
            "DateCreated": "2015-08-06T17:50:02.486Z"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeApplications en la Referencia de comandos de la AWS CLI.

`describe-configuration-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-configuration-options`.

AWS CLI

Para ver las opciones de configuración de un entorno

En el siguiente comando, se recuperan las descripciones de todas las opciones de configuración disponibles en un entorno denominado `my-env`:

```
aws elasticbeanstalk describe-configuration-options --environment-name my-env --
application-name my-app
```

Salida (abreviada):

```
{
    "Options": [
        {
            "Name": "JVMOptions",
            "UserDefined": false,
            "DefaultValue": "Xms=256m,Xmx=256m,XX:MaxPermSize=64m,JVM Options=",
            "ChangeSeverity": "RestartApplicationServer",
            "Namespace": "aws:cloudformation:template:parameter",
            "ValueType": "KeyValueList"
        },
        {
            "Name": "Interval",
            "UserDefined": false,
            "DefaultValue": "30",
            "ChangeSeverity": "NoInterruption",
            "Namespace": "aws:elb:healthcheck",
            "MaxValue": 300,
            "MinValue": 5,
            "ValueType": "Scalar"
        },
        ...
        {
            "Name": "LowerThreshold",
            "UserDefined": false,
            "DefaultValue": "2000000",
            "ChangeSeverity": "NoInterruption",
            "Namespace": "aws:autoscaling:trigger",
```

```
            "MinValue": 0,
            "ValueType": "Scalar"
        },
        {
            "Name": "ListenerEnabled",
            "UserDefined": false,
            "DefaultValue": "true",
            "ChangeSeverity": "Unknown",
            "Namespace": "aws:elb:listener",
            "ValueType": "Boolean"
        }
    ]
}
```

Las opciones de configuración disponibles varían según la plataforma y la versión de configuración. Para obtener más información sobre los espacios de nombres y las opciones admitidas, consulte Option Values en la Guía para desarrolladores de AWS Elastic Beanstalk.

- Para obtener información sobre la API, consulte DescribeConfigurationOptions en la Referencia de comandos de la AWS CLI.

`describe-configuration-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-configuration-settings`.

AWS CLI

Para ver los ajustes de configuración de un entorno

En el siguiente comando, se recuperan los ajustes de configuración de un entorno denominado `my-env`:

```
aws elasticbeanstalk describe-configuration-settings --environment-name my-env --
application-name my-app
```

Salida (abreviada):

```
{
    "ConfigurationSettings": [
        {
            "ApplicationName": "my-app",
```

```
            "EnvironmentName": "my-env",
            "Description": "Environment created from the EB CLI using \"eb create
\"",
            "DeploymentStatus": "deployed",
            "DateCreated": "2015-08-13T19:16:25Z",
            "OptionSettings": [
                {
                    "OptionName": "Availability Zones",
                    "ResourceName": "AWSEBAutoScalingGroup",
                    "Namespace": "aws:autoscaling:asg",
                    "Value": "Any"
                },
                {
                    "OptionName": "Cooldown",
                    "ResourceName": "AWSEBAutoScalingGroup",
                    "Namespace": "aws:autoscaling:asg",
                    "Value": "360"
                },
                ...
                {
                    "OptionName": "ConnectionDrainingTimeout",
                    "ResourceName": "AWSEBLoadBalancer",
                    "Namespace": "aws:elb:policies",
                    "Value": "20"
                },
                {
                    "OptionName": "ConnectionSettingIdleTimeout",
                    "ResourceName": "AWSEBLoadBalancer",
                    "Namespace": "aws:elb:policies",
                    "Value": "60"
                }
            ],
            "DateUpdated": "2015-08-13T23:30:07Z",
            "SolutionStackName": "64bit Amazon Linux 2015.03 v2.0.0 running Tomcat 8
 Java 8"
        }
    ]
}
```

Para obtener más información sobre los espacios de nombres y las opciones admitidas, consulte Option Values en la Guía para desarrolladores de AWS Elastic Beanstalk.

- Para obtener información sobre la API, consulte DescribeConfigurationSettings en la Referencia de comandos de la AWS CLI.

`describe-environment-health`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-environment-health`.

AWS CLI

Para ver el estado de un entorno

En el siguiente comando, se recupera información sobre el estado general de un entorno denominado `my-env`:

```
aws elasticbeanstalk describe-environment-health --environment-name my-env --
attribute-names All
```

Salida:

```
{
    "Status": "Ready",
    "EnvironmentName": "my-env",
    "Color": "Green",
    "ApplicationMetrics": {
        "Duration": 10,
        "Latency": {
            "P99": 0.004,
            "P75": 0.002,
            "P90": 0.003,
            "P95": 0.004,
            "P85": 0.003,
            "P10": 0.001,
            "P999": 0.004,
            "P50": 0.001
        },
        "RequestCount": 45,
        "StatusCodes": {
            "Status3xx": 0,
            "Status2xx": 45,
            "Status5xx": 0,
            "Status4xx": 0
        }
    },
    "RefreshedAt": "2015-08-20T21:09:18Z",
    "HealthStatus": "Ok",
    "InstancesHealth": {
```

```
        "Info": 0,
        "Ok": 1,
        "Unknown": 0,
        "Severe": 0,
        "Warning": 0,
        "Degraded": 0,
        "NoData": 0,
        "Pending": 0
    },
    "Causes": []
}
```

La información de estado solo está disponible para los entornos en los que se han habilitado los informes de estado mejorados. Para obtener más información, consulte Enhanced Health Reporting and Monitoring en la Guía para desarrolladores de AWS Elastic Beanstalk.

- Para obtener información sobre la API, consulte DescribeEnvironmentHealth en la Referencia de comandos de la AWS CLI.

`describe-environment-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-environment-resources`.

AWS CLI

Para ver información sobre los recursos de AWS de su entorno

En el siguiente comando, se recupera información sobre los recursos de un entorno denominado `my-env`:

```
aws elasticbeanstalk describe-environment-resources --environment-name my-env
```

Salida:

```
{
    "EnvironmentResources": {
        "EnvironmentName": "my-env",
        "AutoScalingGroups": [
            {
                "Name": "awseb-e-qu3fyyjyjs-stack-AWSEBAutoScalingGroup-
QSB2ZO88SXZT"
```

```
            }
        ],
        "Triggers": [],
        "LoadBalancers": [
            {
                "Name": "awseb-e-q-AWSEBLoa-1EEPZ0K98BIF0"
            }
        ],
        "Queues": [],
        "Instances": [
            {
                "Id": "i-0c91c786"
            }
        ],
        "LaunchConfigurations": [
            {
                "Name": "awseb-e-qu3fyyjyjs-stack-
AWSEBAutoScalingLaunchConfiguration-1UUVQIBC96TQ2"
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte DescribeEnvironmentResources en la Referencia de comandos de la AWS CLI.

`describe-environments`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-environments`.

AWS CLI

Para ver información sobre un entorno

En el siguiente comando, se recupera información sobre un entorno denominado `my-env`:

```
aws elasticbeanstalk describe-environments --environment-names my-env
```

Salida:

```
{
    "Environments": [
```

```
        {
            "ApplicationName": "my-app",
            "EnvironmentName": "my-env",
            "VersionLabel": "7f58-stage-150812_025409",
            "Status": "Ready",
            "EnvironmentId": "e-rpqsewtp2j",
            "EndpointURL": "awseb-e-w-AWSEBLoa-1483140XB0Q4L-109QXY8121.us-
west-2.elb.amazonaws.com",
            "SolutionStackName": "64bit Amazon Linux 2015.03 v2.0.0 running Tomcat 8
 Java 8",
            "CNAME": "my-env.elasticbeanstalk.com",
            "Health": "Green",
            "AbortableOperationInProgress": false,
            "Tier": {
                "Version": " ",
                "Type": "Standard",
                "Name": "WebServer"
            },
            "DateUpdated": "2015-08-12T18:16:55.019Z",
            "DateCreated": "2015-08-07T20:48:49.599Z"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeEnvironments en la Referencia de comandos de la AWS CLI.

`describe-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-events`.

AWS CLI

Para ver los eventos de un entorno

En el siguiente comando, se recuperan los eventos de un entorno denominado `my-env`:

```
aws elasticbeanstalk describe-events --environment-name my-env
```

Salida (abreviada):

```
{
```

```
    "Events": [
        {
            "ApplicationName": "my-app",
            "EnvironmentName": "my-env",
            "Message": "Environment health has transitioned from Info to Ok.",
            "EventDate": "2015-08-20T07:06:53.535Z",
            "Severity": "INFO"
        },
        {
            "ApplicationName": "my-app",
            "EnvironmentName": "my-env",
            "Severity": "INFO",
            "RequestId": "b7f3960b-4709-11e5-ba1e-07e16200da41",
            "Message": "Environment update completed successfully.",
            "EventDate": "2015-08-20T07:06:02.049Z"
        },
        ...
        {
            "ApplicationName": "my-app",
            "EnvironmentName": "my-env",
            "Severity": "INFO",
            "RequestId": "ca8dfbf6-41ef-11e5-988b-651aa638f46b",
            "Message": "Using elasticbeanstalk-us-west-2-012445113685 as Amazon S3
 storage bucket for environment data.",
            "EventDate": "2015-08-13T19:16:27.561Z"
        },
        {
            "ApplicationName": "my-app",
            "EnvironmentName": "my-env",
            "Severity": "INFO",
            "RequestId": "cdfba8f6-41ef-11e5-988b-65638f41aa6b",
            "Message": "createEnvironment is starting.",
            "EventDate": "2015-08-13T19:16:26.581Z"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeEvents en la Referencia de comandos de la AWS CLI.

`describe-instances-health`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instances-health`.

AWS CLI

Para ver el estado de un entorno

En el siguiente comando, se recupera la información de estado de las instancias de un entorno denominado `my-env`:

```
aws elasticbeanstalk describe-instances-health --environment-name my-env --
attribute-names All
```

Salida:

```
{
    "InstanceHealthList": [
        {
            "InstanceId": "i-08691cc7",
            "ApplicationMetrics": {
                "Duration": 10,
                "Latency": {
                    "P99": 0.006,
                    "P75": 0.002,
                    "P90": 0.004,
                    "P95": 0.005,
                    "P85": 0.003,
                    "P10": 0.0,
                    "P999": 0.006,
                    "P50": 0.001
                },
                "RequestCount": 48,
                "StatusCodes": {
                    "Status3xx": 0,
                    "Status2xx": 47,
                    "Status5xx": 0,
                    "Status4xx": 1
                }
            },
            "System": {
                "LoadAverage": [
                    0.0,
                    0.02,
                    0.05
                ],
                "CPUUtilization": {
```

```
                    "SoftIRQ": 0.1,
                    "IOWait": 0.2,
                    "System": 0.3,
                    "Idle": 97.8,
                    "User": 1.5,
                    "IRQ": 0.0,
                    "Nice": 0.1
                }
            },
            "Color": "Green",
            "HealthStatus": "Ok",
            "LaunchedAt": "2015-08-13T19:17:09Z",
            "Causes": []
        }
    ],
    "RefreshedAt": "2015-08-20T21:09:08Z"
}
```

La información de estado solo está disponible para los entornos en los que se han habilitado los informes de estado mejorados. Para obtener más información, consulte Enhanced Health Reporting and Monitoring en la Guía para desarrolladores de AWS Elastic Beanstalk.

- Para obtener información sobre la API, consulte DescribeInstancesHealth en la Referencia de comandos de la AWS CLI.

`list-available-solution-stacks`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-available-solution-stacks`.

AWS CLI

Para ver las pilas de soluciones

En el siguiente comando, se muestran los conjuntos de soluciones para todas las configuraciones de plataforma disponibles actualmente y para todas las que haya utilizado en el pasado:

```
aws elasticbeanstalk list-available-solution-stacks
```

Salida (abreviada):

```
{
    "SolutionStacks": [
```

```
        "64bit Amazon Linux 2015.03 v2.0.0 running Node.js",
        "64bit Amazon Linux 2015.03 v2.0.0 running PHP 5.6",
        "64bit Amazon Linux 2015.03 v2.0.0 running PHP 5.5",
        "64bit Amazon Linux 2015.03 v2.0.0 running PHP 5.4",
        "64bit Amazon Linux 2015.03 v2.0.0 running Python 3.4",
        "64bit Amazon Linux 2015.03 v2.0.0 running Python 2.7",
        "64bit Amazon Linux 2015.03 v2.0.0 running Python",
        "64bit Amazon Linux 2015.03 v2.0.0 running Ruby 2.2 (Puma)",
        "64bit Amazon Linux 2015.03 v2.0.0 running Ruby 2.2 (Passenger Standalone)",
        "64bit Amazon Linux 2015.03 v2.0.0 running Ruby 2.1 (Puma)",
        "64bit Amazon Linux 2015.03 v2.0.0 running Ruby 2.1 (Passenger Standalone)",
        "64bit Amazon Linux 2015.03 v2.0.0 running Ruby 2.0 (Puma)",
        "64bit Amazon Linux 2015.03 v2.0.0 running Ruby 2.0 (Passenger Standalone)",
        "64bit Amazon Linux 2015.03 v2.0.0 running Ruby 1.9.3",
        "64bit Amazon Linux 2015.03 v2.0.0 running Tomcat 8 Java 8",
        "64bit Amazon Linux 2015.03 v2.0.0 running Tomcat 7 Java 7",
        "64bit Amazon Linux 2015.03 v2.0.0 running Tomcat 7 Java 6",
        "64bit Windows Server Core 2012 R2 running IIS 8.5",
        "64bit Windows Server 2012 R2 running IIS 8.5",
        "64bit Windows Server 2012 running IIS 8",
        "64bit Windows Server 2008 R2 running IIS 7.5",
        "64bit Amazon Linux 2015.03 v2.0.0 running Docker 1.6.2",
        "64bit Amazon Linux 2015.03 v2.0.0 running Multi-container Docker 1.6.2
 (Generic)",
        "64bit Debian jessie v2.0.0 running GlassFish 4.1 Java 8 (Preconfigured -
 Docker)",
        "64bit Debian jessie v2.0.0 running GlassFish 4.0 Java 7 (Preconfigured -
 Docker)",
        "64bit Debian jessie v2.0.0 running Go 1.4 (Preconfigured - Docker)",
        "64bit Debian jessie v2.0.0 running Go 1.3 (Preconfigured - Docker)",
        "64bit Debian jessie v2.0.0 running Python 3.4 (Preconfigured - Docker)",
    ],
    "SolutionStackDetails": [
        {
            "PermittedFileTypes": [
                "zip"
            ],
            "SolutionStackName": "64bit Amazon Linux 2015.03 v2.0.0 running Node.js"
        },
        ...
    ]
}
```

- Para obtener información sobre la API, consulte ListAvailableSolutionStacks en la Referencia de comandos de la AWS CLI.

`rebuild-environment`

En el siguiente ejemplo de código, se muestra cómo utilizar `rebuild-environment`.

AWS CLI

Para volver a crear un entorno

En el siguiente comando, se terminan y se vuelven a crear los recursos de un entorno denominado `my-env`:

```
aws elasticbeanstalk rebuild-environment --environment-name my-env
```

- Para obtener información sobre la API, consulte RebuildEnvironment en la Referencia de comandos de la AWS CLI.

`request-environment-info`

En el siguiente ejemplo de código, se muestra cómo utilizar `request-environment-info`.

AWS CLI

Para solicitar registros guardados

En el siguiente comando, se solicitan registros de un entorno denominado `my-env`:

```
aws elasticbeanstalk request-environment-info --environment-name my-env --info-
type tail
```

Después de solicitar los registros, recupere su ubicación mediante retrieve-environment-info.

- Para obtener información sobre la API, consulte RequestEnvironmentInfo en la Referencia de comandos de la AWS CLI.

`restart-app-server`

En el siguiente ejemplo de código, se muestra cómo utilizar `restart-app-server`.

AWS CLI

Para reiniciar los servidores de aplicaciones

El siguiente comando reinicia los servidores de aplicaciones en todas las instancias de un entorno denominado `my-env`:

```
aws elasticbeanstalk restart-app-server --environment-name my-env
```

- Para obtener información sobre la API, consulte RestartAppServer en la Referencia de comandos de la AWS CLI.

`retrieve-environment-info`

En el siguiente ejemplo de código, se muestra cómo utilizar `retrieve-environment-info`.

AWS CLI

Para recuperar los registros guardados

En el siguiente comando, se recupera un enlace a los registros de un entorno denominado `my-env`:

```
aws elasticbeanstalk retrieve-environment-info --environment-name my-env --info-type tail
```

Salida:

```
{
    "EnvironmentInfo": [
        {
            "SampleTimestamp": "2015-08-20T22:23:17.703Z",
            "Message": "https://elasticbeanstalk-us-
west-2-0123456789012.s3.amazonaws.com/resources/environments/
logs/tail/e-fyqyju3yjs/i-09c1c867/TailLogs-1440109397703.out?
AWSAccessKeyId=AKGPT4J56IAJ2EUBL5CQ&Expires=1440195891&Signature=n
%2BEalOV6A2HIOx4Rcfb7LT16bBM%3D",
            "InfoType": "tail",
            "Ec2InstanceId": "i-09c1c867"
        }
    ]
```

```
}
```

Vea el enlace en un navegador. Antes de la recuperación, deben solicitarse los registros mediante request-environment-info.

- Para obtener información sobre la API, consulte RetrieveEnvironmentInfo en la Referencia de comandos de la AWS CLI.

`swap-environment-cnames`

En el siguiente ejemplo de código, se muestra cómo utilizar `swap-environment-cnames`.

AWS CLI

Para intercambiar registros CNAME del entorno

En el siguiente comando, se intercambian los subdominios asignados de dos entornos:

```
aws elasticbeanstalk swap-environment-cnames --source-environment-name my-env-blue
 --destination-environment-name my-env-green
```

- Para obtener información sobre la API, consulte SwapEnvironmentCnames en la Referencia de comandos de la AWS CLI.

`terminate-environment`

En el siguiente ejemplo de código, se muestra cómo utilizar `terminate-environment`.

AWS CLI

Para terminar un entorno

En el siguiente comando, se termina un entorno de Elastic Beanstalk denominado `my-env`:

```
aws elasticbeanstalk terminate-environment --environment-name my-env
```

Salida:

```
{
    "ApplicationName": "my-app",
    "EnvironmentName": "my-env",
```

```
    "Status": "Terminating",
    "EnvironmentId": "e-fh2eravpns",
    "EndpointURL": "awseb-e-f-AWSEBLoa-1I9XUMP4-8492WNUP202574.us-
west-2.elb.amazonaws.com",
    "SolutionStackName": "64bit Amazon Linux 2015.03 v2.0.0 running Tomcat 8 Java
 8",
    "CNAME": "my-env.elasticbeanstalk.com",
    "Health": "Grey",
    "AbortableOperationInProgress": false,
    "Tier": {
        "Version": " ",
        "Type": "Standard",
        "Name": "WebServer"
    },
    "DateUpdated": "2015-08-12T19:05:54.744Z",
    "DateCreated": "2015-08-12T18:52:53.622Z"
}
```

- Para obtener información sobre la API, consulte TerminateEnvironment en la Referencia de comandos de la AWS CLI.

`update-application-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-application-version`.

AWS CLI

Para cambiar la descripción de la versión de una aplicación

En el siguiente comando, se actualiza la descripción de una versión de la aplicación denominada `22a0-stage-150819_185942`:

```
aws elasticbeanstalk update-application-version --version-label 22a0-
stage-150819_185942 --application-name my-app --description "new description"
```

Salida:

```
{
    "ApplicationVersion": {
        "ApplicationName": "my-app",
        "VersionLabel": "22a0-stage-150819_185942",
        "Description": "new description",
```

```
        "DateCreated": "2015-08-19T18:59:17.646Z",
        "DateUpdated": "2015-08-20T22:53:28.871Z",
        "SourceBundle": {
            "S3Bucket": "elasticbeanstalk-us-west-2-0123456789012",
            "S3Key": "my-app/22a0-stage-150819_185942.war"
        }
    }
}
```

- Para obtener información sobre la API, consulte UpdateApplicationVersion en la Referencia de comandos de la AWS CLI.

`update-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-application`.

AWS CLI

Para cambiar la descripción de una aplicación

En el siguiente comando, se actualiza la descripción de una aplicación denominada `my-app`:

```
aws elasticbeanstalk update-application --application-name my-app --description "my
 Elastic Beanstalk application"
```

Salida:

```
{
    "Application": {
        "ApplicationName": "my-app",
        "Description": "my Elastic Beanstalk application",
        "Versions": [
            "2fba-stage-150819_234450",
            "bf07-stage-150820_214945",
            "93f8",
            "fd7c-stage-150820_000431",
            "22a0-stage-150819_185942"
        ],
        "DateCreated": "2015-08-13T19:15:50.449Z",
        "ConfigurationTemplates": [],
        "DateUpdated": "2015-08-20T22:34:56.195Z"
    }
```

```
}
```

- Para obtener información sobre la API, consulte UpdateApplication en la Referencia de comandos de la AWS CLI.

`update-configuration-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-configuration-template`.

AWS CLI

Para actualizar una plantilla de configuración

En el siguiente comando, se elimina la configuración de métricas de estado personalizadas de CloudWatch configurada `ConfigDocument` de una plantilla de configuración guardada denominada `my-template`:

```
aws elasticbeanstalk update-configuration-template --template-
name my-template --application-name my-app --options-to-
remove Namespace=aws:elasticbeanstalk:healthreporting:system,OptionName=ConfigDocument
```

Salida:

```
{
    "ApplicationName": "my-app",
    "TemplateName": "my-template",
    "DateCreated": "2015-08-20T22:39:31Z",
    "DateUpdated": "2015-08-20T22:43:11Z",
    "SolutionStackName": "64bit Amazon Linux 2015.03 v2.0.0 running Tomcat 8 Java 8"
}
```

Para obtener más información sobre los espacios de nombres y las opciones admitidas, consulte Option Values en la Guía para desarrolladores de AWS Elastic Beanstalk.

- Para obtener información sobre la API, consulte UpdateConfigurationTemplate en la Referencia de comandos de la AWS CLI.

`update-environment`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-environment`.

AWS CLI

Para actualizar un entorno a una nueva versión

En el siguiente comando, se actualiza un entorno denominado my-env a la versión v2 de la aplicación a la que pertenece:

```
aws elasticbeanstalk update-environment --environment-name my-env --version-label v2
```

Para este comando, se requiere que el entorno my-env ya exista y pertenezca a una aplicación que tenga una versión de aplicación válida con la etiqueta v2.

Salida:

```
{
  "ApplicationName": "my-app",
  "EnvironmentName": "my-env",
  "VersionLabel": "v2",
  "Status": "Updating",
  "EnvironmentId": "e-szqipays4h",
  "EndpointURL": "awseb-e-i-AWSEBLoa-1RDLX6TC9VUAO-0123456789.us-
west-2.elb.amazonaws.com",
  "SolutionStackName": "64bit Amazon Linux running Tomcat 7",
  "CNAME": "my-env.elasticbeanstalk.com",
  "Health": "Grey",
  "Tier": {
      "Version": " ",
      "Type": "Standard",
      "Name": "WebServer"
  },
  "DateUpdated": "2015-02-03T23:12:29.119Z",
  "DateCreated": "2015-02-03T23:04:54.453Z"
}
```

Para establecer una variable de entorno

En el siguiente comando, se establece en ParamValue el valor de la variable PARAM1 del entorno my-env:

```
aws elasticbeanstalk update-environment --environment-name my-env --option-
settings Namespace=aws:elasticbeanstalk:application:environment,OptionName=PARAM1,Value=Para
```

El parámetro `option-settings` toma un espacio de nombres además del nombre y el valor de la variable. Elastic Beanstalk admite varios espacios de nombres para las opciones, además de las variables de entorno.

Para configurar valores de opciones a partir de un archivo

En el siguiente comando, se configuran varias opciones en el espacio de nombres `aws:elb:loadbalancer` a partir de un archivo:

```
aws elasticbeanstalk update-environment --environment-name my-env --option-
settings file://options.json
```

`options.json` es un objeto de JSON que define varios ajustes:

```
[
  {
    "Namespace": "aws:elb:healthcheck",
    "OptionName": "Interval",
    "Value": "15"
  },
  {
    "Namespace": "aws:elb:healthcheck",
    "OptionName": "Timeout",
    "Value": "8"
  },
  {
    "Namespace": "aws:elb:healthcheck",
    "OptionName": "HealthyThreshold",
    "Value": "2"
  },
  {
    "Namespace": "aws:elb:healthcheck",
    "OptionName": "UnhealthyThreshold",
    "Value": "3"
  }
]
```

Salida:

```
{
    "ApplicationName": "my-app",
    "EnvironmentName": "my-env",
```

```
    "VersionLabel": "7f58-stage-150812_025409",
    "Status": "Updating",
    "EnvironmentId": "e-wtp2rpqsej",
    "EndpointURL": "awseb-e-w-AWSEBLoa-14XB83101Q4L-104QXY80921.sa-
east-1.elb.amazonaws.com",
    "SolutionStackName": "64bit Amazon Linux 2015.03 v2.0.0 running Tomcat 8 Java
 8",
    "CNAME": "my-env.elasticbeanstalk.com",
    "Health": "Grey",
    "AbortableOperationInProgress": true,
    "Tier": {
        "Version": " ",
        "Type": "Standard",
        "Name": "WebServer"
    },
    "DateUpdated": "2015-08-12T18:15:23.804Z",
    "DateCreated": "2015-08-07T20:48:49.599Z"
}
```

Para obtener más información sobre los espacios de nombres y las opciones admitidas, consulte Option Values en la Guía para desarrolladores de AWS Elastic Beanstalk.

- Para obtener información sobre la API, consulte UpdateEnvironment en la Referencia de comandos de la AWS CLI.

`validate-configuration-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `validate-configuration-settings`.

AWS CLI

Para validar los ajustes de configuración

En el siguiente comando, se valida un documento de configuración de métricas personalizadas de CloudWatch:

```
aws elasticbeanstalk validate-configuration-settings --application-name my-app --
environment-name my-env --option-settings file://options.json
```

`options.json` es un documento de JSON que contiene uno o varios ajustes de configuración que validar:

```
[
    {
        "Namespace": "aws:elasticbeanstalk:healthreporting:system",
        "OptionName": "ConfigDocument",
        "Value": "{\"CloudWatchMetrics\": {\"Environment\":
 {\"ApplicationLatencyP99.9\": null,\"InstancesSevere\": 60,
\"ApplicationLatencyP90\": 60,\"ApplicationLatencyP99\": null,
\"ApplicationLatencyP95\": 60,\"InstancesUnknown\": 60,\"ApplicationLatencyP85\":
 60,\"InstancesInfo\": null,\"ApplicationRequests2xx\": null,\"InstancesDegraded
\": null,\"InstancesWarning\": 60,\"ApplicationLatencyP50\": 60,
\"ApplicationRequestsTotal\": null,\"InstancesNoData\": null,\"InstancesPending
\": 60,\"ApplicationLatencyP10\": null,\"ApplicationRequests5xx\": null,
\"ApplicationLatencyP75\": null,\"InstancesOk\": 60,\"ApplicationRequests3xx\":
 null,\"ApplicationRequests4xx\": null},\"Instance\": {\"ApplicationLatencyP99.9\":
 null,\"ApplicationLatencyP90\": 60,\"ApplicationLatencyP99\": null,
\"ApplicationLatencyP95\": null,\"ApplicationLatencyP85\": null,\"CPUUser\": 60,
\"ApplicationRequests2xx\": null,\"CPUIdle\": null,\"ApplicationLatencyP50\":
 null,\"ApplicationRequestsTotal\": 60,\"RootFilesystemUtil\": null,
\"LoadAverage1min\": null,\"CPUIrq\": null,\"CPUNice\": 60,\"CPUIowait\": 60,
\"ApplicationLatencyP10\": null,\"LoadAverage5min\": null,\"ApplicationRequests5xx
\": null,\"ApplicationLatencyP75\": 60,\"CPUSystem\": 60,\"ApplicationRequests3xx\":
 60,\"ApplicationRequests4xx\": null,\"InstanceHealth\": null,\"CPUSoftirq\": 60}},
\"Version\": 1}"
    }
]
```

Si las opciones que especifica son válidas para el entorno especificado, Elastic Beanstalk devuelve una matriz Messages vacía:

```
{
    "Messages": []
}
```

Si la validación genera un error, la respuesta incluirá información sobre el error:

```
{
    "Messages": [
        {
            "OptionName": "ConfigDocumet",
            "Message": "Invalid option specification (Namespace:
 'aws:elasticbeanstalk:healthreporting:system', OptionName: 'ConfigDocumet'):
 Unknown configuration setting.",
```

```
            "Namespace": "aws:elasticbeanstalk:healthreporting:system",
            "Severity": "error"
        }
    ]
}
```

Para obtener más información sobre los espacios de nombres y las opciones admitidas, consulte Option Values en la Guía para desarrolladores de AWS Elastic Beanstalk.

- Para obtener información sobre la API, consulte ValidateConfigurationSettings en la Referencia de comandos de la AWS CLI.

ELB: ejemplos de la versión 1 mediante AWS CLI

Los ejemplos de código siguientes muestran cómo realizar acciones e implementar escenarios comunes mediante AWS Command Line Interface con ELB: versión 1.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-tags`.

AWS CLI

Para agregar una etiqueta a un equilibrador de carga

En este ejemplo, se agregan etiquetas al equilibrador de carga especificado.

Comando:

```
aws elb add-tags --load-balancer-name my-load-balancer --
tags "Key=project,Value=lima" "Key=department,Value=digital-media"
```

- Para obtener información sobre la API, consulte AddTags en la Referencia de comandos de la AWS CLI.

`apply-security-groups-to-load-balancer`

En el siguiente ejemplo de código, se muestra cómo utilizar `apply-security-groups-to-load-balancer`.

AWS CLI

Para asociar un grupo de seguridad a un equilibrador de carga en una nube privada virtual

En este ejemplo, se asocia un grupo de seguridad al equilibrador de carga especificado en una nube privada virtual (VPC).

Comando:

```
aws elb apply-security-groups-to-load-balancer --load-balancer-name my-load-balancer
 --security-groups sg-fc448899
```

Salida:

```
{
  "SecurityGroups": [
      "sg-fc448899"
  ]
}
```

- Para obtener información sobre la API, consulte ApplySecurityGroupsToLoadBalancer en la Referencia de comandos de la AWS CLI.

`attach-load-balancer-to-subnets`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-load-balancer-to-subnets`.

AWS CLI

Para asociar subredes a un equilibrador de carga

En este ejemplo, se agrega la subred especificada al conjunto de subredes configuradas para el equilibrador de carga especificado.

Comando:

```
aws elb attach-load-balancer-to-subnets --load-balancer-name my-load-balancer --
subnets subnet-0ecac448
```

Salida:

```
{
   "Subnets": [
       "subnet-15aaab61",
       "subnet-0ecac448"
   ]
}
```

- Para obtener información sobre la API, consulte AttachLoadBalancerToSubnets en la Referencia de comandos de la AWS CLI.

`configure-health-check`

En el siguiente ejemplo de código, se muestra cómo utilizar `configure-health-check`.

AWS CLI

Para especificar la configuración de comprobación de estado de las instancias de EC2 del backend

En este ejemplo, se especifica la configuración de la comprobación de estado que se utiliza para evaluar el estado de las instancias de EC2 del backend.

Comando:

```
aws elb configure-health-check --load-balancer-name my-load-balancer --health-
check Target=HTTP:80/
png,Interval=30,UnhealthyThreshold=2,HealthyThreshold=2,Timeout=3
```

Salida:

```
{
   "HealthCheck": {
       "HealthyThreshold": 2,
       "Interval": 30,
       "Target": "HTTP:80/png",
       "Timeout": 3,
       "UnhealthyThreshold": 2
   }
}
```

- Para obtener información sobre la API, consulte ConfigureHealthCheck en la Referencia de comandos de la AWS CLI.

`create-app-cookie-stickiness-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-app-cookie-stickiness-policy`.

AWS CLI

Para generar una política de persistencia para el equilibrador de carga de HTTPS

En este ejemplo, se genera una política de persistencia que sigue las vidas útiles de las sesiones persistentes de las cookies generadas por una aplicación.

Comando:

```
aws elb create-app-cookie-stickiness-policy --load-balancer-name my-load-balancer --policy-name my-app-cookie-policy --cookie-name my-app-cookie
```

- Para obtener información sobre la API, consulte CreateAppCookieStickinessPolicy en la Referencia de comandos de la AWS CLI.

`create-lb-cookie-stickiness-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-lb-cookie-stickiness-policy`.

AWS CLI

Para generar una política de persistencia basada en duración para el equilibrador de carga de HTTPS

En este ejemplo, se genera una política de persistencia en la que las vidas útiles de las sesiones persistentes se controlan en función del período de vencimiento especificado.

Comando:

```
aws elb create-lb-cookie-stickiness-policy --load-balancer-name my-load-balancer --
policy-name my-duration-cookie-policy --cookie-expiration-period 60
```

- Para obtener información sobre la API, consulte CreateLbCookieStickinessPolicy en la Referencia de comandos de la AWS CLI.

`create-load-balancer-listeners`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-load-balancer-listeners`.

AWS CLI

Para crear oyentes de HTTP para un equilibrador de carga

En este ejemplo, se crea un oyente para el equilibrador de carga en el puerto 80 mediante el protocolo HTTP.

Comando:

```
aws elb create-load-balancer-listeners --load-balancer-name my-load-balancer --
listeners "Protocol=HTTP,LoadBalancerPort=80,InstanceProtocol=HTTP,InstancePort=80"
```

Para crear oyentes de HTTPS para un equilibrador de carga

En este ejemplo, se crea un oyente para el equilibrador de carga en el puerto 443 mediante el protocolo HTTPS.

Comando:

```
aws elb create-load-balancer-listeners --load-balancer-name my-load-balancer --
listeners "Protocol=HTTPS,LoadBalancerPort=443,InstanceProtocol=HTTP,InstancePort=80"
```

- Para obtener información sobre la API, consulte CreateLoadBalancerListeners en la Referencia de comandos de la AWS CLI.

`create-load-balancer-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-load-balancer-policy`.

AWS CLI

Para crear una política que habilita Proxy Protocol en un equilibrador de carga

En este ejemplo, se crea una política que habilita Proxy Protocol en un equilibrador de carga.

Comando:

```
aws elb create-load-balancer-policy --load-balancer-name my-load-balancer --policy-name my-ProxyProtocol-policy --policy-type-name ProxyProtocolPolicyType --policy-attributes AttributeName=ProxyProtocol,AttributeValue=true
```

Para crear una política de negociación de SSL con la política de seguridad recomendada

En este ejemplo, se crea una política de negociación de SSL para el equilibrador de carga de HTTPS especificado con la política de seguridad recomendada.

Comando:

```
aws elb create-load-balancer-policy --load-balancer-name my-load-balancer --policy-name my-SSLNegotiation-policy --policy-type-name SSLNegotiationPolicyType --policy-attributes AttributeName=Reference-Security-Policy,AttributeValue=ELBSecurityPolicy-2015-03
```

Para crear una política de negociación de SSL con una política de seguridad personalizada

En este ejemplo, se crea una política de negociación de SSL para el equilibrador de carga de HTTPS con una política de seguridad personalizada en la que se habilitan los protocolos y los cifrados.

Comando:

```
aws elb create-load-balancer-policy --load-balancer-name my-load-balancer --policy-name my-SSLNegotiation-policy --policy-type-name SSLNegotiationPolicyType --policy-
```

```
attributes AttributeName=Protocol-SSLv3,AttributeValue=true AttributeName=Protocol-
TLSv1.1,AttributeValue=true AttributeName=DHE-RSA-AES256-
SHA256,AttributeValue=true AttributeName=Server-Defined-Cipher-
Order,AttributeValue=true
```

Para crear una política de claves públicas

En este ejemplo, se crea una política de claves públicas.

Comando:

```
aws elb create-load-balancer-policy --load-balancer-name my-load-balancer --
policy-name my-PublicKey-policy --policy-type-name PublicKeyPolicyType --policy-
attributes AttributeName=PublicKey,AttributeValue=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQ
+dS74kj//c6x7ROtusUaeQCTgIUkayttRDWchuqo1pHC1u
+n5xxXnBBe2ejbb2WRsKIQ5rXEeixsjFpFsojpSQKkzhVGI6mJVZBJDVKSHmswnwLBdofLhzvllpovBPTHe
+o4haAWvDBALJU0pkSI1FecPHcs2hwxf14zHoXy1e2k36A64nXW43wtfx5qcVSIxtCEOjnYRg7RPvybaGfQ
+v6Iaxb/+7J5kEvZhTFQId+bSiJImF1FSUT1W1xwzBZPUbcUkkXDj45vC2s3Z8E
+Lk7a3uZhvsQHLZnrfuWjBWGWvZ/MhZYgEXAMPLE
```

Para crear una política de autenticación de servidor de backend

En este ejemplo, se crea una política de autenticación de servidor de backend que habilita la autenticación en la instancia de backend mediante una política de claves públicas.

Comando:

```
aws elb create-load-balancer-policy --load-balancer-name my-
load-balancer --policy-name my-authentication-policy --policy-
type-name BackendServerAuthenticationPolicyType --policy-
attributes AttributeName=PublicKeyPolicyName,AttributeValue=my-PublicKey-policy
```

- Para obtener información sobre la API, consulte CreateLoadBalancerPolicy en la Referencia de comandos de la AWS CLI.

`create-load-balancer`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-load-balancer`.

AWS CLI

Para crear un equilibrador de carga de HTTP

En este ejemplo, se crea un equilibrador de carga con un oyente de HTTP en una nube privada virtual.

Comando:

```
aws elb create-load-balancer --load-balancer-name my-load-balancer --
listeners "Protocol=HTTP,LoadBalancerPort=80,InstanceProtocol=HTTP,InstancePort=80"
 --subnets subnet-15aaab61 --security-groups sg-a61988c3
```

Salida:

```
{
    "DNSName": "my-load-balancer-1234567890.us-west-2.elb.amazonaws.com"
}
```

En este ejemplo, se crea un equilibrador de carga con un oyente de HTTP en EC2-Classic.

Comando:

```
aws elb create-load-balancer --load-balancer-name my-load-balancer --
listeners "Protocol=HTTP,LoadBalancerPort=80,InstanceProtocol=HTTP,InstancePort=80"
 --availability-zones us-west-2a us-west-2b
```

Salida:

```
{
    "DNSName": "my-load-balancer-123456789.us-west-2.elb.amazonaws.com"
}
```

Para crear un equilibrador de carga de HTTPS

En este ejemplo, se crea un equilibrador de carga con un oyente de HTTPS en una nube privada virtual.

Comando:

```
aws elb create-load-balancer --load-balancer-name my-load-balancer --
listeners "Protocol=HTTP,LoadBalancerPort=80,InstanceProtocol=HTTP,InstancePort=80" "Protoco
certificate/my-server-cert" --subnets subnet-15aaab61 --security-groups sg-a61988c3
```

Salida:

```
{
    "DNSName": "my-load-balancer-1234567890.us-west-2.elb.amazonaws.com"
}
```

En este ejemplo, se crea un equilibrador de carga con un oyente de HTTPS en EC2-Classic.

Comando:

```
aws elb create-load-balancer --load-balancer-name my-load-balancer --
listeners "Protocol=HTTP,LoadBalancerPort=80,InstanceProtocol=HTTP,InstancePort=80" "Protoco
certificate/my-server-cert" --availability-zones us-west-2a us-west-2b
```

Salida:

```
{
    "DNSName": "my-load-balancer-123456789.us-west-2.elb.amazonaws.com"
}
```

Para crear un equilibrador de carga interno

En este ejemplo, se crea un equilibrador de carga con un oyente de HTTP en una nube privada virtual.

Comando:

```
aws elb create-load-balancer --load-balancer-name my-load-balancer --
listeners "Protocol=HTTP,LoadBalancerPort=80,InstanceProtocol=HTTP,InstancePort=80"
 --scheme internal --subnets subnet-a85db0df --security-groups sg-a61988c3
```

Salida:

```
{
    "DNSName": "internal-my-load-balancer-123456789.us-west-2.elb.amazonaws.com"
}
```

- Para obtener información sobre la API, consulte CreateLoadBalancer en la Referencia de comandos de la AWS CLI.

`delete-load-balancer-listeners`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-load-balancer-listeners`.

AWS CLI

Para eliminar un oyente del equilibrador de carga

En este ejemplo, se elimina el oyente del puerto especificado del equilibrador de carga especificado.

Comando:

```
aws elb delete-load-balancer-listeners --load-balancer-name my-load-balancer --load-balancer-ports 80
```

- Para obtener información sobre la API, consulte DeleteLoadBalancerListeners en la Referencia de comandos de la AWS CLI.

`delete-load-balancer-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-load-balancer-policy`.

AWS CLI

Para eliminar una política del equilibrador de carga

En este ejemplo, se elimina la política especificada del equilibrador de carga especificado. La política no debe estar habilitada en ningún oyente.

Comando:

```
aws elb delete-load-balancer-policy --load-balancer-name my-load-balancer --policy-name my-duration-cookie-policy
```

- Para obtener información sobre la API, consulte DeleteLoadBalancerPolicy en la Referencia de comandos de la AWS CLI.

`delete-load-balancer`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-load-balancer`.

AWS CLI

Eliminación de un equilibrador de carga

En este ejemplo, se elimina el equilibrador de carga especificado.

Comando:

```
aws elb delete-load-balancer --load-balancer-name my-load-balancer
```

- Para obtener información sobre la API, consulte DeleteLoadBalancer en la Referencia de comandos de la AWS CLI.

`deregister-instances-from-load-balancer`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-instances-from-load-balancer`.

AWS CLI

Para anular el registro de instancias de un equilibrador de carga

En este ejemplo, se anula el registro de la instancia especificada en el equilibrador de carga especificado.

Comando:

```
aws elb deregister-instances-from-load-balancer --load-balancer-name my-load-balancer --instances i-d6f6fae3
```

Salida:

```
{
    "Instances": [
        {
            "InstanceId": "i-207d9717"
        },
        {
            "InstanceId": "i-afefb49b"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DeregisterInstancesFromLoadBalancer en la Referencia de comandos de la AWS CLI.

`describe-account-limits`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-account-limits`.

AWS CLI

Para describir los límites del equilibrador de carga clásico

En el siguiente ejemplo de `describe-account-limits`, se muestran los detalles de los límites del equilibrador de carga clásico de la cuenta de AWS.

```
aws elb describe-account-limits
```

Salida:

```
{
    "Limits": [
        {
            "Name": "classic-load-balancers",
            "Max": "20"
        },
        {
            "Name": "classic-listeners",
            "Max": "100"
        },
        {
            "Name": "classic-registered-instances",
            "Max": "1000"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeAccountLimits en la Referencia de comandos de la AWS CLI.

`describe-instance-health`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-health`.

AWS CLI

Para describir el estado de las instancias de un equilibrador de carga

En este ejemplo, se describe el estado de las instancias del equilibrador de carga especificado.

Comando:

```
aws elb describe-instance-health --load-balancer-name my-load-balancer
```

Salida:

```
{
  "InstanceStates": [
      {
          "InstanceId": "i-207d9717",
          "ReasonCode": "N/A",
          "State": "InService",
          "Description": "N/A"
      },
      {
          "InstanceId": "i-afefb49b",
          "ReasonCode": "N/A",
          "State": "InService",
          "Description": "N/A"
      }
  ]
}
```

Para describir el estado de una instancia de un equilibrador de carga

En este ejemplo, se describe el estado de la instancia especificada del equilibrador de carga especificado.

Comando:

```
aws elb describe-instance-health --load-balancer-name my-load-balancer --
instances i-7299c809
```

A continuación, se muestra un ejemplo de respuesta para una instancia que se está registrando.

Salida:

```
{
  "InstanceStates": [
      {
          "InstanceId": "i-7299c809",
```

```
            "ReasonCode": "ELB",
            "State": "OutOfService",
            "Description": "Instance registration is still in progress."
        }
    ]
}
```

A continuación, se muestra un ejemplo de respuesta para una instancia en mal estado.

Salida:

```
{
    "InstanceStates": [
        {
            "InstanceId": "i-7299c809",
            "ReasonCode": "Instance",
            "State": "OutOfService",
            "Description": "Instance has failed at least the UnhealthyThreshold number
 of health checks consecutively."
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeInstanceHealth en la Referencia de comandos de la AWS CLI.

`describe-load-balancer-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-load-balancer-attributes`.

AWS CLI

Para describir los atributos de un equilibrador de carga

En este ejemplo, se describen los atributos del equilibrador de carga especificado.

Comando:

```
aws elb describe-load-balancer-attributes --load-balancer-name my-load-balancer
```

Salida:

```
{
  "LoadBalancerAttributes": {
      "ConnectionDraining": {
          "Enabled": false,
          "Timeout": 300
      },
      "CrossZoneLoadBalancing": {
          "Enabled": true
      },
      "ConnectionSettings": {
          "IdleTimeout": 30
      },
      "AccessLog": {
          "Enabled": false
    }
  }
}
```

- Para obtener información sobre la API, consulte DescribeLoadBalancerAttributes en la Referencia de comandos de la AWS CLI.

`describe-load-balancer-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-load-balancer-policies`.

AWS CLI

Para describir todas las políticas asociadas a un equilibrador de carga

En este ejemplo, se describen todas las políticas asociadas al equilibrador de carga especificado.

Comando:

```
aws elb describe-load-balancer-policies --load-balancer-name my-load-balancer
```

Salida:

```
{
  "PolicyDescriptions": [
    {
      "PolicyAttributeDescriptions": [
```

```
        {
          "AttributeName": "ProxyProtocol",
          "AttributeValue": "true"
        }
      ],
      "PolicyName": "my-ProxyProtocol-policy",
      "PolicyTypeName": "ProxyProtocolPolicyType"
    },
    {
        "PolicyAttributeDescriptions": [
            {
                "AttributeName": "CookieName",
                "AttributeValue": "my-app-cookie"
            }
        ],
        "PolicyName": "my-app-cookie-policy",
        "PolicyTypeName": "AppCookieStickinessPolicyType"
    },
    {
      "PolicyAttributeDescriptions": [
        {
          "AttributeName": "CookieExpirationPeriod",
          "AttributeValue": "60"
        }
      ],
      "PolicyName": "my-duration-cookie-policy",
      "PolicyTypeName": "LBCookieStickinessPolicyType"
    },
    .
    .
    .
  ]
}
```

Para describir una política concreta asociada a un equilibrador de carga

En este ejemplo, se describe la política especificada que está asociada al equilibrador de carga especificado.

Comando:

```
aws elb describe-load-balancer-policies --load-balancer-name my-load-balancer --
policy-name my-authentication-policy
```

Salida:

```
{
  "PolicyDescriptions": [
      {
          "PolicyAttributeDescriptions": [
              {
                  "AttributeName": "PublicKeyPolicyName",
                  "AttributeValue": "my-PublicKey-policy"
              }
          ],
          "PolicyName": "my-authentication-policy",
          "PolicyTypeName": "BackendServerAuthenticationPolicyType"
      }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeLoadBalancerPolicies en la Referencia de comandos de la AWS CLI.

`describe-load-balancer-policy-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-load-balancer-policy-types`.

AWS CLI

Para describir los tipos de políticas del equilibrador de carga definidos por Elastic Load Balancing

En este ejemplo, se describen los tipos de políticas del equilibrador de carga que se pueden usar para crear configuraciones de políticas para el equilibrador de carga.

Comando:

```
aws elb describe-load-balancer-policy-types
```

Salida:

```
{
  "PolicyTypeDescriptions": [
      {
          "PolicyAttributeTypeDescriptions": [
```

```
            {
                "Cardinality": "ONE",
                "AttributeName": "ProxyProtocol",
                "AttributeType": "Boolean"
            }
        ],
        "PolicyTypeName": "ProxyProtocolPolicyType",
        "Description": "Policy that controls whether to include the IP address and
port of the originating request for TCP messages. This policy operates on TCP/SSL
listeners only"
    },
    {
        "PolicyAttributeTypeDescriptions": [
            {
                "Cardinality": "ONE",
                "AttributeName": "PublicKey",
                "AttributeType": "String"
            }
        ],
        "PolicyTypeName": "PublicKeyPolicyType",
        "Description": "Policy containing a list of public keys to
accept when authenticating the back-end server(s). This policy cannot be
applied directly to back-end servers or listeners but must be part of a
BackendServerAuthenticationPolicyType."
    },
    {
        "PolicyAttributeTypeDescriptions": [
            {
                "Cardinality": "ONE",
                "AttributeName": "CookieName",
                "AttributeType": "String"
            }
        ],
        "PolicyTypeName": "AppCookieStickinessPolicyType",
        "Description": "Stickiness policy with session lifetimes controlled by the
lifetime of the application-generated cookie. This policy can be associated only
with HTTP/HTTPS listeners."
    },
    {
        "PolicyAttributeTypeDescriptions": [
            {
                "Cardinality": "ZERO_OR_ONE",
                "AttributeName": "CookieExpirationPeriod",
                "AttributeType": "Long"
```

```
            }
        ],
        "PolicyTypeName": "LBCookieStickinessPolicyType",
        "Description": "Stickiness policy with session lifetimes controlled by
 the browser (user-agent) or a specified expiration period. This policy can be
 associated only with HTTP/HTTPS listeners."
    },
    {
        "PolicyAttributeTypeDescriptions": [
            .
            .
            .
        ],
        "PolicyTypeName": "SSLNegotiationPolicyType",
        "Description": "Listener policy that defines the ciphers and protocols
 that will be accepted by the load balancer. This policy can be associated only with
 HTTPS/SSL listeners."
    },
    {
        "PolicyAttributeTypeDescriptions": [
            {
                "Cardinality": "ONE_OR_MORE",
                "AttributeName": "PublicKeyPolicyName",
                "AttributeType": "PolicyName"
            }
        ],
        "PolicyTypeName": "BackendServerAuthenticationPolicyType",
        "Description": "Policy that controls authentication to back-end server(s)
 and contains one or more policies, such as an instance of a PublicKeyPolicyType.
 This policy can be associated only with back-end servers that are using HTTPS/SSL."
    }
 ]
}
```

- Para obtener información sobre la API, consulte DescribeLoadBalancerPolicyTypes en la Referencia de comandos de la AWS CLI.

`describe-load-balancers`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-load-balancers`.

AWS CLI

Para describir sus equilibradores de carga

En este ejemplo, se describen todos los equilibradores de carga.

Comando:

```
aws elb describe-load-balancers
```

Para describir uno de sus equilibradores de carga

En este ejemplo se describe el equilibrador de carga especificado.

Comando:

```
aws elb describe-load-balancers --load-balancer-name my-load-balancer
```

El ejemplo de respuesta siguiente se refiere a un nuevo equilibrador de carga de HTTPS en una nube privada virtual.

Salida:

```
{
  "LoadBalancerDescriptions": [
    {
      "Subnets": [
          "subnet-15aaab61"
      ],
      "CanonicalHostedZoneNameID": "Z3DZXE0EXAMPLE",
      "CanonicalHostedZoneName": "my-load-balancer-1234567890.us-
west-2.elb.amazonaws.com",
      "ListenerDescriptions": [
          {
              "Listener": {
                  "InstancePort": 80,
                  "LoadBalancerPort": 80,
                  "Protocol": "HTTP",
                  "InstanceProtocol": "HTTP"
              },
              "PolicyNames": []
          },
          {
```

```
            "Listener": {
                "InstancePort": 443,
                "SSLCertificateId": "arn:aws:iam::123456789012:server-certificate/
my-server-cert",
                "LoadBalancerPort": 443,
                "Protocol": "HTTPS",
                "InstanceProtocol": "HTTPS"
            },
            "PolicyNames": [
                "ELBSecurityPolicy-2015-03"
            ]
        }
    ],
    "HealthCheck": {
        "HealthyThreshold": 2,
        "Interval": 30,
        "Target": "HTTP:80/png",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    },
    "VPCId": "vpc-a01106c2",
    "BackendServerDescriptions": [
        {
            "InstancePort": 80,
            "PolicyNames": [
                "my-ProxyProtocol-policy"
            ]
        }
    ],
    "Instances": [
        {
            "InstanceId": "i-207d9717"
        },
        {
            "InstanceId": "i-afefb49b"
        }
    ],
    "DNSName": "my-load-balancer-1234567890.us-west-2.elb.amazonaws.com",
    "SecurityGroups": [
        "sg-a61988c3"
    ],
    "Policies": {
        "LBCookieStickinessPolicies": [
            {
```

```
                "PolicyName": "my-duration-cookie-policy",
                "CookieExpirationPeriod": 60
            }
        ],
        "AppCookieStickinessPolicies": [],
        "OtherPolicies": [
            "my-PublicKey-policy",
            "my-authentication-policy",
            "my-SSLNegotiation-policy",
            "my-ProxyProtocol-policy",
            "ELBSecurityPolicy-2015-03"
        ]
    },
    "LoadBalancerName": "my-load-balancer",
    "CreatedTime": "2015-03-19T03:24:02.650Z",
    "AvailabilityZones": [
        "us-west-2a"
    ],
    "Scheme": "internet-facing",
    "SourceSecurityGroup": {
        "OwnerAlias": "123456789012",
        "GroupName": "my-elb-sg"
    }
  }
 ]
}
```

- Para obtener información sobre la API, consulte DescribeLoadBalancers en la Referencia de comandos de la AWS CLI.

`describe-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-tags`.

AWS CLI

Para describir las etiquetas asignadas a un equilibrador de carga

En este ejemplo, se describen las etiquetas asignadas al equilibrador de carga especificado.

Comando:

```
aws elb describe-tags --load-balancer-name my-load-balancer
```

Salida:

```
{
  "TagDescriptions": [
      {
          "Tags": [
              {
                  "Value": "lima",
                  "Key": "project"
              },
              {
                  "Value": "digital-media",
                  "Key": "department"
              }
          ],
          "LoadBalancerName": "my-load-balancer"
      }
  ]
}
```

- Para obtener detalles sobre la API, consulte DescribeTags en la Referencia de comandos de la AWS CLI.

`detach-load-balancer-from-subnets`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-load-balancer-from-subnets`.

AWS CLI

Para desasociar los equilibradores de carga de las subredes

En este ejemplo, se desasocia el equilibrador de carga especificado de la subred especificada.

Comando:

```
aws elb detach-load-balancer-from-subnets --load-balancer-name my-load-balancer --
subnets subnet-0ecac448
```

Salida:

```
{
```

```
    "Subnets": [
        "subnet-15aaab61"
    ]
}
```

- Para obtener información sobre la API, consulte DetachLoadBalancerFromSubnets en la Referencia de comandos de la AWS CLI.

`disable-availability-zones-for-load-balancer`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-availability-zones-for-load-balancer`.

AWS CLI

Para deshabilitar las zonas de disponibilidad para un equilibrador de carga

En este ejemplo, se quitan las zonas de disponibilidad especificadas del conjunto de zonas de disponibilidad para el equilibrador de carga especificado.

Comando:

```
aws elb disable-availability-zones-for-load-balancer --load-balancer-name my-load-balancer --availability-zones us-west-2a
```

Salida:

```
{
    "AvailabilityZones": [
        "us-west-2b"
    ]
}
```

- Para obtener información sobre la API, consulte DisableAvailabilityZonesForLoadBalancer en la Referencia de comandos de la AWS CLI.

`enable-availability-zones-for-load-balancer`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-availability-zones-for-load-balancer`.

AWS CLI

Para habilitar las zonas de disponibilidad para un equilibrador de carga

En este ejemplo, se agrega la zona de disponibilidad especificada al equilibrador de carga especificado.

Comando:

```
aws elb enable-availability-zones-for-load-balancer --load-balancer-name my-load-balancer --availability-zones us-west-2b
```

Salida:

```
{
    "AvailabilityZones": [
        "us-west-2a",
        "us-west-2b"
    ]
}
```

- Para obtener información sobre la API, consulte EnableAvailabilityZonesForLoadBalancer en la Referencia de comandos de la AWS CLI.

`modify-load-balancer-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-load-balancer-attributes`.

AWS CLI

Para modificar los atributos de un equilibrador de carga

En este ejemplo, se modifica el atributo `CrossZoneLoadBalancing` del equilibrador de carga especificado.

Comando:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-load-balancer --load-balancer-attributes "{\"CrossZoneLoadBalancing\":{\"Enabled\":true}}"
```

Salida:

```
{
    "LoadBalancerAttributes": {
        "CrossZoneLoadBalancing": {
            "Enabled": true
        }
    },
    "LoadBalancerName": "my-load-balancer"
}
```

En este ejemplo, se modifica el atributo `ConnectionDraining` del equilibrador de carga especificado.

Comando:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-load-balancer
 --load-balancer-attributes "{\"ConnectionDraining\":{\"Enabled\":true,\"Timeout
\":300}}"
```

Salida:

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": true,
            "Timeout": 300
        }
    },
    "LoadBalancerName": "my-load-balancer"
}
```

- Para obtener información sobre la API, consulte ModifyLoadBalancerAttributes en la Referencia de comandos de la AWS CLI.

`register-instances-with-load-balancer`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-instances-with-load-balancer`.

AWS CLI

Para registrar instancias en un equilibrador de carga

En este ejemplo, se registra la instancia especificada en el equilibrador de carga especificado.

Comando:

```
aws elb register-instances-with-load-balancer --load-balancer-name my-load-balancer
 --instances i-d6f6fae3
```

Salida:

```
{
   "Instances": [
       {
           "InstanceId": "i-d6f6fae3"
       },
       {
           "InstanceId": "i-207d9717"
       },
       {
           "InstanceId": "i-afefb49b"
       }
   ]
}
```

- Para obtener información sobre la API, consulte RegisterInstancesWithLoadBalancer en la Referencia de comandos de la AWS CLI.

`remove-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-tags`.

AWS CLI

Para eliminar etiquetas de un equilibrador de carga

En este ejemplo, se quita una etiqueta del equilibrador de carga especificado.

Comando:

```
aws elb remove-tags --load-balancer-name my-load-balancer --tags project
```

- Para obtener información sobre la API, consulte RemoveTags en la Referencia de comandos de la AWS CLI.

`set-load-balancer-listener-ssl-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-load-balancer-listener-ssl-certificate`.

AWS CLI

Para actualizar el certificado de SSL de un equilibrador de carga de HTTPS

En este ejemplo, se reemplaza el certificado de SSL existente del equilibrador de carga de HTTPS especificado.

Comando:

```
aws elb set-load-balancer-listener-ssl-certificate --load-balancer-
name my-load-balancer --load-balancer-port 443 --ssl-certificate-
id arn:aws:iam::123456789012:server-certificate/new-server-cert
```

- Para obtener información sobre la API, consulte SetLoadBalancerListenerSslCertificate en la Referencia de comandos de la AWS CLI.

`set-load-balancer-policies-for-backend-server`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-load-balancer-policies-for-backend-server`.

AWS CLI

Para reemplazar las políticas asociadas a un puerto para una instancia de backend

En este ejemplo, se reemplazan las políticas que están asociadas en este momento al puerto especificado.

Comando:

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-load-
balancer --instance-port 80 --policy-names my-ProxyProtocol-policy
```

Para eliminar todas las políticas que están asociadas en este momento a un puerto de la instancia de backend

En este ejemplo, se quitan todas las políticas asociadas al puerto especificado.

Comando:

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-load-balancer --instance-port 80 --policy-names []
```

Para confirmar que se han eliminado las políticas, utilice el comando `describe-load-balancer-policies`.

- Para obtener información sobre la API, consulte SetLoadBalancerPoliciesForBackendServer en la Referencia de comandos de la AWS CLI.

`set-load-balancer-policies-of-listener`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-load-balancer-policies-of-listener`.

AWS CLI

Para reemplazar las políticas asociadas a un oyente

En este ejemplo, se reemplazan las políticas que están asociadas en este momento al oyente especificado.

Comando:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-load-balancer
 --load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

Para eliminar todas las políticas asociadas a su oyente

En este ejemplo, se quitan todas las políticas que están asociadas en este momento al oyente especificado.

Comando:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-load-balancer
 --load-balancer-port 443 --policy-names []
```

Para confirmar que las políticas se han quitado del equilibrador de carga, utilice el comando `describe-load-balancer-policies`.

- Para obtener información sobre la API, consulte SetLoadBalancerPoliciesOfListener en la Referencia de comandos de la AWS CLI.

ELB: ejemplos de la versión 2 mediante AWS CLI

Los ejemplos de código siguientes muestran cómo realizar acciones e implementar escenarios comunes mediante AWS Command Line Interface con ELB: versión 2.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-listener-certificates`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-listener-certificates`.

AWS CLI

Para agregar un certificado a un oyente seguro

En este ejemplo, se añade el certificado especificado al oyente seguro especificado.

Comando:

```
aws elbv2 add-listener-certificates --listener-arn arn:aws:elasticloadbalancing:us-west-2:123456789012:listener/app/my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2 --certificates CertificateArn=arn:aws:acm:us-west-2:123456789012:certificate/5cc54884-f4a3-4072-80be-05b9ba72f705
```

Salida:

```
{
```

```
  "Certificates": [
      {
          "CertificateArn": "arn:aws:acm:us-
west-2:123456789012:certificate/5cc54884-f4a3-4072-80be-05b9ba72f705",
          "IsDefault": false
      }
  ]
}
```

- Para obtener información sobre la API, consulte AddListenerCertificates en la Referencia de comandos de la AWS CLI.

`add-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-tags`.

AWS CLI

Para agregar etiquetas a un equilibrador de carga

En el siguiente ejemplo de `add-tags`, se agregan las etiquetas `project` y `department` al equilibrador de carga especificado.

```
aws elbv2 add-tags \
    --resource-arns arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188 \
    --tags "Key=project,Value=lima" "Key=department,Value=digital-media"
```

- Para obtener información sobre la API, consulte AddTags en la Referencia de comandos de la AWS CLI.

`create-listener`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-listener`.

AWS CLI

Ejemplo 1: Creación de un oyente HTTP

En el siguiente ejemplo de `create-listener` se crea un oyente HTTP para el Equilibrador de carga de aplicación especificado que reenvía las solicitudes al grupo de destino especificado.

```
aws elbv2 create-listener \
    --load-balancer-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188 \
    --protocol HTTP \
    --port 80 \
    --default-actions Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
```

Para obtener más información, consulte Tutorial: crear un equilibrador de carga de aplicación con la CLI de AWS en la Guía del usuario para Equilibradores de carga de aplicación.

Ejemplo 2: creación de un oyente de HTTPS

En el siguiente ejemplo de `create-listener` se crea un oyente de HTTPS para el equilibrador de carga de aplicación especificado que reenvía las solicitudes al grupo de destino especificado. Debe especificar un certificado SSL para un oyente de HTTPS. Puede crear y administrar certificados mediante AWS Certificate Manager (ACM). Como alternativa, puede crear un certificado mediante herramientas de SSL/TLS, obtener el certificado firmado por una autoridad de certificación (CA) y cargarlo en AWS Identity and Access Management (IAM).

```
aws elbv2 create-listener \
    --load-balancer-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188 \
    --protocol HTTPS \
    --port 443 \
    --certificates CertificateArn=arn:aws:acm:us-
west-2:123456789012:certificate/3dcb0a41-bd72-4774-9ad9-756919c40557 \
    --ssl-policy ELBSecurityPolicy-2016-08 \
    --default-actions Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
```

Para obtener más información, consulte Agregar un oyente HTTPS en la Guía del usuario de equilibradores de carga de aplicación.

Ejemplo 3: creación de un oyente TCP

En el siguiente ejemplo de `create-listener` se crea un oyente TCP para el Equilibrador de carga de red especificado que reenvía las solicitudes al grupo de destino especificado.

```
aws elbv2 create-listener \
```

```
    --load-balancer-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/net/my-network-load-balancer/5d1b75f4f1cee11e \
    --protocol TCP \
    --port 80 \
    --default-actions Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-tcp-targets/b6bba954d1361c78
```

Para obtener más información, consulte Tutorial: Crear un equilibrador de carga de red mediante la CLI de AWS en la Guía del usuario para Equilibradores de carga de red.

Ejemplo 4: creación de un oyente TLS

En el siguiente ejemplo de `create-listener` se crea un oyente TLS para el Equilibrador de carga de red especificado que reenvía las solicitudes al grupo de destino especificado. Debe especificar un certificado SSL para un oyente de TLS.

```
aws elbv2 create-listener \
    --load-balancer-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188 \
    --protocol TLS \
    --port 443 \
    --certificates CertificateArn=arn:aws:acm:us-
west-2:123456789012:certificate/3dcb0a41-bd72-4774-9ad9-756919c40557 \
    --ssl-policy ELBSecurityPolicy-2016-08 \
    --default-actions Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
```

Para obtener más información, consulte Oyente TLS para su equilibrador de carga de red en la Guía del usuario para Equilibradores de carga de red.

Ejemplo 5: creación de un oyente UDP

En el siguiente ejemplo de `create-listener` se crea un oyente UDP para el Equilibrador de carga de red especificado que reenvía las solicitudes al grupo de destino especificado.

```
aws elbv2 create-listener \
    --load-balancer-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/net/my-network-load-balancer/5d1b75f4f1cee11e \
    --protocol UDP \
    --port 53 \
    --default-actions Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-tcp-targets/b6bba954d1361c78
```

Para obtener más información, consulte Tutorial: Crear un equilibrador de carga de red mediante la CLI de AWS en la Guía del usuario para Equilibradores de carga de red.

Ejemplo 6: creación de un oyente para la puerta de enlace y el reenvío especificados

En el siguiente ejemplo de `create-listener` se crea un oyente para el Equilibrador de carga de puerta de enlace especificado que reenvía las solicitudes al grupo de destino especificado.

```
aws elbv2 create-listener \
    --load-balancer-arn arn:aws:elasticloadbalancing:us-
east-1:850631746142:loadbalancer/gwy/my-gateway-load-balancer/e0f9b3d5c7f7d3d6 \
    --default-actions Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:us-
east-1:850631746142:targetgroup/my-glb-targets/007ca469fae3bb1615
```

Salida:

```
{
    "Listeners": [
        {
            "ListenerArn": "arn:aws:elasticloadbalancing:us-
east-1:850631746142:listener/gwy/my-agw-lb-example2/e0f9b3d5c7f7d3d6/
afc127db15f925de",
            "LoadBalancerArn": "arn:aws:elasticloadbalancing:us-
east-1:850631746142:loadbalancer/gwy/my-agw-lb-example2/e0f9b3d5c7f7d3d6",
            "DefaultActions": [
                {
                    "Type": "forward",
                    "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
east-1:850631746142:targetgroup/test-tg-agw-2/007ca469fae3bb1615",
                    "ForwardConfig": {
                        "TargetGroups": [
                            {
                                "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
east-1:850631746142:targetgroup/test-tg-agw-2/007ca469fae3bb1615"
                            }
                        ]
                    }
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Introducción con los equilibradores de carga de puerta de enlace mediante la CLI de AWS en la Guía del usuario de equilibradores de carga de puerta de enlace.

- Para obtener información sobre la API, consulte CreateListener en la Referencia de comandos de la AWS CLI.

`create-load-balancer`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-load-balancer`.

AWS CLI

Ejemplo 1: creación de un equilibrador de carga expuesto a Internet

En el siguiente ejemplo de `create-load-balancer` se crea un equilibrador de carga de aplicación expuesto a Internet y se habilitan las zonas de disponibilidad para las subredes especificadas.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --subnets subnet-b7d581c0 subnet-8360a9e7
```

Salida:

```
{
    "LoadBalancers": [
        {
            "Type": "application",
            "Scheme": "internet-facing",
            "IpAddressType": "ipv4",
            "VpcId": "vpc-3ac0fb5f",
            "AvailabilityZones": [
                {
                    "ZoneName": "us-west-2a",
                    "SubnetId": "subnet-8360a9e7"
                },
                {
                    "ZoneName": "us-west-2b",
                    "SubnetId": "subnet-b7d581c0"
                }
            ],
```

```
            "CreatedTime": "2017-08-25T21:26:12.920Z",
            "CanonicalHostedZoneId": "Z2P70J7EXAMPLE",
            "DNSName": "my-load-balancer-424835706.us-west-2.elb.amazonaws.com",
            "SecurityGroups": [
                "sg-5943793c"
            ],
            "LoadBalancerName": "my-load-balancer",
            "State": {
                "Code": "provisioning"
            },
            "LoadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188"
        }
    ]
}
```

Para obtener más información, consulte Tutorial: crear un equilibrador de carga de aplicación con la CLI de AWS en la Guía del usuario para Equilibradores de carga de aplicación.

Ejemplo 2: Creación de un equilibrador de carga interno

En el siguiente ejemplo de `create-load-balancer` se crea un equilibrador de carga de aplicación interno y se habilitan las zonas de disponibilidad para las subredes especificadas.

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internal \
    --subnets subnet-b7d581c0 subnet-8360a9e7
```

Salida:

```
{
    "LoadBalancers": [
        {
            "Type": "application",
            "Scheme": "internal",
            "IpAddressType": "ipv4",
            "VpcId": "vpc-3ac0fb5f",
            "AvailabilityZones": [
                {
                    "ZoneName": "us-west-2a",
                    "SubnetId": "subnet-8360a9e7"
```

```
                },
                {
                    "ZoneName": "us-west-2b",
                    "SubnetId": "subnet-b7d581c0"
                }
            ],
            "CreatedTime": "2016-03-25T21:29:48.850Z",
            "CanonicalHostedZoneId": "Z2P70J7EXAMPLE",
            "DNSName": "internal-my-internal-load-balancer-1529930873.us-
west-2.elb.amazonaws.com",
            "SecurityGroups": [
                "sg-5943793c"
            ],
            "LoadBalancerName": "my-internal-load-balancer",
            "State": {
                "Code": "provisioning"
            },
            "LoadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-internal-load-balancer/5b49b8d4303115c2"
        }
    ]
}
```

Para obtener más información, consulte Tutorial: crear un equilibrador de carga de aplicación con la CLI de AWS en la Guía del usuario para Equilibradores de carga de aplicación.

Ejemplo 3: creación de un equilibrador de carga de red

En el siguiente ejemplo de `create-load-balancer` se crea un equilibrador de carga de red expuesto a Internet y se habilitan las zonas de disponibilidad para la subred especificada. Utiliza un mapeo de subred para asociar la dirección IP elástica especificada con la interfaz de red utilizada por los nodos del equilibrador de carga de la zona de disponibilidad.

```
aws elbv2 create-load-balancer \
    --name my-network-load-balancer \
    --type network \
    --subnet-mappings SubnetId=subnet-b7d581c0,AllocationId=eipalloc-64d5890a
```

Salida:

```
{
    "LoadBalancers": [
```

```
        {
            "Type": "network",
            "Scheme": "internet-facing",
            "IpAddressType": "ipv4",
            "VpcId": "vpc-3ac0fb5f",
            "AvailabilityZones": [
                {
                    "LoadBalancerAddresses": [
                        {
                            "IpAddress": "35.161.207.171",
                            "AllocationId": "eipalloc-64d5890a"
                        }
                    ],
                    "ZoneName": "us-west-2b",
                    "SubnetId": "subnet-5264e837"
                }
            ],
            "CreatedTime": "2017-10-15T22:41:25.657Z",
            "CanonicalHostedZoneId": "Z2P70J7EXAMPLE",
            "DNSName": "my-network-load-balancer-5d1b75f4f1cee11e.elb.us-
west-2.amazonaws.com",
            "LoadBalancerName": "my-network-load-balancer",
            "State": {
                "Code": "provisioning"
            },
            "LoadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/net/my-network-load-balancer/5d1b75f4f1cee11e"
        }
    ]
}
```

Para obtener más información, consulte Tutorial: Crear un equilibrador de carga de red mediante la CLI de AWS en la Guía del usuario para Equilibradores de carga de red.

Ejemplo 4: creación de un equilibrador de carga de puerta de enlace

En el siguiente ejemplo de `create-load-balancer` se crea un equilibrador de carga de puerta de enlace y se habilitan las zonas de disponibilidad para las subredes especificadas.

```
aws elbv2 create-load-balancer \
    --name my-gateway-load-balancer \
    --type gateway \
    --subnets subnet-dc83f691 subnet-a62583f9
```

Salida:

```
{
    "LoadBalancers": [
        {
            "Type": "gateway",
            "VpcId": "vpc-838475fe",
            "AvailabilityZones": [
                {
                    "ZoneName": "us-east-1b",
                    "SubnetId": "subnet-a62583f9"
                },
            {
                    "ZoneName": "us-east-1a",
                    "SubnetId": "subnet-dc83f691"
                }
            ],
            "CreatedTime": "2021-07-14T19:33:43.324000+00:00",
            "LoadBalancerName": "my-gateway-load-balancer",
            "State": {
                "Code": "provisioning"
            },
            "LoadBalancerArn": "arn:aws:elasticloadbalancing:us-
east-1:850631746142:loadbalancer/gwy/my-gateway-load-balancer/dfbb5a7d32cdee79"
        }
    ]
}
```

Para obtener más información, consulte Introducción con los equilibradores de carga de puerta de enlace mediante la CLI de AWS en la Guía del usuario de equilibradores de carga de puerta de enlace.

- Para obtener información sobre la API, consulte CreateLoadBalancer en la Referencia de comandos de la AWS CLI.

`create-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-rule`.

AWS CLI

Ejemplo 1: creación de una regla mediante una condición de ruta y una acción de reenvío

En el siguiente ejemplo de `create-rule`, se crea una regla que reenvía las solicitudes al grupo de destino especificado si la dirección URL de la solicitud contiene el patrón especificado.

```
aws elbv2 create-rule \
    --listener-arn arn:aws:elasticloadbalancing:us-west-2:123456789012:listener/app/my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2 \
    --priority 5 \
    --conditions file://conditions-pattern.json
    --actions Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:us-west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
```

Contenido de `conditions-pattern.json`:

```
[
    {
        "Field": "path-pattern",
        "PathPatternConfig": {
            "Values": ["/images/*"]
        }
    }
]
```

Ejemplo 2: creación de una regla mediante una condición de host y una respuesta fija

En el siguiente ejemplo de `create-rule`, se crea una regla que proporciona una respuesta fija si el nombre de host del encabezado del host coincide con el nombre de host especificado.

```
aws elbv2 create-rule \
    --listener-arn arn:aws:elasticloadbalancing:us-west-2:123456789012:listener/app/my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2 \
    --priority 10 \
    --conditions file://conditions-host.json \
    --actions file://actions-fixed-response.json
```

Contenido de `conditions-host.json`

```
[
  {
      "Field": "host-header",
      "HostHeaderConfig": {
          "Values": ["*.example.com"]
      }
```

```
  }
]
```

Contenido de `actions-fixed-response.json`

```
[
    {
        "Type": "fixed-response",
        "FixedResponseConfig": {
            "MessageBody": "Hello world",
            "StatusCode": "200",
            "ContentType": "text/plain"
        }
    }
]
```

Ejemplo 3: creación de una regla mediante una condición de dirección IP de origen, una acción de autenticación y una acción de reenvío

En el siguiente ejemplo de `create-rule`, se crea una regla que autentica al usuario si la dirección IP de origen coincide con la dirección IP especificada y reenvía la solicitud al grupo de destino especificado si la autenticación se realiza correctamente.

```
aws elbv2 create-rule \
    --listener-arn arn:aws:elasticloadbalancing:us-west-2:123456789012:listener/app/
my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2 \
    --priority 20 \
    --conditions file://conditions-source-ip.json \
    --actions file://actions-authenticate.json
```

Contenido de `conditions-source-ip.json`

```
[
    {
        "Field": "source-ip",
        "SourceIpConfig": {
            "Values": ["192.0.2.0/24", "198.51.100.10/32"]
        }
    }
]
```

Contenido de `actions-authenticate.json`

```
[
    {
        "Type": "authenticate-oidc",
        "AuthenticateOidcConfig": {
            "Issuer": "https://idp-issuer.com",
            "AuthorizationEndpoint": "https://authorization-endpoint.com",
            "TokenEndpoint": "https://token-endpoint.com",
            "UserInfoEndpoint": "https://user-info-endpoint.com",
            "ClientId": "abcdefghijklmnopqrstuvwxyz123456789",
            "ClientSecret": "12345678901234567890123456789O",
            "SessionCookieName": "my-cookie",
            "SessionTimeout": 3600,
            "Scope": "email",
            "AuthenticationRequestExtraParams": {
                "display": "page",
                "prompt": "login"
            },
            "OnUnauthenticatedRequest": "deny"
        },
        "Order": 1
    },
    {
        "Type": "forward",
        "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
east-1:880185128111:targetgroup/cli-test/642a97ecb0e0f26b",
        "Order": 2
    }
]
```

- Para obtener información sobre la API, consulte CreateRule en la Referencia de comandos de la AWS CLI.

`create-target-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-target-group`.

AWS CLI

Example 1: creación de un grupo de destino para el equilibrador de carga de aplicación

En el siguiente ejemplo de `create-target-group` se crea un grupo de destino para un Equilibrador de carga de aplicación en el que se registran los destinos por ID de instancia (el

tipo de destino es `instance`). Este grupo de destino usa el protocolo HTTP, el puerto 80 y la configuración de comprobación de estado predeterminada para un grupo de destino HTTP.

```
aws elbv2 create-target-group \
    --name my-targets \
    --protocol HTTP \
    --port 80 \
    --target-type instance \
    --vpc-id vpc-3ac0fb5f
```

Salida:

```
{
    "TargetGroups": [
        {
            "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067",
            "TargetGroupName": "my-targets",
            "Protocol": "HTTP",
            "Port": 80,
            "VpcId": "vpc-3ac0fb5f",
            "HealthCheckProtocol": "HTTP",
            "HealthCheckPort": "traffic-port",
            "HealthCheckEnabled": true,
            "HealthCheckIntervalSeconds": 30,
            "HealthCheckTimeoutSeconds": 5,
            "HealthyThresholdCount": 5,
            "UnhealthyThresholdCount": 2,
            "HealthCheckPath": "/",
            "Matcher": {
                "HttpCode": "200"
            },
            "TargetType": "instance",
            "ProtocolVersion": "HTTP1",
            "IpAddressType": "ipv4"
        }
    ]
}
```

Para obtener más información, consulte Crear un grupo de destino en la Guía del usuario para Equilibradores de carga de aplicación.

Ejemplo 2: creación de un grupo de destino para enrutar el tráfico de un equilibrador de carga de aplicación a una función de Lambda

En el siguiente ejemplo de `create-target-group` se crea un grupo de destino para un Equilibrador de carga de aplicación donde el destino es una función de Lambda (el tipo de destino es `lambda`). De forma predeterminada, las comprobaciones de estado están deshabilitadas para este grupo de destino.

```
aws elbv2 create-target-group \
    --name my-lambda-target \
    --target-type lambda
```

Salida:

```
{
    "TargetGroups": [
        {
            "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-lambda-target/a3003e085dbb8ddc",
            "TargetGroupName": "my-lambda-target",
            "HealthCheckEnabled": false,
            "HealthCheckIntervalSeconds": 35,
            "HealthCheckTimeoutSeconds": 30,
            "HealthyThresholdCount": 5,
            "UnhealthyThresholdCount": 2,
            "HealthCheckPath": "/",
            "Matcher": {
                "HttpCode": "200"
            },
            "TargetType": "lambda",
            "IpAddressType": "ipv4"
        }
    ]
}
```

Para obtener más información, consulte Funciones de Lambda como destinos en la Guía del usuario de Equilibradores de carga de aplicación.

Ejemplo 3: creación de un grupo de destino para un equilibrador de carga de red

En el siguiente ejemplo de `create-target-group` se crea un grupo de destino para un Equilibrador de carga de red en el que se registran los destinos por dirección IP (el tipo de

destino es `ip`). Este grupo de destino usa el protocolo TCP, el puerto 80 y la configuración de comprobación de estado predeterminada para un grupo de destino TCP.

```
aws elbv2 create-target-group \
    --name my-ip-targets \
    --protocol TCP \
    --port 80 \
    --target-type ip \
    --vpc-id vpc-3ac0fb5f
```

Salida:

```
{
    "TargetGroups": [
        {
            "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-ip-targets/b6bba954d1361c78",
            "TargetGroupName": "my-ip-targets",
            "Protocol": "TCP",
            "Port": 80,
            "VpcId": "vpc-3ac0fb5f",
            "HealthCheckEnabled": true,
            "HealthCheckProtocol": "TCP",
            "HealthCheckPort": "traffic-port",
            "HealthCheckIntervalSeconds": 30,
            "HealthCheckTimeoutSeconds": 10,
            "HealthyThresholdCount": 5,
            "UnhealthyThresholdCount": 2,
            "TargetType": "ip",
            "IpAddressType": "ipv4"
        }
    ]
}
```

Para obtener más información, consulte Create a target group en la Guía del usuario de equilibradores de carga de red.

Ejemplo 4: creación de un grupo de destino para enrutar el tráfico de un equilibrador de carga de red a un equilibrador de carga de aplicación

En el siguiente ejemplo de `create-target-group`, se crea un grupo de destino para un equilibrador de carga de red en el que se registra como destino un equilibrador de carga de aplicación (el tipo de destino es `alb`).

aws elbv2 create-target-group --name my-alb-target --protocol TCP --port 80 --target-type alb --vpc-id vpc-3ac0fb5f

Salida:

```
{
    "TargetGroups": [
        {
            "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-alb-target/a3003e085dbb8ddc",
            "TargetGroupName": "my-alb-target",
            "Protocol": "TCP",
            "Port": 80,
            "VpcId": "vpc-838475fe",
            "HealthCheckProtocol": "HTTP",
            "HealthCheckPort": "traffic-port",
            "HealthCheckEnabled": true,
            "HealthCheckIntervalSeconds": 30,
            "HealthCheckTimeoutSeconds": 6,
            "HealthyThresholdCount": 5,
            "UnhealthyThresholdCount": 2,
            "HealthCheckPath": "/",
            "Matcher": {
                "HttpCode": "200-399"
            },
            "TargetType": "alb",
            "IpAddressType": "ipv4"
        }
    ]
}
```

Para obtener más información, consulte Create a target group with an Application Load Balancer as the target en la Guía del usuario de equilibradores de carga de red.

Ejemplo 5: creación de un grupo de destino para un equilibrador de carga de puerta de enlace

En el siguiente ejemplo de `create-target-group`, se crea un grupo de destino para un equilibrador de carga de puerta de enlace donde el destino es una instancia y el protocolo del grupo de destino es `GENEVE`.

```
aws elbv2 create-target-group \
    --name my-glb-targetgroup \
    --protocol GENEVE \
    --port 6081 \
    --target-type instance \
    --vpc-id vpc-838475fe
```

Salida:

```
{
    "TargetGroups": [
        {
            "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-glb-targetgroup/00c3d57eacd6f40b6f",
            "TargetGroupName": "my-glb-targetgroup",
            "Protocol": "GENEVE",
            "Port": 6081,
            "VpcId": "vpc-838475fe",
            "HealthCheckProtocol": "TCP",
            "HealthCheckPort": "80",
            "HealthCheckEnabled": true,
            "HealthCheckIntervalSeconds": 10,
            "HealthCheckTimeoutSeconds": 5,
            "HealthyThresholdCount": 5,
            "UnhealthyThresholdCount": 2,
            "TargetType": "instance"
        }
    ]
}
```

Para obtener más información, consulte Create a target group <https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/create-target-group.html>`__ en la Guía del usuario de equilibradores de carga de puerta de enlace.

- Para obtener información sobre la API, consulte CreateTargetGroup en la Referencia de comandos de la AWS CLI.

`delete-listener`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-listener`.

AWS CLI

Para eliminar un oyente

En el siguiente ejemplo de `delete-listener`, se elimina el oyente especificado.

```
aws elbv2 delete-listener \
    --listener-arn arn:aws:elasticloadbalancing:ua-west-2:123456789012:listener/app/
my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2
```

- Para obtener información sobre la API, consulte DeleteListener en la Referencia de comandos de la AWS CLI.

`delete-load-balancer`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-load-balancer`.

AWS CLI

Eliminación de un equilibrador de carga

En el siguiente ejemplo de `delete-load-balancer` se elimina el equilibrador de carga especificado.

```
aws elbv2 delete-load-balancer \
    --load-balancer-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188
```

- Para obtener información sobre la API, consulte DeleteLoadBalancer en la Referencia de comandos de la AWS CLI.

`delete-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-rule`.

AWS CLI

Para eliminar una regla

En el siguiente ejemplo de `delete-rule` se elimina la regla especificada.

```
aws elbv2 delete-rule \
```

```
    --rule-arn arn:aws:elasticloadbalancing:us-west-2:123456789012:listener-rule/
app/my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2/1291d13826f405c3
```

- Para obtener información sobre la API, consulte DeleteRule en la Referencia de comandos de la AWS CLI.

`delete-target-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-target-group`.

AWS CLI

Para eliminar un grupo de destino

En el siguiente ejemplo de `delete-target-group` se elimina el grupo de destino especificado.

```
aws elbv2 delete-target-group \
    --target-group-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Delete a load balancer en la Guía del usuario de equilibradores de carga de aplicación.

- Para obtener información sobre la API, consulte DeleteTargetGroup en la Referencia de comandos de la AWS CLI.

`deregister-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-targets`.

AWS CLI

Ejemplo 1: anulación del registro de un destino en un grupo de destino

En el siguiente ejemplo de `deregister-targets`, se elimina la instancia especificada del grupo de destino especificado.

```
aws elbv2 deregister-targets \
    --target-group-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067 \
```

```
    --targets Id=i-1234567890abcdef0
```

Ejemplo 2: anulación del registro de un destino registrado mediante anulaciones de puertos

En el siguiente ejemplo de `deregister-targets`, se elimina una instancia de un grupo de destino registrado mediante anulaciones de puertos.

```
aws elbv2 deregister-targets \
    --target-group-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-internal-targets/3bb63f11dfb0faf9 \
    --targets Id=i-1234567890abcdef0,Port=80 Id=i-1234567890abcdef0,Port=766
```

- Para obtener información sobre la API, consulte DeregisterTargets en la Referencia de comandos de la AWS CLI.

`describe-account-limits`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-account-limits`.

AWS CLI

Para describir sus límites de Elastic Load Balancing

En el siguiente ejemplo de `describe-account-limits`, se muestran los límites de Elastic Load Balancing para su cuenta de AWS en la región actual.

```
aws elbv2 describe-account-limits
```

Salida:

```
{
    "Limits": [
        {
            "Name": "target-groups",
            "Max": "3000"
        },
        {
            "Name": "targets-per-application-load-balancer",
            "Max": "1000"
        },
        {
            "Name": "listeners-per-application-load-balancer",
```

```
            "Max": "50"
        },
        {
            "Name": "rules-per-application-load-balancer",
            "Max": "100"
        },
        {
            "Name": "network-load-balancers",
            "Max": "50"
        },
        {
            "Name": "targets-per-network-load-balancer",
            "Max": "3000"
        },
        {
            "Name": "targets-per-availability-zone-per-network-load-balancer",
            "Max": "500"
        },
        {
            "Name": "listeners-per-network-load-balancer",
            "Max": "50"
        },
        {
            "Name": "condition-values-per-alb-rule",
            "Max": "5"
        },
        {
            "Name": "condition-wildcards-per-alb-rule",
            "Max": "5"
        },
        {
            "Name": "target-groups-per-application-load-balancer",
            "Max": "100"
        },
        {
            "Name": "target-groups-per-action-on-application-load-balancer",
            "Max": "5"
        },
        {
            "Name": "target-groups-per-action-on-network-load-balancer",
            "Max": "1"
        },
        {
            "Name": "certificates-per-application-load-balancer",
```

```
            "Max": "25"
        },
        {
            "Name": "certificates-per-network-load-balancer",
            "Max": "25"
        },
        {
            "Name": "targets-per-target-group",
            "Max": "1000"
        },
        {
            "Name": "target-id-registrations-per-application-load-balancer",
            "Max": "1000"
        },
        {
            "Name": "network-load-balancer-enis-per-vpc",
            "Max": "1200"
        },
        {
            "Name": "application-load-balancers",
            "Max": "50"
        },
        {
            "Name": "gateway-load-balancers",
            "Max": "100"
        },
        {
            "Name": "gateway-load-balancers-per-vpc",
            "Max": "100"
        },
        {
            "Name": "geneve-target-groups",
            "Max": "100"
        },
        {
            "Name": "targets-per-availability-zone-per-gateway-load-balancer",
            "Max": "300"
        }
    ]
}
```

Para obtener más información, consulte Service Quotas en la Referencia general de AWS.

- Para obtener información sobre la API, consulte DescribeAccountLimits en la Referencia de comandos de la AWS CLI.

`describe-listener-certificates`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-listener-certificates`.

AWS CLI

Para describir los certificados de un oyente seguro

En este ejemplo, se describen los certificados del oyente seguro especificado.

Comando:

```
aws elbv2 describe-listener-certificates --listener-
arn arn:aws:elasticloadbalancing:us-west-2:123456789012:listener/app/my-load-
balancer/50dc6c495c0c9188/f2f7dc8efc522ab2
```

Salida:

```
{
  "Certificates": [
      {
          "CertificateArn": "arn:aws:acm:us-
west-2:123456789012:certificate/5cc54884-f4a3-4072-80be-05b9ba72f705",
          "IsDefault": false
      },
      {
          "CertificateArn": "arn:aws:acm:us-
west-2:123456789012:certificate/3dcb0a41-bd72-4774-9ad9-756919c40557",
          "IsDefault": false
      },
      {
          "CertificateArn": "arn:aws:acm:us-west-2:123456789012:certificate/
fe59da96-6f58-4a22-8eed-6d0d50477e1d",
          "IsDefault": true
      }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeListenerCertificates en la Referencia de comandos de la AWS CLI.

`describe-listeners`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-listeners`.

AWS CLI

Para describir un oyente

En este ejemplo, se describe el oyente especificado.

Comando:

```
aws elbv2 describe-listeners --listener-arns arn:aws:elasticloadbalancing:us-west-2:123456789012:listener/app/my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2
```

Salida:

```
{
  "Listeners": [
      {
          "Port": 80,
          "Protocol": "HTTP",
          "DefaultActions": [
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067",
                  "Type": "forward"
              }
          ],
          "LoadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188",
          "ListenerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:listener/app/my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2"
      }
  ]
}
```

Para describir los oyentes de un equilibrador de carga

En este ejemplo, se describen los oyentes del equilibrador de carga especificado.

Comando:

```
aws elbv2 describe-listeners --load-balancer-arn arn:aws:elasticloadbalancing:us-west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188
```

Salida:

```
{
  "Listeners": [
      {
          "Port": 443,
          "Protocol": "HTTPS",
          "DefaultActions": [
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067",
                  "Type": "forward"
              }
          ],
          "SslPolicy": "ELBSecurityPolicy-2015-05",
          "Certificates": [
              {
                  "CertificateArn": "arn:aws:iam::123456789012:server-certificate/
my-server-cert"
              }
          ],
          "LoadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188",
          "ListenerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:listener/app/my-load-balancer/50dc6c495c0c9188/0467ef3c8400ae65"
      },
      {
          "Port": 80,
          "Protocol": "HTTP",
          "DefaultActions": [
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067",
                  "Type": "forward"
              }
          ],
```

```
            "LoadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188",
            "ListenerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:listener/app/my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeListeners en la Referencia de comandos de la AWS CLI.

`describe-load-balancer-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-load-balancer-attributes`.

AWS CLI

Para describir los atributos del equilibrador de carga

En el siguiente ejemplo de `describe-load-balancer-attributes`, se muestran los atributos del equilibrador de carga especificado.

```
aws elbv2 describe-load-balancer-attributes \
    --load-balancer-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188
```

En la salida del ejemplo siguiente, se muestran los atributos de un equilibrador de carga de aplicación.

```
{
    "Attributes": [
        {
            "Value": "false",
            "Key": "access_logs.s3.enabled"
        },
        {
            "Value": "",
            "Key": "access_logs.s3.bucket"
        },
        {
            "Value": "",
```

```
            "Key": "access_logs.s3.prefix"
        },
        {
            "Value": "60",
            "Key": "idle_timeout.timeout_seconds"
        },
        {
            "Value": "false",
            "Key": "deletion_protection.enabled"
        },
        {
            "Value": "true",
            "Key": "routing.http2.enabled"
        }
    ]
}
```

En la salida del ejemplo siguiente, se muestran los atributos de un equilibrador de carga de red.

```
{
    "Attributes": [
        {
            "Value": "false",
            "Key": "access_logs.s3.enabled"
        },
        {
            "Value": "",
            "Key": "access_logs.s3.bucket"
        },
        {
            "Value": "",
            "Key": "access_logs.s3.prefix"
        },
        {
            "Value": "false",
            "Key": "deletion_protection.enabled"
        },
        {
            "Value": "false",
            "Key": "load_balancing.cross_zone.enabled"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeLoadBalancerAttributes en la Referencia de comandos de la AWS CLI.

`describe-load-balancers`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-load-balancers`.

AWS CLI

Para describir un equilibrador de cargas

En este ejemplo se describe el equilibrador de carga especificado.

Comando:

```
aws elbv2 describe-load-balancers --load-balancer-
arns arn:aws:elasticloadbalancing:us-west-2:123456789012:loadbalancer/app/my-load-
balancer/50dc6c495c0c9188
```

Salida:

```
{
  "LoadBalancers": [
      {
          "Type": "application",
          "Scheme": "internet-facing",
          "IpAddressType": "ipv4",
          "VpcId": "vpc-3ac0fb5f",
          "AvailabilityZones": [
              {
                  "ZoneName": "us-west-2a",
                  "SubnetId": "subnet-8360a9e7"
              },
              {
                  "ZoneName": "us-west-2b",
                  "SubnetId": "subnet-b7d581c0"
              }
          ],
          "CreatedTime": "2016-03-25T21:26:12.920Z",
          "CanonicalHostedZoneId": "Z2P70J7EXAMPLE",
          "DNSName": "my-load-balancer-424835706.us-west-2.elb.amazonaws.com",
          "SecurityGroups": [
```

```
                "sg-5943793c"
            ],
            "LoadBalancerName": "my-load-balancer",
            "State": {
                "Code": "active"
            },
            "LoadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188"
        }
    ]
}
```

Para describir todos los equilibradores de carga

En este ejemplo, se describen todos los equilibradores de carga.

Comando:

```
aws elbv2 describe-load-balancers
```

- Para obtener información sobre la API, consulte DescribeLoadBalancers en la Referencia de comandos de la AWS CLI.

`describe-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-rules`.

AWS CLI

Ejemplo 1: descripción de una regla

En el siguiente ejemplo de `describe-rules`, se muestran los detalles de la regla especificada.

```
aws elbv2 describe-rules \
    --rule-arns arn:aws:elasticloadbalancing:us-west-2:123456789012:listener-rule/
app/my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2/9683b2d02a6cabee
```

Ejemplo 2: descripción de las reglas de un oyente

En el siguiente ejemplo de `describe-rules`, se muestran los detalles de las reglas del oyente especificado. En la salida se incluyen la regla predeterminada y todas las demás reglas que se hayan agregado.

```
aws elbv2 describe-rules \
    --listener-arn arn:aws:elasticloadbalancing:us-west-2:123456789012:listener/app/
my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2
```

- Para obtener información sobre la API, consulte DescribeRules en la Referencia de comandos de la AWS CLI.

`describe-ssl-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-ssl-policies`.

AWS CLI

Ejemplo 1: enumeración de las políticas utilizadas para la negociación de SSL por tipo de equilibrador de carga

En el siguiente ejemplo de `describe-ssl-policies`, se muestran los nombres de las políticas que puede usar para la negociación de SSL con un equilibrador de carga de aplicación. En el ejemplo se usa el parámetro `--query` para mostrar solo los nombres de las políticas.

```
aws elbv2 describe-ssl-policies \
    --load-balancer-type application \
    --query SslPolicies[*].Name
```

Salida:

```
[
    "ELBSecurityPolicy-2016-08",
    "ELBSecurityPolicy-TLS13-1-2-2021-06",
    "ELBSecurityPolicy-TLS13-1-2-Res-2021-06",
    "ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06",
    "ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06",
    "ELBSecurityPolicy-TLS13-1-1-2021-06",
    "ELBSecurityPolicy-TLS13-1-0-2021-06",
    "ELBSecurityPolicy-TLS13-1-3-2021-06",
    "ELBSecurityPolicy-TLS-1-2-2017-01",
    "ELBSecurityPolicy-TLS-1-1-2017-01",
    "ELBSecurityPolicy-TLS-1-2-Ext-2018-06",
    "ELBSecurityPolicy-FS-2018-06",
    "ELBSecurityPolicy-2015-05",
    "ELBSecurityPolicy-TLS-1-0-2015-04",
```

```
    "ELBSecurityPolicy-FS-1-2-Res-2019-08",
    "ELBSecurityPolicy-FS-1-1-2019-08",
    "ELBSecurityPolicy-FS-1-2-2019-08",
    "ELBSecurityPolicy-FS-1-2-Res-2020-10"
]
```

Ejemplo 2: enumeración de las políticas que admiten un protocolo específico

En el siguiente ejemplo de `describe-ssl-policies`, se muestran los nombres de las políticas que admiten el protocolo TLS 1.3. En el ejemplo se usa el parámetro `--query` para mostrar solo los nombres de las políticas.

```
aws elbv2 describe-ssl-policies \
    --load-balancer-type application \
    --query SslPolicies[?contains(SslProtocols,'TLSv1.3')].Name
```

Salida:

```
[
    "ELBSecurityPolicy-TLS13-1-2-2021-06",
    "ELBSecurityPolicy-TLS13-1-2-Res-2021-06",
    "ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06",
    "ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06",
    "ELBSecurityPolicy-TLS13-1-1-2021-06",
    "ELBSecurityPolicy-TLS13-1-0-2021-06",
    "ELBSecurityPolicy-TLS13-1-3-2021-06"
]
```

Ejemplo 3: visualización de los cifrados de una política

En el siguiente ejemplo de `describe-ssl-policies`, se muestran los nombres de los cifrados de la política especificada. En el ejemplo se usa el parámetro `--query` para mostrar solo los nombres de los cifrados. Los cifrados aparecen en la lista por orden de prioridad, de tal forma que el primero tiene la prioridad 1.

```
aws elbv2 describe-ssl-policies \
    --names ELBSecurityPolicy-TLS13-1-2-2021-06 \
    --query SslPolicies[*].Ciphers[*].Name
```

Salida:

```
[
    "TLS_AES_128_GCM_SHA256",
    "TLS_AES_256_GCM_SHA384",
    "TLS_CHACHA20_POLY1305_SHA256",
    "ECDHE-ECDSA-AES128-GCM-SHA256",
    "ECDHE-RSA-AES128-GCM-SHA256",
    "ECDHE-ECDSA-AES128-SHA256",
    "ECDHE-RSA-AES128-SHA256",
    "ECDHE-ECDSA-AES256-GCM-SHA384",
    "ECDHE-RSA-AES256-GCM-SHA384",
    "ECDHE-ECDSA-AES256-SHA384",
    "ECDHE-RSA-AES256-SHA384"
]
```

Para obtener más información, consulte Security policies en la Guía del usuario de equilibradores de carga de aplicación.

- Para obtener información sobre la API, consulte DescribeSslPolicies en la Referencia de comandos de la AWS CLI.

`describe-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-tags`.

AWS CLI

Para describir las etiquetas asignadas a un equilibrador de carga

En este ejemplo, se describen las etiquetas asignadas al equilibrador de carga especificado.

Comando:

```
aws elbv2 describe-tags --resource-arns arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188
```

Salida:

```
{
  "TagDescriptions": [
      {
          "ResourceArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188",
```

```
            "Tags": [
                {
                    "Value": "lima",
                    "Key": "project"
                },
                {
                    "Value": "digital-media",
                    "Key": "department"
                }
            ]
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeTags en la Referencia de comandos de la AWS CLI.

`describe-target-group-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-target-group-attributes`.

AWS CLI

Para describir los atributos del grupo de destino

En el siguiente ejemplo de `describe-target-group-attributes`, se muestran los atributos del grupo de destino especificado.

```
aws elbv2 describe-target-group-attributes \
    --target-group-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
```

La salida incluye los atributos si el protocolo es HTTP o HTTPS y el tipo de destino es `instance` o `ip`.

```
{
    "Attributes": [
        {
            "Value": "false",
            "Key": "stickiness.enabled"
```

```
        },
        {
            "Value": "300",
            "Key": "deregistration_delay.timeout_seconds"
        },
        {
            "Value": "lb_cookie",
            "Key": "stickiness.type"
        },
        {
            "Value": "86400",
            "Key": "stickiness.lb_cookie.duration_seconds"
        },
        {
            "Value": "0",
            "Key": "slow_start.duration_seconds"
        }
    ]
}
```

La salida siguiente incluye los atributos si el protocolo es HTTP o HTTPS y el tipo de destino es `lambda`.

```
{
    "Attributes": [
        {
            "Value": "false",
            "Key": "lambda.multi_value_headers.enabled"
        }
    ]
}
```

La salida siguiente incluye los atributos si el protocolo es TCP, TLS, UDP o TCP_UDP.

```
{
    "Attributes": [
        {
            "Value": "false",
            "Key": "proxy_protocol_v2.enabled"
        },
        {
            "Value": "300",
            "Key": "deregistration_delay.timeout_seconds"
```

```
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeTargetGroupAttributes en la Referencia de comandos de la AWS CLI.

`describe-target-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-target-groups`.

AWS CLI

Ejemplo 1: Descripción de un grupo de destino

En el siguiente ejemplo de `describe-target-groups` se muestran los detalles del grupo de destino especificado.

```
aws elbv2 describe-target-groups \
    --target-group-arns arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
```

Salida:

```
{
    "TargetGroups": [
        {
            "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067",
            "TargetGroupName": "my-targets",
            "Protocol": "HTTP",
            "Port": 80,
            "VpcId": "vpc-3ac0fb5f",
            "HealthCheckProtocol": "HTTP",
            "HealthCheckPort": "traffic-port",
            "HealthCheckEnabled": true,
            "HealthCheckIntervalSeconds": 30,
            "HealthCheckTimeoutSeconds": 5,
            "HealthyThresholdCount": 5,
            "UnhealthyThresholdCount": 2,
            "HealthCheckPath": "/",
            "Matcher": {
```

```
                "HttpCode": "200"
            },
            "LoadBalancerArns": [
                "arn:aws:elasticloadbalancing:us-west-2:123456789012:loadbalancer/
app/my-load-balancer/50dc6c495c0c9188"
            ],
            "TargetType": "instance",
            "ProtocolVersion": "HTTP1",
            "IpAddressType": "ipv4"
        }
    ]
}
```

Ejemplo 2: descripción de todos los grupos de destino de un equilibrador de carga

En el siguiente ejemplo de `describe-target-groups` se muestran los detalles de todos los grupos de destino del equilibrador de cargas especificado. En el ejemplo se usa el parámetro `--query` para mostrar solo los nombres de los grupos de destino.

```
aws elbv2 describe-target-groups \
    --load-balancer-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188 \
    --query TargetGroups[*].TargetGroupName
```

Salida:

```
[
    "my-instance-targets",
    "my-ip-targets",
    "my-lambda-target"
]
```

Para obtener más información, consulte Target groups en la Guía del usuario de equilibradores de carga de aplicación.

- Para obtener información sobre la API, consulte DescribeTargetGroups en la Referencia de comandos de la AWS CLI.

`describe-target-health`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-target-health`.

AWS CLI

Ejemplo 1: Descripción del estado de los destinos para un grupo de destino

En el siguiente ejemplo de `describe-target-health` se muestran los detalles del estado de los destinos del grupo de destino especificado. Estos destinos se encuentran en buen estado.

```
aws elbv2 describe-target-health \
    --target-group-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
```

Salida:

```
{
    "TargetHealthDescriptions": [
        {
            "HealthCheckPort": "80",
            "Target": {
                "Id": "i-ceddcd4d",
                "Port": 80
            },
            "TargetHealth": {
                "State": "healthy"
            }
        },
        {
            "HealthCheckPort": "80",
            "Target": {
                "Id": "i-0f76fade",
                "Port": 80
            },
            "TargetHealth": {
                "State": "healthy"
            }
        }
    ]
}
```

Ejemplo 2: descripción del estado de un destino

En el siguiente ejemplo de `describe-target-health` se muestran los detalles del estado del destino especificado. Este destino se encuentra en buen estado.

```
aws elbv2 describe-target-health \
    --targets Id=i-0f76fade,Port=80 \
    --target-group-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
```

Salida:

```
{
    "TargetHealthDescriptions": [
        {
            "HealthCheckPort": "80",
            "Target": {
                "Id": "i-0f76fade",
                "Port": 80
            },
            "TargetHealth": {
                "State": "healthy"
            }
        }
    ]
}
```

La siguiente salida de ejemplo es para un destino cuyo grupo de destino no está especificado en una acción para un oyente. Este destino no puede recibir el tráfico del equilibrador de carga.

```
{
    "TargetHealthDescriptions": [
    {
        "HealthCheckPort": "80",
        "Target": {
            "Id": "i-0f76fade",
            "Port": 80
        },
            "TargetHealth": {
                "State": "unused",
                "Reason": "Target.NotInUse",
                "Description": "Target group is not configured to receive traffic
 from the load balancer"
            }
        }
    ]
}
```

La siguiente salida de ejemplo es para un destino cuyo grupo de destino no se especificó en una acción para un oyente. El destino sigue registrado.

```
{
    "TargetHealthDescriptions": [
        {
            "HealthCheckPort": "80",
            "Target": {
                "Id": "i-0f76fade",
                "Port": 80
            },
            "TargetHealth": {
                "State": "initial",
                "Reason": "Elb.RegistrationInProgress",
                "Description": "Target registration is in progress"
            }
        }
    ]
}
```

El siguiente ejemplo de salida es un destino en mal estado.

```
{
    "TargetHealthDescriptions": [
        {
            "HealthCheckPort": "80",
            "Target": {
                "Id": "i-0f76fade",
                "Port": 80
            },
            "TargetHealth": {
                "State": "unhealthy",
                "Reason": "Target.Timeout",
                "Description": "Connection to target timed out"
            }
        }
    ]
}
```

La siguiente salida de ejemplo es para un destino que es una función de Lambda y las comprobaciones de estado están deshabilitadas.

```
{
    "TargetHealthDescriptions": [
        {
            "Target": {
                "Id": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
                "AvailabilityZone": "all",
            },
            "TargetHealth": {
                "State": "unavailable",
                "Reason": "Target.HealthCheckDisabled",
                "Description": "Health checks are not enabled for this target"
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeTargetHealth en la Referencia de comandos de la AWS CLI.

`modify-listener`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-listener`.

AWS CLI

Ejemplo 1: cambio de la acción predeterminada por una acción de reenvío

En el siguiente ejemplo de `modify-listener`, se cambia la acción predeterminada por una acción `forward` para el oyente especificado.

```
aws elbv2 modify-listener \
    --listener-arn arn:aws:elasticloadbalancing:us-west-2:123456789012:listener/app/my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2 \
    --default-actions Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:us-west-2:123456789012:targetgroup/my-new-targets/2453ed029918f21f
```

Salida:

```
{
    "Listeners": [
        {
```

```
            "ListenerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:listener/app/my-load-balancer/50dc6c495c0c9188/
f2f7dc8efc522ab2",
            "LoadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188",
            "Protocol": "HTTP",
            "Port": 80,
            "DefaultActions": [
                {
                    "Type": "forward",
                    "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-new-targets/2453ed029918f21f"
                }
            ]
        }
    ]
}
```

Ejemplo 2: cambio de la acción predeterminada por una acción de redireccionamiento

En el siguiente ejemplo de `modify-listener`, se cambia la acción predeterminada por una acción `redirect` para el oyente especificado.

```
aws elbv2 modify-listener \
    --listener-arn arn:aws:elasticloadbalancing:us-west-2:123456789012:listener/app/
my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2 \
    --default-actions Type=redirect,
 RedirectConfig='{Protocol=HTTPS,StatusCode=HTTP_302}'
```

Salida:

```
{
    "Listeners": [
        {
            "ListenerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:listener/app/my-load-balancer/50dc6c495c0c9188/
f2f7dc8efc522ab2",
            "LoadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188",
            "Protocol": "HTTP",
            "Port": 80,
            "DefaultActions": [
                {
```

```
                    "Type": "redirect",
                    "RedirectConfig": {
                        "Protocol": "HTTPS",
                        "Port": "#{port}",
                        "Host": "#{host}",
                        "Path": "/#{path}",
                        "Query": "#{query}",
                        "StatusCode": "HTTP_302",
                    }
                }
            ]
        }
    ]
}
```

Ejemplo 3: cambio del certificado del servidor

En el siguiente ejemplo de `modify-listener`, se cambia el certificado del servidor del oyente de HTTPS especificado.

```
aws elbv2 modify-listener \
    --listener-arn arn:aws:elasticloadbalancing:us-west-2:123456789012:listener/app/my-load-balancer/50dc6c495c0c9188/0467ef3c8400ae65 \
    --certificates CertificateArn=arn:aws:iam::123456789012:server-certificate/my-new-server-cert
```

Salida:

```
{
    "Listeners": [
        {
            "ListenerArn": "arn:aws:elasticloadbalancing:us-west-2:123456789012:listener/app/my-load-balancer/50dc6c495c0c9188/0467ef3c8400ae65",
            "LoadBalancerArn": "arn:aws:elasticloadbalancing:us-west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188",
            "Protocol": "HTTPS",
            "Port": 443,
            "DefaultActions": [
                {
                    "Type": "forward",
                    "TargetGroupArn": "arn:aws:elasticloadbalancing:us-west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067"
```

```
                }
            ],
            "SslPolicy": "ELBSecurityPolicy-2015-05",
            "Certificates": [
                {
                    "CertificateArn": "arn:aws:iam::123456789012:server-certificate/
my-new-server-cert"
                }
            ],
        }
    ]
}
```

Para obtener más información, consulte Reglas del oyente en la Guía del usuario de equilibradores de carga de aplicaciones.

- Para obtener información sobre la API, consulte ModifyListener en la Referencia de comandos de la AWS CLI.

`modify-load-balancer-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-load-balancer-attributes`.

AWS CLI

Para habilitar la protección contra eliminación

En este ejemplo, se habilita la protección contra eliminación del equilibrador de carga especificado.

Comando:

```
aws elbv2 modify-load-balancer-attributes --load-balancer-
arn arn:aws:elasticloadbalancing:us-west-2:123456789012:loadbalancer/app/my-load-
balancer/50dc6c495c0c9188 --attributes Key=deletion_protection.enabled,Value=true
```

Salida:

```
{
  "Attributes": [
      {
```

```
            "Value": "true",
            "Key": "deletion_protection.enabled"
        },
        {
            "Value": "false",
            "Key": "access_logs.s3.enabled"
        },
        {
            "Value": "60",
            "Key": "idle_timeout.timeout_seconds"
        },
        {
            "Value": "",
            "Key": "access_logs.s3.prefix"
        },
        {
            "Value": "",
            "Key": "access_logs.s3.bucket"
        }
    ]
}
```

Para cambiar el tiempo de espera de inactividad

En este ejemplo, se cambia el valor del tiempo de espera de inactividad del equilibrador de carga especificado.

Comando:

```
aws elbv2 modify-load-balancer-attributes --load-balancer-
arn arn:aws:elasticloadbalancing:us-west-2:123456789012:loadbalancer/app/my-load-
balancer/50dc6c495c0c9188 --attributes Key=idle_timeout.timeout_seconds,Value=30
```

Salida:

```
{
    "Attributes": [
        {
            "Value": "30",
            "Key": "idle_timeout.timeout_seconds"
        },
        {
            "Value": "false",
```

```
            "Key": "access_logs.s3.enabled"
        },
        {
            "Value": "",
            "Key": "access_logs.s3.prefix"
        },
        {
            "Value": "true",
            "Key": "deletion_protection.enabled"
        },
        {
            "Value": "",
            "Key": "access_logs.s3.bucket"
        }
    ]
}
```

Para habilitar los registros de acceso

En este ejemplo, se habilitan los registros de acceso del equilibrador de carga especificado. Tenga en cuenta que el bucket de S3 debe existir en la misma región que el equilibrador de carga. Además, debe tener asociada una política que conceda acceso al servicio Elastic Load Balancing.

Comando:

```
aws elbv2 modify-load-balancer-attributes --load-balancer-
arn arn:aws:elasticloadbalancing:us-west-2:123456789012:loadbalancer/app/my-load-
balancer/50dc6c495c0c9188 --
attributes Key=access_logs.s3.enabled,Value=true Key=access_logs.s3.bucket,Value=my-
loadbalancer-logs Key=access_logs.s3.prefix,Value=myapp
```

Salida:

```
{
    "Attributes": [
        {
            "Value": "true",
            "Key": "access_logs.s3.enabled"
        },
        {
            "Value": "my-load-balancer-logs",
```

```
            "Key": "access_logs.s3.bucket"
        },
        {
            "Value": "myapp",
            "Key": "access_logs.s3.prefix"
        },
        {
            "Value": "60",
            "Key": "idle_timeout.timeout_seconds"
        },
        {
            "Value": "false",
            "Key": "deletion_protection.enabled"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ModifyLoadBalancerAttributes en la Referencia de comandos de la AWS CLI.

`modify-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-rule`.

AWS CLI

Para modificar una regla

En el siguiente de ejemplo de `modify-rule`, se actualizan las acciones y las condiciones de la regla especificada.

```
aws elbv2 modify-rule \
  --actions Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067 \
  --conditions Field=path-pattern,Values='/images/*'
  --rule-arn arn:aws:elasticloadbalancing:us-west-2:123456789012:listener-rule/app/
my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2/9683b2d02a6cabee
```

Salida:

```
{
    "Rules": [
```

```
        {
            "Priority": "10",
            "Conditions": [
                {
                    "Field": "path-pattern",
                    "Values": [
                        "/images/*"
                    ]
                }
            ],
            "RuleArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:listener-rule/app/my-load-balancer/50dc6c495c0c9188/
f2f7dc8efc522ab2/9683b2d02a6cabee",
            "IsDefault": false,
            "Actions": [
                {
                    "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067",
                    "Type": "forward"
                }
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte ModifyRule en la Referencia de comandos de la AWS CLI.

`modify-target-group-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-target-group-attributes`.

AWS CLI

Para modificar el tiempo de espera de anulación de registro

En este ejemplo, el tiempo de espera de anulación de registro se establece en el valor especificado para el grupo de destino especificado.

Comando:

```
aws elbv2 modify-target-group-attributes --target-group-
arn arn:aws:elasticloadbalancing:us-west-2:123456789012:targetgroup/my-
```

```
targets/73e2d6bc24d8a067 --
attributes Key=deregistration_delay.timeout_seconds,Value=600
```

Salida:

```
{
  "Attributes": [
      {
          "Value": "false",
          "Key": "stickiness.enabled"
      },
      {
          "Value": "600",
          "Key": "deregistration_delay.timeout_seconds"
      },
      {
          "Value": "lb_cookie",
          "Key": "stickiness.type"
      },
      {
          "Value": "86400",
          "Key": "stickiness.lb_cookie.duration_seconds"
      }
  ]
}
```

- Para obtener información sobre la API, consulte ModifyTargetGroupAttributes en la Referencia de comandos de la AWS CLI.

`modify-target-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-target-group`.

AWS CLI

Para modificar la configuración de comprobación de estado de un grupo de destino

En el siguiente ejemplo de `modify-target-group`, se cambia la configuración de las comprobaciones de estado utilizadas para evaluar el estado de los destinos del grupo de destino especificado. Tenga en cuenta que, debido a la forma en que la CLI analiza las comas, el intervalo de la opción `--matcher` debe ir entre comillas simples en lugar de dobles.

```
aws elbv2 modify-target-group \
    --target-group-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-https-targets/2453ed029918f21f \
    --health-check-protocol HTTPS \
    --health-check-port 443 \
    --matcher HttpCode='200,299'
```

Salida:

```
{
    "TargetGroups": [
        {
            "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-https-targets/2453ed029918f21f",
            "TargetGroupName": "my-https-targets",
            "Protocol": "HTTPS",
            "Port": 443,
            "VpcId": "vpc-3ac0fb5f",
            "HealthCheckProtocol": "HTTPS",
            "HealthCheckPort": "443",
            "HealthCheckEnabled": true,
            "HealthCheckIntervalSeconds": 30,
            "HealthCheckTimeoutSeconds": 5,
            "HealthyThresholdCount": 5,
            "UnhealthyThresholdCount": 2,
            "Matcher": {
                "HttpCode": "200,299"
            },
            "LoadBalancerArns": [
                "arn:aws:elasticloadbalancing:us-west-2:123456789012:loadbalancer/
app/my-load-balancer/50dc6c495c0c9188"
            ],
            "TargetType": "instance",
            "ProtocolVersion": "HTTP1",
            "IpAddressType": "ipv4"
        }
    ]
}
```

Para obtener más información, consulte Target groups en la Guía del usuario de equilibradores de carga de aplicación.

- Para obtener información sobre la API, consulte ModifyTargetGroup en la Referencia de comandos de la AWS CLI.

`register-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-targets`.

AWS CLI

Ejemplo 1: registro de destinos en un grupo de destino por ID de instancia

En el siguiente ejemplo de `register-targets`, se registran las instancias especificadas en un grupo de destino. El grupo de destino debe tener el tipo de destino `instance`.

```
aws elbv2 register-targets \
    --target-group-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067 \
    --targets Id=i-1234567890abcdef0 Id=i-0abcdef1234567890
```

Ejemplo 2: registro de destinos en un grupo de destino mediante anulaciones de puertos

En el siguiente ejemplo de `register-targets`, se registra la instancia especificada en un grupo de destino mediante varios puertos. Esto permite registrar los contenedores en la misma instancia que los destinos del grupo de destino.

```
aws elbv2 register-targets \
    --target-group-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-internal-targets/3bb63f11dfb0faf9 \
    --targets Id=i-0598c7d356eba48d7,Port=80 Id=i-0598c7d356eba48d7,Port=766
```

Ejemplo 3: registro de destinos en un grupo de destino por dirección IP

En el siguiente ejemplo de `register-targets`, se registran las direcciones IP especificadas en un grupo de destino. El grupo de destino debe tener el tipo de destino `ip`.

```
aws elbv2 register-targets \
    --target-group-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-tcp-ip-targets/8518e899d173178f \
    --targets Id=10.0.1.15 Id=10.0.1.23
```

Ejemplo 4: registro de una función de Lambda como destino

En el siguiente ejemplo de `register-targets`, se registran las direcciones IP especificadas en un grupo de destino. El grupo de destino debe tener el tipo de destino `lambda`. Es preciso conceder permisos a Elastic Load Balancing para invocar la función de Lambda.

```
aws elbv2 register-targets \
    --target-group-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-tcp-ip-targets/8518e899d173178f \
    --targets Id=arn:aws:lambda:us-west-2:123456789012:function:my-function
```

- Para obtener información sobre la API, consulte RegisterTargets en la Referencia de comandos de la AWS CLI.

`remove-listener-certificates`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-listener-certificates`.

AWS CLI

Para eliminar un certificado de un oyente seguro

En este ejemplo, se elimina el certificado especificado del oyente seguro especificado.

Comando:

```
aws elbv2 remove-listener-certificates --listener-
arn arn:aws:elasticloadbalancing:us-west-2:123456789012:listener/
app/my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2 --
certificates CertificateArn=arn:aws:acm:us-west-2:123456789012:certificate/5cc54884-
f4a3-4072-80be-05b9ba72f705
```

- Para obtener información sobre la API, consulte RemoveListenerCertificates en la Referencia de comandos de la AWS CLI.

`remove-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-tags`.

AWS CLI

Para eliminar etiquetas de un equilibrador de carga

En el siguiente ejemplo de `remove-tags`, se eliminan las etiquetas `project` y `department` del equilibrador de carga especificado.

```
aws elbv2 remove-tags \
    --resource-arns arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188 \
    --tag-keys project department
```

- Para obtener información sobre la API, consulte RemoveTags en la Referencia de comandos de la AWS CLI.

`set-ip-address-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-ip-address-type`.

AWS CLI

Para establecer el tipo de dirección de un equilibrador de carga

En este ejemplo, se establece en `dualstack` el tipo de dirección del equilibrador de carga especificado. Las subredes del equilibrador de carga deben tener asociados bloques de CIDR de IPv6.

Comando:

```
aws elbv2 set-ip-address-type --load-balancer-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188 --ip-address-
type dualstack
```

Salida:

```
{
    "IpAddressType": "dualstack"
}
```

- Para obtener información sobre la API, consulte SetIpAddressType en la Referencia de comandos de la AWS CLI.

`set-rule-priorities`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-rule-priorities`.

AWS CLI

Para establecer la prioridad de la regla

En este ejemplo, se establece la prioridad de la regla especificada.

Comando:

```
aws elbv2 set-rule-priorities --rule-
priorities RuleArn=arn:aws:elasticloadbalancing:us-west-2:123456789012:listener-
rule/app/my-load-balancer/50dc6c495c0c9188/
f2f7dc8efc522ab2/1291d13826f405c3,Priority=5
```

Salida:

```
{
  "Rules": [
      {
          "Priority": "5",
          "Conditions": [
              {
                  "Field": "path-pattern",
                  "Values": [
                      "/img/*"
                  ]
              }
          ],
          "RuleArn": "arn:aws:elasticloadbalancing:us-west-2:123456789012:listener-
rule/app/my-load-balancer/50dc6c495c0c9188/f2f7dc8efc522ab2/1291d13826f405c3",
          "IsDefault": false,
          "Actions": [
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067",
                  "Type": "forward"
              }
          ]
      }
  ]
}
```

- Para obtener información sobre la API, consulte SetRulePriorities en la Referencia de comandos de la AWS CLI.

`set-security-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-security-groups`.

AWS CLI

Para asociar un grupo de seguridad a un equilibrador de carga

En este ejemplo, se asocia el grupo de seguridad especificado al equilibrador de carga especificado.

Comando:

```
aws elbv2 set-security-groups --load-balancer-arn arn:aws:elasticloadbalancing:us-west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188 --security-groups sg-5943793c
```

Salida:

```
{
  "SecurityGroupIds": [
      "sg-5943793c"
  ]
}
```

- Para obtener información sobre la API, consulte SetSecurityGroups en la Referencia de comandos de la AWS CLI.

`set-subnets`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-subnets`.

AWS CLI

Para habilitar las zonas de disponibilidad para un equilibrador de carga

En este ejemplo, se habilita la zona de disponibilidad de la subred especificada para el equilibrador de carga especificado.

Comando:

```
aws elbv2 set-subnets --load-balancer-arn arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/50dc6c495c0c9188 --
subnets subnet-8360a9e7 subnet-b7d581c0
```

Salida:

```
{
  "AvailabilityZones": [
      {
          "SubnetId": "subnet-8360a9e7",
          "ZoneName": "us-west-2a"
      },
      {
          "SubnetId": "subnet-b7d581c0",
          "ZoneName": "us-west-2b"
      }
  ]
}
```

- Para obtener información sobre la API, consulte SetSubnets en la Referencia de comandos de la AWS CLI.

Ejemplos de ElastiCache que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con ElastiCache.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-tags-to-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-tags-to-resource`.

AWS CLI

Para agregar etiquetas a un recurso

En el siguiente ejemplo de `add-tags-to-resource`, se agregan hasta 10 etiquetas, pares clave-valor, a un clúster o recurso de instantánea.

```
aws elasticache add-tags-to-resource \
    --resource-name "arn:aws:elasticache:us-east-1:1234567890:cluster:my-mem-cluster" \
    --tags '{"20150202":15, "ElastiCache":"Service"}'
```

Salida:

```
{
    "TagList": [
        {
            "Value": "20150202",
            "Key": "APIVersion"
        },
        {
            "Value": "ElastiCache",
            "Key": "Service"
        }
    ]
}
```

Para obtener más información, consulte Monitoring Costs with Cost Allocation Tags en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte AddTagsToResource en la Referencia de comandos de la AWS CLI.

`authorize-cache-security-group-ingress`

En el siguiente ejemplo de código, se muestra cómo utilizar `authorize-cache-security-group-ingress`.

AWS CLI

Para autorizar el grupo de seguridad de caché para entrada

En el siguiente ejemplo de `authorize-cache-security-group-ingress`, se permite la entrada de red a un grupo de seguridad de caché.

```
aws elasticache authorize-cache-security-group-ingress \
     --cache-security-group-name  "my-sec-grp" \
     --ec2-security-group-name "my-ec2-sec-grp" \
     --ec2-security-group-owner-id "1234567890"
```

El comando no genera ninguna salida.

Para obtener más información, consulte Self-Service Updates in Amazon ElastiCache en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte AuthorizeCacheSecurityGroupIngress en la Referencia de comandos de la AWS CLI.

`batch-apply-update-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-apply-update-action`.

AWS CLI

Para aplicar una actualización de servicio

En el siguiente ejemplo de `batch-apply-update-action`, se aplica una actualización de servicio a un clúster de Redis.

```
aws elasticache batch-apply-update-action \
    --service-update-name elc-xxxxx406-xxx \
    --replication-group-ids test-cluster
```

Salida:

```
{
    "ProcessedUpdateActions": [
        {
            "ReplicationGroupId": "pat-cluster",
            "ServiceUpdateName": "elc-xxxxx406-xxx",
            "UpdateActionStatus": "waiting-to-start"
        }
    ],
    "UnprocessedUpdateActions": []
}
```

Para obtener más información, consulte Self-Service Updates in Amazon ElastiCache en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte BatchApplyUpdateAction en la Referencia de comandos de la AWS CLI.

`batch-stop-update-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-stop-update-action`.

AWS CLI

Para detener una actualización de servicio

En el siguiente ejemplo de `batch-stop-update-action`, se aplica una actualización de servicio a un clúster de Redis.

```
aws elasticache batch-stop-update-action \
    --service-update-name elc-xxxxx406-xxx \
    --replication-group-ids test-cluster
```

Salida:

```
{
    "ProcessedUpdateActions": [
        {
            "ReplicationGroupId": "pat-cluster",
            "ServiceUpdateName": "elc-xxxxx406-xxx",
            "UpdateActionStatus": "stopping"
        }
```

```
    ],
    "UnprocessedUpdateActions": []
}
```

Para obtener más información, consulte Self-Service Updates in Amazon ElastiCache en la Guía del usuario de ElastiCache.

- Para obtener detalles sobre la API, consulte BatchStopUpdateAction en la Referencia de comandos de la AWS CLI.

`copy-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-snapshot`.

AWS CLI

Para copiar una instantánea

En el ejemplo siguiente de `copy-snapshot`, se realiza una copia de una instantánea existente.

```
aws elasticache copy-snapshot \
    --source-snapshot-name "my-snapshot" \
    --target-snapshot-name "my-snapshot-copy"
```

Salida:

```
{
    "Snapshot":{
        "Engine": "redis",
        "CacheParameterGroupName": "default.redis3.2",
        "VpcId": "vpc-3820329f3",
        "CacheClusterId": "my-redis4",
        "SnapshotRetentionLimit": 7,
        "NumCacheNodes": 1,
        "SnapshotName": "my-snapshot-copy",
        "CacheClusterCreateTime": "2016-12-21T22:24:04.955Z",
        "AutoMinorVersionUpgrade": true,
        "PreferredAvailabilityZone": "us-east-1c",
        "SnapshotStatus": "creating",
        "SnapshotSource": "manual",
        "SnapshotWindow": "07:00-08:00",
        "EngineVersion": "3.2.4",
```

```
        "NodeSnapshots": [
            {
                "CacheSize": "3 MB",
                "SnapshotCreateTime": "2016-12-28T07:00:52Z",
                "CacheNodeId": "0001",
                "CacheNodeCreateTime": "2016-12-21T22:24:04.955Z"
            }
        ],
        "CacheSubnetGroupName": "default",
        "Port": 6379,
        "PreferredMaintenanceWindow": "tue:09:30-tue:10:30",
        "CacheNodeType": "cache.m3.large"
    }
}
```

Para obtener más información, consulte Exporting a Backup en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte CopySnapshot en la Referencia de comandos de la AWS CLI.

`create-cache-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-cache-cluster`.

AWS CLI

Para crear un clúster de caché

En el siguiente ejemplo de `create-cache-cluster`, se crea un clúster de caché mediante el motor de Redis.

```
aws elasticache create-cache-cluster \
    --cache-cluster-id "cluster-test" \
    --engine redis \
    --cache-node-type cache.m5.large \
    --num-cache-nodes 1
```

Salida:

```
{
    "CacheCluster": {
```

```
        "CacheClusterId": "cluster-test",
        "ClientDownloadLandingPage": "https://console.aws.amazon.com/elasticache/
home#client-download:",
        "CacheNodeType": "cache.m5.large",
        "Engine": "redis",
        "EngineVersion": "5.0.5",
        "CacheClusterStatus": "creating",
        "NumCacheNodes": 1,
        "PreferredMaintenanceWindow": "sat:13:00-sat:14:00",
        "PendingModifiedValues": {},
        "CacheSecurityGroups": [],
        "CacheParameterGroup": {
            "CacheParameterGroupName": "default.redis5.0",
            "ParameterApplyStatus": "in-sync",
            "CacheNodeIdsToReboot": []
        },
        "CacheSubnetGroupName": "default",
        "AutoMinorVersionUpgrade": true,
        "SnapshotRetentionLimit": 0,
        "SnapshotWindow": "06:30-07:30",
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
}
```

Para obtener más información, consulte Creating a Cluster en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte CreateCacheCluster en la Referencia de comandos de la AWS CLI.

`create-cache-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-cache-parameter-group`.

AWS CLI

Para crear un grupo de parámetros de caché

En el siguiente ejemplo de `create-cache-parameter-group`, se crea un nuevo grupo de parámetros de caché de Amazon ElastiCache.

```
aws elasticache create-cache-parameter-group \
    --cache-parameter-group-family "redis5.0" \
```

```
    --cache-parameter-group-name "mygroup" \
    --description "mygroup"
```

Salida:

```
{
    "CacheParameterGroup": {
        "CacheParameterGroupName": "mygroup",
        "CacheParameterGroupFamily": "redis5.0",
        "Description": "my group"
    }
}
```

Para obtener más información, consulte Creating a Parameter Group en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte CreateCacheParameterGroup en la Referencia de comandos de la AWS CLI.

`create-cache-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-cache-subnet-group`.

AWS CLI

Para crear un grupo de subredes de caché

En el siguiente ejemplo de `create-cache-subnet-group`, se crea un nuevo grupo de subred de caché.

```
aws elasticache create-cache-subnet-group \
    --cache-subnet-group-name "mygroup" \
    --cache-subnet-group-description "my subnet group" \
    --subnet-ids "subnet-xxxxec4f"
```

Salida:

```
{
    "CacheSubnetGroup": {
        "CacheSubnetGroupName": "mygroup",
        "CacheSubnetGroupDescription": "my subnet group",
```

```
        "VpcId": "vpc-a3e97cdb",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-xxxxec4f",
                "SubnetAvailabilityZone": {
                    "Name": "us-west-2d"
                }
            }
        ]
    }
}
```

Para obtener más información, consulte Creating a Cache Subnet Group en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte CreateCacheSubnetGroup en la Referencia de comandos de la AWS CLI.

`create-global-replication-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-global-replication-group`.

AWS CLI

Para crear un grupo de replicación global

En el siguiente ejemplo de `create-global-replication-group`, se crea un nuevo grupo de replicación global.

```
aws elasticache create-global-replication-group \
    --global-replication-group-id-suffix my-global-replication-group \
    --primary-replication-group-id my-primary-cluster
```

Salida:

```
{
    "GlobalReplicationGroup": {
        "GlobalReplicationGroupId": "sgaui-my-global-replication-group",
        "GlobalReplicationGroupDescription": " ",
        "Status": "creating",
        "CacheNodeType": "cache.r5.large",
```

```
        "Engine": "redis",
        "EngineVersion": "5.0.6",
        "Members": [
            {
                "ReplicationGroupId": "my-primary-cluster",
                "ReplicationGroupRegion": "us-west-2",
                "Role": "PRIMARY",
                "AutomaticFailover": "enabled",
                "Status": "associating"
            }
        ],
        "ClusterEnabled": true,
        "GlobalNodeGroups": [
            {
                "GlobalNodeGroupId": "sgaui-my-global-replication-group-0001",
                "Slots": "0-16383"
            }
        ],
        "AuthTokenEnabled": false,
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
}
```

Para obtener más información, consulte Replication Across AWS Regions Using Global Datastore en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte CreateGlobalReplicationGroup en la Referencia de comandos de la AWS CLI.

`create-replication-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-replication-group`.

AWS CLI

Para crear un grupo de replicación

En el siguiente ejemplo de `create-replication-group`, se crea un grupo de replicación de Redis (modo de clúster deshabilitado) o Redis (modo de clúster habilitado). Esta operación solo es válida para Redis.

```
aws elasticache create-replication-group \
```

```
    --replication-group-id "mygroup" \
    --replication-group-description "my group" \
    --engine "redis" \
    --cache-node-type "cache.m5.large"
```

Salida:

```
{
    "ReplicationGroup": {
        "ReplicationGroupId": "mygroup",
        "Description": "my group",
        "Status": "creating",
        "PendingModifiedValues": {},
        "MemberClusters": [
            "mygroup-001"
        ],
        "AutomaticFailover": "disabled",
        "SnapshotRetentionLimit": 0,
        "SnapshotWindow": "06:00-07:00",
        "ClusterEnabled": false,
        "CacheNodeType": "cache.m5.large",
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
}
```

Para obtener más información, consulte Creating a Redis Replication Group en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte CreateReplicationGroup en la Referencia de comandos de la AWS CLI.

`create-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-snapshot`.

AWS CLI

Para crear una instantánea

En el siguiente ejemplo de `create-snapshot`, se crea una instantánea mediante el motor de Redis.

```
aws elasticache create-snapshot \
    --snapshot-name mysnapshot \
    --cache-cluster-id cluster-test
```

Salida:

```
{
    "Snapshot": {
        "SnapshotName": "mysnapshot",
        "CacheClusterId": "cluster-test",
        "SnapshotStatus": "creating",
        "SnapshotSource": "manual",
        "CacheNodeType": "cache.m5.large",
        "Engine": "redis",
        "EngineVersion": "5.0.5",
        "NumCacheNodes": 1,
        "PreferredAvailabilityZone": "us-west-2b",
        "CacheClusterCreateTime": "2020-03-19T03:12:01.483Z",
        "PreferredMaintenanceWindow": "sat:13:00-sat:14:00",
        "Port": 6379,
        "CacheParameterGroupName": "default.redis5.0",
        "CacheSubnetGroupName": "default",
        "VpcId": "vpc-a3e97cdb",
        "AutoMinorVersionUpgrade": true,
        "SnapshotRetentionLimit": 0,
        "SnapshotWindow": "06:30-07:30",
        "NodeSnapshots": [
            {
                "CacheNodeId": "0001",
                "CacheSize": "",
                "CacheNodeCreateTime": "2020-03-19T03:12:01.483Z"
            }
        ]
    }
}
```

Para obtener más información, consulte Backup and Restore for ElastiCache for Redis en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte CreateSnapshot en la Referencia de comandos de la AWS CLI.

`create-user-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-user-group`.

AWS CLI

Para crear un grupo de usuarios

En el siguiente ejemplo de `create-user-group`, se crea un nuevo grupo de usuarios.

```
aws elasticache create-user-group \
    --user-group-id myusergroup \
    --engine redis \
    --user-ids default
```

Salida:

```
{
    "UserGroupId": "myusergroup",
    "Status": "creating",
    "Engine": "redis",
    "UserIds": [
        "default"
    ],
    "ReplicationGroups": [],
    "ARN": "arn:aws:elasticache:us-west-2:xxxxxxxxxx52:usergroup:myusergroup"
}
```

Para obtener más información, consulte Authenticating Users with Role-Based Access Control (RBAC) en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte CreateUserGroup en la Referencia de comandos de la AWS CLI.

`create-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-user`.

AWS CLI

Para crear un usuario

En el siguiente ejemplo de `create-user` se crea un nuevo usuario.

```
aws elasticache create-user \
    --user-id user1 \
    --user-name myUser \
    --passwords mYnuUzrpAxXw2rdzx \
    --engine redis \
    --access-string "on ~app::* -@all +@read"
```

Salida:

```
{
    "UserId": "user2",
    "UserName": "myUser",
    "Status": "active",
    "Engine": "redis",
    "AccessString": "on ~app::* -@all +@read +@hash +@bitmap +@geo -setbit -bitfield
 -hset -hsetnx -hmset -hincrby -hincrbyfloat -hdel -bitop -geoadd -georadius -
georadiusbymember",
    "UserGroupIds": [],
    "Authentication": {
        "Type": "password",
        "PasswordCount": 1
    },
    "ARN": "arn:aws:elasticache:us-west-2:xxxxxxxxxx52:user:user2"
}
```

Para obtener más información, consulte Authenticating Users with Role-Based Access Control (RBAC) en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte CreateUser en la Referencia de comandos de la AWS CLI.

`decrease-node-groups-in-global-replication-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `decrease-node-groups-in-global-replication-group`.

AWS CLI

Para disminuir el número de grupos de nodos en un grupo de replicación global

El siguiente `decrease-node-groups-in-global-replication-group` reduce el recuento de grupos de nodos mediante el motor de Redis.

```
aws elasticache decrease-node-groups-in-global-replication-group \
    --global-replication-group-id sgaui-test \
    --node-group-count 1 \
    --apply-immediately \
    --global-node-groups-to-retain sgaui-test-0003
```

Salida:

```
{
    "GlobalReplicationGroup":
    {
        "GlobalReplicationGroupId": "sgaui-test",
        "GlobalReplicationGroupDescription": "test",
        "Status": "modifying",
        "CacheNodeType": "cache.r5.large",
        "Engine": "redis",
        "EngineVersion": "5.0.6",
        "Members": [
            {
                "ReplicationGroupId": "test-2",
                "ReplicationGroupRegion": "us-east-1",
                "Role": "SECONDARY",
                "AutomaticFailover": "enabled",
                "Status": "associated"
            },
            {
                "ReplicationGroupId": "test-1",
                "ReplicationGroupRegion": "us-west-2",
                "Role": "PRIMARY",
                "AutomaticFailover": "enabled",
                "Status": "associated"
            }
        ],
        "ClusterEnabled": true,
        "GlobalNodeGroups": [
            {
                "GlobalNodeGroupId": "sgaui-test-0001",
                "Slots": "0-449,1816-5461"
            },
            {
```

```
                "GlobalNodeGroupId": "sgaui-test-0002",
                "Slots": "6827-10922"
            },
            {
                "GlobalNodeGroupId": "sgaui-test-0003",
                "Slots": "10923-14052,15418-16383"
            },
            {
                "GlobalNodeGroupId": "sgaui-test-0004",
                "Slots": "450-1815,5462-6826,14053-15417"
            }
        ],
        "AuthTokenEnabled": false,
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
}
```

Para obtener más información, consulte Replication Across AWS Regions Using Global Datastore en la Guía del usuario de ElastiCache.

- Para obtener más información sobre la API, consulte DecreaseNodeGroupsInGlobalReplicationGroup en la Referencia de comandos de la AWS CLI.

`decrease-replica-count`

En el siguiente ejemplo de código, se muestra cómo utilizar `decrease-replica-count`.

AWS CLI

Para reducir el recuento de réplicas

En el siguiente ejemplo de `decrease-replica-count`, se disminuye dinámicamente el número de réplicas en un grupo de replicación de Redis (modo de clúster deshabilitado) o la cantidad de nodos de réplica en uno o más grupos de nodos (particiones) de un grupo de replicación de Redis (modo de clúster habilitado). Esta operación se realiza sin tiempo de inactividad del clúster.

```
aws elasticache decrease-replica-count \
    --replication-group-id my-cluster \
    --apply-immediately  \
    --new-replica-count 2
```

Salida:

```
{
    "ReplicationGroup": {
        "ReplicationGroupId": "my-cluster",
        "Description": " ",
        "Status": "modifying",
        "PendingModifiedValues": {},
        "MemberClusters": [
            "myrepliace",
            "my-cluster-001",
            "my-cluster-002",
            "my-cluster-003"
        ],
        "NodeGroups": [
            {
                "NodeGroupId": "0001",
                "Status": "modifying",
                "PrimaryEndpoint": {
                    "Address": "my-cluster.xxxxx.ng.0001.usw2.cache.amazonaws.com",
                    "Port": 6379
                },
                "ReaderEndpoint": {
                    "Address": "my-cluster-
ro.xxxxx.ng.0001.usw2.cache.amazonaws.com",
                    "Port": 6379
                },
                "NodeGroupMembers": [
                    {
                        "CacheClusterId": "myrepliace",
                        "CacheNodeId": "0001",
                        "ReadEndpoint": {
                            "Address":
 "myrepliace.xxxxx.0001.usw2.cache.amazonaws.com",
                            "Port": 6379
                        },
                        "PreferredAvailabilityZone": "us-west-2a",
                        "CurrentRole": "replica"
                    },
                    {
                        "CacheClusterId": "my-cluster-001",
                        "CacheNodeId": "0001",
                        "ReadEndpoint": {
```

```
                            "Address": "my-
cluster-001.xxxxx.0001.usw2.cache.amazonaws.com",
                            "Port": 6379
                        },
                        "PreferredAvailabilityZone": "us-west-2a",
                        "CurrentRole": "primary"
                    },
                    {
                        "CacheClusterId": "my-cluster-002",
                        "CacheNodeId": "0001",
                        "ReadEndpoint": {
                            "Address": "my-
cluster-002.xxxxx.0001.usw2.cache.amazonaws.com",
                            "Port": 6379
                        },
                        "PreferredAvailabilityZone": "us-west-2a",
                        "CurrentRole": "replica"
                    },
                    {
                        "CacheClusterId": "my-cluster-003",
                        "CacheNodeId": "0001",
                        "ReadEndpoint": {
                            "Address": "my-
cluster-003.xxxxx.0001.usw2.cache.amazonaws.com",
                            "Port": 6379
                        },
                        "PreferredAvailabilityZone": "us-west-2a",
                        "CurrentRole": "replica"
                    }
                ]
            }
        ],
        "AutomaticFailover": "disabled",
        "SnapshotRetentionLimit": 0,
        "SnapshotWindow": "07:30-08:30",
        "ClusterEnabled": false,
        "CacheNodeType": "cache.r5.xlarge",
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
}
```

Para obtener más información, consulte Changing the Number of Replicas en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DecreaseReplicaCount en la Referencia de comandos de la AWS CLI.

`delete-cache-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-cache-cluster`.

AWS CLI

Para eliminar un clúster de caché

En el siguiente ejemplo de `delete-cache-cluster`, se elimina el clúster aprovisionado que se ha especificado anteriormente. El comando elimina todos los nodos de caché asociados, los puntos de conexión de los nodos y el propio clúster. Cuando reciba una respuesta afirmativa de esta operación, Amazon ElastiCache empezará de inmediato a eliminar el clúster; no podrá cancelar ni revertir esta operación.

Esta operación no es válida para lo siguiente:

Clústeres de Redis (modo de clúster habilitado) Un clúster que es la última réplica de lectura de un grupo de replicación Un grupo de nodos (partición) que tiene habilitado el modo Multi-AZ Un clúster de un grupo de replicación de Redis (modo de clúster habilitado) Un clúster que no se encuentra en el estado disponible

```
aws elasticache delete-cache-cluster \
    --cache-cluster-id "my-cluster-002"
```

Salida:

```
{
    "CacheCluster": {
        "CacheClusterId": "my-cluster-002",
        "ClientDownloadLandingPage": "https://console.aws.amazon.com/elasticache/
home#client-download:",
        "CacheNodeType": "cache.r5.xlarge",
        "Engine": "redis",
        "EngineVersion": "5.0.5",
        "CacheClusterStatus": "deleting",
```

```
        "NumCacheNodes": 1,
        "PreferredAvailabilityZone": "us-west-2a",
        "CacheClusterCreateTime": "2019-11-26T03:35:04.546Z",
        "PreferredMaintenanceWindow": "mon:04:05-mon:05:05",
        "PendingModifiedValues": {},
        "NotificationConfiguration": {
            "TopicArn": "arn:aws:sns:us-west-x:xxxxxxx4152:My_Topic",
            "TopicStatus": "active"
        },
        "CacheSecurityGroups": [],
        "CacheParameterGroup": {
            "CacheParameterGroupName": "mygroup",
            "ParameterApplyStatus": "in-sync",
            "CacheNodeIdsToReboot": []
        },
        "CacheSubnetGroupName": "kxkxk",
        "AutoMinorVersionUpgrade": true,
        "SecurityGroups": [
            {
                "SecurityGroupId": "sg-xxxxxxxxxx9836",
                "Status": "active"
            },
            {
                "SecurityGroupId": "sg-xxxxxxxxxxxx7b",
                "Status": "active"
            }
        ],
        "ReplicationGroupId": "my-cluster",
        "SnapshotRetentionLimit": 0,
        "SnapshotWindow": "07:30-08:30",
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
}
```

Para obtener más información, consulte Deleting a Cluster en la Guía del usuario de ElastiCache.

- Para obtener más información sobre la API, consulte DeleteCacheCluster en la Referencia de comandos de la AWS CLI.

`delete-cache-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-cache-parameter-group`.

AWS CLI

Para eliminar un grupo de parámetros de caché

En el siguiente ejemplo de `delete-cache-parameter-group`, se elimina el grupo de parámetros de caché especificado. No podrá eliminar un grupo de parámetros de caché si está asociado a clústeres de caché.

```
aws elasticache delete-cache-parameter-group \
    --cache-parameter-group-name myparamgroup
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting a Parameter Group en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DeleteCacheParameterGroup en la Referencia de comandos de la AWS CLI.

`delete-cache-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-cache-subnet-group`.

AWS CLI

Para eliminar un grupo de subredes de caché

En el siguiente ejemplo de `delete-cache-subnet-group`, se elimina el grupo de subredes de caché especificado. No podrá eliminar un grupo de subredes de caché si está asociado a cualquier clúster.

```
aws elasticache delete-cache-subnet-group \
    --cache-subnet-group-name "mygroup"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting a Subnet Group en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DeleteCacheSubnetGroup en la Referencia de comandos de la AWS CLI.

delete-global-replication-group

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-global-replication-group`.

AWS CLI

Para eliminar un grupo de replicación global

En el siguiente ejemplo de `delete-global-replication-group`, se elimina un nuevo grupo de replicación global.

```
aws elasticache delete-global-replication-group \
    --global-replication-group-id my-global-replication-group \
    --retain-primary-replication-group
```

Salida:

```
{
    "GlobalReplicationGroup": {
        "GlobalReplicationGroupId": "sgaui-my-grg",
        "GlobalReplicationGroupDescription": "my-grg",
        "Status": "deleting",
        "CacheNodeType": "cache.r5.large",
        "Engine": "redis",
        "EngineVersion": "5.0.6",
        "Members": [
            {
                "ReplicationGroupId": "my-cluster-grg",
                "ReplicationGroupRegion": "us-west-2",
                "Role": "PRIMARY",
                "AutomaticFailover": "enabled",
                "Status": "associated"
            }
        ],
        "ClusterEnabled": false,
        "AuthTokenEnabled": false,
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
}
```

Para obtener más información, consulte Replication Across AWS Regions Using Global Datastore en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DeleteGlobalReplicationGroup en la Referencia de comandos de la AWS CLI.

`delete-replication-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-replication-group`.

AWS CLI

Para eliminar un grupo de replicación

En el siguiente ejemplo de `delete-replication-group`, se elimina un grupo de replicación existente. De manera predeterminada, esta operación elimina todo el grupo de replicación, incluidas las réplicas principales y todas las réplicas de lectura. Si el grupo de replicación solo tiene una principal, si lo desea, puede eliminar solo las réplicas de lectura y retener la principal estableciendo retainPrimaryCluster=true.

Cuando reciba una respuesta afirmativa de esta operación, Amazon ElastiCache empezará de inmediato a eliminar los recursos seleccionados; no podrá cancelar ni revertir esta operación. Válido solo para Redis

```
aws elasticache delete-replication-group \
    --replication-group-id "mygroup"
```

Salida:

```
{
     "ReplicationGroup": {
         "ReplicationGroupId": "mygroup",
         "Description": "my group",
         "Status": "deleting",
         "PendingModifiedValues": {},
         "AutomaticFailover": "disabled",
         "SnapshotRetentionLimit": 0,
         "SnapshotWindow": "06:00-07:00",
         "TransitEncryptionEnabled": false,
         "AtRestEncryptionEnabled": false
     }
```

```
}
```

- Para obtener información sobre la API, consulte DeleteReplicationGroup en la Referencia de comandos de la AWS CLI.

`delete-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-snapshot`.

AWS CLI

Eliminar una instantánea

En el siguiente ejemplo de `delete-snapshot`, se ha eliminado una instantánea mediante el motor de Redis.

```
aws elasticache delete-snapshot \
    --snapshot-name mysnapshot
```

Salida:

```
{
    "Snapshot": {
        "SnapshotName": "my-cluster-snapshot",
        "ReplicationGroupId": "mycluster",
        "ReplicationGroupDescription": "mycluster",
        "SnapshotStatus": "deleting",
        "SnapshotSource": "manual",
        "CacheNodeType": "cache.r5.xlarge",
        "Engine": "redis",
        "EngineVersion": "5.0.5",
        "PreferredMaintenanceWindow": "thu:12:00-thu:13:00",
        "TopicArn": "arn:aws:sns:us-west-2:xxxxxxxxxxxxx152:My_Topic",
        "Port": 6379,
        "CacheParameterGroupName": "default.redis5.0.cluster.on",
        "CacheSubnetGroupName": "default",
        "VpcId": "vpc-a3e97cdb",
        "AutoMinorVersionUpgrade": true,
        "SnapshotRetentionLimit": 1,
        "SnapshotWindow": "13:00-14:00",
        "NumNodeGroups": 4,
```

```
        "AutomaticFailover": "enabled",
        "NodeSnapshots": [
            {
                "CacheClusterId": "mycluster-0002-003",
                "NodeGroupId": "0002",
                "CacheNodeId": "0001",
                "CacheSize": "6 MB",
                "CacheNodeCreateTime": "2020-06-18T00:05:44.719000+00:00",
                "SnapshotCreateTime": "2020-06-25T20:34:30+00:00"
            },
            {
                "CacheClusterId": "mycluster-0003-003",
                "NodeGroupId": "0003",
                "CacheNodeId": "0001",
                "CacheSize": "6 MB",
                "CacheNodeCreateTime": "2019-12-05T19:13:15.912000+00:00",
                "SnapshotCreateTime": "2020-06-25T20:34:30+00:00"
            },
            {
                "CacheClusterId": "mycluster-0004-002",
                "NodeGroupId": "0004",
                "CacheNodeId": "0001",
                "CacheSize": "6 MB",
                "CacheNodeCreateTime": "2019-12-09T19:44:34.324000+00:00",
                "SnapshotCreateTime": "2020-06-25T20:34:30+00:00"
            },
            {
                "CacheClusterId": "mycluster-0005-003",
                "NodeGroupId": "0005",
                "CacheNodeId": "0001",
                "CacheSize": "6 MB",
                "CacheNodeCreateTime": "2020-06-18T00:05:44.775000+00:00",
                "SnapshotCreateTime": "2020-06-25T20:34:30+00:00"
            }
        ]
    }
}
```


Para obtener más información, consulte Backup and Restore for ElastiCache for Redis en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DeleteSnapshot en la Referencia de comandos de la AWS CLI.

`delete-user-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-user-group`.

AWS CLI

Para eliminar un grupo de usuarios

En el siguiente ejemplo de `delete-user-group`, se elimina un grupo de usuarios.

```
aws elasticache delete-user-group \
    --user-group-id myusergroup
```

Salida:

```
{
    "UserGroupId": "myusergroup",
    "Status": "deleting",
    "Engine": "redis",
    "UserIds": [
        "default"
    ],
    "ReplicationGroups": [],
    "ARN": "arn:aws:elasticache:us-west-2:xxxxxxxxxx52:usergroup:myusergroup"
}
```

Para obtener más información, consulte Authenticating Users with Role-Based Access Control (RBAC) en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DeleteUserGroup en la Referencia de comandos de la AWS CLI.

`delete-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-user`.

AWS CLI

Cómo eliminar un usuario

En el siguiente ejemplo de `delete-user` se elimina un usuario.

```
aws elasticache delete-user \
```

```
    --user-id user2
```

Salida:

```
{
    "UserId": "user1",
    "UserName": "myUser",
    "Status": "deleting",
    "Engine": "redis",
    "AccessString": "on ~* +@all",
    "UserGroupIds": [
        "myusergroup"
    ],
    "Authentication": {
        "Type": "password",
        "PasswordCount": 1
    },
    "ARN": "arn:aws:elasticache:us-west-2:xxxxxxxxxx52:user:user1"
}
```

Para obtener más información, consulte Authenticating Users with Role-Based Access Control (RBAC) en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DeleteUser en la Referencia de comandos de la AWS CLI.

`describe-cache-clusters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cache-clusters`.

AWS CLI

Para describir un clúster de caché

En el siguiente ejemplo de `describe-cache-clusters`, se describe un clúster de caché.

```
aws elasticache describe-cache-clusters
```

Salida:

```
{
    "CacheClusters": [
```

```
    {
            "CacheClusterId": "my-cluster-003",
            "ClientDownloadLandingPage": "https://console.aws.amazon.com/
elasticache/home#client-download:",
            "CacheNodeType": "cache.r5.large",
            "Engine": "redis",
            "EngineVersion": "5.0.5",
            "CacheClusterStatus": "available",
            "NumCacheNodes": 1,
            "PreferredAvailabilityZone": "us-west-2a",
            "CacheClusterCreateTime": "2019-11-26T01:22:52.396Z",
            "PreferredMaintenanceWindow": "mon:17:30-mon:18:30",
            "PendingModifiedValues": {},
            "NotificationConfiguration": {
                "TopicArn": "arn:aws:sns:us-west-2:xxxxxxxxxxx152:My_Topic",
                "TopicStatus": "active"
            },
            "CacheSecurityGroups": [],
            "CacheParameterGroup": {
                "CacheParameterGroupName": "default.redis5.0",
                "ParameterApplyStatus": "in-sync",
                "CacheNodeIdsToReboot": []
            },
            "CacheSubnetGroupName": "kxkxk",
            "AutoMinorVersionUpgrade": true,
            "SecurityGroups": [
                {
                    "SecurityGroupId": "sg-xxxxxd7b",
                    "Status": "active"
                }
            ],
            "ReplicationGroupId": "my-cluster",
            "SnapshotRetentionLimit": 0,
            "SnapshotWindow": "06:30-07:30",
            "AuthTokenEnabled": false,
            "TransitEncryptionEnabled": false,
            "AtRestEncryptionEnabled": false,
            "ARN": "arn:aws:elasticache:us-west-2:xxxxxxxxxxx152:cluster:my-cache-
cluster",
            "ReplicationGroupLogDeliveryEnabled": false,
            "LogDeliveryConfigurations": [
                {
                    "LogType": "slow-log",
                    "DestinationType": "cloudwatch-logs",
```

```
                    "DestinationDetails": {
                        "CloudWatchLogsDetails": {
                            "LogGroup": "test-log"
                        }
                    },
                    "LogFormat": "text",
                    "Status": "active"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Managing Clusters en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DescribeCacheClusters en la Referencia de comandos de la AWS CLI.

`describe-cache-engine-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cache-engine-versions`.

AWS CLI

Para describir una versión del motor de caché

En el siguiente ejemplo de `describe-cache-engine-versions`, se devuelve una lista de los motores de caché disponibles y sus versiones.

```
aws elasticache describe-cache-engine-versions \
    --engine "Redis"
```

Salida:

```
{
    "CacheEngineVersions": [
        {
            "Engine": "redis",
            "EngineVersion": "2.6.13",
            "CacheParameterGroupFamily": "redis2.6",
            "CacheEngineDescription": "Redis",
            "CacheEngineVersionDescription": "redis version 2.6.13"
```

```
        },
        {
            "Engine": "redis",
            "EngineVersion": "2.8.19",
            "CacheParameterGroupFamily": "redis2.8",
            "CacheEngineDescription": "Redis",
            "CacheEngineVersionDescription": "redis version 2.8.19"
        },
        {
            "Engine": "redis",
            "EngineVersion": "2.8.21",
            "CacheParameterGroupFamily": "redis2.8",
            "CacheEngineDescription": "Redis",
            "CacheEngineVersionDescription": "redis version 2.8.21"
        },
        {
            "Engine": "redis",
            "EngineVersion": "2.8.22",
            "CacheParameterGroupFamily": "redis2.8",
            "CacheEngineDescription": "Redis",
            "CacheEngineVersionDescription": "redis version 2.8.22"
        },
        {
            "Engine": "redis",
            "EngineVersion": "2.8.23",
            "CacheParameterGroupFamily": "redis2.8",
            "CacheEngineDescription": "Redis",
            "CacheEngineVersionDescription": "redis version 2.8.23"
        },
        {
            "Engine": "redis",
            "EngineVersion": "2.8.24",
            "CacheParameterGroupFamily": "redis2.8",
            "CacheEngineDescription": "Redis",
            "CacheEngineVersionDescription": "redis version 2.8.24"
        },
        {
            "Engine": "redis",
            "EngineVersion": "2.8.6",
            "CacheParameterGroupFamily": "redis2.8",
            "CacheEngineDescription": "Redis",
            "CacheEngineVersionDescription": "redis version 2.8.6"
        },
        {
```

```
            "Engine": "redis",
            "EngineVersion": "3.2.10",
            "CacheParameterGroupFamily": "redis3.2",
            "CacheEngineDescription": "Redis",
            "CacheEngineVersionDescription": "redis version 3.2.10"
        },
        {
            "Engine": "redis",
            "EngineVersion": "3.2.4",
            "CacheParameterGroupFamily": "redis3.2",
            "CacheEngineDescription": "Redis",
            "CacheEngineVersionDescription": "redis version 3.2.4"
        },
        {
            "Engine": "redis",
            "EngineVersion": "3.2.6",
            "CacheParameterGroupFamily": "redis3.2",
            "CacheEngineDescription": "Redis",
            "CacheEngineVersionDescription": "redis version 3.2.6"
        },
        {
            "Engine": "redis",
            "EngineVersion": "4.0.10",
            "CacheParameterGroupFamily": "redis4.0",
            "CacheEngineDescription": "Redis",
            "CacheEngineVersionDescription": "redis version 4.0.10"
        },
        {
            "Engine": "redis",
            "EngineVersion": "5.0.0",
            "CacheParameterGroupFamily": "redis5.0",
            "CacheEngineDescription": "Redis",
            "CacheEngineVersionDescription": "redis version 5.0.0"
        },
        {
            "Engine": "redis",
            "EngineVersion": "5.0.3",
            "CacheParameterGroupFamily": "redis5.0",
            "CacheEngineDescription": "Redis",
            "CacheEngineVersionDescription": "redis version 5.0.3"
        },
        {
            "Engine": "redis",
            "EngineVersion": "5.0.4",
```

```
            "CacheParameterGroupFamily": "redis5.0",
            "CacheEngineDescription": "Redis",
            "CacheEngineVersionDescription": "redis version 5.0.4"
        },
        {
            "Engine": "redis",
            "EngineVersion": "5.0.5",
            "CacheParameterGroupFamily": "redis5.0",
            "CacheEngineDescription": "Redis",
            "CacheEngineVersionDescription": "redis version 5.0.5"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeCacheEngineVersions en la Referencia de comandos de la AWS CLI.

`describe-cache-parameter-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cache-parameter-groups`.

AWS CLI

Para describir un grupo de parámetros de caché

En el siguiente ejemplo de `describe-cache-parameter-groups`, se devuelve una lista de descripciones de grupos de parámetros de caché.

```
aws elasticache describe-cache-parameter-groups \
    --cache-parameter-group-name "mygroup"
```

Salida:

```
{
    "CacheParameterGroups": [
        {
            "CacheParameterGroupName": "mygroup",
            "CacheParameterGroupFamily": "redis5.0",
            "Description": " "
        }
    ]
```

```
}
```

Para obtener más información, consulte Configuring Engine Parameters Using Parameter Groups en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DescribeCacheParameterGroups en la Referencia de comandos de la AWS CLI.

`describe-cache-parameters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cache-parameters`.

AWS CLI

Para describir los parámetros de caché

El siguiente ejemplo de describe-cache-parameters, se devuelve la lista de parámetros detallada para el grupo de parámetros de caché especificado.

```
aws elasticache describe-cache-parameters \
    --cache-parameter-group-name "myparamgroup"
```

Salida:

```
{
    "Parameters": [
        {
            "ParameterName": "activedefrag",
            "ParameterValue": "yes",
            "Description": "Enabled active memory defragmentation",
            "Source": "user",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "active-defrag-cycle-max",
            "ParameterValue": "75",
            "Description": "Maximal effort for defrag in CPU percentage",
            "Source": "user",
            "DataType": "integer",
```

```
            "AllowedValues": "1-75",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "active-defrag-cycle-min",
            "ParameterValue": "5",
            "Description": "Minimal effort for defrag in CPU percentage",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "1-75",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "active-defrag-ignore-bytes",
            "ParameterValue": "104857600",
            "Description": "Minimum amount of fragmentation waste to start active
defrag",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "1048576-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "active-defrag-max-scan-fields",
            "ParameterValue": "1000",
            "Description": "Maximum number of set/hash/zset/list fields that will be
processed from the main dictionary scan",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "1-1000000",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "active-defrag-threshold-lower",
            "ParameterValue": "10",
```

```
            "Description": "Minimum percentage of fragmentation to start active
defrag",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "1-100",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "active-defrag-threshold-upper",
            "ParameterValue": "100",
            "Description": "Maximum percentage of fragmentation at which we use
maximum effort",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "1-100",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "activerehashing",
            "ParameterValue": "yes",
            "Description": "Apply rehashing or not.",
            "Source": "user",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "requires-reboot"
        },
        {
            "ParameterName": "appendfsync",
            "ParameterValue": "everysec",
            "Description": "fsync policy for AOF persistence",
            "Source": "system",
            "DataType": "string",
            "AllowedValues": "always,everysec,no",
            "IsModifiable": false,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
```

```
            "ParameterName": "appendonly",
            "ParameterValue": "no",
            "Description": "Enable Redis persistence.",
            "Source": "system",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "IsModifiable": false,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "client-output-buffer-limit-normal-hard-limit",
            "ParameterValue": "0",
            "Description": "Normal client output buffer hard limit in bytes.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "client-output-buffer-limit-normal-soft-limit",
            "ParameterValue": "0",
            "Description": "Normal client output buffer soft limit in bytes.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "client-output-buffer-limit-normal-soft-seconds",
            "ParameterValue": "0",
            "Description": "Normal client output buffer soft limit in seconds.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
```

```
            "ParameterName": "client-output-buffer-limit-pubsub-hard-limit",
            "ParameterValue": "33554432",
            "Description": "Pubsub client output buffer hard limit in bytes.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "client-output-buffer-limit-pubsub-soft-limit",
            "ParameterValue": "8388608",
            "Description": "Pubsub client output buffer soft limit in bytes.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "client-output-buffer-limit-pubsub-soft-seconds",
            "ParameterValue": "60",
            "Description": "Pubsub client output buffer soft limit in seconds.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "client-output-buffer-limit-replica-soft-seconds",
            "ParameterValue": "60",
            "Description": "Replica client output buffer soft limit in seconds.",
            "Source": "system",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": false,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
```

```
            "ParameterName": "client-query-buffer-limit",
            "ParameterValue": "1073741824",
            "Description": "Max size of a single client query buffer",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "1048576-1073741824",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "close-on-replica-write",
            "ParameterValue": "yes",
            "Description": "If enabled, clients who attempt to write to a read-only
replica will be disconnected. Applicable to 2.8.23 and higher.",
            "Source": "user",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "cluster-enabled",
            "ParameterValue": "no",
            "Description": "Enable cluster mode",
            "Source": "user",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "requires-reboot"
        },
        {
            "ParameterName": "cluster-require-full-coverage",
            "ParameterValue": "no",
            "Description": "Whether cluster becomes unavailable if one or more slots
are not covered",
            "Source": "user",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
```

```
        },
        {
            "ParameterName": "databases",
            "ParameterValue": "16",
            "Description": "Set the number of databases.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "1-1200000",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "requires-reboot"
        },
        {
            "ParameterName": "hash-max-ziplist-entries",
            "ParameterValue": "512",
            "Description": "The maximum number of hash entries in order for the
dataset to be compressed.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "hash-max-ziplist-value",
            "ParameterValue": "64",
            "Description": "The threshold of biggest hash entries in order for the
dataset to be compressed.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "hll-sparse-max-bytes",
            "ParameterValue": "3000",
            "Description": "HyperLogLog sparse representation bytes limit",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "1-16000",
            "IsModifiable": true,
```

```
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "lazyfree-lazy-eviction",
            "ParameterValue": "no",
            "Description": "Perform an asynchronous delete on evictions",
            "Source": "user",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "lazyfree-lazy-expire",
            "ParameterValue": "no",
            "Description": "Perform an asynchronous delete on expired keys",
            "Source": "user",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "lazyfree-lazy-server-del",
            "ParameterValue": "no",
            "Description": "Perform an asynchronous delete on key updates",
            "Source": "user",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "lfu-decay-time",
            "ParameterValue": "1",
            "Description": "The amount of time in minutes to decrement the key
counter for LFU eviction policy",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
```

```
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "lfu-log-factor",
            "ParameterValue": "10",
            "Description": "The log factor for incrementing key counter for LFU
eviction policy",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "1-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "list-compress-depth",
            "ParameterValue": "0",
            "Description": "Number of quicklist ziplist nodes from each side of
the list to exclude from compression. The head and tail of the list are always
uncompressed for fast push/pop operations",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "list-max-ziplist-size",
            "ParameterValue": "-2",
            "Description": "The number of entries allowed per internal list node can
be specified as a fixed maximum size or a maximum number of elements",
            "Source": "system",
            "DataType": "integer",
            "AllowedValues": "-5,-4,-3,-2,-1,1-",
            "IsModifiable": false,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "lua-replicate-commands",
            "ParameterValue": "yes",
```

```
            "Description": "Always enable Lua effect replication or not",
            "Source": "user",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "lua-time-limit",
            "ParameterValue": "5000",
            "Description": "Max execution time of a Lua script in milliseconds. 0
 for unlimited execution without warnings.",
            "Source": "system",
            "DataType": "integer",
            "AllowedValues": "5000",
            "IsModifiable": false,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "maxclients",
            "ParameterValue": "65000",
            "Description": "The maximum number of Redis clients.",
            "Source": "system",
            "DataType": "integer",
            "AllowedValues": "1-65000",
            "IsModifiable": false,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "requires-reboot"
        },
        {
            "ParameterName": "maxmemory-policy",
            "ParameterValue": "volatile-lru",
            "Description": "Max memory policy.",
            "Source": "user",
            "DataType": "string",
            "AllowedValues": "volatile-lru,allkeys-lru,volatile-lfu,allkeys-
lfu,volatile-random,allkeys-random,volatile-ttl,noeviction",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
```

```
            "ParameterName": "maxmemory-samples",
            "ParameterValue": "3",
            "Description": "Max memory samples.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "1-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "min-replicas-max-lag",
            "ParameterValue": "10",
            "Description": "The maximum amount of replica lag in seconds beyond
which the master would stop taking writes. A value of 0 means the master always
takes writes.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "min-replicas-to-write",
            "ParameterValue": "0",
            "Description": "The minimum number of replicas that must be present with
lag no greater than min-replicas-max-lag for master to take writes. Setting this to
0 means the master always takes writes.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "notify-keyspace-events",
            "Description": "The keyspace events for Redis to notify Pub/Sub clients
about. By default all notifications are disabled",
            "Source": "user",
            "DataType": "string",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
```

```
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "proto-max-bulk-len",
            "ParameterValue": "536870912",
            "Description": "Max size of a single element request",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "1048576-536870912",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "rename-commands",
            "ParameterValue": "",
            "Description": "Redis commands that can be dynamically renamed by the
customer",
            "Source": "user",
            "DataType": "string",
            "AllowedValues":
"APPEND,BITCOUNT,BITFIELD,BITOP,BITPOS,BLPOP,BRPOP,BRPOPLPUSH,BZPOPMIN,BZPOPMAX,CLIENT,COMM
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.3",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "repl-backlog-size",
            "ParameterValue": "1048576",
            "Description": "The replication backlog size in bytes for PSYNC. This is
the size of the buffer which accumulates slave data when slave is disconnected for
some time, so that when slave reconnects again, only transfer the portion of data
which the slave missed. Minimum value is 16K.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "16384-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "repl-backlog-ttl",
            "ParameterValue": "3600",
```

```
            "Description": "The amount of time in seconds after the master no longer
have any slaves connected for the master to free the replication backlog. A value
of 0 means to never release the backlog.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "replica-allow-chaining",
            "ParameterValue": "no",
            "Description": "Configures if chaining of replicas is allowed",
            "Source": "system",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "IsModifiable": false,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "replica-ignore-maxmemory",
            "ParameterValue": "yes",
            "Description": "Determines if replica ignores maxmemory setting by not
evicting items independent from the master",
            "Source": "system",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "IsModifiable": false,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "replica-lazy-flush",
            "ParameterValue": "no",
            "Description": "Perform an asynchronous flushDB during replica sync",
            "Source": "system",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "IsModifiable": false,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
```

```
        {
            "ParameterName": "reserved-memory-percent",
            "ParameterValue": "25",
            "Description": "The percent of memory reserved for non-cache memory
usage. You may want to increase this parameter for nodes with read replicas, AOF
enabled, etc, to reduce swap usage.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-100",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "set-max-intset-entries",
            "ParameterValue": "512",
            "Description": "The limit in the size of the set in order for the
dataset to be compressed.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "slowlog-log-slower-than",
            "ParameterValue": "10000",
            "Description": "The execution time, in microseconds, to exceed in order
for the command to get logged. Note that a negative number disables the slow log,
while a value of zero forces the logging of every command.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "slowlog-max-len",
            "ParameterValue": "128",
            "Description": "The length of the slow log. There is no limit to this
length. Just be aware that it will consume memory. You can reclaim memory used by
the slow log with SLOWLOG RESET.",
```

```
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "stream-node-max-bytes",
            "ParameterValue": "4096",
            "Description": "The maximum size of a single node in a stream in bytes",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "stream-node-max-entries",
            "ParameterValue": "100",
            "Description": "The maximum number of items a single node in a stream
can contain",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "tcp-keepalive",
            "ParameterValue": "300",
            "Description": "If non-zero, send ACKs every given number of seconds.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "timeout",
            "ParameterValue": "0",
```

```
            "Description": "Close connection if client is idle for a given number of
 seconds, or never if 0.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0,20-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "zset-max-ziplist-entries",
            "ParameterValue": "128",
            "Description": "The maximum number of sorted set entries in order for
 the dataset to be compressed.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "zset-max-ziplist-value",
            "ParameterValue": "64",
            "Description": "The threshold of biggest sorted set entries in order for
 the dataset to be compressed.",
            "Source": "user",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        }
    ]
}
```

Para obtener más información, consulte Parameter Management en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DescribeCacheParameters en la Referencia de comandos de la AWS CLI.

describe-cache-subnet-groups

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cache-subnet-groups`.

AWS CLI

Para describir los grupos de subredes de caché

En el siguiente ejemplo de `describe-cache-subnet-groups`, se devuelve una lista de grupos de subredes.

```
aws elasticache describe-cache-subnet-groups
```

Salida:

```
{
    "CacheSubnetGroups": [
        {
            "CacheSubnetGroupName": "default",
            "CacheSubnetGroupDescription": "Default CacheSubnetGroup",
            "VpcId": "vpc-a3e97cdb",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-8d4bacf5",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2b"
                    }
                },
                {
                    "SubnetIdentifier": "subnet-dde21380",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2c"
                    }
                },
                {
                    "SubnetIdentifier": "subnet-6485ec4f",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2d"
                    }
                },
                {
                    "SubnetIdentifier": "subnet-b4ebebff",
                    "SubnetAvailabilityZone": {
```

```
                        "Name": "us-west-2a"
                    }
                }
            ]
        },
        {
            "CacheSubnetGroupName": "kxkxk",
            "CacheSubnetGroupDescription": "mygroup",
            "VpcId": "vpc-a3e97cdb",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-b4ebebff",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2a"
                    }
                }
            ]
        },
        {
            "CacheSubnetGroupName": "test",
            "CacheSubnetGroupDescription": "test",
            "VpcId": "vpc-a3e97cdb",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-b4ebebff",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2a"
                    }
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Subnets and Subnet Groups en la Guía del usuario de ElastiCache o Subnets and Subnet Groups en la Guía del usuario de ElastiCache para Memcached.

- Para obtener información sobre la API, consulte DescribeCacheSubnetGroups en la Referencia de comandos de la AWS CLI.

describe-engine-default-parameters

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-engine-default-parameters`.

AWS CLI

Para describir los parámetros predeterminados del motor

En el siguiente ejemplo de `describe-engine-default-parameters`, se devuelve la información de parámetros del sistema y del motor predeterminada para el motor de base de datos especificado.

```
aws elasticache describe-engine-default-parameters \
    --cache-parameter-group-family "redis5.0"
```

Salida:

```
{
    "EngineDefaults": {
        "Parameters": [
            {
                "ParameterName": "activedefrag",
                "ParameterValue": "no",
                "Description": "Enabled active memory defragmentation",
                "Source": "system",
                "DataType": "string",
                "AllowedValues": "yes,no",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "active-defrag-cycle-max",
                "ParameterValue": "75",
                "Description": "Maximal effort for defrag in CPU percentage",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "1-75",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
```

```
            {
                "ParameterName": "active-defrag-cycle-min",
                "ParameterValue": "5",
                "Description": "Minimal effort for defrag in CPU percentage",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "1-75",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "active-defrag-ignore-bytes",
                "ParameterValue": "104857600",
                "Description": "Minimum amount of fragmentation waste to start
active defrag",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "1048576-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "active-defrag-max-scan-fields",
                "ParameterValue": "1000",
                "Description": "Maximum number of set/hash/zset/list fields that
will be processed from the main dictionary scan",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "1-1000000",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "active-defrag-threshold-lower",
                "ParameterValue": "10",
                "Description": "Minimum percentage of fragmentation to start active
defrag",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "1-100",
                "IsModifiable": true,
```

```
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "active-defrag-threshold-upper",
                "ParameterValue": "100",
                "Description": "Maximum percentage of fragmentation at which we use
maximum effort",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "1-100",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "activerehashing",
                "ParameterValue": "yes",
                "Description": "Apply rehashing or not.",
                "Source": "system",
                "DataType": "string",
                "AllowedValues": "yes,no",
                "IsModifiable": false,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "requires-reboot"
            },
            {
                "ParameterName": "appendfsync",
                "ParameterValue": "everysec",
                "Description": "fsync policy for AOF persistence",
                "Source": "system",
                "DataType": "string",
                "AllowedValues": "always,everysec,no",
                "IsModifiable": false,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "appendonly",
                "ParameterValue": "no",
                "Description": "Enable Redis persistence.",
                "Source": "system",
                "DataType": "string",
                "AllowedValues": "yes,no",
```

```
            "IsModifiable": false,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "client-output-buffer-limit-normal-hard-limit",
            "ParameterValue": "0",
            "Description": "Normal client output buffer hard limit in bytes.",
            "Source": "system",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "client-output-buffer-limit-normal-soft-limit",
            "ParameterValue": "0",
            "Description": "Normal client output buffer soft limit in bytes.",
            "Source": "system",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "client-output-buffer-limit-normal-soft-seconds",
            "ParameterValue": "0",
            "Description": "Normal client output buffer soft limit in seconds.",
            "Source": "system",
            "DataType": "integer",
            "AllowedValues": "0-",
            "IsModifiable": true,
            "MinimumEngineVersion": "5.0.0",
            "ChangeType": "immediate"
        },
        {
            "ParameterName": "client-output-buffer-limit-pubsub-hard-limit",
            "ParameterValue": "33554432",
            "Description": "Pubsub client output buffer hard limit in bytes.",
            "Source": "system",
            "DataType": "integer",
            "AllowedValues": "0-",
```

```
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "client-output-buffer-limit-pubsub-soft-limit",
                "ParameterValue": "8388608",
                "Description": "Pubsub client output buffer soft limit in bytes.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "client-output-buffer-limit-pubsub-soft-seconds",
                "ParameterValue": "60",
                "Description": "Pubsub client output buffer soft limit in seconds.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "client-output-buffer-limit-replica-soft-seconds",
                "ParameterValue": "60",
                "Description": "Replica client output buffer soft limit in
seconds.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
                "IsModifiable": false,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "client-query-buffer-limit",
                "ParameterValue": "1073741824",
                "Description": "Max size of a single client query buffer",
                "Source": "system",
                "DataType": "integer",
```

```
                "AllowedValues": "1048576-1073741824",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "close-on-replica-write",
                "ParameterValue": "yes",
                "Description": "If enabled, clients who attempt to write to a read-
only replica will be disconnected. Applicable to 2.8.23 and higher.",
                "Source": "system",
                "DataType": "string",
                "AllowedValues": "yes,no",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "cluster-enabled",
                "ParameterValue": "no",
                "Description": "Enable cluster mode",
                "Source": "system",
                "DataType": "string",
                "AllowedValues": "yes,no",
                "IsModifiable": false,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "requires-reboot"
            },
            {
                "ParameterName": "cluster-require-full-coverage",
                "ParameterValue": "no",
                "Description": "Whether cluster becomes unavailable if one or more
 slots are not covered",
                "Source": "system",
                "DataType": "string",
                "AllowedValues": "yes,no",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "databases",
                "ParameterValue": "16",
                "Description": "Set the number of databases.",
```

```
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "1-1200000",
                "IsModifiable": false,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "requires-reboot"
            },
            {
                "ParameterName": "hash-max-ziplist-entries",
                "ParameterValue": "512",
                "Description": "The maximum number of hash entries in order for the
dataset to be compressed.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "hash-max-ziplist-value",
                "ParameterValue": "64",
                "Description": "The threshold of biggest hash entries in order for
the dataset to be compressed.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "hll-sparse-max-bytes",
                "ParameterValue": "3000",
                "Description": "HyperLogLog sparse representation bytes limit",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "1-16000",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "lazyfree-lazy-eviction",
```

```
                "ParameterValue": "no",
                "Description": "Perform an asynchronous delete on evictions",
                "Source": "system",
                "DataType": "string",
                "AllowedValues": "yes,no",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "lazyfree-lazy-expire",
                "ParameterValue": "no",
                "Description": "Perform an asynchronous delete on expired keys",
                "Source": "system",
                "DataType": "string",
                "AllowedValues": "yes,no",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "lazyfree-lazy-server-del",
                "ParameterValue": "no",
                "Description": "Perform an asynchronous delete on key updates",
                "Source": "system",
                "DataType": "string",
                "AllowedValues": "yes,no",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "lfu-decay-time",
                "ParameterValue": "1",
                "Description": "The amount of time in minutes to decrement the key
counter for LFU eviction policy",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
```

```
                "ParameterName": "lfu-log-factor",
                "ParameterValue": "10",
                "Description": "The log factor for incrementing key counter for LFU
eviction policy",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "1-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "list-compress-depth",
                "ParameterValue": "0",
                "Description": "Number of quicklist ziplist nodes from each side
of the list to exclude from compression. The head and tail of the list are always
uncompressed for fast push/pop operations",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "list-max-ziplist-size",
                "ParameterValue": "-2",
                "Description": "The number of entries allowed per internal list node
can be specified as a fixed maximum size or a maximum number of elements",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "-5,-4,-3,-2,-1,1-",
                "IsModifiable": false,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "lua-replicate-commands",
                "ParameterValue": "yes",
                "Description": "Always enable Lua effect replication or not",
                "Source": "system",
                "DataType": "string",
                "AllowedValues": "yes,no",
                "IsModifiable": true,
```

```
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "lua-time-limit",
                "ParameterValue": "5000",
                "Description": "Max execution time of a Lua script in milliseconds.
 0 for unlimited execution without warnings.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "5000",
                "IsModifiable": false,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "maxclients",
                "ParameterValue": "65000",
                "Description": "The maximum number of Redis clients.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "1-65000",
                "IsModifiable": false,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "requires-reboot"
            },
            {
                "ParameterName": "maxmemory-policy",
                "ParameterValue": "volatile-lru",
                "Description": "Max memory policy.",
                "Source": "system",
                "DataType": "string",
                "AllowedValues": "volatile-lru,allkeys-lru,volatile-lfu,allkeys-
lfu,volatile-random,allkeys-random,volatile-ttl,noeviction",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "maxmemory-samples",
                "ParameterValue": "3",
                "Description": "Max memory samples.",
                "Source": "system",
                "DataType": "integer",
```

```
                "AllowedValues": "1-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "min-replicas-max-lag",
                "ParameterValue": "10",
                "Description": "The maximum amount of replica lag in seconds beyond
which the master would stop taking writes. A value of 0 means the master always
takes writes.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "min-replicas-to-write",
                "ParameterValue": "0",
                "Description": "The minimum number of replicas that must be present
with lag no greater than min-replicas-max-lag for master to take writes. Setting
this to 0 means the master always takes writes.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "notify-keyspace-events",
                "Description": "The keyspace events for Redis to notify Pub/Sub
clients about. By default all notifications are disabled",
                "Source": "system",
                "DataType": "string",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "proto-max-bulk-len",
                "ParameterValue": "536870912",
```

```
                "Description": "Max size of a single element request",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "1048576-536870912",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "rename-commands",
                "ParameterValue": "",
                "Description": "Redis commands that can be dynamically renamed by
the customer",
                "Source": "system",
                "DataType": "string",
                "AllowedValues":
"APPEND,BITCOUNT,BITFIELD,BITOP,BITPOS,BLPOP,BRPOP,BRPOPLPUSH,BZPOPMIN,BZPOPMAX,CLIENT,COMM
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.3",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "repl-backlog-size",
                "ParameterValue": "1048576",
                "Description": "The replication backlog size in bytes for PSYNC.
This is the size of the buffer which accumulates slave data when slave is
disconnected for some time, so that when slave reconnects again, only transfer the
portion of data which the slave missed. Minimum value is 16K.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "16384-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "repl-backlog-ttl",
                "ParameterValue": "3600",
                "Description": "The amount of time in seconds after the master no
longer have any slaves connected for the master to free the replication backlog. A
value of 0 means to never release the backlog.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
```

```
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "replica-allow-chaining",
                "ParameterValue": "no",
                "Description": "Configures if chaining of replicas is allowed",
                "Source": "system",
                "DataType": "string",
                "AllowedValues": "yes,no",
                "IsModifiable": false,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "replica-ignore-maxmemory",
                "ParameterValue": "yes",
                "Description": "Determines if replica ignores maxmemory setting by
not evicting items independent from the master",
                "Source": "system",
                "DataType": "string",
                "AllowedValues": "yes,no",
                "IsModifiable": false,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "replica-lazy-flush",
                "ParameterValue": "no",
                "Description": "Perform an asynchronous flushDB during replica
sync",
                "Source": "system",
                "DataType": "string",
                "AllowedValues": "yes,no",
                "IsModifiable": false,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "reserved-memory-percent",
                "ParameterValue": "25",
```

```
                "Description": "The percent of memory reserved for non-cache memory
usage. You may want to increase this parameter for nodes with read replicas, AOF
enabled, etc, to reduce swap usage.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-100",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "set-max-intset-entries",
                "ParameterValue": "512",
                "Description": "The limit in the size of the set in order for the
dataset to be compressed.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "slowlog-log-slower-than",
                "ParameterValue": "10000",
                "Description": "The execution time, in microseconds, to exceed in
order for the command to get logged. Note that a negative number disables the slow
log, while a value of zero forces the logging of every command.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "slowlog-max-len",
                "ParameterValue": "128",
                "Description": "The length of the slow log. There is no limit to
this length. Just be aware that it will consume memory. You can reclaim memory used
by the slow log with SLOWLOG RESET.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
```

```
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "stream-node-max-bytes",
                "ParameterValue": "4096",
                "Description": "The maximum size of a single node in a stream in
bytes",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "stream-node-max-entries",
                "ParameterValue": "100",
                "Description": "The maximum number of items a single node in a
stream can contain",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "tcp-keepalive",
                "ParameterValue": "300",
                "Description": "If non-zero, send ACKs every given number of
seconds.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "timeout",
                "ParameterValue": "0",
```

```
                "Description": "Close connection if client is idle for a given
 number of seconds, or never if 0.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0,20-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "zset-max-ziplist-entries",
                "ParameterValue": "128",
                "Description": "The maximum number of sorted set entries in order
 for the dataset to be compressed.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            },
            {
                "ParameterName": "zset-max-ziplist-value",
                "ParameterValue": "64",
                "Description": "The threshold of biggest sorted set entries in order
 for the dataset to be compressed.",
                "Source": "system",
                "DataType": "integer",
                "AllowedValues": "0-",
                "IsModifiable": true,
                "MinimumEngineVersion": "5.0.0",
                "ChangeType": "immediate"
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte DescribeEngineDefaultParameters en la Referencia de comandos de la AWS CLI.

`describe-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-events`.

AWS CLI

Para describir los eventos de un grupo de replicación

En el siguiente ejemplo de `describe-events`, se devuelve una lista de eventos para un grupo de replicación.

```
aws elasticache describe-events \
    --source-identifier test-cluster \
    --source-type replication-group
```

Salida:

```
{
    "Events": [
        {
            "SourceIdentifier": "test-cluster",
            "SourceType": "replication-group",
            "Message": "Automatic failover has been turned on for replication group
 test-cluster",
            "Date": "2020-03-18T23:51:34.457Z"
        },
        {
            "SourceIdentifier": "test-cluster",
            "SourceType": "replication-group",
            "Message": "Replication group test-cluster created",
            "Date": "2020-03-18T23:50:31.378Z"
        }
    ]
}
```

Para obtener más información, consulte Monitoring Events en la Guía del usuario de ElastiCache.

- Para obtener detalles sobre la API, consulte DescribeEvents en la Referencia de comandos de la AWS CLI.

`describe-global-replication-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-global-replication-groups`.

AWS CLI

Para describir los grupos de reproducción globales

En el siguiente ejemplo de `describe-global-replication-groups`, se devuelven detalles de un almacén de datos global.

```
aws elasticache describe-global-replication-groups \
    --global-replication-group-id my-grg
```

Salida:

```
{
    "GlobalReplicationGroups": [
        {
            "GlobalReplicationGroupId": "my-grg",
            "GlobalReplicationGroupDescription": "my-grg",
            "Status": "creating",
            "CacheNodeType": "cache.r5.large",
            "Engine": "redis",
            "EngineVersion": "5.0.6",
            "ClusterEnabled": false,
            "AuthTokenEnabled": false,
            "TransitEncryptionEnabled": false,
            "AtRestEncryptionEnabled": false
        }
    ]
}
```

Para obtener más información, consulte Replication Across AWS Regions Using Global Datastore en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DescribeGlobalReplicationGroups en la Referencia de comandos de la AWS CLI.

`describe-replication-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-replication-groups`.

AWS CLI

Para devolver una lista de los detalles del grupo de replicación

En el siguiente ejemplo de `describe-replication-groups`, se devuelven los grupos de replicación.

```
aws elasticache describe-replication-groups
```

Salida:

```
{
    "ReplicationGroups": [
        {
            "ReplicationGroupId": "my-cluster",
            "Description": "mycluster",
            "Status": "available",
            "PendingModifiedValues": {},
            "MemberClusters": [
                "pat-cluster-001",
                "pat-cluster-002",
                "pat-cluster-003",
                "pat-cluster-004"
            ],
            "NodeGroups": [
                {
                    "NodeGroupId": "0001",
                    "Status": "available",
                    "PrimaryEndpoint": {
                        "Address": "my-
cluster.xxxxih.ng.0001.usw2.cache.amazonaws.com",
                        "Port": 6379
                    },
                    "ReaderEndpoint": {
                        "Address": "my-cluster-
ro.xxxxih.ng.0001.usw2.cache.amazonaws.com",
                        "Port": 6379
                    },
                    "NodeGroupMembers": [
                        {
                            "CacheClusterId": "my-cluster-001",
                            "CacheNodeId": "0001",
                            "ReadEndpoint": {
                                "Address": "pat-
cluster-001.xxxih.0001.usw2.cache.amazonaws.com",
                                "Port": 6379
                            },
```

```
                            "PreferredAvailabilityZone": "us-west-2a",
                            "CurrentRole": "primary"
                        },
                        {
                            "CacheClusterId": "my-cluster-002",
                            "CacheNodeId": "0001",
                            "ReadEndpoint": {
                                "Address": "pat-
cluster-002.xxxxih.0001.usw2.cache.amazonaws.com",
                                "Port": 6379
                            },
                            "PreferredAvailabilityZone": "us-west-2a",
                            "CurrentRole": "replica"
                        },
                        {
                            "CacheClusterId": "my-cluster-003",
                            "CacheNodeId": "0001",
                            "ReadEndpoint": {
                                "Address": "pat-
cluster-003.xxxxih.0001.usw2.cache.amazonaws.com",
                                "Port": 6379
                            },
                            "PreferredAvailabilityZone": "us-west-2a",
                            "CurrentRole": "replica"
                        },
                        {
                            "CacheClusterId": "my-cluster-004",
                            "CacheNodeId": "0001",
                            "ReadEndpoint": {
                                "Address": "pat-
cluster-004.xxxih.0001.usw2.cache.amazonaws.com",
                                "Port": 6379
                            },
                            "PreferredAvailabilityZone": "us-west-2a",
                            "CurrentRole": "replica"
                        }
                    ]
                }
            ],
            "AutomaticFailover": "disabled",
            "SnapshotRetentionLimit": 0,
            "SnapshotWindow": "07:30-08:30",
            "ClusterEnabled": false,
            "CacheNodeType": "cache.r5.xlarge",
```

```
            "AuthTokenEnabled": false,
            "TransitEncryptionEnabled": false,
            "AtRestEncryptionEnabled": false,
            "ARN": "arn:aws:elasticache:us-
west-2:xxxxxxxxxxx152:replicationgroup:my-cluster",
            "LogDeliveryConfigurations": [
                {
                    "LogType": "slow-log",
                    "DestinationType": "cloudwatch-logs",
                    "DestinationDetails": {
                        "CloudWatchLogsDetails": {
                            "LogGroup": "test-log"
                        }
                    },
                    "LogFormat": "json",
                    "Status": "active"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Managing Clusters en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DescribeReplicationGroups en la Referencia de comandos de la AWS CLI.

`describe-reserved-cache-nodes-offerings`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-reserved-cache-nodes-offerings`.

AWS CLI

Para describir reserved-cache-nodes-offerings

En el siguiente ejemplo de `describe-reserved-cache-nodes-offerings`, se devuelven detalles de las opciones de reserved-cache-node.

```
aws elasticache describe-reserved-cache-nodes-offerings
```

Salida:

```
{
    "ReservedCacheNodesOfferings": [
        {
            "ReservedCacheNodesOfferingId": "01ce0a19-a476-41cb-8aee-48eacbcdc8e5",
            "CacheNodeType": "cache.t3.small",
            "Duration": 31536000,
            "FixedPrice": 97.0,
            "UsagePrice": 0.0,
            "ProductDescription": "memcached",
            "OfferingType": "Partial Upfront",
            "RecurringCharges": [
                {
                    "RecurringChargeAmount": 0.011,
                    "RecurringChargeFrequency": "Hourly"
                }
            ]
        },
        {
            "ReservedCacheNodesOfferingId": "0443a27b-4da5-4b90-b92d-929fbd7abed2",
            "CacheNodeType": "cache.m3.2xlarge",
            "Duration": 31536000,
            "FixedPrice": 1772.0,
            "UsagePrice": 0.0,
            "ProductDescription": "redis",
            "OfferingType": "Heavy Utilization",
            "RecurringCharges": [
                {
                    "RecurringChargeAmount": 0.25,
                    "RecurringChargeFrequency": "Hourly"
                }
            ]
        },

        ...

    ]
}
```

Para obtener más información, consulte Getting Info About Reserved Node Offerings en la Guía del usuario de Elasticache para Redis o Getting Info About Reserved Node Offerings en la Guía del usuario de Elasticache para Memcached.

- Para obtener información sobre la API, consulte DescribeReservedCacheNodesOfferings en la Referencia de comandos de la AWS CLI.

`describe-reserved-cache-nodes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-reserved-cache-nodes`.

AWS CLI

Para describir los nodos de caché reservados

En el siguiente ejemplo de `describe-reserved-cache-nodes`, se devuelve la información sobre los nodos de caché reservados para esta cuenta o sobre un nodo de caché reservado especificado.

aws elasticache describe-reserved-cache-nodes

Salida:

```
{
    "ReservedCacheNodes": [
        {
            "ReservedCacheNodeId": "mynode",
            "ReservedCacheNodesOfferingId": "xxxxxxxxx-xxxxx-xxxxx-xxxx-xxxxxxxx71",
            "CacheNodeType": "cache.t3.small",
            "StartTime": "2019-12-06T02:50:44.003Z",
            "Duration": 31536000,
            "FixedPrice": 0.0,
            "UsagePrice": 0.0,
            "CacheNodeCount": 1,
            "ProductDescription": "redis",
            "OfferingType": "No Upfront",
            "State": "payment-pending",
            "RecurringCharges": [
                {
                    "RecurringChargeAmount": 0.023,
                    "RecurringChargeFrequency": "Hourly"
                }
            ],
            "ReservationARN": "arn:aws:elasticache:us-
west-2:xxxxxxxxxxx52:reserved-instance:mynode"
        }
    ]
```

```
}
```

Para obtener más información, consulte Managing Costs with Reserved Nodes en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DescribeReservedCacheNodes en la Referencia de comandos de la AWS CLI.

`describe-service-updates`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-service-updates`.

AWS CLI

Para describir las actualizaciones de servicio

En el siguiente ejemplo de `describe-service-updates`, se devuelven detalles sobre actualizaciones de servicios.

```
aws elasticache describe-service-updates
```

Salida:

```
{
    "ServiceUpdates": [
        {
            "ServiceUpdateName": "elc-xxxxxxxx7-001",
            "ServiceUpdateReleaseDate": "2019-10-09T16:00:00Z",
            "ServiceUpdateEndDate": "2020-02-09T15:59:59Z",
            "ServiceUpdateSeverity": "important",
            "ServiceUpdateRecommendedApplyByDate": "2019-11-08T15:59:59Z",
            "ServiceUpdateStatus": "available",
            "ServiceUpdateDescription": "Upgrades to improve the security,
 reliability, and operational performance of your ElastiCache nodes",
            "ServiceUpdateType": "security-update",
            "Engine": "redis, memcached",
            "EngineVersion": "redis 2.6.13 and onwards, memcached 1.4.5 and
 onwards",
            "AutoUpdateAfterRecommendedApplyByDate": false,
            "EstimatedUpdateTime": "30 minutes per node"
        },
        {
            "ServiceUpdateName": "elc-xxxxxxxx4-001",
```

```
            "ServiceUpdateReleaseDate": "2019-06-11T15:00:00Z",
            "ServiceUpdateEndDate": "2019-10-01T09:24:00Z",
            "ServiceUpdateSeverity": "important",
            "ServiceUpdateRecommendedApplyByDate": "2019-07-11T14:59:59Z",
            "ServiceUpdateStatus": "expired",
            "ServiceUpdateDescription": "Upgrades to improve the security,
reliability, and operational performance of your ElastiCache nodes",
            "ServiceUpdateType": "security-update",
            "Engine": "redis",
            "EngineVersion": "redis 3.2.6, redis 4.0 and onwards",
            "AutoUpdateAfterRecommendedApplyByDate": false,
            "EstimatedUpdateTime": "30 minutes per node"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeServiceUpdates en la Referencia de comandos de la AWS CLI.

`describe-snapshots`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-snapshots`.

AWS CLI

Para describir instantáneas

El siguiente ejemplo de describe-snapshots devuelve información sobre las instantáneas de su clúster o grupo de replicación.

```
aws elasticache describe-snapshots
```

Salida:

```
{
    "Snapshots": [
        {
            "SnapshotName": "automatic.my-cluster2-002-2019-12-05-06-38",
            "CacheClusterId": "my-cluster2-002",
            "SnapshotStatus": "available",
            "SnapshotSource": "automated",
            "CacheNodeType": "cache.r5.large",
```

```
            "Engine": "redis",
            "EngineVersion": "5.0.5",
            "NumCacheNodes": 1,
            "PreferredAvailabilityZone": "us-west-2a",
            "CacheClusterCreateTime": "2019-11-26T01:22:52.396Z",
            "PreferredMaintenanceWindow": "mon:17:30-mon:18:30",
            "TopicArn": "arn:aws:sns:us-west-2:xxxxxxxxx52:My_Topic",
            "Port": 6379,
            "CacheParameterGroupName": "default.redis5.0",
            "CacheSubnetGroupName": "kxkxk",
            "VpcId": "vpc-a3e97cdb",
            "AutoMinorVersionUpgrade": true,
            "SnapshotRetentionLimit": 1,
            "SnapshotWindow": "06:30-07:30",
            "NodeSnapshots": [
                {
                    "CacheNodeId": "0001",
                    "CacheSize": "5 MB",
                    "CacheNodeCreateTime": "2019-11-26T01:22:52.396Z",
                    "SnapshotCreateTime": "2019-12-05T06:38:23Z"
                }
            ]
        },
        {
            "SnapshotName": "myreplica-backup",
            "CacheClusterId": "myreplica",
            "SnapshotStatus": "available",
            "SnapshotSource": "manual",
            "CacheNodeType": "cache.r5.large",
            "Engine": "redis",
            "EngineVersion": "5.0.5",
            "NumCacheNodes": 1,
            "PreferredAvailabilityZone": "us-west-2a",
            "CacheClusterCreateTime": "2019-11-26T00:14:52.439Z",
            "PreferredMaintenanceWindow": "sat:10:00-sat:11:00",
            "TopicArn": "arn:aws:sns:us-west-2:xxxxxxxxxx152:My_Topic",
            "Port": 6379,
            "CacheParameterGroupName": "default.redis5.0",
            "CacheSubnetGroupName": "kxkxk",
            "VpcId": "vpc-a3e97cdb",
            "AutoMinorVersionUpgrade": true,
            "SnapshotRetentionLimit": 0,
            "SnapshotWindow": "09:00-10:00",
            "NodeSnapshots": [
```

```
                {
                    "CacheNodeId": "0001",
                    "CacheSize": "5 MB",
                    "CacheNodeCreateTime": "2019-11-26T00:14:52.439Z",
                    "SnapshotCreateTime": "2019-11-26T00:25:01Z"
                }
            ]
        },
        {
            "SnapshotName": "my-cluster",
            "CacheClusterId": "my-cluster-003",
            "SnapshotStatus": "available",
            "SnapshotSource": "manual",
            "CacheNodeType": "cache.r5.large",
            "Engine": "redis",
            "EngineVersion": "5.0.5",
            "NumCacheNodes": 1,
            "PreferredAvailabilityZone": "us-west-2a",
            "CacheClusterCreateTime": "2019-11-25T23:56:17.186Z",
            "PreferredMaintenanceWindow": "sat:10:00-sat:11:00",
            "TopicArn": "arn:aws:sns:us-west-2:xxxxxxxxxx152:My_Topic",
            "Port": 6379,
            "CacheParameterGroupName": "default.redis5.0",
            "CacheSubnetGroupName": "kxkxk",
            "VpcId": "vpc-a3e97cdb",
            "AutoMinorVersionUpgrade": true,
            "SnapshotRetentionLimit": 0,
            "SnapshotWindow": "09:00-10:00",
            "NodeSnapshots": [
                {
                    "CacheNodeId": "0001",
                    "CacheSize": "5 MB",
                    "CacheNodeCreateTime": "2019-11-25T23:56:17.186Z",
                    "SnapshotCreateTime": "2019-11-26T03:08:33Z"
                }
            ]
        }
    ]
}
```


Para obtener más información, consulte Backup and Restore for ElastiCache for Redis en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DescribeSnapshots en la Referencia de comandos de la AWS CLI.

`describe-update-actions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-update-actions`.

AWS CLI

Para describir acciones de actualización

En el siguiente ejemplo de `describe-update-actions`, se devuelven detalles de las acciones de actualización.

```
aws elasticache describe-update-actions
```

Salida:

```
{
    "UpdateActions": [
        {
            "ReplicationGroupId": "mycluster",
            "ServiceUpdateName": "elc-20191007-001",
            "ServiceUpdateReleaseDate": "2019-10-09T16:00:00Z",
            "ServiceUpdateSeverity": "important",
            "ServiceUpdateStatus": "available",
            "ServiceUpdateRecommendedApplyByDate": "2019-11-08T15:59:59Z",
            "ServiceUpdateType": "security-update",
            "UpdateActionAvailableDate": "2019-12-05T19:15:19.995Z",
            "UpdateActionStatus": "complete",
            "NodesUpdated": "9/9",
            "UpdateActionStatusModifiedDate": "2019-12-05T19:15:20.461Z",
            "SlaMet": "n/a",
            "Engine": "redis"
        },
        {
            "CacheClusterId": "my-memcached-cluster",
            "ServiceUpdateName": "elc-20191007-001",
            "ServiceUpdateReleaseDate": "2019-10-09T16:00:00Z",
            "ServiceUpdateSeverity": "important",
            "ServiceUpdateStatus": "available",
            "ServiceUpdateRecommendedApplyByDate": "2019-11-08T15:59:59Z",
```

```
            "ServiceUpdateType": "security-update",
            "UpdateActionAvailableDate": "2019-12-04T18:26:05.349Z",
            "UpdateActionStatus": "complete",
            "NodesUpdated": "1/1",
            "UpdateActionStatusModifiedDate": "2019-12-04T18:26:05.352Z",
            "SlaMet": "n/a",
            "Engine": "redis"
        },
        {
            "ReplicationGroupId": "my-cluster",
            "ServiceUpdateName": "elc-20191007-001",
            "ServiceUpdateReleaseDate": "2019-10-09T16:00:00Z",
            "ServiceUpdateSeverity": "important",
            "ServiceUpdateStatus": "available",
            "ServiceUpdateRecommendedApplyByDate": "2019-11-08T15:59:59Z",
            "ServiceUpdateType": "security-update",
            "UpdateActionAvailableDate": "2019-11-26T03:36:26.320Z",
            "UpdateActionStatus": "complete",
            "NodesUpdated": "4/4",
            "UpdateActionStatusModifiedDate": "2019-12-04T22:11:12.664Z",
            "SlaMet": "n/a",
            "Engine": "redis"
        },
        {
            "ReplicationGroupId": "my-cluster2",
            "ServiceUpdateName": "elc-20191007-001",
            "ServiceUpdateReleaseDate": "2019-10-09T16:00:00Z",
            "ServiceUpdateSeverity": "important",
            "ServiceUpdateStatus": "available",
            "ServiceUpdateRecommendedApplyByDate": "2019-11-08T15:59:59Z",
            "ServiceUpdateType": "security-update",
            "UpdateActionAvailableDate": "2019-11-26T01:26:01.617Z",
            "UpdateActionStatus": "complete",
            "NodesUpdated": "3/3",
            "UpdateActionStatusModifiedDate": "2019-11-26T01:26:01.753Z",
            "SlaMet": "n/a",
            "Engine": "redis"
        }
    ]
}
```


Para obtener más información, consulte Self-Service Updates in Amazon ElastiCache en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DescribeUpdateActions en la Referencia de comandos de la AWS CLI.

`describe-user-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-user-groups`.

AWS CLI

Para describir grupos de usuarios

En el siguiente ejemplo de `describe-user-groups`, se devuelve una lista de grupos de usuarios.

```
aws elasticache describe-user-groups
```

Salida:

```
{
    "UserGroups": [
        {
            "UserGroupId": "myusergroup",
            "Status": "active",
            "Engine": "redis",
            "UserIds": [
                "default"
            ],
            "ReplicationGroups": [],
            "ARN": "arn:aws:elasticache:us-
west-2:xxxxxxxxxx52:usergroup:myusergroup"
        }
    ]
}
```

Para obtener más información, consulte Authenticating Users with Role-Based Access Control (RBAC) en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DescribeUserGroups en la Referencia de comandos de la AWS CLI.

describe-users

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-users`.

AWS CLI

Para describir usuarios

En el siguiente ejemplo de `describe-users`, se devuelve una lista de recursos.

```
aws elasticache describe-users
```

Salida:

```
{
    "Users": [
        {
            "UserId": "default",
            "UserName": "default",
            "Status": "active",
            "Engine": "redis",
            "AccessString": "on ~* +@all",
            "UserGroupIds": [
                "myusergroup"
            ],
            "Authentication": {
                "Type": "no-password"
            },
            "ARN": "arn:aws:elasticache:us-west-2:xxxxxxxxxx52:user:default"
        },
        {
            "UserId": "user1",
            "UserName": "myUser",
            "Status": "active",
            "Engine": "redis",
            "AccessString": "on ~* +@all",
            "UserGroupIds": [],
            "Authentication": {
                "Type": "password",
                "PasswordCount": 1
            },
            "ARN": "arn:aws:elasticache:us-west-2:xxxxxxxxxx52:user:user1"
        },
```

```
        {
            "UserId": "user2",
            "UserName": "myUser",
            "Status": "active",
            "Engine": "redis",
            "AccessString": "on ~app::* -@all +@read +@hash +@bitmap +@geo -setbit -
bitfield -hset -hsetnx -hmset -hincrby -hincrbyfloat -hdel -bitop -geoadd -georadius
 -georadiusbymember",
            "UserGroupIds": [],
            "Authentication": {
                "Type": "password",
                "PasswordCount": 1
            },
            "ARN": "arn:aws:elasticache:us-west-2:xxxxxxxxxx52:user:user2"
        }
    ]
}
```

Para obtener más información, consulte Authenticating Users with Role-Based Access Control (RBAC) en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DescribeUsers en la Referencia de comandos de la AWS CLI.

`disassociate-global-replication-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-global-replication-group`.

AWS CLI

Para desasociar un clúster secundario de un grupo de replicación global

En el siguiente ejemplo de `disassociate-global-replication-group`, se elimina un clúster secundario de un almacén de datos global.

```
aws elasticache disassociate-global-replication-group \
    --global-replication-group-id my-grg \
    --replication-group-id my-cluster-grg-secondary \
    --replication-group-region us-east-1
```

Salida:

```
{
    "GlobalReplicationGroup": {
        "GlobalReplicationGroupId": "my-grg",
        "GlobalReplicationGroupDescription": "my-grg",
        "Status": "modifying",
        "CacheNodeType": "cache.r5.large",
        "Engine": "redis",
        "EngineVersion": "5.0.6",
        "Members": [
            {
                "ReplicationGroupId": "my-cluster-grg-secondary",
                "ReplicationGroupRegion": "us-east-1",
                "Role": "SECONDARY",
                "AutomaticFailover": "enabled",
                "Status": "associated"
            },
            {
                "ReplicationGroupId": "my-cluster-grg",
                "ReplicationGroupRegion": "us-west-2",
                "Role": "PRIMARY",
                "AutomaticFailover": "enabled",
                "Status": "associated"
            }
        ],
        "ClusterEnabled": false,
        "AuthTokenEnabled": false,
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
}
```

Para obtener más información, consulte Replication Across AWS Regions Using Global Datastore en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte DisassociateGlobalReplicationGroup en Referencia de comandos de la AWS CLI.

`increase-node-groups-in-global-replication-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `increase-node-groups-in-global-replication-group`.

AWS CLI

Para aumentar el número de grupos de nodos en un grupo de replicación global

En el siguiente `increase-node-groups-in-global-replication-group`, se aumenta el número de grupos de nodos mediante el motor de Redis.

```
aws elasticache increase-node-groups-in-global-replication-group \
    --global-replication-group-id sgaui-pat-test-4 \
    --node-group-count 6 \
    --apply-immediately
```

Salida:

```
{
    "GlobalReplicationGroup": {
        "GlobalReplicationGroupId": "sgaui-test-4",
        "GlobalReplicationGroupDescription": "test-4",
        "Status": "modifying",
        "CacheNodeType": "cache.r5.large",
        "Engine": "redis",
        "EngineVersion": "5.0.6",
        "Members": [
            {
                "ReplicationGroupId": "my-cluster-b",
                "ReplicationGroupRegion": "us-east-1",
                "Role": "SECONDARY",
                "AutomaticFailover": "enabled",
                "Status": "associated"
            },
            {
                "ReplicationGroupId": "my-cluster-a",
                "ReplicationGroupRegion": "us-west-2",
                "Role": "PRIMARY",
                "AutomaticFailover": "enabled",
                "Status": "associated"
            }
        ],
        "ClusterEnabled": true,
        "GlobalNodeGroups": [
            {
                "GlobalNodeGroupId": "sgaui-test-4-0001",
                "Slots": "0-234,2420-5461"
```

```
            },
            {
                "GlobalNodeGroupId": "sgaui-test-4-0002",
                "Slots": "5462-5904,6997-9830"
            },
            {
                "GlobalNodeGroupId": "sgaui-test-4-0003",
                "Slots": "10923-11190,13375-16383"
            },
            {
                "GlobalNodeGroupId": "sgaui-test-4-0004",
                "Slots": "235-2419,5905-6996"
            },
            {
                "GlobalNodeGroupId": "sgaui-test-4-0005",
                "Slots": "9831-10922,11191-13374"
            }
        ],
        "AuthTokenEnabled": false,
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
}
```

Para obtener más información, consulte Replication Across AWS Regions Using Global Datastore en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte IncreaseNodeGroupsInGlobalReplicationGroup en Referencia de comandos de la AWS CLI.

`increase-replica-count`

En el siguiente ejemplo de código, se muestra cómo utilizar `increase-replica-count`.

AWS CLI

Para aumentar el número de réplicas

En el siguiente ejemplo de `increase-replica-count`, se lleva a cabo una de las dos acciones siguientes: Puede aumentar de manera dinámica el número de réplicas en un grupo de replicación (modo de clúster deshabilitado) de Redis. O puede aumentar de manera dinámica el número de nodos de réplica en uno o más grupos de nodos (particiones) de un grupo de

replicación (modo de clúster habilitado) de Redis. Esta operación se realiza sin tiempo de inactividad del clúster.

```
aws elasticache increase-replica-count \
    --replication-group-id "my-cluster" \
    --apply-immediately \
    --new-replica-count 3
```

Salida:

```
{
     "ReplicationGroup": {
         "ReplicationGroupId": "my-cluster",
         "Description": " ",
         "Status": "modifying",
         "PendingModifiedValues": {},
         "MemberClusters": [
             "my-cluster-001",
             "my-cluster-002",
             "my-cluster-003",
             "my-cluster-004"
         ],
         "NodeGroups": [
             {
                 "NodeGroupId": "0001",
                 "Status": "modifying",
                 "PrimaryEndpoint": {
                     "Address": "my-
cluster.xxxxxih.ng.0001.usw2.cache.amazonaws.com",
                     "Port": 6379
                 },
                 "ReaderEndpoint": {
                     "Address": "my-cluster-
ro.xxxxxxih.ng.0001.usw2.cache.amazonaws.com",
                     "Port": 6379
                 },
                 "NodeGroupMembers": [
                     {
                         "CacheClusterId": "my-cluster-001",
                         "CacheNodeId": "0001",
                         "ReadEndpoint": {
                             "Address": "my-
cluster-001.xxxxxih.0001.usw2.cache.amazonaws.com",
```

```
                            "Port": 6379
                        },
                        "PreferredAvailabilityZone": "us-west-2a",
                        "CurrentRole": "primary"
                    },
                    {
                        "CacheClusterId": "my-cluster-003",
                        "CacheNodeId": "0001",
                        "ReadEndpoint": {
                            "Address": "my-
cluster-003.xxxxxih.0001.usw2.cache.amazonaws.com",
                            "Port": 6379
                        },
                        "PreferredAvailabilityZone": "us-west-2a",
                        "CurrentRole": "replica"
                    }
                ]
            }
        ],
        "AutomaticFailover": "disabled",
        "SnapshotRetentionLimit": 0,
        "SnapshotWindow": "07:30-08:30",
        "ClusterEnabled": false,
        "CacheNodeType": "cache.r5.xlarge",
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
}
```

Para obtener más información, consulte Increasing the Number of Replicas in a Shard en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte IncreaseReplicaCount en la Referencia de comandos de la AWS CLI.

`list-allowed-node-type-modifications`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-allowed-node-type-modifications`.

AWS CLI

Para enumerar las modificaciones de nodo permitidas

En el siguiente ejemplo de `list-allowed-node-type-modifications`, se muestran todos los tipos de nodos disponibles a los que puede escalar el tipo de nodo actual de su grupo de replicación o clúster de Redis.

```
aws elasticache list-allowed-node-type-modifications \
    --replication-group-id "my-replication-group"
```

Salida:

```
{
    "ScaleUpModifications": [
        "cache.m5.12xlarge",
        "cache.m5.24xlarge",
        "cache.m5.4xlarge",
        "cache.r5.12xlarge",
        "cache.r5.24xlarge",
        "cache.r5.2xlarge",
        "cache.r5.4xlarge"
    ],
    "ScaleDownModifications": [
        "cache.m3.large",
        "cache.m3.medium",
        "cache.m3.xlarge",
        "cache.m4.large",
        "cache.m4.xlarge",
        "cache.m5.2xlarge",
        "cache.m5.large",
        "cache.m5.xlarge",
        "cache.r3.large",
        "cache.r4.large",
        "cache.r4.xlarge",
        "cache.r5.large",
        "cache.t2.medium",
        "cache.t2.micro",
        "cache.t2.small",
        "cache.t3.medium",
        "cache.t3.micro",
        "cache.t3.small"
    ]
}
```

Para obtener más información, consulte Scaling ElastiCache for Redis Clusters en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte ListAllowedNodeTypeModifications en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran las etiquetas para un recurso.

```
aws elasticache list-tags-for-resource \
    --resource-name "arn:aws:elasticache:us-east-1:123456789012:cluster:my-cluster"
```

Salida:

```
{
    "TagList": [
        {
            "Key": "Project",
            "Value": "querySpeedUp"
        },
        {
            "Key": "Environment",
            "Value": "PROD"
        }
    ]
}
```

Para obtener más información, consulte Listing Tags Using the AWS CLI en la Guía del usuario de ElastiCache.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`modify-cache-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-cache-cluster`.

AWS CLI

Para modificar los clústeres de caché

En el siguiente ejemplo de `modify-cache-cluster`, se modifica la configuración del clúster especificado.

```
aws elasticache modify-cache-cluster \
    --cache-cluster-id "my-cluster" \
    --num-cache-nodes 1
```

Salida:

```
{
    "CacheCluster": {
        "CacheClusterId": "my-cluster",
        "ClientDownloadLandingPage": "https://console.aws.amazon.com/elasticache/
home#client-download:",
        "CacheNodeType": "cache.m5.large",
        "Engine": "redis",
        "EngineVersion": "5.0.5",
        "CacheClusterStatus": "available",
        "NumCacheNodes": 1,
        "PreferredAvailabilityZone": "us-west-2c",
        "CacheClusterCreateTime": "2019-12-04T18:24:56.652Z",
        "PreferredMaintenanceWindow": "sat:10:00-sat:11:00",
        "PendingModifiedValues": {},
        "CacheSecurityGroups": [],
        "CacheParameterGroup": {
            "CacheParameterGroupName": "default.redis5.0",
            "ParameterApplyStatus": "in-sync",
            "CacheNodeIdsToReboot": []
        },
        "CacheSubnetGroupName": "default",
        "AutoMinorVersionUpgrade": true,
        "SnapshotRetentionLimit": 0,
        "SnapshotWindow": "07:00-08:00",
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
```

```
    }
}
```

Para obtener más información, consulte Modifying an ElastiCache Cluster en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte ModifyCacheCluster en la Referencia de comandos de la AWS CLI.

`modify-cache-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-cache-parameter-group`.

AWS CLI

Para modificar un grupo de parámetros de caché

En el siguiente ejemplo de `modify-cache-parameter-group`, se modifica los parámetros del grupo de parámetros de caché especificado.

```
aws elasticache modify-cache-parameter-group \
    --cache-parameter-group-name "mygroup" \
    --parameter-name-values "ParameterName=activedefrag, ParameterValue=no"
```

Salida:

```
{
    "CacheParameterGroupName": "mygroup"
}
```

Para obtener más información, consulte Modifying a Parameter Group en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte ModifyCacheParameterGroup en la Referencia de comandos de la AWS CLI.

`modify-cache-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-cache-subnet-group`.

AWS CLI

Para modificar un grupo de subredes de caché

En el siguiente ejemplo de `modify-cache-subnet-group`, se modifica el grupo de subredes de caché especificado.

```
aws elasticache modify-cache-subnet-group \
    --cache-subnet-group-name kxkxk \
    --cache-subnet-group-description "mygroup"
```

Salida:

```
{
    "CacheSubnetGroup": {
        "CacheSubnetGroupName": "kxkxk",
        "CacheSubnetGroupDescription": "mygroup",
        "VpcId": "vpc-xxxxcdb",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-xxxxbff",
                "SubnetAvailabilityZone": {
                    "Name": "us-west-2a"
                }
            }
        ]
    }
}
```

Para obtener más información, consulte Modifying a Subnet Group en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte ModifyCacheSubnetGroup en la Referencia de comandos de la AWS CLI.

`modify-global-replication-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-global-replication-group`.

AWS CLI

Para modificar un grupo de replicación global

En el siguiente `modify-global-replication-group`, se modifican las propiedades de un grupo de replicación global y, en este caso, se deshabilita la conmutación por error automática mediante el motor de Redis.

```
aws elasticache modify-global-replication-group \
    --global-replication-group-id sgaui-pat-group \
    --apply-immediately \
    --no-automatic-failover-enabled
```

Output

```
{
    "GlobalReplicationGroup": {
        "GlobalReplicationGroupId": "sgaui-test-group",
        "GlobalReplicationGroupDescription": " ",
        "Status": "modifying",
        "CacheNodeType": "cache.r5.large",
        "Engine": "redis",
        "EngineVersion": "5.0.6",
        "ClusterEnabled": false,
        "AuthTokenEnabled": false,
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
}
```

Para obtener más información, consulte Replication Across AWS Regions Using Global Datastore en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte ModifyGlobalReplicationGroup en la Referencia de comandos de la AWS CLI.

`modify-replication-group-shard-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-replication-group-shard-configuration`.

AWS CLI

Para modificar una configuración de partición de grupo de replicación

El siguiente `modify-replication-group-shard-configuration` reduce el recuento de grupos de nodos mediante el motor de Redis.

```
aws elasticache modify-replication-group-shard-configuration \
    --replication-group-id mycluster \
    --node-group-count 3 \
    --apply-immediately \
    --node-groups-to-remove 0002
```

Output

```
{
    "ReplicationGroup": {
        "ReplicationGroupId": "mycluster",
        "Description": "mycluster",
        "GlobalReplicationGroupInfo": {},
        "Status": "modifying",
        "PendingModifiedValues": {},
        "MemberClusters": [
            "mycluster-0002-001",
            "mycluster-0002-002",
            "mycluster-0002-003",
            "mycluster-0003-001",
            "mycluster-0003-002",
            "mycluster-0003-003",
            "mycluster-0003-004",
            "mycluster-0004-001",
            "mycluster-0004-002",
            "mycluster-0004-003",
            "mycluster-0005-001",
            "mycluster-0005-002",
            "mycluster-0005-003"
        ],
        "NodeGroups": [
            {
                "NodeGroupId": "0002",
                "Status": "modifying",
                "Slots": "894-1767,3134-4443,5149-5461,6827-7332,12570-13662",
                "NodeGroupMembers": [
```

```
                    {
                        "CacheClusterId": "mycluster-0002-001",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2c"
                    },
                    {
                        "CacheClusterId": "mycluster-0002-002",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2a"
                    },
                    {
                        "CacheClusterId": "mycluster-0002-003",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2b"
                    }
                ]
            },
            {
                "NodeGroupId": "0003",
                "Status": "modifying",
                "Slots":
"0-324,5462-5692,6784-6826,7698-8191,10923-11075,12441-12569,13663-16383",
                "NodeGroupMembers": [
                    {
                        "CacheClusterId": "mycluster-0003-001",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2c"
                    },
                    {
                        "CacheClusterId": "mycluster-0003-002",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2b"
                    },
                    {
                        "CacheClusterId": "mycluster-0003-003",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2a"
                    },
                    {
                        "CacheClusterId": "mycluster-0003-004",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2c"
                    }
                ]
```

```
            },
            {
                "NodeGroupId": "0004",
                "Status": "modifying",
                "Slots": "325-336,4706-5148,7333-7697,9012-10922,11076-12440",
                "NodeGroupMembers": [
                    {
                        "CacheClusterId": "mycluster-0004-001",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2b"
                    },
                    {
                        "CacheClusterId": "mycluster-0004-002",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2a"
                    },
                    {
                        "CacheClusterId": "mycluster-0004-003",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2c"
                    }
                ]
            },
            {
                "NodeGroupId": "0005",
                "Status": "modifying",
                "Slots": "337-893,1768-3133,4444-4705,5693-6783,8192-9011",
                "NodeGroupMembers": [
                    {
                        "CacheClusterId": "mycluster-0005-001",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2a"
                    },
                    {
                        "CacheClusterId": "mycluster-0005-002",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2c"
                    },
                    {
                        "CacheClusterId": "mycluster-0005-003",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2b"
                    }
                ]
```

```
            }
        ],
        "AutomaticFailover": "enabled",
        "MultiAZ": "enabled",
        "ConfigurationEndpoint": {
            "Address": "mycluster.g2xbih.clustercfg.usw2.cache.amazonaws.com",
            "Port": 6379
        },
        "SnapshotRetentionLimit": 1,
        "SnapshotWindow": "13:00-14:00",
        "ClusterEnabled": true,
        "CacheNodeType": "cache.r5.xlarge",
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
}
```

Para obtener más información, consulte Scaling ElastiCache for Redis Clusters en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte ModifyReplicationGroupShardConfiguration en la Referencia de comandos de la AWS CLI.

`modify-replication-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-replication-group`.

AWS CLI

Para modificar un grupo de replicación

El siguiente `modify-replication-group` deshabilita Multi-AZ mediante el motor de Redis.

```
aws elasticache modify-replication-group \
    --replication-group-id test-cluster \
    --no-multi-az-enabled \
    --apply-immediately
```

Output

```
{
    "ReplicationGroup": {
        "ReplicationGroupId": "test-cluster",
```

```
        "Description": "test-cluster",
        "GlobalReplicationGroupInfo": {
            "GlobalReplicationGroupId": "sgaui-pat-group",
            "GlobalReplicationGroupMemberRole": "PRIMARY"
        },
        "Status": "available",
        "PendingModifiedValues": {},
        "MemberClusters": [
            "test-cluster-001",
            "test-cluster-002",
            "test-cluster-003"
        ],
        "NodeGroups": [
            {
                "NodeGroupId": "0001",
                "Status": "available",
                "PrimaryEndpoint": {
                    "Address": "test-
cluster.g2xbih.ng.0001.usw2.cache.amazonaws.com",
                    "Port": 6379
                },
                "ReaderEndpoint": {
                    "Address": "test-cluster-
ro.g2xbih.ng.0001.usw2.cache.amazonaws.com",
                    "Port": 6379
                },
                "NodeGroupMembers": [
                    {
                        "CacheClusterId": "test-cluster-001",
                        "CacheNodeId": "0001",
                        "ReadEndpoint": {
                            "Address": "test-
cluster-001.g2xbih.0001.usw2.cache.amazonaws.com",
                            "Port": 6379
                        },
                        "PreferredAvailabilityZone": "us-west-2c",
                        "CurrentRole": "primary"
                    },
                    {
                        "CacheClusterId": "test-cluster-002",
                        "CacheNodeId": "0001",
                        "ReadEndpoint": {
                            "Address": "test-
cluster-002.g2xbih.0001.usw2.cache.amazonaws.com",
```

```
                            "Port": 6379
                        },
                        "PreferredAvailabilityZone": "us-west-2b",
                        "CurrentRole": "replica"
                    },
                    {
                        "CacheClusterId": "test-cluster-003",
                        "CacheNodeId": "0001",
                        "ReadEndpoint": {
                            "Address": "test-
cluster-003.g2xbih.0001.usw2.cache.amazonaws.com",
                            "Port": 6379
                        },
                        "PreferredAvailabilityZone": "us-west-2a",
                        "CurrentRole": "replica"
                    }
                ]
            }
        ],
        "SnapshottingClusterId": "test-cluster-002",
        "AutomaticFailover": "enabled",
        "MultiAZ": "disabled",
        "SnapshotRetentionLimit": 1,
        "SnapshotWindow": "08:00-09:00",
        "ClusterEnabled": false,
        "CacheNodeType": "cache.r5.large",
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
}
```

Para obtener más información, consulte Modifying a Replication Group en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte ModifyReplicationGroup en la Referencia de comandos de la AWS CLI.

`modify-user-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-user-group`.

AWS CLI

Para modificar un grupo de usuarios

En el siguiente ejemplo de `modify-user-group`, se agrega un usuario al grupo de usuarios.

```
aws elasticache modify-user-group \
    --user-group-id myusergroup \
    --user-ids-to-add user1
```

Salida:

```
{
    "UserGroupId": "myusergroup",
    "Status": "modifying",
    "Engine": "redis",
    "UserIds": [
        "default"
    ],
    "PendingChanges": {
        "UserIdsToAdd": [
            "user1"
        ]
    },
    "ReplicationGroups": [],
    "ARN": "arn:aws:elasticache:us-west-2:xxxxxxxxxx52:usergroup:myusergroup"
}
```

Para obtener más información, consulte Authenticating Users with Role-Based Access Control (RBAC) en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte ModifyUserGroup en la Referencia de comandos de la AWS CLI.

`modify-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-user`.

AWS CLI

Para modificar un usuario

En el siguiente ejemplo de `modify-user`, se modifica la cadena de acceso de un usuario.

```
aws elasticache modify-user \
    --user-id user2 \
    --append-access-string "on ~* +@all"
```

Salida:

```
{
    "UserId": "user2",
    "UserName": "myUser",
    "Status": "modifying",
    "Engine": "redis",
    "AccessString": "on ~* +@all",
    "UserGroupIds": [],
    "Authentication": {
        "Type": "password",
        "PasswordCount": 1
    },
    "ARN": "arn:aws:elasticache:us-west-2:xxxxxxxxxx52:user:user2"
}
```

Para obtener más información, consulte Authenticating Users with Role-Based Access Control (RBAC) en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte ModifyUser en la Referencia de comandos de la AWS CLI.

`purchase-reserved-cache-nodes-offering`

En el siguiente ejemplo de código, se muestra cómo utilizar `purchase-reserved-cache-nodes-offering`.

AWS CLI

Para adquirir una reserved-cache-node-offering

En el siguiente ejemplo de `purchase-reserved-cache-nodes-offering`, se le permite comprar una oferta de nodo de caché reservada.

```
aws elasticache purchase-reserved-cache-nodes-offering \
    --reserved-cache-nodes-offering-id xxxxxxx-4da5-4b90-b92d-929fbd7abed2
```

Output

```
{
    "ReservedCacheNode": {
        "ReservedCacheNodeId": "ri-2020-06-30-17-59-40-474",
        "ReservedCacheNodesOfferingId": "xxxxxxx-4da5-4b90-b92d-929fbd7abed2",
        "CacheNodeType": "cache.m3.2xlarge",
        "StartTime": "2020-06-30T17:59:40.474000+00:00",
        "Duration": 31536000,
        "FixedPrice": 1772.0,
        "UsagePrice": 0.0,
        "CacheNodeCount": 1,
        "ProductDescription": "redis",
        "OfferingType": "Heavy Utilization",
        "State": "payment-pending",
        "RecurringCharges": [
            {
                "RecurringChargeAmount": 0.25,
                "RecurringChargeFrequency": "Hourly"
            }
        ]
    }
}
```

Para obtener más información, consulte Getting Info About Reserved Node Offerings en la Guía del usuario de Elasticache para Redis o Getting Info About Reserved Node Offerings en la Guía del usuario de Elasticache para Memcached.

- Para obtener más información, consulte PurchaseReservedCacheNodesOffering en la Referencia de comandos de la AWS CLI.

`reboot-cache-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `reboot-cache-cluster`.

AWS CLI

Para reiniciar un clúster de caché

En el siguiente ejemplo de `reboot-cache-cluster`, se reinicia parte o la totalidad de los nodos de caché dentro de un clúster aprovisionado. Esta operación aplica cualquier grupo de parámetros de caché modificado al clúster. La operación de reinicio se lleva a cabo lo antes

posible y provoca una interrupción momentánea del clúster. Durante el reinicio, el estado del clúster se establece en `REBOOTING`.

```
aws elasticache reboot-cache-cluster \
    --cache-cluster-id "my-cluster-001" \
    --cache-node-ids-to-reboot "0001"
```

Salida:

```
{
    "CacheCluster": {
        "CacheClusterId": "my-cluster-001",
        "ClientDownloadLandingPage": "https://console.aws.amazon.com/elasticache/
home#client-download:",
        "CacheNodeType": "cache.r5.xlarge",
        "Engine": "redis",
        "EngineVersion": "5.0.5",
        "CacheClusterStatus": "rebooting cache cluster nodes",
        "NumCacheNodes": 1,
        "PreferredAvailabilityZone": "us-west-2a",
        "CacheClusterCreateTime": "2019-11-26T03:35:04.546Z",
        "PreferredMaintenanceWindow": "mon:04:05-mon:05:05",
        "PendingModifiedValues": {},
        "NotificationConfiguration": {
            "TopicArn": "arn:aws:sns:us-west-2:xxxxxxxxxx152:My_Topic",
            "TopicStatus": "active"
        },
        "CacheSecurityGroups": [],
        "CacheParameterGroup": {
            "CacheParameterGroupName": "mygroup",
            "ParameterApplyStatus": "in-sync",
            "CacheNodeIdsToReboot": []
        },
        "CacheSubnetGroupName": "kxkxk",
        "AutoMinorVersionUpgrade": true,
        "SecurityGroups": [
            {
                "SecurityGroupId": "sg-xxxxxxxxxxxxx836",
                "Status": "active"
            },
            {
                "SecurityGroupId": "sg-xxxxxxxx7b",
                "Status": "active"
```

```
            }
        ],
        "ReplicationGroupId": "my-cluster",
        "SnapshotRetentionLimit": 0,
        "SnapshotWindow": "07:30-08:30",
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
}
```

Para obtener más información, consulte Rebooting a Cluster <https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/Clusters.Rebooting.html en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte RebootCacheCluster en la Referencia de comandos de la AWS CLI.

`reset-cache-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-cache-parameter-group`.

AWS CLI

Restablecimiento de un grupo de parámetros de caché

En el siguiente ejemplo de `reset-cache-parameter-group`, se modifican los parámetros de un grupo de parámetros de caché al valor predeterminado del sistema o del motor. Puede restablecer parámetros específicos enviando una lista de nombres de parámetros. Para restablecer el grupo de parámetros de caché completo, especifique los parámetros `--reset-all-parameters` y `--cache-parameter-group-name`.

```
aws elasticache reset-cache-parameter-group \
    --cache-parameter-group-name "mygroup" \
    --reset-all-parameters
```

Salida:

```
{
    "CacheParameterGroupName": "mygroup"
}
```

- Para ver los detalles de la API, consulte ResetCacheParameterGroup en la Referencia de comandos de la AWS CLI.

`start-migration`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-migration`.

AWS CLI

Para iniciar una migración

El siguiente `start-migration` migra los datos desde Redis autoalojados en Amazon EC2 a Amazon ElastiCache mediante el motor de Redis.

```
aws elasticache start-migration \
   --replication-group-id test \
   --customer-node-endpoint-
list "Address='test.g2xbih.ng.0001.usw2.cache.amazonaws.com',Port=6379"
```

Output

```
{
    "ReplicationGroup": {
        "ReplicationGroupId": "test",
        "Description": "test",
        "GlobalReplicationGroupInfo": {},
        "Status": "modifying",
        "PendingModifiedValues": {},
        "MemberClusters": [
            "test-001",
            "test-002",
            "test-003"
        ],
        "NodeGroups": [
            {
                "NodeGroupId": "0001",
                "Status": "available",
                "PrimaryEndpoint": {
                    "Address": "test.g2xbih.ng.0001.usw2.cache.amazonaws.com",
                    "Port": 6379
                },
                "ReaderEndpoint": {
```

```
                    "Address": "test-ro.g2xbih.ng.0001.usw2.cache.amazonaws.com",
                    "Port": 6379
                },
                "NodeGroupMembers": [
                    {
                        "CacheClusterId": "test-001",
                        "CacheNodeId": "0001",
                        "ReadEndpoint": {
                            "Address":
"test-001.g2xbih.0001.usw2.cache.amazonaws.com",
                            "Port": 6379
                        },
                        "PreferredAvailabilityZone": "us-west-2a",
                        "CurrentRole": "primary"
                    },
                    {
                        "CacheClusterId": "test-002",
                        "CacheNodeId": "0001",
                        "ReadEndpoint": {
                            "Address":
"test-002.g2xbih.0001.usw2.cache.amazonaws.com",
                            "Port": 6379
                        },
                        "PreferredAvailabilityZone": "us-west-2c",
                        "CurrentRole": "replica"
                    },
                    {
                        "CacheClusterId": "test-003",
                        "CacheNodeId": "0001",
                        "ReadEndpoint": {
                            "Address":
"test-003.g2xbih.0001.usw2.cache.amazonaws.com",
                            "Port": 6379
                        },
                        "PreferredAvailabilityZone": "us-west-2b",
                        "CurrentRole": "replica"
                    }
                ]
            }
        ],
        "SnapshottingClusterId": "test-002",
        "AutomaticFailover": "enabled",
        "MultiAZ": "enabled",
        "SnapshotRetentionLimit": 1,
```

```
        "SnapshotWindow": "07:30-08:30",
        "ClusterEnabled": false,
        "CacheNodeType": "cache.r5.large",
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
}
```

Para obtener más información, consulte Online Migration to ElastiCache en la Guía del usuario de ElastiCache.

- Para obtener información sobre la API, consulte StartMigration en la Referencia de comandos de la AWS CLI.

`test-failover`

En el siguiente ejemplo de código, se muestra cómo utilizar `test-failover`.

AWS CLI

Para probar la conmutación por error de un grupo de nodos

En el siguiente ejemplo de `test-failover`, se prueba la conmutación por error automática en el grupo de nodos especificado (llamado partición en la consola) es un grupo de replicación (llamado clúster en la consola).

```
aws elasticache test-failover /
    --replication-group-id "mycluster" /
    --node-group-id "0001"
```

Salida:

```
{
    "ReplicationGroup": {
        "ReplicationGroupId": "mycluster",
        "Description": "My Cluster",
        "Status": "available",
        "PendingModifiedValues": {},
        "MemberClusters": [
            "mycluster-0001-001",
            "mycluster-0001-002",
            "mycluster-0001-003",
```

```
            "mycluster-0002-001",
            "mycluster-0002-002",
            "mycluster-0002-003",
            "mycluster-0003-001",
            "mycluster-0003-002",
            "mycluster-0003-003"
        ],
        "NodeGroups": [
            {
                "NodeGroupId": "0001",
                "Status": "available",
                "Slots": "0-5461",
                "NodeGroupMembers": [
                    {
                        "CacheClusterId": "mycluster-0001-001",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2b"
                    },
                    {
                        "CacheClusterId": "mycluster-0001-002",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2a"
                    },
                    {
                        "CacheClusterId": "mycluster-0001-003",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2c"
                    }
                ]
            },
            {
                "NodeGroupId": "0002",
                "Status": "available",
                "Slots": "5462-10922",
                "NodeGroupMembers": [
                    {
                        "CacheClusterId": "mycluster-0002-001",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2a"
                    },
                    {
                        "CacheClusterId": "mycluster-0002-002",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2b"
```

```
                    },
                    {
                        "CacheClusterId": "mycluster-0002-003",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2c"
                    }
                ]
            },
            {
                "NodeGroupId": "0003",
                "Status": "available",
                "Slots": "10923-16383",
                "NodeGroupMembers": [
                    {
                        "CacheClusterId": "mycluster-0003-001",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2c"
                    },
                    {
                        "CacheClusterId": "mycluster-0003-002",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2b"
                    },
                    {
                        "CacheClusterId": "mycluster-0003-003",
                        "CacheNodeId": "0001",
                        "PreferredAvailabilityZone": "us-west-2a"
                    }
                ]
            }
        ],
        "AutomaticFailover": "enabled",
        "ConfigurationEndpoint": {
            "Address": "mycluster.xxxxih.clustercfg.usw2.cache.amazonaws.com",
            "Port": 6379
        },
        "SnapshotRetentionLimit": 1,
        "SnapshotWindow": "13:00-14:00",
        "ClusterEnabled": true,
        "CacheNodeType": "cache.r5.large",
        "TransitEncryptionEnabled": false,
        "AtRestEncryptionEnabled": false
    }
```

```
}
```

- Para obtener información sobre la API, consulte TestFailover en la Referencia de comandos de la AWS CLI.

Ejemplos de MediaStore que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo ejecutar acciones e implementar escenarios comunes usando AWS Command Line Interface con MediaStore.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-container`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-container`.

AWS CLI

Para crear un contenedor

En el siguiente ejemplo de `create-container`, se crea un nuevo contenedor vacío.

```
aws mediastore create-container --container-name ExampleContainer
```

Salida:

```
{
    "Container": {
```

```
        "AccessLoggingEnabled": false,
        "CreationTime": 1563557265,
        "Name": "ExampleContainer",
        "Status": "CREATING",
        "ARN": "arn:aws:mediastore:us-west-2:111122223333:container/
ExampleContainer"
    }
}
```

Para obtener más información, consulte Creating a Container en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte CreateContainer en la Referencia de comandos de la AWS CLI.

`delete-container-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-container-policy`.

AWS CLI

Para eliminar una política de contenedor

En el siguiente ejemplo de `delete-container-policy`, se elimina la política asignada al contenedor especificado. Cuando se elimina la política, AWS Elemental MediaStore asigna automáticamente la política predeterminada al contenedor.

```
aws mediastore delete-container-policy \
    --container-name LiveEvents
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteContainerPolicy en la Referencia de la API de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte DeleteContainerPolicy en la Referencia de comandos de la AWS CLI.

`delete-container`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-container`.

AWS CLI

Para eliminar un contenedor

En el siguiente ejemplo de `delete-container`, se elimina el contenedor especificado. Un contenedor únicamente se puede eliminar si no tiene objetos.

```
aws mediastore delete-container \
    --container-name=ExampleLiveDemo
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting a Container en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte DeleteContainer en la Referencia de comandos de la AWS CLI.

`delete-cors-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-cors-policy`.

AWS CLI

Para eliminar una política del CORS

En el siguiente ejemplo de `delete-cors-policy`, se elimina la política de uso compartido de recursos entre orígenes (CORS) que está asignada al contenedor especificado.

```
aws mediastore delete-cors-policy \
    --container-name ExampleContainer
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting a CORS Policy en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte DeleteCorsPolicy en la Referencia de comandos de la AWS CLI.

`delete-lifecycle-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-lifecycle-policy`.

AWS CLI

Para eliminar una política de ciclo de vida de objetos

En el siguiente ejemplo de `delete-lifecycle-policy`, se elimina la política de ciclo de vida de objetos asociada al contenedor especificado. Este cambio puede tardar hasta 20 minutos en surtir efecto.

```
aws mediastore delete-lifecycle-policy \
    --container-name LiveEvents
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting an Object Lifecycle Policy en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte DeleteLifecyclePolicy en la Referencia de comandos de la AWS CLI.

`describe-container`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-container`.

AWS CLI

Para ver los detalles de un contenedor

En el siguiente ejemplo de `describe-container`, se muestran los detalles del contenedor especificado.

```
aws mediastore describe-container \
    --container-name ExampleContainer
```

Salida:

```
{
    "Container": {
        "CreationTime": 1563558086,
```

```
        "AccessLoggingEnabled": false,
        "ARN": "arn:aws:mediastore:us-west-2:111122223333:container/
ExampleContainer",
        "Status": "ACTIVE",
        "Name": "ExampleContainer",
        "Endpoint": "https://aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com"
    }
}
```

Para obtener más información, consulte Viewing the Details for a Container en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte DescribeContainer en la Referencia de comandos de la AWS CLI.

`describe-object`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-object`.

AWS CLI

Para ver una lista de objetos y carpetas de un contenedor específico

El siguiente ejemplo de `describe-object` muestra elementos (objetos y carpetas) almacenados en un contenedor específico.

```
aws mediastore-data describe-object \
    --endpoint https://aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com \
    --path /folder_name/file1234.jpg
```

Salida:

```
{
    "ContentType": "image/jpeg",
    "LastModified": "Fri, 19 Jul 2019 21:32:20 GMT",
    "ContentLength": "2307346",
    "ETag": "2aa333bbcc8d8d22d777e999c88d4aa9eeeeee4dd89ff7f555555555555da6d3"
}
```

Para obtener más información, consulte Viewing the Details of an Object en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte DescribeObject en la Referencia de comandos de la AWS CLI.

`get-container-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-container-policy`.

AWS CLI

Para ver una política de contenedor

En el siguiente ejemplo de `get-container-policy`, se muestra la política basada en recursos del contenedor especificado.

```
aws mediastore get-container-policy \
    --container-name ExampleLiveDemo
```

Salida:

```
{
    "Policy": {
        "Version":"2012-10-17",
        "Statement": [
            {
                "Sid": "PublicReadOverHttps",
                "Effect": "Allow",
                "Principal": {
                    "AWS": "arn:aws:iam::111122223333:root"
                },
                "Action": [
                    "mediastore:GetObject",
                    "mediastore:DescribeObject"
                ],
                "Resource": "arn:aws:mediastore:us-west-2:111122223333:container/
ExampleLiveDemo/",
                "Condition": {
                    "Bool": {
                        "aws:SecureTransport": "true"
                    }
                }
            }
        ]
```

```
    }
}
```

Para obtener más información, consulte Viewing a Container Policy en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte GetContainerPolicy en la Referencia de comandos de la AWS CLI.

`get-cors-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-cors-policy`.

AWS CLI

Para ver una política de CORS

En el siguiente ejemplo de `get-cors-policy`, se muestra la política de uso compartido de recursos entre orígenes (CORS) que está asignada al contenedor especificado.

```
aws mediastore get-cors-policy \
    --container-name ExampleContainer \
    --region us-west-2
```

Salida:

```
{
    "CorsPolicy": [
        {
            "AllowedMethods": [
                "GET",
                "HEAD"
            ],
            "MaxAgeSeconds": 3000,
            "AllowedOrigins": [
                ""
            ],
            "AllowedHeaders": [
                ""
            ]
        }
    ]
```

```
}
```

Para obtener más información, consulte Viewing a CORS Policy en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte GetCorsPolicy en la Referencia de comandos de la AWS CLI.

`get-lifecycle-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-lifecycle-policy`.

AWS CLI

Para ver una política de ciclo de vida de objetos

En el siguiente ejemplo de `get-lifecycle-policy`, se muestra la política de ciclo de vida de objetos asociada al contenedor especificado.

```
aws mediastore get-lifecycle-policy \
    --container-name LiveEvents
```

Salida:

```
{
    "LifecyclePolicy": {
        "rules": [
            {
                "definition": {
                    "path": [
                        {
                            "prefix": "Football/"
                        },
                        {
                            "prefix": "Baseball/"
                        }
                    ],
                    "days_since_create": [
                        {
                            "numeric": [
                                ">",
                                28
```

```
                        ]
                    }
                ]
            },
            "action": "EXPIRE"
        }
    ]
  }
}
```

Para obtener más información, consulte Viewing an Object Lifecycle Policy en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte GetLifecyclePolicy en la Referencia de comandos de la AWS CLI.

`get-object`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-object`.

AWS CLI

Para descargar un objeto

En el siguiente ejemplo de `get-object`, se descarga un objeto en el punto de conexión especificado.

```
aws mediastore-data get-object \
    --endpoint https://aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com \
    --path=/folder_name/README.md README.md
```

Salida:

```
{
    "ContentLength": "2307346",
    "ContentType": "image/jpeg",
    "LastModified": "Fri, 19 Jul 2019 21:32:20 GMT",
    "ETag": "2aa333bbcc8d8d22d777e999c88d4aa9eeeeee4dd89ff7f555555555555da6d3",
    "StatusCode": 200
}
```

Para descargar parte de un objeto

En el siguiente ejemplo de `get-object`, se descarga parte de un objeto en el punto de conexión especificado.

```
aws mediastore-data get-object \
    --endpoint https://aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com \
    --path /folder_name/README.md \
    --range="bytes=0-100" README2.md
```

Salida:

```
{
    "StatusCode": 206,
    "ContentRange": "bytes 0-100/2307346",
    "ContentLength": "101",
    "LastModified": "Fri, 19 Jul 2019 21:32:20 GMT",
    "ContentType": "image/jpeg",
    "ETag": "2aa333bbcc8d8d22d777e999c88d4aa9eeeeee4dd89ff7f555555555555da6d3"
}
```

Para obtener más información, consulte Downloading an Object en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte GetObject en la Referencia de comandos de AWS CLI.

`list-containers`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-containers`.

AWS CLI

Para ver una lista de contenedores

En el siguiente ejemplo de `list-containers`, se muestra una lista de todos los contenedores que están asociados a la cuenta.

```
aws mediastore list-containers
```

Salida:

```
{
```

```
    "Containers": [
        {
            "CreationTime": 1505317931,
            "Endpoint": "https://aaabbbcccdddee.data.mediastore.us-
west-2.amazonaws.com",
            "Status": "ACTIVE",
            "ARN": "arn:aws:mediastore:us-west-2:111122223333:container/
ExampleLiveDemo",
            "AccessLoggingEnabled": false,
            "Name": "ExampleLiveDemo"
        },
        {
            "CreationTime": 1506528818,
            "Endpoint": "https://fffggghhhiiijj.data.mediastore.us-
west-2.amazonaws.com",
            "Status": "ACTIVE",
            "ARN": "arn:aws:mediastore:us-west-2:111122223333:container/
ExampleContainer",
            "AccessLoggingEnabled": false,
            "Name": "ExampleContainer"
        }
    ]
}
```

Para obtener más información, consulte Viewing a List of Containers en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte ListContainers en la Referencia de comandos de la AWS CLI.

`list-items`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-items`.

AWS CLI

Ejemplo 1: ver una lista de objetos y carpetas de un contenedor específico

En el siguiente ejemplo de `list-items`, se muestran elementos (objetos y carpetas) almacenados en el contenedor especificado.

```
aws mediastore-data list-items \
```

```
    --endpoint https://aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com
```

Salida:

```
{
    "Items": [
        {
            "ContentType": "image/jpeg",
            "LastModified": 1563571859.379,
            "Name": "filename.jpg",
            "Type": "OBJECT",
            "ETag":
 "543ab21abcd1a234ab123456a1a2b12345ab12abc12a1234abc1a2bc12345a12",
            "ContentLength": 3784
        },
        {
            "Type": "FOLDER",
            "Name": "ExampleLiveDemo"
        }
    ]
}
```

Ejemplo 2: ver una lista de los objetos y las carpetas de una carpeta específica

En el siguiente ejemplo de `list-items`, se muestran elementos (objetos y carpetas) almacenados en una carpeta específica.

```
aws mediastore-data list-items \
    --endpoint https://aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com
```

Salida:

```
{
    "Items": [
        {
            "ContentType": "image/jpeg",
            "LastModified": 1563571859.379,
            "Name": "filename.jpg",
            "Type": "OBJECT",
            "ETag":
 "543ab21abcd1a234ab123456a1a2b12345ab12abc12a1234abc1a2bc12345a12",
```

```
            "ContentLength": 3784
        },
        {
            "Type": "FOLDER",
            "Name": "ExampleLiveDemo"
        }
    ]
}
```

Para obtener más información, consulte Viewing a List of Objects en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte ListItems en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un contenedor

En el siguiente ejemplo de `list-tags-for-resource`, se muestran las claves y los valores de etiqueta asignados al contenedor especificado.

```
aws mediastore list-tags-for-resource \
    --resource arn:aws:mediastore:us-west-2:1213456789012:container/ExampleContainer
```

Salida:

```
{
    "Tags": [
        {
            "Value": "Test",
            "Key": "Environment"
        },
        {
            "Value": "West",
            "Key": "Region"
        }
```

```
    ]
}
```

Para obtener más información, consulte ListTagsForResource en la Referencia de la API de AWS Elemental MediaStore.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-container-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-container-policy`.

AWS CLI

Para editar una política de contenedor

En el siguiente ejemplo de `put-container-policy`, se asigna una política diferente al contenedor especificado. En este ejemplo, la política actualizada se define en un archivo llamado `LiveEventsContainerPolicy.json`.

```
aws mediastore put-container-policy \
    --container-name LiveEvents \
    --policy file://LiveEventsContainerPolicy.json
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Editing a Container Policy en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte PutContainerPolicy en la Referencia de comandos de la AWS CLI.

`put-cors-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-cors-policy`.

AWS CLI

Ejemplo 1: añadir una política de CORS

En el siguiente ejemplo de `put-cors-policy`, se añade una política de uso compartido de recursos entre orígenes (CORS) al contenedor especificado. El contenido de la política de CORS se encuentra en el archivo llamado `corsPolicy.json`.

```
aws mediastore put-cors-policy \
    --container-name ExampleContainer \
    --cors-policy file://corsPolicy.json
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adding a CORS Policy to a Container en la Guía del usuario de AWS Elemental MediaStore.

Ejemplo 2: editar una política de CORS

En el siguiente ejemplo de `put-cors-policy`, se actualiza la política de uso compartido de recursos entre orígenes (CORS) que está asignada al contenedor especificado. El contenido de la política de CORS actualizada se encuentra en el archivo llamado `corsPolicy2.json`.

Para obtener más información, consulte Editing a CORS Policy en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información acerca de la API, consulte PutCorsPolicy en la Referencia de comandos de la AWS CLI.

`put-lifecycle-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-lifecycle-policy`.

AWS CLI

Para crear una política de ciclo de vida de objetos

En el siguiente ejemplo de `put-lifecycle-policy`, se asocia la política de ciclo de vida de objetos al contenedor especificado. Esto le permite especificar durante cuánto tiempo debe almacenar el servicio los objetos en su contenedor. MediaStore elimina los objetos del contenedor una vez que llegan a su fecha de caducidad, indicada en la política, que se encuentra en el archivo llamado `LiveEventsLifecyclePolicy.json`.

```
aws mediastore put-lifecycle-policy \
    --container-name ExampleContainer \
```

```
    --lifecycle-policy file://ExampleLifecyclePolicy.json
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adding an Object Lifecycle Policy to a Container en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte PutLifecyclePolicy en la Referencia de comandos de la AWS CLI.

put-object

En el siguiente ejemplo de código, se muestra cómo utilizar `put-object`.

AWS CLI

Para cargar un objeto

En el siguiente ejemplo de `put-object`, se carga un objeto en el contenedor especificado. Puede especificar una ruta de carpeta en la que se guardará el objeto dentro del contenedor. Si la carpeta ya existe, AWS Elemental MediaStore almacena el objeto en la carpeta. Si la carpeta no existe, el servicio la crea y, a continuación, almacena el objeto en ella.

```
aws mediastore-data put-object \
    --endpoint https://aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com \
    --body README.md \
    --path /folder_name/README.md \
    --cache-control "max-age=6, public" \
    --content-type binary/octet-stream
```

Salida:

```
{
    "ContentSHA256":
 "74b5fdb517f423ed750ef214c44adfe2be36e37d861eafe9c842cbe1bf387a9d",
    "StorageClass": "TEMPORAL",
    "ETag": "af3e4731af032167a106015d1f2fe934e68b32ed1aa297a9e325f5c64979277b"
}
```

Para obtener más información, consulte Uploading an Object en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte PutObject en la Referencia de comandos de AWS CLI.

`start-access-logging`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-access-logging`.

AWS CLI

Para habilitar el registro de acceso en un contenedor

En el siguiente ejemplo de `start-access-logging`, se habilita el registro de acceso en el contenedor especificado.

```
aws mediastore start-access-logging \
    --container-name LiveEvents
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Enabling Access Logging for a Container en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte StartAccessLogging en la Referencia de comandos de la AWS CLI.

`stop-access-logging`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-access-logging`.

AWS CLI

Para deshabilitar el registro de acceso en un contenedor

En el siguiente ejemplo de `stop-access-logging`, se deshabilita el registro de acceso en el contenedor especificado.

```
aws mediastore stop-access-logging \
    --container-name LiveEvents
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Disabling Access Logging for a Container en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte StopAccessLogging en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para añadir etiquetas a un contenedor

En el siguiente ejemplo de `tag-resource`, se añaden las claves y los valores de etiqueta al contenedor especificado.

```
aws mediastore tag-resource \
    --resource arn:aws:mediastore:us-west-2:123456789012:container/ExampleContainer
 \
    --tags '[{"Key": "Region", "Value": "West"}, {"Key": "Environment", "Value":
 "Test"}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte TagResource en la Referencia de la API de AWS Elemental MediaStore.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar etiquetas de un contenedor

En el siguiente ejemplo de `untag-resource`, se elimina la clave de etiqueta especificada y su valor asociado de un contenedor.

```
aws mediastore untag-resource \
    --resource arn:aws:mediastore:us-west-2:123456789012:container/ExampleContainer
 \
    --tag-keys Region
```

Este comando no genera ninguna salida.

Para obtener más información, consulte UntagResource en la Referencia de la API de AWS Elemental MediaStore.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon EMR que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon EMR.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-instance-fleet`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-instance-fleet`.

AWS CLI

Para agregar una flota de instancias de tarea a un clúster

En este ejemplo, se agrega una nueva flota de instancias de tareas al clúster especificado.

Comando:

```
aws emr add-instance-fleet --cluster-id 'j-12ABCDEFGHI34JK' --instance-fleet
 InstanceFleetType=TASK,TargetSpotCapacity=1,LaunchSpecifications={SpotSpecification='{Timeo
```

Salida:

```
{
   "ClusterId": "j-12ABCDEFGHI34JK",
   "InstanceFleetId": "if-23ABCDEFGHI45JJ"
}
```

- Para obtener información sobre la API, consulte AddInstanceFleet en la Referencia de comandos de la AWS CLI.

`add-steps`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-steps`.

AWS CLI

1. Para agregar pasos JAR personalizado a un clúster

Comando:

```
aws emr add-steps --cluster-id j-XXXXXXXX --steps
 Type=CUSTOM_JAR,Name=CustomJAR,ActionOnFailure=CONTINUE,Jar=s3://amzn-s3-demo-
bucket/mytest.jar,Args=arg1,arg2,arg3
 Type=CUSTOM_JAR,Name=CustomJAR,ActionOnFailure=CONTINUE,Jar=s3://amzn-s3-demo-
bucket/mytest.jar,MainClass=mymainclass,Args=arg1,arg2,arg3
```

Parámetros requeridos:

```
Jar
```

Parámetros opcionales:

```
Type, Name, ActionOnFailure, Args
```

Salida:

```
{
    "StepIds":[
        "s-XXXXXXXX",
        "s-YYYYYYYY"
    ]
}
```

2. Para agregar pasos de transmisión a un clúster

Comando:

```
aws emr add-steps --cluster-id j-XXXXXXXX --steps Type=STREAMING,Name='Streaming
 Program',ActionOnFailure=CONTINUE,Args=[-files,s3://elasticmapreduce/samples/
wordcount/wordSplitter.py,-mapper,wordSplitter.py,-reducer,aggregate,-input,s3://
elasticmapreduce/samples/wordcount/input,-output,s3://amzn-s3-demo-bucket/wordcount/
output]
```

Parámetros requeridos:

```
Type, Args
```

Parámetros opcionales:

```
Name, ActionOnFailure
```

Equivalente de JSON (contenido de step.json):

```
 [
  {
    "Name": "JSON Streaming Step",
    "Args": ["-files","s3://elasticmapreduce/samples/wordcount/wordSplitter.py","-
mapper","wordSplitter.py","-reducer","aggregate","-input","s3://elasticmapreduce/
samples/wordcount/input","-output","s3://amzn-s3-demo-bucket/wordcount/output"],
    "ActionOnFailure": "CONTINUE",
    "Type": "STREAMING"
  }
]
```

NOTA: Los argumentos de JSON deben incluir opciones y valores como elementos propios de la lista.

Comando (usando step.json):

```
aws emr add-steps --cluster-id j-XXXXXXXX --steps file://./step.json
```

Salida:

```
{
    "StepIds":[
        "s-XXXXXXXX",
        "s-YYYYYYYY"
    ]
}
```

3. Para agregar un paso de transmisión con varios archivos a un clúster (solo JSON)

JSON (multiplefiles.json):

```
[
  {
     "Name": "JSON Streaming Step",
     "Type": "STREAMING",
     "ActionOnFailure": "CONTINUE",
     "Args": [
         "-files",
         "s3://amzn-s3-demo-bucket/mapper.py,s3://amzn-s3-demo-bucket/reducer.py",
         "-mapper",
         "mapper.py",
         "-reducer",
         "reducer.py",
         "-input",
         "s3://amzn-s3-demo-bucket/input",
         "-output",
         "s3://amzn-s3-demo-bucket/output"]
  }
]
```

Comando:

```
aws emr add-steps --cluster-id j-XXXXXXXX  --steps file://./multiplefiles.json
```

Parámetros requeridos:

```
Type, Args
```

Parámetros opcionales:

```
Name, ActionOnFailure
```

Salida:

```
{
    "StepIds":[
        "s-XXXXXXXX",
    ]
}
```

4. Para agregar pasos de Hive a un clúster

Comando:

```
aws emr add-steps --cluster-id j-XXXXXXXX --steps Type=HIVE,Name='Hive
 program',ActionOnFailure=CONTINUE,Args=[-f,s3://amzn-s3-demo-bucket/
myhivescript.q,-d,INPUT=s3://amzn-s3-demo-bucket/myhiveinput,-d,OUTPUT=s3://
amzn-s3-demo-bucket/myhiveoutput,arg1,arg2] Type=HIVE,Name='Hive
 steps',ActionOnFailure=TERMINATE_CLUSTER,Args=[-f,s3://elasticmapreduce/samples/
hive-ads/libs/model-build.q,-d,INPUT=s3://elasticmapreduce/samples/hive-ads/tables,-
d,OUTPUT=s3://amzn-s3-demo-bucket/hive-ads/output/2014-04-18/11-07-32,-d,LIBS=s3://
elasticmapreduce/samples/hive-ads/libs]
```

Parámetros requeridos:

```
Type, Args
```

Parámetros opcionales:

```
Name, ActionOnFailure
```

Salida:

```
{
    "StepIds":[
        "s-XXXXXXXX",
        "s-YYYYYYYY"
    ]
}
```

5. Para agregar pasos de Pig a un clúster

Comando:

```
aws emr add-steps --cluster-id j-XXXXXXXX --steps Type=PIG,Name='Pig
 program',ActionOnFailure=CONTINUE,Args=[-f,s3://amzn-s3-demo-bucket/
mypigscript.pig,-p,INPUT=s3://amzn-s3-demo-bucket/mypiginput,-p,OUTPUT=s3://
amzn-s3-demo-bucket/mypigoutput,arg1,arg2] Type=PIG,Name='Pig program',Args=[-
f,s3://elasticmapreduce/samples/pig-apache/do-reports2.pig,-p,INPUT=s3://
elasticmapreduce/samples/pig-apache/input,-p,OUTPUT=s3://amzn-s3-demo-bucket/pig-
apache/output,arg1,arg2]
```

Parámetros requeridos:

```
Type, Args
```

Parámetros opcionales:

```
Name, ActionOnFailure
```

Salida:

```
{
    "StepIds":[
        "s-XXXXXXXX",
        "s-YYYYYYYY"
    ]
}
```

6. Para agregar pasos de Impala a un clúster

Comando:

```
aws emr add-steps --cluster-id j-XXXXXXXX --steps Type=IMPALA,Name='Impala
 program',ActionOnFailure=CONTINUE,Args=--impala-script,s3://myimpala/input,--
console-output-path,s3://myimpala/output
```

Parámetros requeridos:

```
Type, Args
```

Parámetros opcionales:

```
Name, ActionOnFailure
```

Salida:

```
{
    "StepIds":[
        "s-XXXXXXXX",
        "s-YYYYYYYY"
    ]
}
```

- Para obtener información sobre la API, consulte AddSteps en la Referencia de comandos de la AWS CLI.

`add-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-tags`.

AWS CLI

1. Para agregar etiquetas a un clúster

Comando:

```
aws emr add-tags --resource-id j-xxxxxxx --tags name="John Doe" age=29 sex=male
 address="123 East NW Seattle"
```

Salida:

```
None
```

2. Para enumerar las etiquetas de un clúster

--Comando:

```
aws emr describe-cluster --cluster-id j-XXXXXXYY --query Cluster.Tags
```

Salida:

```
[
    {
        "Value": "male",
        "Key": "sex"
    },
    {
        "Value": "123 East NW Seattle",
        "Key": "address"
    },
    {
        "Value": "John Doe",
        "Key": "name"
    },
    {
        "Value": "29",
        "Key": "age"
    }
]
```

- Para obtener información sobre la API, consulte AddTags en la Referencia de comandos de la AWS CLI.

`create-cluster-examples`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-cluster-examples`.

AWS CLI

En la mayoría de los ejemplos siguientes se supone que ha especificado el rol de servicio de Amazon EMR y el perfil de instancia de Amazon EC2. Si no lo ha hecho, debe especificar cada

rol de IAM requerido o utilizar el parámetro `--use-default-roles` al crear el clúster. Para obtener información sobre cómo especificar roles de IAM, consulte Configuración de los roles de servicio de IAM de los permisos de Amazon EMR para los servicios y recursos de AWS en la Guía de administración de Amazon EMR.

Ejemplo 1: creación de un clúster

En el siguiente ejemplo de `create-cluster`, se crea un clúster de EMR sencillo.

```
aws emr create-cluster \
    --release-label emr-5.14.0 \
    --instance-type m4.large \
    --instance-count 2
```

Este comando no genera ninguna salida.

Ejemplo 2: creación de un clúster de Amazon EMR con los roles ServiceRole e InstanceProfile predeterminados

En el siguiente ejemplo de `create-cluster`, crea un clúster de Amazon EMR que usa la configuración de `--instance-groups`.

```
aws emr create-cluster \
    --release-label emr-5.14.0 \
    --service-role EMR_DefaultRole \
    --ec2-attributes InstanceProfile=EMR_EC2_DefaultRole \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
```

Ejemplo 3: creación de un clúster de Amazon EMR que utiliza una flota de instancias

En el siguiente ejemplo de `create-cluster`, se crea un clúster de Amazon EMR que usa la configuración de `--instance-fleets` y especifica dos tipos de instancias para cada flota y dos subredes de EC2.

```
aws emr create-cluster \
    --release-label emr-5.14.0 \
    --service-role EMR_DefaultRole \
    --ec2-attributes InstanceProfile=EMR_EC2_DefaultRole,SubnetIds=['subnet-
ab12345c','subnet-de67890f'] \
```

```
    --instance-fleets
 InstanceFleetType=MASTER,TargetOnDemandCapacity=1,InstanceTypeConfigs=['{InstanceType=m4.la
 InstanceFleetType=CORE,TargetSpotCapacity=11,InstanceTypeConfigs=['{InstanceType=m4.large,B
```

Ejemplo 4: creación de un clúster con los roles predeterminados

En el siguiente ejemplo de `create-cluster`, se utiliza el parámetro `--use-default-roles` para especificar el rol de servicio y el perfil de instancia predeterminados.

```
aws emr create-cluster \
    --release-label emr-5.9.0 \
    --use-default-roles \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
 \
    --auto-terminate
```

Ejemplo 5: creación de un clúster y especificación de las aplicaciones que se instalarán

En el siguiente ejemplo de `create-cluster`, se utiliza el parámetro `--applications` para especificar las aplicaciones que Amazon EMR instala. En este ejemplo, se instalan Hadoop, Hive y Pig.

```
aws emr create-cluster \
    --applications Name=Hadoop Name=Hive Name=Pig \
    --release-label emr-5.9.0 \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
 \
    --auto-terminate
```

Ejemplo 6: creación un clúster que incluya Spark

En el siguiente ejemplo, se instala Spark.

```
aws emr create-cluster \
    --release-label emr-5.9.0 \
    --applications Name=Spark \
    --ec2-attributes KeyName=myKey \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
 \
```

```
    --auto-terminate
```

Ejemplo 7: especificación de una AMI personalizada para utilizarla en las instancias de clúster

En el siguiente ejemplo de `create-cluster`, se crea una instancia de clúster basada en la AMI de Amazon Linux con ID `ami-a518e6df`.

```
aws emr create-cluster \
    --name "Cluster with My Custom AMI" \
    --custom-ami-id ami-a518e6df \
    --ebs-root-volume-size 20 \
    --release-label emr-5.9.0 \
    --use-default-roles \
    --instance-count 2 \
    --instance-type m4.large
```

Ejemplo 8: personalización de las configuraciones de las aplicaciones

En los ejemplos siguientes, se utiliza el parámetro `--configurations` para especificar un archivo de configuración JSON que contiene personalizaciones de aplicaciones para Hadoop. Para obtener más información, consulte Configuración de aplicaciones en la Guía de publicación de Amazon EMR.

Contenido de `configurations.json`:

```
[
    {
       "Classification": "mapred-site",
       "Properties": {
           "mapred.tasktracker.map.tasks.maximum": 2
       }
    },
    {
        "Classification": "hadoop-env",
        "Properties": {},
        "Configurations": [
            {
                "Classification": "export",
                "Properties": {
                    "HADOOP_DATANODE_HEAPSIZE": 2048,
                    "HADOOP_NAMENODE_OPTS": "-XX:GCTimeRatio=19"
                }
```

```
            }
        ]
    }
]
```

En el siguiente ejemplo, se hace referencia a `configurations.json` como archivo local.

```
aws emr create-cluster \
    --configurations file://configurations.json \
    --release-label emr-5.9.0 \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
 \
    --auto-terminate
```

En el siguiente ejemplo, se hace referencia a `configurations.json` como archivo en Amazon S3.

```
aws emr create-cluster \
    --configurations https://s3.amazonaws.com/amzn-s3-demo-bucket/
configurations.json \
    --release-label emr-5.9.0 \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
 \
    --auto-terminate
```

Ejemplo 9: creación de un clúster con grupos de instancias maestras, principales y de tareas

En el siguiente ejemplo de `create-cluster`, se utiliza `--instance-groups` para especificar el tipo y el número de instancias de EC2 que se utilizarán para grupos de instancias maestras, principales y de tareas.

```
aws emr create-cluster \
    --release-label emr-5.9.0 \
    --instance-
groups Name=Master,InstanceGroupType=MASTER,InstanceType=m4.large,InstanceCount=1 Name=Core,
```

Ejemplo 10: especificación de que un clúster debe terminar después de completar todos los pasos

En el siguiente ejemplo de `create-cluster`, se usa `--auto-terminate` para especificar que el clúster debe cerrarse automáticamente después de completar todos los pasos.

```
aws emr create-cluster \
    --release-label emr-5.9.0 \
    --instance-groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large
  InstanceGroupType=CORE,InstanceCount=2,InstanceType=m4.large \
    --auto-terminate
```

Ejemplo 11: especificación de los detalles de la configuración del clúster, como el par de claves de Amazon EC2, la configuración de la red y los grupos de seguridad

En el siguiente ejemplo de `create-cluster`, se crea un clúster con el nombre del par de claves de Amazon EC2 llamado `myKey` y perfil de instancia personalizado llamado `myProfile`. Los pares de claves se utilizan para autorizar las conexiones de SSH a los nodos de clúster, por lo general, al nodo maestro. Para obtener más información, consulte Usar un par de claves de Amazon EC2 para credenciales de SSH en la Guía de administración de Amazon EMR.

```
aws emr create-cluster \
    --ec2-attributes KeyName=myKey,InstanceProfile=myProfile \
    --release-label emr-5.9.0 \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
 \
    --auto-terminate
```

En el siguiente ejemplo, se crea un clúster una subred de Amazon VPC.

```
aws emr create-cluster \
    --ec2-attributes SubnetId=subnet-xxxxx \
    --release-label emr-5.9.0 \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
 \
    --auto-terminate
```

En el siguiente ejemplo, se crea un clúster en la zona de disponibilidad de `us-east-1b`.

```
aws emr create-cluster \
    --ec2-attributes AvailabilityZone=us-east-1b \
```

```
    --release-label emr-5.9.0 \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
```

En el siguiente ejemplo, se crea un clúster y se especifican únicamente los grupos de seguridad administrados por Amazon EMR.

```
aws emr create-cluster \
    --release-label emr-5.9.0 \
    --service-role myServiceRole \
    --ec2-attributes InstanceProfile=myRole,EmrManagedMasterSecurityGroup=sg-
master1,EmrManagedSlaveSecurityGroup=sg-slave1 \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
```

En el siguiente ejemplo, se crea un clúster y se especifican únicamente los grupos de seguridad de Amazon EC2 adicionales.

```
aws emr create-cluster \
    --release-label emr-5.9.0 \
    --service-role myServiceRole \
    --ec2-attributes InstanceProfile=myRole,AdditionalMasterSecurityGroups=[sg-
addMaster1,sg-addMaster2,sg-addMaster3,sg-
addMaster4],AdditionalSlaveSecurityGroups=[sg-addSlave1,sg-addSlave2,sg-
addSlave3,sg-addSlave4] \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
```

En el siguiente ejemplo, se crea un clúster y se especifican los grupos de seguridad administrados por EMR, así como los grupos de seguridad adicionales.

```
aws emr create-cluster \
    --release-label emr-5.9.0 \
    --service-role myServiceRole \
    --ec2-attributes InstanceProfile=myRole,EmrManagedMasterSecurityGroup=sg-
master1,EmrManagedSlaveSecurityGroup=sg-slave1,AdditionalMasterSecurityGroups=[sg-
addMaster1,sg-addMaster2,sg-addMaster3,sg-
addMaster4],AdditionalSlaveSecurityGroups=[sg-addSlave1,sg-addSlave2,sg-
addSlave3,sg-addSlave4] \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
```

En el siguiente ejemplo, se crea un clúster en una subred privada de VPC y se utiliza un grupo de seguridad de Amazon EC2 específico para habilitar el acceso al servicio de Amazon EMR, que es necesario para los clústeres de las subredes privadas.

```
aws emr create-cluster \
    --release-label emr-5.9.0 \
    --service-role myServiceRole \
    --ec2-attributes InstanceProfile=myRole,ServiceAccessSecurityGroup=sg-service-
access,EmrManagedMasterSecurityGroup=sg-master,EmrManagedSlaveSecurityGroup=sg-slave
 \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
```

En el siguiente ejemplo, se especifican los parámetros de configuración del grupo de seguridad mediante un archivo JSON llamado `ec2_attributes.json` que se almacena localmente. NOTA: Los argumentos de JSON deben incluir opciones y valores como elementos propios de la lista.

```
aws emr create-cluster \
    --release-label emr-5.9.0 \
    --service-role myServiceRole \
    --ec2-attributes file://ec2_attributes.json  \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
```

Contenido de `ec2_attributes.json`:

```
[
    {
        "SubnetId": "subnet-xxxxx",
        "KeyName": "myKey",
        "InstanceProfile":"myRole",
        "EmrManagedMasterSecurityGroup": "sg-master1",
        "EmrManagedSlaveSecurityGroup": "sg-slave1",
        "ServiceAccessSecurityGroup": "sg-service-access",
        "AdditionalMasterSecurityGroups": ["sg-addMaster1","sg-addMaster2","sg-
addMaster3","sg-addMaster4"],
        "AdditionalSlaveSecurityGroups": ["sg-addSlave1","sg-addSlave2","sg-
addSlave3","sg-addSlave4"]
    }
]
```

Ejemplo 12: habilitación de la depuración y especificación de un URI de registro

En el siguiente ejemplo de `create-cluster`, se utiliza el parámetro `--enable-debugging`, que le permite ver los archivos de registro con mayor facilidad mediante la herramienta de depuración de la consola de Amazon EMR. El parámetro `--log-uri` es obligatorio con `--enable-debugging`.

```
aws emr create-cluster \
    --enable-debugging \
    --log-uri s3://amzn-s3-demo-bucket/myLog \
    --release-label emr-5.9.0 \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
 \
    --auto-terminate
```

Ejemplo 13: adición de etiquetas al crear un nuevo clúster

Las etiquetas son pares clave-valor que le ayudan a identificar y administrar clústeres. En el siguiente ejemplo de `create-cluster`, se utiliza el parámetro `--tags` para crear tres etiquetas para un clúster: una con el nombre de clave `name` y el valor `Shirley Rodriguez`, una segunda con el nombre de clave `age` y el valor 29, y una tercera etiqueta con el nombre de clave `department` y el valor `Analytics`.

```
aws emr create-cluster \
    --tags name="Shirley Rodriguez" age=29 department="Analytics" \
    --release-label emr-5.32.0 \
    --instance-type m5.xlarge \
    --instance-count 3 \
    --use-default-roles
```

En el siguiente ejemplo, se enumeran las etiquetas aplicadas a un clúster.

```
aws emr describe-cluster \
    --cluster-id j-XXXXXXYY \
    --query Cluster.Tags
```

Ejemplo 14: uso de una configuración de seguridad que habilite el cifrado y otras características de seguridad

En el siguiente ejemplo de `create-cluster`, se utiliza el parámetro `--security-configuration` para especificar una configuración de seguridad para un clúster de EMR. Puede utilizar la configuraciones de seguridad con Amazon EMR versión 4.8.0 o versiones posteriores.

```
aws emr create-cluster \
    --instance-type m4.large \
    --release-label emr-5.9.0 \
    --security-configuration mySecurityConfiguration
```

Ejemplo 15: creación de un clúster con volúmenes de almacenamiento de EBS adicionales configurados para los grupos de instancias

Al especificar volúmenes de EBS adicionales, se requieren los siguientes argumentos: `VolumeType`, `SizeInGB` si se especifica `EbsBlockDeviceConfigs`.

En el siguiente ejemplo de `create-cluster`, se crea un clúster con varios volúmenes de EBS asociados a las instancias de EC2 del grupo de instancias principal.

```
aws emr create-cluster \
    --release-label emr-5.9.0  \
    --use-default-roles \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=d2.xlarge
 'InstanceGroupType=CORE,InstanceCount=2,InstanceType=d2.xlarge,EbsConfiguration={EbsOptimiz
{VolumeSpecification={VolumeType=io1,SizeInGB=100,Iops=100},VolumesPerInstance=4}]}'
 \
    --auto-terminate
```

En el siguiente ejemplo, se crea un clúster con varios volúmenes de EBS asociados a las instancias de EC2 del grupo de instancias maestro.

```
aws emr create-cluster \
    --release-label emr-5.9.0 \
    --use-default-roles \
    --instance-groups 'InstanceGroupType=MASTER, InstanceCount=1,
 InstanceType=d2.xlarge, EbsConfiguration={EbsOptimized=true,
 EbsBlockDeviceConfigs=[{VolumeSpecification={VolumeType=io1, SizeInGB=100,
 Iops=100}},
{VolumeSpecification={VolumeType=standard,SizeInGB=50},VolumesPerInstance=3}]}' InstanceGrou
 \
```

```
    --auto-terminate
```

Ejemplo 16: creación de un clúster con una política de escalado automático

Puede asociar políticas de escalado automático a grupos de instancias principales y de tareas mediante Amazon EMR versión 4.0 y versiones posteriores. La política de escalado automático agrega y elimina de manera dinámica instancias de EC2 en respuesta a una métrica de Amazon CloudWatch. Para obtener más información, consulte Uso del escalado automático en Amazon EMR <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-automatic-scaling.html>`_ en la Guía de administración de Amazon EMR.

Al asociar una política de escalado automático, también debe especificar el rol predeterminado para el escalado automático mediante `--auto-scaling-role EMR_AutoScaling_DefaultRole`.

En el siguiente ejemplo de `create-cluster`, se especifica la política de escalado automático para el grupo de instancias de `CORE` mediante el argumento `AutoScalingPolicy` con una estructura JSON incrustada, que especifica la configuración de la política de escalado. Los grupos de instancias con una estructura de JSON incrustada deben tener toda la colección de argumentos entre comillas simples. El uso de comillas simples es opcional para los grupos de instancias sin una estructura de JSON incrustada.

```
aws emr create-cluster
    --release-label emr-5.9.0 \
    --use-default-roles --auto-scaling-role EMR_AutoScaling_DefaultRole \
    --instance-
groups InstanceGroupType=MASTER,InstanceType=d2.xlarge,InstanceCount=1
 'InstanceGroupType=CORE,InstanceType=d2.xlarge,InstanceCount=2,AutoScalingPolicy={Constrain
```

En el siguiente ejemplo, se usa un archivo JSON, `instancegroupconfig.json`, para especificar la configuración de todos los grupos de instancias de un clúster. El archivo JSON especifica la configuración de la política de escalado automático para el grupo de instancias principal.

```
aws emr create-cluster \
    --release-label emr-5.9.0 \
    --service-role EMR_DefaultRole \
    --ec2-attributes InstanceProfile=EMR_EC2_DefaultRole \
    --instance-groups file://myfolder/instancegroupconfig.json \
    --auto-scaling-role EMR_AutoScaling_DefaultRole
```

Contenido de `instancegroupconfig.json`:

```
[
    {
        "InstanceCount": 1,
        "Name": "MyMasterIG",
        "InstanceGroupType": "MASTER",
        "InstanceType": "m4.large"
    },
    {
        "InstanceCount": 2,
        "Name": "MyCoreIG",
        "InstanceGroupType": "CORE",
        "InstanceType": "m4.large",
        "AutoScalingPolicy": {
            "Constraints": {
                "MinCapacity": 2,
                "MaxCapacity": 10
            },
            "Rules": [
                {
                    "Name": "Default-scale-out",
                    "Description": "Replicates the default scale-out rule in the
 console for YARN memory.",
                    "Action": {
                        "SimpleScalingPolicyConfiguration": {
                            "AdjustmentType": "CHANGE_IN_CAPACITY",
                            "ScalingAdjustment": 1,
                            "CoolDown": 300
                        }
                    },
                    "Trigger": {
                        "CloudWatchAlarmDefinition": {
                            "ComparisonOperator": "LESS_THAN",
                            "EvaluationPeriods": 1,
                            "MetricName": "YARNMemoryAvailablePercentage",
                            "Namespace": "AWS/ElasticMapReduce",
                            "Period": 300,
                            "Threshold": 15,
                            "Statistic": "AVERAGE",
                            "Unit": "PERCENT",
                            "Dimensions": [
                                {
                                    "Key": "JobFlowId",
```

```
                                    "Value": "${emr.clusterId}"
                                }
                            ]
                        }
                    }
                }
            ]
        }
    }
]
```

Ejemplo 17: adición de pasos JAR personalizados al crear un clúster

En el siguiente ejemplo de `create-cluster`, se agregan pasos especificando un archivo JAR almacenado en Amazon S3. Pasos para enviar trabajos a un clúster La función principal definida en el archivo JAR se ejecuta después del aprovisionamiento de las instancias EC2, de la ejecución de cualquier acción de arranque y de la instalación de las aplicaciones. Los pasos se especifican mediante `Type=CUSTOM_JAR`.

Los pasos JAR personalizados requieren el parámetro `Jar=`, que especifica la ruta y el nombre de archivo del JAR. Los parámetros opcionales son `Type`, `Name`, `ActionOnFailure`, `Args` y `MainClass`. Si no se especifica la clase principal, el archivo JAR debe especificar `Main-Class` en su archivo de manifiesto.

```
aws emr create-cluster \
    --steps Type=CUSTOM_JAR,Name=CustomJAR,ActionOnFailure=CONTINUE,Jar=s3://amzn-
s3-demo-bucket/
mytest.jar,Args=arg1,arg2,arg3 Type=CUSTOM_JAR,Name=CustomJAR,ActionOnFailure=CONTINUE,Jar=s
amzn-s3-demo-bucket/mytest.jar,MainClass=mymainclass,Args=arg1,arg2,arg3  \
    --release-label emr-5.3.1 \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
 \
    --auto-terminate
```

Ejemplo 18: adición de pasos de transmisión al crear un clúster

En los siguientes ejemplos de `create-cluster`, se agrega un paso de transmisión a un clúster que finaliza una vez se han ejecutado todos los pasos. Los pasos de transmisión requieren los parámetros `Type` y `Args`. Los parámetros opcionales de los pasos de transmisión son `Name` y `ActionOnFailure`.

En el siguiente ejemplo, se especifica el paso insertado.

```
aws emr create-cluster \
    --steps Type=STREAMING,Name='Streaming Program',ActionOnFailure=CONTINUE,Args=[-
files,s3://elasticmapreduce/samples/wordcount/wordSplitter.py,-
mapper,wordSplitter.py,-reducer,aggregate,-input,s3://elasticmapreduce/samples/
wordcount/input,-output,s3://amzn-s3-demo-bucket/wordcount/output] \
    --release-label emr-5.3.1 \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
 \
    --auto-terminate
```

En el siguiente ejemplo, se utiliza un archivo de configuración JSON almacenado localmente llamado `multiplefiles.json`. La configuración de JSON especifica varios archivos. Para especificar varios archivos en un paso, debe usar un archivo de configuración JSON para especificar el paso. Los argumentos de JSON deben incluir opciones y valores como elementos propios de la lista.

```
aws emr create-cluster \
    --steps file://./multiplefiles.json \
    --release-label emr-5.9.0  \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
 \
    --auto-terminate
```

Contenido de `multiplefiles.json`:

```
[
    {
        "Name": "JSON Streaming Step",
        "Args": [
            "-files",
            "s3://elasticmapreduce/samples/wordcount/wordSplitter.py",
            "-mapper",
            "wordSplitter.py",
            "-reducer",
            "aggregate",
            "-input",
            "s3://elasticmapreduce/samples/wordcount/input",
            "-output",
```

```
            "s3://amzn-s3-demo-bucket/wordcount/output"
        ],
        "ActionOnFailure": "CONTINUE",
        "Type": "STREAMING"
    }
]
```

Ejemplo 19: adición de los pasos de Hive al crear un clúster

En el siguiente ejemplo, se agregan los pasos de Hive al crear un clúster. Los pasos de Hive requieren los parámetros `Type` y `Args`. Los parámetros opcionales de los pasos de Hive son `Name` y `ActionOnFailure`.

```
aws emr create-cluster \
    --steps Type=HIVE,Name='Hive
 program',ActionOnFailure=CONTINUE,ActionOnFailure=TERMINATE_CLUSTER,Args=[-
f,s3://elasticmapreduce/samples/hive-ads/libs/model-build.q,-d,INPUT=s3://
elasticmapreduce/samples/hive-ads/tables,-d,OUTPUT=s3://amzn-s3-demo-bucket/hive-
ads/output/2014-04-18/11-07-32,-d,LIBS=s3://elasticmapreduce/samples/hive-ads/libs]
 \
    --applications Name=Hive \
    --release-label emr-5.3.1 \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
```

Ejemplo 20: adición de los pasos de Pig al crear un clúster

En el siguiente ejemplo, se agregan los pasos de Pig al crear un clúster. Los parámetros obligatorios de los pasos de Pig son `Type` y `Args`. Los parámetros opcionales de los pasos de Pig son `Name` y `ActionOnFailure`.

```
aws emr create-cluster \
    --steps Type=PIG,Name='Pig program',ActionOnFailure=CONTINUE,Args=[-f,s3://
elasticmapreduce/samples/pig-apache/do-reports2.pig,-p,INPUT=s3://elasticmapreduce/
samples/pig-apache/input,-p,OUTPUT=s3://amzn-s3-demo-bucket/pig-apache/output] \
    --applications Name=Pig \
    --release-label emr-5.3.1 \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
```

Ejemplo 21: adición de las acciones de arranque

En el siguiente ejemplo de `create-cluster`, se ejecutan dos acciones de arranque definidas como scripts que se almacenan en Amazon S3.

```
aws emr create-cluster \
    --bootstrap-actions Path=s3://amzn-s3-demo-bucket/
myscript1,Name=BootstrapAction1,Args=[arg1,arg2] Path=s3://amzn-s3-demo-bucket/
myscript2,Name=BootstrapAction2,Args=[arg1,arg2] \
    --release-label emr-5.3.1 \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
 \
    --auto-terminate
```

Ejemplo 22: habilitación de la vista coherente de EMRFS y personalización de la configuración de RetryCount y RetryPeriod

En el siguiente ejemplo de `create-cluster`, se especifica el recuento de reintentos y el período de reintentos para una vista coherente de EMRFS. El argumento `Consistent=true` es obligatorio.

```
aws emr create-cluster \
    --instance-type m4.large \
    --release-label emr-5.9.0 \
    --emrfs Consistent=true,RetryCount=6,RetryPeriod=30
```

En el siguiente ejemplo, se especifica la misma configuración de EMRFS que en el ejemplo anterior, utilizando un archivo de configuración JSON almacenado localmente llamado `emrfsconfig.json`.

```
aws emr create-cluster \
    --instance-type m4.large \
    --release-label emr-5.9.0 \
    --emrfs file://emrfsconfig.json
```

Contenido de `emrfsconfig.json`:

```
{
    "Consistent": true,
    "RetryCount": 6,
    "RetryPeriod": 30
}
```

Ejemplo 23: creación de un clúster con Kerberos configurado

En los siguientes ejemplos de `create-cluster`, se crea un clúster mediante una configuración de seguridad con Kerberos activado y se establecen los parámetros de Kerberos para el clúster usando `--kerberos-attributes`.

El siguiente comando especifica los atributos de Kerberos para el clúster insertado.

```
aws emr create-cluster \
    --instance-type m3.xlarge \
    --release-label emr-5.10.0 \
    --service-role EMR_DefaultRole \
    --ec2-attributes InstanceProfile=EMR_EC2_DefaultRole \
    --security-configuration mySecurityConfiguration \
    --kerberos-
attributes Realm=EC2.INTERNAL,KdcAdminPassword=123,CrossRealmTrustPrincipalPassword=123
```

El siguiente comando especifica los mismos atributos, pero hace referencia a un archivo JSON almacenado localmente llamado `kerberos_attributes.json`. En este ejemplo, el archivo se guarda en el mismo directorio en el que ejecuta el comando. También puede hacer referencia a un archivo de configuración guardado en Amazon S3.

```
aws emr create-cluster \
    --instance-type m3.xlarge \
    --release-label emr-5.10.0 \
    --service-role EMR_DefaultRole \
    --ec2-attributes InstanceProfile=EMR_EC2_DefaultRole \
    --security-configuration mySecurityConfiguration \
    --kerberos-attributes file://kerberos_attributes.json
```

Contenido de `kerberos_attributes.json`:

```
{
    "Realm": "EC2.INTERNAL",
    "KdcAdminPassword": "123",
    "CrossRealmTrustPrincipalPassword": "123",
}
```

En el siguiente ejemplo de `create-cluster`, se crea un clúster de Amazon EMR que utiliza la configuración de `--instance-groups` y tiene una política de escalado administrado.

```
aws emr create-cluster \
    --release-label emr-5.30.0 \
    --service-role EMR_DefaultRole \
    --ec2-attributes InstanceProfile=EMR_EC2_DefaultRole \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
    --managed-scaling-policy
 ComputeLimits='{MinimumCapacityUnits=2,MaximumCapacityUnits=4,UnitType=Instances}'
```

En el siguiente ejemplo de `create-cluster`, se crea un clúster de Amazon EMR que utiliza --log-encryption-kms-key-id para definir el ID de clave de KMS utilizado para el cifrado de registros.

```
aws emr create-cluster \
    --release-label emr-5.30.0 \
    --log-uri s3://amzn-s3-demo-bucket/myLog \
    --log-encryption-kms-key-id arn:aws:kms:us-east-1:110302272565:key/
dd559181-283e-45d7-99d1-66da348c4d33 \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
```

En el siguiente ejemplo de `create-cluster`, se crea un clúster de Amazon EMR que utiliza la configuración de --placement-group-configs para colocar los nodos maestros en un clúster de alta disponibilidad (HA) dentro de un grupo de ubicación de EC2 mediante una estrategia de ubicación de SPREAD.

```
aws emr create-cluster \
    --release-label emr-5.30.0 \
    --service-role EMR_DefaultRole \
    --ec2-attributes InstanceProfile=EMR_EC2_DefaultRole \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=3,InstanceType=m4.largeInstanceGroupType=CORE,
 \
    --placement-group-configs InstanceRole=MASTER
```

En el siguiente ejemplo de `create-cluster`, se crea un clúster de Amazon EMR que utiliza la configuración de --auto-termination-policy para ubicar un umbral de terminación automática por inactividad para el clúster.

```
aws emr create-cluster \
    --release-label emr-5.34.0 \
    --service-role EMR_DefaultRole \
```

```
    --ec2-attributes InstanceProfile=EMR_EC2_DefaultRole \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
 \
    --auto-termination-policy IdleTimeout=100
```

En el siguiente ejemplo de `create-cluster`, se crea un clúster de Amazon EMR que usa --os-release-label para definir una versión de Amazon Linux para el inicio del clúster.

```
aws emr create-cluster \
    --release-label emr-6.6.0 \
    --os-release-label 2.0.20220406.1 \
    --service-role EMR_DefaultRole \
    --ec2-attributes InstanceProfile=EMR_EC2_DefaultRole \
    --instance-
groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE
```

Ejemplo 24: especificación de los atributos de un volumen raíz de EBS: tamaño, IOPS y rendimiento para las instancias de clúster creadas con las versiones 6.15.0 y posteriores de EMR

En el siguiente ejemplo de `create-cluster`, se crea un clúster de Amazon EMR que utiliza atributos de volumen raíz para configurar las especificaciones de los volúmenes raíz para las instancias de EC2.

```
aws emr create-cluster \
    --name "Cluster with My Custom AMI" \
    --custom-ami-id ami-a518e6df \
    --ebs-root-volume-size 20 \
    --ebs-root-volume-iops 3000 \
    --ebs-root-volume-throughput 125 \
    --release-label emr-6.15.0 \
    --use-default-roles \
    --instance-count 2 \
    --instance-type m4.large
```

- Para obtener información sobre la API, consulte CreateClusterExamples en la Referencia de comandos de la AWS CLI.

`create-default-roles`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-default-roles`.

AWS CLI

1. Para crear el rol de IAM predeterminado para EC2

Comando:

```
aws emr create-default-roles
```

Salida:

```
If the role already exists then the command returns nothing.

If the role does not exist then the output will be:

[
    {
        "RolePolicy": {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Action": [
                        "cloudwatch:*",
                        "dynamodb:*",
                        "ec2:Describe*",
                        "elasticmapreduce:Describe*",
                        "elasticmapreduce:ListBootstrapActions",
                        "elasticmapreduce:ListClusters",
                        "elasticmapreduce:ListInstanceGroups",
                        "elasticmapreduce:ListInstances",
                        "elasticmapreduce:ListSteps",
                        "kinesis:CreateStream",
                        "kinesis:DeleteStream",
                        "kinesis:DescribeStream",
                        "kinesis:GetRecords",
                        "kinesis:GetShardIterator",
                        "kinesis:MergeShards",
                        "kinesis:PutRecord",
                        "kinesis:SplitShard",
                        "rds:Describe*",
                        "s3:*",
                        "sdb:*",
                        "sns:*",
                        "sqs:*"
```

```
                ],
                "Resource": "*",
                "Effect": "Allow"
            }
        ]
    },
    "Role": {
        "AssumeRolePolicyDocument": {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Action": "sts:AssumeRole",
                    "Sid": "",
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "ec2.amazonaws.com"
                    }
                }
            ]
        },
        "RoleId": "AROAIQ5SIQUGL5KMYBJX6",
        "CreateDate": "2015-06-09T17:09:04.602Z",
        "RoleName": "EMR_EC2_DefaultRole",
        "Path": "/",
        "Arn": "arn:aws:iam::176430881729:role/EMR_EC2_DefaultRole"
    }
},
{
    "RolePolicy": {
        "Version":"2012-10-17",
        "Statement": [
            {
                "Action": [
                    "ec2:AuthorizeSecurityGroupIngress",
                    "ec2:CancelSpotInstanceRequests",
                    "ec2:CreateSecurityGroup",
                    "ec2:CreateTags",
                    "ec2:DeleteTags",
                    "ec2:DescribeAvailabilityZones",
                    "ec2:DescribeAccountAttributes",
                    "ec2:DescribeInstances",
                    "ec2:DescribeInstanceStatus",
                    "ec2:DescribeKeyPairs",
                    "ec2:DescribePrefixLists",
```

```
                    "ec2:DescribeRouteTables",
                    "ec2:DescribeSecurityGroups",
                    "ec2:DescribeSpotInstanceRequests",
                    "ec2:DescribeSpotPriceHistory",
                    "ec2:DescribeSubnets",
                    "ec2:DescribeVpcAttribute",
                    "ec2:DescribeVpcEndpoints",
                    "ec2:DescribeVpcEndpointServices",
                    "ec2:DescribeVpcs",
                    "ec2:ModifyImageAttribute",
                    "ec2:ModifyInstanceAttribute",
                    "ec2:RequestSpotInstances",
                    "ec2:RunInstances",
                    "ec2:TerminateInstances",
                    "iam:GetRole",
                    "iam:GetRolePolicy",
                    "iam:ListInstanceProfiles",
                    "iam:ListRolePolicies",
                    "iam:PassRole",
                    "s3:CreateBucket",
                    "s3:Get*",
                    "s3:List*",
                    "sdb:BatchPutAttributes",
                    "sdb:Select",
                    "sqs:CreateQueue",
                    "sqs:Delete*",
                    "sqs:GetQueue*",
                    "sqs:ReceiveMessage"
                ],
                "Resource": "*",
                "Effect": "Allow"
            }
        ]
    },
    "Role": {
        "AssumeRolePolicyDocument": {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Action": "sts:AssumeRole",
                    "Sid": "",
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "elasticmapreduce.amazonaws.com"
```

```
                        }
                    }
                ]
            },
            "RoleId": "AROAI3SRVPPVSRDLARBPY",
            "CreateDate": "2015-06-09T17:09:10.401Z",
            "RoleName": "EMR_DefaultRole",
            "Path": "/",
            "Arn": "arn:aws:iam::176430881729:role/EMR_DefaultRole"
        }
    }
]
```

- Para obtener información sobre la API, consulte CreateDefaultRoles en la Referencia de comandos de la AWS CLI.

`create-security-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-security-configuration`.

AWS CLI

1. Para crear una configuración de seguridad con cifrado en tránsito habilitado con PEM para el proveedor de certificados y el cifrado en reposo habilitado con SSE-S3 para cifrado de S3 y AWS-KMS para el proveedor de claves de disco local

   Comando:

```
 aws emr create-security-configuration --name MySecurityConfig --security-
configuration '{
        "EncryptionConfiguration": {
                "EnableInTransitEncryption" : true,
                "EnableAtRestEncryption" : true,
                "InTransitEncryptionConfiguration" : {
                        "TLSCertificateConfiguration" : {
                                "CertificateProviderType" : "PEM",
                                "S3Object" : "s3://mycertstore/artifacts/
MyCerts.zip"
                        }
                },
                "AtRestEncryptionConfiguration" : {
                        "S3EncryptionConfiguration" : {
                                "EncryptionMode" : "SSE-S3"
```

```
                        },
                        "LocalDiskEncryptionConfiguration" : {
                                "EncryptionKeyProviderType" : "AwsKms",
                                "AwsKmsKey" : "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
                        }
                }
        }
}'
```

Salida:

```
{
"CreationDateTime": 1474070889.129,
"Name": "MySecurityConfig"
}
```

Equivalente de JSON (contenido de security_configuration.json):

```
{
    "EncryptionConfiguration": {
        "EnableInTransitEncryption": true,
        "EnableAtRestEncryption": true,
        "InTransitEncryptionConfiguration": {
            "TLSCertificateConfiguration": {
                "CertificateProviderType": "PEM",
                "S3Object": "s3://mycertstore/artifacts/MyCerts.zip"
            }
        },
        "AtRestEncryptionConfiguration": {
            "S3EncryptionConfiguration": {
                "EncryptionMode": "SSE-S3"
            },
            "LocalDiskEncryptionConfiguration": {
                "EncryptionKeyProviderType": "AwsKms",
                "AwsKmsKey": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
            }
        }
    }
}
```

Comando (usando security_configuration.json):

```
aws emr create-security-configuration --name "MySecurityConfig" --security-
configuration file://./security_configuration.json
```

Salida:

```
{
"CreationDateTime": 1474070889.129,
"Name": "MySecurityConfig"
}
```

2. Para crear una configuración de seguridad con Kerberos habilitado mediante un KDC dedicado a clúster y la confianza entre dominios

Comando:

```
 aws emr create-security-configuration --name MySecurityConfig --security-
configuration '{
     "AuthenticationConfiguration": {
         "KerberosConfiguration": {
             "Provider": "ClusterDedicatedKdc",
             "ClusterDedicatedKdcConfiguration": {
                 "TicketLifetimeInHours": 24,
                 "CrossRealmTrustConfiguration": {
                   "Realm": "AD.DOMAIN.COM",
                   "Domain": "ad.domain.com",
                   "AdminServer": "ad.domain.com",
                   "KdcServer": "ad.domain.com"
                 }
             }
         }
     }
}'
```

Salida:

```
{
"CreationDateTime": 1490225558.982,
"Name": "MySecurityConfig"
}
```

Equivalente de JSON (contenido de security_configuration.json):

```
{
    "AuthenticationConfiguration": {
        "KerberosConfiguration": {
            "Provider": "ClusterDedicatedKdc",
            "ClusterDedicatedKdcConfiguration": {
                "TicketLifetimeInHours": 24,
                "CrossRealmTrustConfiguration": {
                    "Realm": "AD.DOMAIN.COM",
                    "Domain": "ad.domain.com",
                    "AdminServer": "ad.domain.com",
                    "KdcServer": "ad.domain.com"
                }
            }
        }
    }
}
```

Comando (usando security_configuration.json):

```
aws emr create-security-configuration --name "MySecurityConfig" --security-
configuration file://./security_configuration.json
```

Salida:

```
{
"CreationDateTime": 1490225558.982,
"Name": "MySecurityConfig"
}
```

- Para obtener información sobre la API, consulte CreateSecurityConfiguration en la Referencia de comandos de la AWS CLI.

`delete-security-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-security-configuration`.

AWS CLI

Para eliminar una configuración de seguridad en la región actual

Comando:

```
aws emr delete-security-configuration --name MySecurityConfig
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte DeleteSecurityConfiguration en la Referencia de comandos de la AWS CLI.

`describe-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cluster`.

AWS CLI

Comando:

```
aws emr describe-cluster --cluster-id j-XXXXXXXX
```

Salida:

```
For release-label based uniform instance groups cluster:

        {
            "Cluster": {
                "Status": {
                    "Timeline": {
                        "ReadyDateTime": 1436475075.199,
                        "CreationDateTime": 1436474656.563,
                    },
                    "State": "WAITING",
                    "StateChangeReason": {
                        "Message": "Waiting for steps to run"
                    }
                },
                "Ec2InstanceAttributes": {
                    "ServiceAccessSecurityGroup": "sg-xxxxxxxx",
                    "EmrManagedMasterSecurityGroup": "sg-xxxxxxxx",
                    "IamInstanceProfile": "EMR_EC2_DefaultRole",
                    "Ec2KeyName": "myKey",
                    "Ec2AvailabilityZone": "us-east-1c",
```

```
            "EmrManagedSlaveSecurityGroup": "sg-yyyyyyyyy"
        },
        "Name": "My Cluster",
        "ServiceRole": "EMR_DefaultRole",
        "Tags": [],
        "TerminationProtected": true,
        "UnhealthyNodeReplacement": true,
        "ReleaseLabel": "emr-4.0.0",
        "NormalizedInstanceHours": 96,
        "InstanceGroups": [
            {
                "RequestedInstanceCount": 2,
                "Status": {
                    "Timeline": {
                        "ReadyDateTime": 1436475074.245,
                        "CreationDateTime": 1436474656.564,
                        "EndDateTime": 1436638158.387
                    },
                    "State": "RUNNING",
                    "StateChangeReason": {
                        "Message": "",
                    }
                },
                "Name": "CORE",
                "InstanceGroupType": "CORE",
                "Id": "ig-YYYYYYY",
                "Configurations": [],
                "InstanceType": "m3.large",
                "Market": "ON_DEMAND",
                "RunningInstanceCount": 2
            },
            {
                "RequestedInstanceCount": 1,
                "Status": {
                    "Timeline": {
                        "ReadyDateTime": 1436475074.245,
                        "CreationDateTime": 1436474656.564,
                        "EndDateTime": 1436638158.387
                    },
                    "State": "RUNNING",
                    "StateChangeReason": {
                        "Message": "",
                    }
                },
```

```
                        "Name": "MASTER",
                        "InstanceGroupType": "MASTER",
                        "Id": "ig-XXXXXXXXX",
                        "Configurations": [],
                        "InstanceType": "m3.large",
                        "Market": "ON_DEMAND",
                        "RunningInstanceCount": 1
                    }
                ],
                "Applications": [
                    {
                        "Name": "Hadoop"
                    }
                ],
                "VisibleToAllUsers": true,
                "BootstrapActions": [],
                "MasterPublicDnsName": "ec2-54-147-144-78.compute-1.amazonaws.com",
                "AutoTerminate": false,
                "Id": "j-XXXXXXXX",
                "Configurations": [
                    {
                        "Properties": {
                            "fs.s3.consistent.retryPeriodSeconds": "20",
                            "fs.s3.enableServerSideEncryption": "true",
                            "fs.s3.consistent": "false",
                            "fs.s3.consistent.retryCount": "2"
                        },
                        "Classification": "emrfs-site"
                    }
                ]
            }
        }


For release-label based instance fleet cluster:
{
    "Cluster": {
        "Status": {
            "Timeline": {
                "ReadyDateTime": 1487897289.705,
                "CreationDateTime": 1487896933.942
            },
            "State": "WAITING",
            "StateChangeReason": {
```

```
                "Message": "Waiting for steps to run"
            }
        },
        "Ec2InstanceAttributes": {
            "EmrManagedMasterSecurityGroup": "sg-xxxxx",
            "RequestedEc2AvailabilityZones": [],
            "RequestedEc2SubnetIds": [],
            "IamInstanceProfile": "EMR_EC2_DefaultRole",
            "Ec2AvailabilityZone": "us-east-1a",
            "EmrManagedSlaveSecurityGroup": "sg-xxxxx"
        },
        "Name": "My Cluster",
        "ServiceRole": "EMR_DefaultRole",
        "Tags": [],
        "TerminationProtected": false,
        "UnhealthyNodeReplacement": false,
        "ReleaseLabel": "emr-5.2.0",
        "NormalizedInstanceHours": 472,
        "InstanceCollectionType": "INSTANCE_FLEET",
        "InstanceFleets": [
            {
                "Status": {
                    "Timeline": {
                        "ReadyDateTime": 1487897212.74,
                        "CreationDateTime": 1487896933.948
                    },
                    "State": "RUNNING",
                    "StateChangeReason": {
                        "Message": ""
                    }
                },
                "ProvisionedSpotCapacity": 1,
                "Name": "MASTER",
                "InstanceFleetType": "MASTER",
                "LaunchSpecifications": {
                    "SpotSpecification": {
                        "TimeoutDurationMinutes": 60,
                        "TimeoutAction": "TERMINATE_CLUSTER"
                    }
                },
                "TargetSpotCapacity": 1,
                "ProvisionedOnDemandCapacity": 0,
                "InstanceTypeSpecifications": [
                    {
```

```
                        "BidPrice": "0.5",
                        "InstanceType": "m3.xlarge",
                        "WeightedCapacity": 1
                    }
                ],
                "Id": "if-xxxxxxx",
                "TargetOnDemandCapacity": 0
            }
        ],
        "Applications": [
            {
                "Version": "2.7.3",
                "Name": "Hadoop"
            }
        ],
        "ScaleDownBehavior": "TERMINATE_AT_INSTANCE_HOUR",
        "VisibleToAllUsers": true,
        "BootstrapActions": [],
        "MasterPublicDnsName": "ec2-xxx-xx-xxx-xx.compute-1.amazonaws.com",
        "AutoTerminate": false,
        "Id": "j-xxxxx",
        "Configurations": []
    }
}

For ami based uniform instance group cluster:

    {
        "Cluster": {
            "Status": {
                "Timeline": {
                    "ReadyDateTime": 1399400564.432,
                    "CreationDateTime": 1399400268.62
                },
                "State": "WAITING",
                "StateChangeReason": {
                    "Message": "Waiting for steps to run"
                }
            },
            "Ec2InstanceAttributes": {
                "IamInstanceProfile": "EMR_EC2_DefaultRole",
                "Ec2AvailabilityZone": "us-east-1c"
            },
            "Name": "My Cluster",
```

```
            "Tags": [],
            "TerminationProtected": true,
            "UnhealthyNodeReplacement": true,
            "RunningAmiVersion": "2.5.4",
            "InstanceGroups": [
                {
                    "RequestedInstanceCount": 1,
                    "Status": {
                        "Timeline": {
                            "ReadyDateTime": 1399400558.848,
                            "CreationDateTime": 1399400268.621
                        },
                        "State": "RUNNING",
                        "StateChangeReason": {
                            "Message": ""
                        }
                    },
                    "Name": "Master instance group",
                    "InstanceGroupType": "MASTER",
                    "InstanceType": "m1.small",
                    "Id": "ig-ABCD",
                    "Market": "ON_DEMAND",
                    "RunningInstanceCount": 1
                },
                {
                    "RequestedInstanceCount": 2,
                    "Status": {
                        "Timeline": {
                            "ReadyDateTime": 1399400564.439,
                            "CreationDateTime": 1399400268.621
                        },
                        "State": "RUNNING",
                        "StateChangeReason": {
                            "Message": ""
                        }
                    },
                    "Name": "Core instance group",
                    "InstanceGroupType": "CORE",
                    "InstanceType": "m1.small",
                    "Id": "ig-DEF",
                    "Market": "ON_DEMAND",
                    "RunningInstanceCount": 2
                }
            ],
```

```
            "Applications": [
                {
                    "Version": "1.0.3",
                    "Name": "hadoop"
                }
            ],
            "BootstrapActions": [],
            "VisibleToAllUsers": false,
            "RequestedAmiVersion": "2.4.2",
            "LogUri": "s3://myLogUri/",
            "AutoTerminate": false,
            "Id": "j-XXXXXXXX"
        }
    }
```

- Para obtener información sobre la API, consulte DescribeCluster en la Referencia de comandos de la AWS CLI.

`describe-step`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-step`.

AWS CLI

El siguiente comando describe un paso con el ID del paso `s-3LZC0QUT43AM` en un clúster con el ID de clúster `j-3SD91U2E1L2QX`:

```
aws emr describe-step --cluster-id j-3SD91U2E1L2QX --step-id s-3LZC0QUT43AM
```

Salida:

```
{
    "Step": {
        "Status": {
            "Timeline": {
                "EndDateTime": 1433200470.481,
                "CreationDateTime": 1433199926.597,
                "StartDateTime": 1433200404.959
            },
            "State": "COMPLETED",
            "StateChangeReason": {}
```

```
        },
        "Config": {
            "Args": [
                "s3://us-west-2.elasticmapreduce/libs/hive/hive-script",
                "--base-path",
                "s3://us-west-2.elasticmapreduce/libs/hive/",
                "--install-hive",
                "--hive-versions",
                "0.13.1"
            ],
            "Jar": "s3://us-west-2.elasticmapreduce/libs/script-runner/script-
runner.jar",
            "Properties": {}
        },
        "Id": "s-3LZC0QUT43AM",
        "ActionOnFailure": "TERMINATE_CLUSTER",
        "Name": "Setup hive"
    }
}
```

- Para obtener información sobre la API, consulte DescribeStep en la Referencia de comandos de la AWS CLI.

`get`

En el siguiente ejemplo de código, se muestra cómo utilizar `get`.

AWS CLI

A continuación, se descarga el archivo `hadoop-examples.jar` de la instancia maestra en un clúster con el ID del clúster`j-3SD91U2E1L2QX`:

```
aws emr get --cluster-id j-3SD91U2E1L2QX --key-pair-file ~/.ssh/mykey.pem --src /
home/hadoop-examples.jar --dest ~
```

- Para obtener información sobre la API, consulte Get en la Referencia de comandos de la AWS CLI.

`list-clusters`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-clusters`.

AWS CLI

El siguiente comando enumera todos los clústeres de EMR activos en la región actual:

```
aws emr list-clusters --active
```

Salida:

```
{
    "Clusters": [
        {
            "Status": {
                "Timeline": {
                    "ReadyDateTime": 1433200405.353,
                    "CreationDateTime": 1433199926.596
                },
                "State": "WAITING",
                "StateChangeReason": {
                    "Message": "Waiting after step completed"
                }
            },
            "NormalizedInstanceHours": 6,
            "Id": "j-3SD91U2E1L2QX",
            "Name": "my-cluster"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListClusters en la Referencia de comandos de la AWS CLI.

`list-instance-fleets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-instance-fleets`.

AWS CLI

Para obtener los detalles de configuración de flotas de instancias en un clúster

En este ejemplo, se muestran los detalles de las flotas de instancias del clúster especificado.

Comando:

```
list-instance-fleets --cluster-id 'j-12ABCDEFGHI34JK'
```

Salida:

```
{
  "InstanceFleets": [
      {
          "Status": {
              "Timeline": {
                  "ReadyDateTime": 1488759094.637,
                  "CreationDateTime": 1488758719.817
              },
              "State": "RUNNING",
              "StateChangeReason": {
                  "Message": ""
              }
          },
          "ProvisionedSpotCapacity": 6,
          "Name": "CORE",
          "InstanceFleetType": "CORE",
          "LaunchSpecifications": {
              "SpotSpecification": {
                  "TimeoutDurationMinutes": 60,
                  "TimeoutAction": "TERMINATE_CLUSTER"
              }
          },
          "ProvisionedOnDemandCapacity": 2,
          "InstanceTypeSpecifications": [
              {
                  "BidPrice": "0.5",
                  "InstanceType": "m3.xlarge",
                  "WeightedCapacity": 2
              }
          ],
          "Id": "if-1ABC2DEFGHIJ3"
      },
      {
          "Status": {
              "Timeline": {
                  "ReadyDateTime": 1488759058.598,
                  "CreationDateTime": 1488758719.811
              },
              "State": "RUNNING",
```

```
                "StateChangeReason": {
                    "Message": ""
                }
            },
            "ProvisionedSpotCapacity": 0,
            "Name": "MASTER",
            "InstanceFleetType": "MASTER",
            "ProvisionedOnDemandCapacity": 1,
            "InstanceTypeSpecifications": [
                {
                    "BidPriceAsPercentageOfOnDemandPrice": 100.0,
                    "InstanceType": "m3.xlarge",
                    "WeightedCapacity": 1
                }
            ],
           "Id": "if-2ABC4DEFGHIJ4"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListInstanceFleets en la Referencia de comandos de la AWS CLI.

`list-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-instances`.

AWS CLI

El siguiente comando enumera todas las instancias de un clúster con el ID de clúster `j-3C6XNQ39VR9WL`:

```
aws emr list-instances --cluster-id j-3C6XNQ39VR9WL
```

Salida:

```
For a uniform instance group based cluster
  {
    "Instances": [
         {
            "Status": {
                "Timeline": {
```

```
                    "ReadyDateTime": 1433200400.03,
                    "CreationDateTime": 1433199960.152
                },
                "State": "RUNNING",
                "StateChangeReason": {}
            },
            "Ec2InstanceId": "i-f19ecfee",
            "PublicDnsName": "ec2-52-52-41-150.us-west-2.compute.amazonaws.com",
            "PrivateDnsName": "ip-172-21-11-216.us-west-2.compute.internal",
            "PublicIpAddress": "52.52.41.150",
            "Id": "ci-3NNHQUQ2TWB6Y",
            "PrivateIpAddress": "172.21.11.216"
        },
        {
            "Status": {
                "Timeline": {
                    "ReadyDateTime": 1433200400.031,
                    "CreationDateTime": 1433199949.102
                },
                "State": "RUNNING",
                "StateChangeReason": {}
            },
            "Ec2InstanceId": "i-1feee4c2",
            "PublicDnsName": "ec2-52-63-246-32.us-west-2.compute.amazonaws.com",
            "PrivateDnsName": "ip-172-31-24-130.us-west-2.compute.internal",
            "PublicIpAddress": "52.63.246.32",
            "Id": "ci-GAOCMKNKDCV7",
            "PrivateIpAddress": "172.21.11.215"
        },
        {
            "Status": {
                "Timeline": {
                    "ReadyDateTime": 1433200400.031,
                    "CreationDateTime": 1433199949.102
                },
                "State": "RUNNING",
                "StateChangeReason": {}
            },
            "Ec2InstanceId": "i-15cfeee3",
            "PublicDnsName": "ec2-52-25-246-63.us-west-2.compute.amazonaws.com",
            "PrivateDnsName": "ip-172-31-24-129.us-west-2.compute.internal",
            "PublicIpAddress": "52.25.246.63",
            "Id": "ci-2W3TDFFB47UAD",
            "PrivateIpAddress": "172.21.11.214"
```

```
        }
    ]
  }


For a fleet based cluster:
   {
      "Instances": [
          {
              "Status": {
                  "Timeline": {
                      "ReadyDateTime": 1487810810.878,
                      "CreationDateTime": 1487810588.367,
                      "EndDateTime": 1488022990.924
                  },
                  "State": "TERMINATED",
                  "StateChangeReason": {
                      "Message": "Instance was terminated."
                  }
              },
              "Ec2InstanceId": "i-xxxxx",
              "InstanceFleetId": "if-xxxxx",
              "EbsVolumes": [],
              "PublicDnsName": "ec2-xx-xxx-xxx-xxx.compute-1.amazonaws.com",
              "InstanceType": "m3.xlarge",
              "PrivateDnsName": "ip-xx-xx-xxx-xx.ec2.internal",
              "Market": "SPOT",
              "PublicIpAddress": "xx.xx.xxx.xxx",
              "Id": "ci-xxxxx",
              "PrivateIpAddress": "10.47.191.80"
          }
      ]
  }
```

- Para obtener información sobre la API, consulte ListInstances en la Referencia de comandos de la AWS CLI.

`list-security-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-security-configurations`.

AWS CLI

Para enumerar las configuraciones de seguridad de la región actual

Comando:

```
aws emr list-security-configurations
```

Salida:

```
{
    "SecurityConfigurations": [
        {
            "CreationDateTime": 1473889697.417,
            "Name": "MySecurityConfig-1"
        },
        {
            "CreationDateTime": 1473889697.417,
            "Name": "MySecurityConfig-2"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListSecurityConfigurations en la Referencia de comandos de la AWS CLI.

`list-steps`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-steps`.

AWS CLI

El siguiente comando muestra todos los pasos de un clúster con el ID del clúster `j-3SD91U2E1L2QX`:

```
aws emr list-steps --cluster-id j-3SD91U2E1L2QX
```

- Para obtener información sobre la API, consulte ListSteps en la Referencia de comandos de la AWS CLI.

`modify-cluster-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-cluster-attributes`.

AWS CLI

El siguiente comando establece la visibilidad de un clúster de EMR con el ID `j-301CDNY0J5XM4` para todos los usuarios:

```
aws emr modify-cluster-attributes --cluster-id j-301CDNY0J5XM4 --visible-to-all-
users
```

- Para obtener información sobre la API, consulte ModifyClusterAttributes en la Referencia de comandos de la AWS CLI.

`modify-instance-fleet`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-instance-fleet`.

AWS CLI

Para cambiar las capacidades de destino de una flota de instancias

En este ejemplo, se cambian las capacidades de destino bajo demanda y de spot a 1 para la flota de instancias especificada.

Comando:

```
aws emr modify-instance-fleet --cluster-id 'j-12ABCDEFGHI34JK' --instance-fleet
 InstanceFleetId='if-2ABC4DEFGHIJ4',TargetOnDemandCapacity=1,TargetSpotCapacity=1
```

- Para obtener detalles sobre la API, consulte ModifyInstanceFleet en la Referencia de comandos de la AWS CLI.

`put`

En el siguiente ejemplo de código, se muestra cómo utilizar `put`.

AWS CLI

El siguiente comando carga un archivo con el nombre `healthcheck.sh` de la instancia maestra de un clúster con el ID del clúster: `j-3SD91U2E1L2QX`

```
aws emr put --cluster-id j-3SD91U2E1L2QX --key-pair-file ~/.ssh/mykey.pem --src ~/
scripts/healthcheck.sh --dest /home/hadoop/bin/healthcheck.sh
```

- Para obtener información sobre la API, consulte Put en la Referencia de comandos de la AWS CLI.

`remove-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-tags`.

AWS CLI

El siguiente comando elimina una etiqueta con la clave `prod` de un clúster con el ID de clúster `j-3SD91U2E1L2QX`:

```
aws emr remove-tags --resource-id j-3SD91U2E1L2QX --tag-keys prod
```

- Para obtener información sobre la API, consulte RemoveTags en la Referencia de comandos de la AWS CLI.

`schedule-hbase-backup`

En el siguiente ejemplo de código, se muestra cómo utilizar `schedule-hbase-backup`.

AWS CLI

Nota: Este comando solo se puede usar con HBase en las versiones 2.x y 3.x de AMI.

1. Para programar una copia de seguridad de HBase completa >>>>>>> 06ab6d6e13564b5733d75abaf3b599f93cf39a23

Comando:

```
aws emr schedule-hbase-backup --cluster-id j-XXXXXXYY --type full --dir
s3://amzn-s3-demo-bucket/backup --interval 10 --unit hours --start-time
2014-04-21T05:26:10Z --consistent
```

Salida:

```
None
```

2. Para programar una copia de seguridad de HBase incremental

Comando:

```
aws emr schedule-hbase-backup --cluster-id j-XXXXXXYY --type incremental
 --dir s3://amzn-s3-demo-bucket/backup --interval 30 --unit minutes --start-time
2014-04-21T05:26:10Z --consistent
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte ScheduleHbaseBackup en la Referencia de comandos de la AWS CLI.

`socks`

En el siguiente ejemplo de código, se muestra cómo utilizar `socks`.

AWS CLI

El siguiente comando abre una conexión de Socks con la instancia maestra en un clúster con el ID del clúster `j-3SD91U2E1L2QX`:

```
aws emr socks --cluster-id j-3SD91U2E1L2QX --key-pair-file ~/.ssh/mykey.pem
```

La opción de archivo de par de claves toma una ruta local a un archivo de clave privada.

- Para obtener información sobre la API, consulte Socks en la Referencia de comandos de la AWS CLI.

`ssh`

En el siguiente ejemplo de código, se muestra cómo utilizar `ssh`.

AWS CLI

El siguiente comando abre una conexión ssh con la instancia maestra en un clúster con el ID de clúster `j-3SD91U2E1L2QX`:

```
aws emr ssh --cluster-id j-3SD91U2E1L2QX --key-pair-file ~/.ssh/mykey.pem
```

La opción de archivo de par de claves toma una ruta local a un archivo de clave privada.

Salida:

```
ssh -o StrictHostKeyChecking=no -o ServerAliveInterval=10 -i /home/local/user/.ssh/
mykey.pem hadoop@ec2-52-52-41-150.us-west-2.compute.amazonaws.com
Warning: Permanently added 'ec2-52-52-41-150.us-
west-2.compute.amazonaws.com,52.52.41.150' (ECDSA) to the list of known hosts.
Last login: Mon Jun  1 23:15:38 2015

      __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2015.03-release-notes/
26 package(s) needed for security, out of 39 available
Run "sudo yum update" to apply all updates.

--------------------------------------------------------------------------------

Welcome to Amazon Elastic MapReduce running Hadoop and Amazon Linux.

Hadoop is installed in /home/hadoop. Log files are in /mnt/var/log/hadoop. Check
/mnt/var/log/hadoop/steps for diagnosing step failures.

The Hadoop UI can be accessed via the following commands:

  ResourceManager    lynx http://ip-172-21-11-216:9026/
  NameNode           lynx http://ip-172-21-11-216:9101/

--------------------------------------------------------------------------------

[hadoop@ip-172-31-16-216 ~]$
```

- Para obtener información sobre la API, consulte Ssh en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon EMR en EKS que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando el AWS Command Line Interface con Amazon EMR en EKS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`update-role-trust-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-role-trust-policy`.

AWS CLI

Para actualizar la política de confianza de un rol de IAM que se utilizará con Amazon EMR en EKS

Este comando de ejemplo actualiza la política de confianza de un rol llamado example_iam_role para que pueda usarse con Amazon EMR en EKS con el espacio de nombres example_namespace de un clúster de EKS llamado example_cluster.

Comando:

```
aws emr-containers update-role-trust-policy \
    --cluster example_cluster \
    --namespace example_namespace \
    --role-name example_iam_role
```

Salida:

```
If the trust policy has already been updated, then the output will be:
Trust policy statement already exists for role example_iam_role. No
changes were made!

If the trust policy has not been updated yet, then the output will be:
Successfully updated trust policy of role example_iam_role.
```

- Para obtener información sobre la API, consulte UpdateRoleTrustPolicy en la Referencia de comandos de la AWS CLI.

Ejemplos de EventBridge que utilizan la AWS CLI

En el siguiente ejemplo de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con EventBridge.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`delete-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-rule`.

AWS CLI

Eliminación de una regla de Eventos de CloudWatch

En este ejemplo, se elimina la regla denominada EC2InstanceStateChanges:

```
aws events delete-rule --name "EC2InstanceStateChanges"
```

- Para obtener información sobre la API, consulte DeleteRule en la Referencia de comandos de la AWS CLI.

`describe-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-rule`.

AWS CLI

Visualización de información sobre una regla de Eventos de CloudWatch

En este ejemplo, se muestra información acerca de la regla denominada DailyLambdaFunction:

```
aws events describe-rule --name "DailyLambdaFunction"
```

- Para obtener información sobre la API, consulte DescribeRule en la Referencia de comandos de la AWS CLI.

`disable-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-rule`.

AWS CLI

Desactivación de una regla de Eventos de CloudWatch

En este ejemplo se deshabilita la regla denominada DailyLambdaFunction. La regla no se elimina:

```
aws events disable-rule --name "DailyLambdaFunction"
```

- Para obtener información sobre la API, consulte DisableRule en la Referencia de comandos de la AWS CLI.

`enable-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-rule`.

AWS CLI

Activación de una regla de Eventos de CloudWatch

En este ejemplo se habilita la regla denominada DailyLambdaFunction, que estaba deshabilitada anteriormente:

```
aws events enable-rule --name "DailyLambdaFunction"
```

- Para obtener información sobre la API, consulte EnableRule en la Referencia de comandos de la AWS CLI.

`list-rule-names-by-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-rule-names-by-target`.

AWS CLI

Visualización de una lista de todas las reglas que tienen un destino especificado

En este ejemplo, se muestran todas las reglas que tienen como destino la función de Lambda denominada "MyFunctionName":

```
aws events list-rule-names-by-target --target-arn "arn:aws:lambda:us-east-1:123456789012:function:MyFunctionName"
```

- Para obtener información sobre la API, consulte ListRuleNamesByTarget en la Referencia de comandos de la AWS CLI.

`list-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-rules`.

AWS CLI

Visualización de una lista de todas las reglas de Eventos de CloudWatch

En este ejemplo se muestran todas las reglas de Eventos de CloudWatch de la región:

```
aws events list-rules
```

Visualización de una lista de reglas de Eventos de CloudWatch que comiencen por una cadena determinada.

En este ejemplo se muestran todas las reglas de Eventos de CloudWatch de la región cuyo nombre comience por "Diario":

```
aws events list-rules --name-prefix "Daily"
```

- Para obtener información sobre la API, consulte ListRules en la Referencia de comandos de la AWS CLI.

`list-targets-by-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-targets-by-rule`.

AWS CLI

Visualización de todos los destinos de una regla de Eventos de CloudWatch

En este ejemplo, se muestran todos los destinos de la regla denominada DailyLambdaFunction:

```
aws events list-targets-by-rule --rule  "DailyLambdaFunction"
```

- Para obtener información sobre la API, consulte ListTargetsByRule en la Referencia de comandos de la AWS CLI.

`put-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-events`.

AWS CLI

Envío de un evento personalizado a Eventos de CloudWatch

En este ejemplo se envía un evento personalizado a Eventos de CloudWatch. El evento está incluido en el archivo putevents.json:

```
aws events put-events --entries file://putevents.json
```

Este es el contenido del archivo putevents.json:

```
[
  {
    "Source": "com.mycompany.myapp",
    "Detail": "{ \"key1\": \"value1\", \"key2\": \"value2\" }",
    "Resources": [
      "resource1",
      "resource2"
```

```
    ],
    "DetailType": "myDetailType"
  },
  {
    "Source": "com.mycompany.myapp",
    "Detail": "{ \"key1\": \"value3\", \"key2\": \"value4\" }",
    "Resources": [
      "resource1",
      "resource2"
    ],
    "DetailType": "myDetailType"
   }
]
```

- Para obtener información sobre la API, consulte PutEvents en la Referencia de comandos de la AWS CLI.

`put-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-rule`.

AWS CLI

Creación de las reglas de Eventos de CloudWatch

Este ejemplo crea una regla que se activa cada día a las 9:00 (UTC). Si utiliza put-targets para añadir una función de Lambda como destino de esta regla, puede ejecutar la función de Lambda todos los días a la hora especificada:

```
aws events put-rule --name "DailyLambdaFunction" --schedule-expression "cron(0 9 *
 * ? *)"
```

En este ejemplo se crea una regla que se activa cuando una instancia EC2 de la región cambia de estado:

```
aws events put-rule --name "EC2InstanceStateChanges" --event-pattern "{\"source\":
[\"aws.ec2\"],\"detail-type\":[\"EC2 Instance State-change Notification\"]}"  --
role-arn "arn:aws:iam::123456789012:role/MyRoleForThisRule"
```

En este ejemplo, se crea una regla que se activa cuando se detiene o se termina una instancia de EC2 de la región:

```
aws events put-rule --name "EC2InstanceStateChangeStopOrTerminate" --event-
pattern "{\"source\":[\"aws.ec2\"],\"detail-type\":[\"EC2 Instance State-change
 Notification\"],\"detail\":{\"state\":[\"stopped\",\"terminated\"]}}" --role-
arn "arn:aws:iam::123456789012:role/MyRoleForThisRule"
```

- Para obtener información sobre la API, consulte PutRule en la Referencia del comando de la AWS CLI.

`put-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-targets`.

AWS CLI

Adición de destinos a las reglas de Eventos de CloudWatch

En este ejemplo, se añade una función de Lambda como destino de una regla:

```
aws events put-targets --rule DailyLambdaFunction --targets
 "Id"="1","Arn"="arn:aws:lambda:us-east-1:123456789012:function:MyFunctionName"
```

En este ejemplo, se establece una transmisión de Amazon Kinesis como destino, de modo que los eventos detectados por esta regla se retransmitan a la transmisión:

```
aws events put-targets --rule EC2InstanceStateChanges --targets
 "Id"="1","Arn"="arn:aws:kinesis:us-east-1:123456789012:stream/
MyStream","RoleArn"="arn:aws:iam::123456789012:role/MyRoleForThisRule"
```

En este ejemplo, se establecen dos transmisiones de Amazon Kinesis como destinos para una regla:

```
aws events put-targets --rule DailyLambdaFunction --targets
 "Id"="Target1","Arn"="arn:aws:kinesis:us-east-1:379642911888:stream/
MyStream1","RoleArn"="arn:aws:iam::379642911888:role/ MyRoleToAccessLambda"
  "Id"="Target2"," Arn"="arn:aws:kinesis:us-east-1:379642911888:stream/
MyStream2","RoleArn"="arn:aws:iam::379642911888:role/MyRoleToAccessLambda"
```

- Para obtener información sobre la API, consulte PutTargets en la Referencia de comandos de AWS CLI.

`remove-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-targets`.

AWS CLI

Eliminación de un destino de un evento

En este ejemplo se elimina el flujo de Amazon Kinesis denominado MyStream1 de ser un destino de la regla DailyLambdaFunction. Cuando se creó DailyLambdaFunction, este flujo se estableció como un destino con el ID de Target1:

```
aws events remove-targets --rule "DailyLambdaFunction" --ids "Target1"
```

- Para obtener información sobre la API, consulte RemoveTargets en la Referencia de comandos de la AWS CLI.

`test-event-pattern`

En el siguiente ejemplo de código, se muestra cómo utilizar `test-event-pattern`.

AWS CLI

Para comprobar si un patrón de eventos coincide con un evento específico

En este ejemplo, se comprueba si el patrón source:com.mycompany.myapp coincide con el evento especificado. En este ejemplo, la salida sería true:

```
aws events test-event-pattern --event-pattern "{\"source\":[\"com.mycompany.myapp
\"]}" --event "{\"id\":\"1\",\"source\":\"com.mycompany.myapp\",\"detail-type\":
\"myDetailType\",\"account\":\"123456789012\",\"region\":\"us-east-1\",\"time\":
\"2017-04-11T20:11:04Z\"}"
```

- Para obtener información sobre la API, consulte TestEventPattern en la Referencia de comandos de la AWS CLI.

Ejemplos de canalizaciones de EventBridge con la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante la AWS Command Line Interface con canalizaciones de EventBridge.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-pipe`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-pipe`.

AWS CLI

Creación de una canalización

En el siguiente ejemplo de `create-pipe`, se crea una canalización denominada `Demo_Pipe` con SQS como origen y el grupo de registro de CloudWatch como destino de la canalización.

```
aws pipes create-pipe \
    --name Demo_Pipe \
    --desired-state RUNNING \
    --role-arn arn:aws:iam::123456789012:role/service-role/
Amazon_EventBridge_Pipe_Demo_Pipe_28b3aa4f \
    --source arn:aws:sqs:us-east-1:123456789012:Demo_Queue \
    --target arn:aws:logs:us-east-1:123456789012:log-group:/aws/pipes/Demo_LogGroup
```

Salida:

```
{
    "Arn": "arn:aws:pipes:us-east-1:123456789012:pipe/Demo_Pipe",
    "Name": "Demo_Pipe",
    "DesiredState": "RUNNING",
    "CurrentState": "CREATING",
    "CreationTime": "2024-10-08T12:33:59-05:00",
    "LastModifiedTime": "2024-10-08T12:33:59.684839-05:00"
}
```

Para obtener más información, consulte Conceptos de canalizaciones de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

- Para obtener información sobre la API, consulte CreatePipe en la Referencia de comandos de la AWS CLI.

`delete-pipe`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-pipe`.

AWS CLI

Eliminación de una canalización existente

En el siguiente ejemplo de `delete-pipe`, se elimina una canalización denominada `Demo_Pipe` en la cuenta especificada.

```
aws pipes delete-pipe \
    --name Demo_Pipe
```

Salida:

```
{
    "Arn": "arn:aws:pipes:us-east-1:123456789012:pipe/Demo_Pipe",
    "Name": "Demo_Pipe",
    "DesiredState": "STOPPED",
    "CurrentState": "DELETING",
    "CreationTime": "2024-10-08T09:29:10-05:00",
    "LastModifiedTime": "2024-10-08T11:57:22-05:00"
}
```

Para obtener más información, consulte Conceptos de canalizaciones de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

- Para obtener información sobre la API, consulte DeletePipe en la Referencia de comandos de la AWS CLI.

`describe-pipe`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-pipe`.

AWS CLI

Recuperación de información sobre una canalización

En el siguiente ejemplo de `describe-pipe`, se muestra información acerca de la canalización `Demo_Pipe` en la cuenta especificada.

```
aws pipes describe-pipe \
    --name Demo_Pipe
```

Salida:

```
{
    "Arn": "arn:aws:pipes:us-east-1:123456789012:pipe/Demo_Pipe",
    "Name": "Demo_Pipe",
    "DesiredState": "RUNNING",
    "CurrentState": "RUNNING",
    "StateReason": "User initiated",
    "Source": "arn:aws:sqs:us-east-1:123456789012:Demo_Queue",
    "SourceParameters": {
        "SqsQueueParameters": {
            "BatchSize": 1
        }
    },
    "EnrichmentParameters": {},
    "Target": "arn:aws:logs:us-east-1:123456789012:log-group:/aws/pipes/
Demo_LogGroup",
    "TargetParameters": {},
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/
Amazon_EventBridge_Pipe_Demo_Pipe_28b3aa4f",
    "Tags": {},
    "CreationTime": "2024-10-08T09:29:10-05:00",
    "LastModifiedTime": "2024-10-08T10:23:47-05:00",
    "LogConfiguration": {
        "CloudwatchLogsLogDestination": {
            "LogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-group:/aws/
vendedlogs/pipes/Demo_Pipe"
        },
        "Level": "ERROR"
    }
}
```

Para obtener más información, consulte Conceptos de canalizaciones de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

- Para obtener información sobre la API, consulte DescribePipe en la Referencia de comandos de la AWS CLI.

`list-pipes`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-pipes`.

AWS CLI

Recuperación de una lista de canalizaciones

En el siguiente ejemplo de `list-pipes`, se muestran todas las canalizaciones de la cuenta especificada.

```
aws pipes list-pipes
```

Salida:

```
{
    "Pipes": [
        {
            "Name": "Demo_Pipe",
            "Arn": "arn:aws:pipes:us-east-1:123456789012:pipe/Demo_Pipe",
            "DesiredState": "RUNNING",
            "CurrentState": "RUNNING",
            "StateReason": "User initiated",
            "CreationTime": "2024-10-08T09:29:10-05:00",
            "LastModifiedTime": "2024-10-08T10:23:47-05:00",
            "Source": "arn:aws:sqs:us-east-1:123456789012:Demo_Queue",
            "Target": "arn:aws:logs:us-east-1:123456789012:log-group:/aws/pipes/
Demo_LogGroup"
        }
    ]
}
```

Para obtener más información, consulte Conceptos de canalizaciones de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

- Para obtener información sobre la API, consulte ListPipes en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Muestra de las etiquetas asociadas a una canalización existente

En el siguiente ejemplo de `list-tags-for-resource`, se muestran todas las etiquetas asociadas a una canalización denominada `Demo_Pipe` en la cuenta especificada.

```
aws pipes list-tags-for-resource \
    --resource-arn arn:aws:pipes:us-east-1:123456789012:pipe/Demo_Pipe
```

Salida:

```
{
    "tags": {
        "stack": "Production",
        "team": "DevOps"
    }
}
```

Para obtener más información, consulte Conceptos de canalizaciones de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`start-pipe`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-pipe`.

AWS CLI

Inicio de una canalización existente

En el siguiente ejemplo de `start-pipe`, se inicia una canalización denominada `Demo_Pipe` en la cuenta especificada.

```
aws pipes start-pipe \
    --name Demo_Pipe
```

Salida:

```
{
    "Arn": "arn:aws:pipes:us-east-1:123456789012:pipe/Demo_Pipe",
    "Name": "Demo_Pipe",
    "DesiredState": "RUNNING",
    "CurrentState": "STARTING",
    "CreationTime": "2024-10-08T09:29:10-05:00",
    "LastModifiedTime": "2024-10-08T10:17:24-05:00"
}
```

Para más información, consulte Inicio o detención de una canalización de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

- Para obtener información sobre la API, consulte StartPipe en la Referencia de comandos de la AWS CLI.

`stop-pipe`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-pipe`.

AWS CLI

Detención de una canalización existente

En el siguiente ejemplo de `stop-pipe`, se detiene una canalización denominada `Demo_Pipe` en la cuenta especificada.

```
aws pipes stop-pipe \
    --name Demo_Pipe
```

Salida:

```
{
    "Arn": "arn:aws:pipes:us-east-1:123456789012:pipe/Demo_Pipe",
    "Name": "Demo_Pipe",
    "DesiredState": "STOPPED",
    "CurrentState": "STOPPING",
```

```
    "CreationTime": "2024-10-08T09:29:10-05:00",
    "LastModifiedTime": "2024-10-08T09:29:49-05:00"
}
```

Para más información, consulte Inicio o detención de una canalización de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

- Para obtener información sobre la API, consulte StopPipe en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Etiquetado de una canalización existente

En el siguiente ejemplo de `tag-resource`, se etiqueta una canalización denominada `Demo_Pipe`. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

```
aws pipes tag-resource \
    --resource-arn arn:aws:pipes:us-east-1:123456789012:pipe/Demo_Pipe \
    --tags stack=Production
```

Para obtener más información, consulte Conceptos de canalizaciones de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de una etiqueta de una canalización existente

En el siguiente ejemplo de `untag-resource`, se elimina una etiqueta con la clave `stack` de la canalización denominada `Demo_Pipe`. Si el comando se ejecuta correctamente, no se muestra ningún resultado.

```
aws pipes untag-resource \
    --resource-arn arn:aws:pipes:us-east-1:123456789012:pipe/Demo_Pipe \
    --tags stack
```

Para obtener más información, consulte Conceptos de canalizaciones de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-pipe

En el siguiente ejemplo de código, se muestra cómo utilizar `update-pipe`.

AWS CLI

Actualización de una canalización existente

En el siguiente ejemplo de `update-pipe`, se actualiza la canalización denominada `Demo_Pipe` agregando un parámetro de configuración de registro de CloudWatch. Asegúrese de actualizar el rol de ejecución de la canalización para que tenga los permisos correctos para el destino del registro.

```
aws pipes update-pipe \
    --name Demo_Pipe \
    --desired-state RUNNING \
    --log-configuration CloudwatchLogsLogDestination={LogGroupArn=arn:aws:logs:us-
east-1:123456789012:log-group:/aws/vendedlogs/pipes/Demo_Pipe},Level=TRACE \
    --role-arn arn:aws:iam::123456789012:role/service-role/
Amazon_EventBridge_Pipe_Demo_Pipe_28b3aa4f
```

Salida:

```
{
    "Arn": "arn:aws:pipes:us-east-1:123456789012:pipe/Demo_Pipe",
    "Name": "Demo_Pipe",
    "DesiredState": "RUNNING",
    "CurrentState": "UPDATING",
    "CreationTime": "2024-10-08T09:29:10-05:00",
    "LastModifiedTime": "2024-10-08T11:35:48-05:00"
}
```

Para obtener más información, consulte Conceptos de canalizaciones de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

- Para obtener información sobre la API, consulte UpdatePipe en la Referencia de comandos de la AWS CLI.

Ejemplos de Firewall Manager que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Firewall Manager.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-admin-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-admin-account`.

AWS CLI

Para establecer la cuenta de administrador de Firewall Manager

En el siguiente ejemplo de `associate-admin-account`, se establece la cuenta de administrador para Firewall Manager.

```
aws fms associate-admin-account \
    --admin-account 123456789012
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Set the AWS Firewall Manager Administrator Account en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Advanced.

- Para obtener más detalles sobre la API, consulte AssociateAdminAccount en la Referencia de comandos de la AWS CLI.

`delete-notification-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-notification-channel`.

AWS CLI

Para eliminar la información sobre temas de SNS para los registros de Firewall Manager

En el siguiente ejemplo de `delete-notification-channel`, se elimina la información del tema de SNS.

```
aws fms delete-notification-channel
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configure Amazon SNS Notifications and Amazon CloudWatch Alarms en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Advanced.

- Para obtener información sobre la API, consulte DeleteNotificationChannel en la Referencia de comandos de la AWS CLI.

`delete-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-policy`.

AWS CLI

Para eliminar una política de Firewall Manager

En el siguiente ejemplo de `delete-policy`, se elimina la política con el ID especificado, junto con todos sus recursos.

```
aws fms delete-policy \
    --policy-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --delete-all-policy-resources
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de políticas de AWS Firewall Manager en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Advanced.

- Para obtener información sobre la API, consulte DeletePolicy en la Referencia de comandos de la AWS CLI.

`disassociate-admin-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-admin-account`.

AWS CLI

Para eliminar la cuenta de administrador de Firewall Manager

En el siguiente ejemplo de `disassociate-admin-account`, se elimina la asociación de cuentas de administrador actual de Firewall Manager.

```
aws fms disassociate-admin-account
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Set the AWS Firewall Manager Administrator Account en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Advanced.

- Para obtener información sobre la API, consulte DisassociateAdminAccount en la Referencia de la comandos de la AWS CLI.

`get-admin-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-admin-account`.

AWS CLI

Para recuperar la cuenta de administrador de Firewall Manager

En el siguiente ejemplo de `get-admin-account`, se recupera la cuenta de administrador.

```
aws fms get-admin-account
```

Salida:

```
{
    "AdminAccount": "123456789012",
    "RoleStatus": "READY"
}
```

Para obtener más información, consulte AWS Firewall Manager Prerequisites en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte GetAdminAccount en la Referencia de comandos de la AWS CLI.

`get-compliance-detail`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-compliance-detail`.

AWS CLI

Para recuperar la información de cumplimiento de una cuenta

En el siguiente ejemplo de `get-compliance-detail`, se recupera la información de cumplimiento para la cuenta de miembro y la política especificadas.

```
aws fms get-compliance-detail \
    --policy-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --member-account 123456789012
```

Salida:

```
{
    "PolicyComplianceDetail": {
    "EvaluationLimitExceeded": false,
    "IssueInfoMap": {},
    "MemberAccount": "123456789012",
    "PolicyId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "PolicyOwner": "123456789012",
    "Violators": []
}
```

Para obtener más información, consulte Visualización de información de conformidad para una política de AWS Firewall Manager en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Advanced.

- Para obtener información sobre la API, consulte GetComplianceDetail en la Referencia de comandos de la AWS CLI.

`get-notification-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-notification-channel`.

AWS CLI

Para recuperar la información sobre temas de SNS para los registros de Firewall Manager

En el siguiente ejemplo de `get-notification-channel`, se recupera la información del tema de SNS.

```
aws fms get-notification-channel
```

Salida:

```
{
    "SnsTopicArn": "arn:aws:sns:us-west-2:123456789012:us-west-2-fms",
    "SnsRoleName": "arn:aws:iam::123456789012:role/aws-service-role/
fms.amazonaws.com/AWSServiceRoleForFMS"
}
```

Para obtener más información, consulte Configure Amazon SNS Notifications and Amazon CloudWatch Alarms en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Advanced.

- Para obtener información sobre la API, consulte GetNotificationChannel en la Referencia de comandos de la AWS CLI.

`get-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-policy`.

AWS CLI

Para recuperar una política de Firewall Manager

En el siguiente ejemplo de `get-policy`, se recupera la política con el ID especificado.

```
aws fms get-policy \
    --policy-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "Policy": {
        "PolicyId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "PolicyName": "test",
        "PolicyUpdateToken": "1:p+2RpKR4wPFx7mcrL1UOQQ==",
        "SecurityServicePolicyData": {
            "Type": "SECURITY_GROUPS_COMMON",
            "ManagedServiceData": "{\"type\":\"SECURITY_GROUPS_COMMON\",
\"revertManualSecurityGroupChanges\":true,\"exclusiveResourceSecurityGroupManagement
\":false,\"securityGroups\":[{\"id\":\"sg-045c43ccc9724e63e\"}]}"
        },
        "ResourceType": "AWS::EC2::Instance",
        "ResourceTags": [],
        "ExcludeResourceTags": false,
        "RemediationEnabled": false
    },
    "PolicyArn": "arn:aws:fms:us-west-2:123456789012:policy/d1ac59b8-938e-42b3-
b2e0-7c620422ddc2"
}
```

Para obtener más información, consulte Uso de políticas de AWS Firewall Manager en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Advanced.

- Para obtener información sobre la API, consulte GetPolicy en la Referencia de comandos de la AWS CLI.

`list-compliance-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-compliance-status`.

AWS CLI

Para recuperar la información de cumplimiento de las políticas para las cuentas de miembros

En el siguiente ejemplo de `list-compliance-status`, se recupera la información de cumplimiento de cuenta de miembro para la política especificada.

```
aws fms list-compliance-status \
    --policy-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "PolicyComplianceStatusList": [
        {
            "PolicyOwner": "123456789012",
            "PolicyId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "PolicyName": "test",
            "MemberAccount": "123456789012",
            "EvaluationResults": [
                {
                    "ComplianceStatus": "COMPLIANT",
                    "ViolatorCount": 0,
                    "EvaluationLimitExceeded": false
                },
                {
                    "ComplianceStatus": "NON_COMPLIANT",
                    "ViolatorCount": 2,
                    "EvaluationLimitExceeded": false
                }
            ],
            "LastUpdated": 1576283774.0,
            "IssueInfoMap": {}
        }
    ]
}
```

Para obtener más información, consulte Visualización de información de conformidad para una política de AWS Firewall Manager en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Advanced.

- Para obtener información sobre la API, consulte ListComplianceStatus en la Referencia de comandos de la AWS CLI.

`list-member-accounts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-member-accounts`.

AWS CLI

Para recuperar las cuentas de miembros de la organización

En el siguiente ejemplo de `list-member-accounts`, se enumeran todas las cuentas de miembros que se encuentran en la organización del administrador de Firewall Manager.

```
aws fms list-member-accounts
```

Salida:

```
{
    "MemberAccounts": [
        "222222222222",
        "333333333333",
        "444444444444"
    ]
}
```

Para obtener más información, consulte AWS Firewall Manager en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Advanced.

- Para obtener información sobre la API, consulte ListMemberAccounts en la Referencia de comandos de la AWS CLI.

`list-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-policies`.

AWS CLI

Para recuperar todas las políticas de Firewall Manager

En el siguiente ejemplo de `list-policies`, se recupera la lista de políticas para la cuenta. En este ejemplo, la salida está limitada a dos resultados por solicitud. Cada llamada devuelve un valor de `NextToken` que se puede utilizar como valor del parámetro `--starting-token` en la siguiente llamada de `list-policies` para obtener el siguiente conjunto de resultados para la lista.

```
aws fms list-policies \
    --max-items 2
```

Salida:

```
{
    "PolicyList": [
        {
            "PolicyArn": "arn:aws:fms:us-west-2:123456789012:policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "PolicyId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "PolicyName": "test",
            "ResourceType": "AWS::EC2::Instance",
            "SecurityServiceType": "SECURITY_GROUPS_COMMON",
            "RemediationEnabled": false
        },
        {
            "PolicyArn": "arn:aws:fms:us-west-2:123456789012:policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "PolicyId": "457c9b21-fc94-406c-ae63-21217395ba72",
            "PolicyName": "test",
            "ResourceType": "AWS::EC2::Instance",
            "SecurityServiceType": "SECURITY_GROUPS_COMMON",
            "RemediationEnabled": false
        }
    ],
    "NextToken": "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAyfQ=="
}
```

Para obtener más información, consulte Uso de políticas de AWS Firewall Manager en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Advanced.

- Para obtener información sobre la API, consulte ListPolicies en la Referencia de comandos de la AWS CLI.

`put-notification-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-notification-channel`.

AWS CLI

Para establecer la información del tema SNS para los registros de Firewall Manager

En el siguiente ejemplo de `put-notification-channel`, se establece la información del tema de SNS.

```
aws fms put-notification-channel \
    --sns-topic-arn arn:aws:sns:us-west-2:123456789012:us-west-2-fms \
    --sns-role-name arn:aws:iam::123456789012:role/aws-service-role/
fms.amazonaws.com/AWSServiceRoleForFMS
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configure Amazon SNS Notifications and Amazon CloudWatch Alarms en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Advanced.

- Para obtener información sobre la API, consulte PutNotificationChannel en la Referencia de comandos de la AWS CLI.

`put-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-policy`.

AWS CLI

Para crear una política de Firewall Manager

En el siguiente ejemplo de `put-policy`, se crea una política de grupo de seguridad de Firewall Manager.

```
aws fms put-policy \
    --cli-input-json file://policy.json
```

Contenido de `policy.json`:

```
{
    "Policy": {
        "PolicyName": "test",
        "SecurityServicePolicyData": {
            "Type": "SECURITY_GROUPS_USAGE_AUDIT",
            "ManagedServiceData": "{\"type\":\"SECURITY_GROUPS_USAGE_AUDIT\",
\"deleteUnusedSecurityGroups\":false,\"coalesceRedundantSecurityGroups\":true}"
        },
        "ResourceType": "AWS::EC2::SecurityGroup",
        "ResourceTags": [],
        "ExcludeResourceTags": false,
```

```
        "RemediationEnabled": false
    },
    "TagList": [
        {
            "Key": "foo",
            "Value": "foo"
        }
    ]
}
```

Salida:

```
{
    "Policy": {
        "PolicyId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "PolicyName": "test",
        "PolicyUpdateToken": "1:X9QGexP7HASDlsFp+G31Iw==",
        "SecurityServicePolicyData": {
            "Type": "SECURITY_GROUPS_USAGE_AUDIT",
            "ManagedServiceData": "{\"type\":\"SECURITY_GROUPS_USAGE_AUDIT\",
\"deleteUnusedSecurityGroups\":false,\"coalesceRedundantSecurityGroups\":true,
\"optionalDelayForUnusedInMinutes\":null}"
        },
        "ResourceType": "AWS::EC2::SecurityGroup",
        "ResourceTags": [],
        "ExcludeResourceTags": false,
        "RemediationEnabled": false
    },
    "PolicyArn": "arn:aws:fms:us-west-2:123456789012:policy/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
}
```

Para obtener más información, consulte Uso de políticas de AWS Firewall Manager en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Advanced.

- Para obtener información sobre la API, consulte PutPolicy en la Referencia de comandos de la AWS CLI.

AWS FIS Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS FIS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-experiment-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-experiment-template`.

AWS CLI

Para crear una plantilla de experimento

En el siguiente ejemplo de `create-experiment-template`, se crea una plantilla de experimento en su cuenta de AWS FIS.

```
aws fis create-experiment-template \
    --cli-input-json file://myfile.json
```

Contenidos de `myfile.json`:

```
{
    "description": "experimentTemplate",
    "stopConditions": [
        {
            "source": "aws:cloudwatch:alarm",
            "value": "arn:aws:cloudwatch:us-west-2:123456789012:alarm:alarmName"
        }
    ],
    "targets": {
        "Instances-Target-1": {
            "resourceType": "aws:ec2:instance",
            "resourceArns": [
                "arn:aws:ec2:us-west-2:123456789012:instance/i-12a3b4c56d78e9012"
```

```
            ],
            "selectionMode": "ALL"
        }
    },
    "actions": {
        "reboot": {
            "actionId": "aws:ec2:reboot-instances",
            "description": "reboot",
            "parameters": {},
            "targets": {
                "Instances": "Instances-Target-1"
            }
        }
    },
    "roleArn": "arn:aws:iam::123456789012:role/myRole"
}
```

Salida:

```
{
    "experimentTemplate": {
        "id": "ABCDE1fgHIJkLmNop",
        "description": "experimentTemplate",
        "targets": {
            "Instances-Target-1": {
                "resourceType": "aws:ec2:instance",
                "resourceArns": [
                    "arn:aws:ec2:us-west-2:123456789012:instance/
i-12a3b4c56d78e9012"
                ],
                "selectionMode": "ALL"
            }
        },
        "actions": {
            "reboot": {
                "actionId": "aws:ec2:reboot-instances",
                "description": "reboot",
                "parameters": {},
                "targets": {
                    "Instances": "Instances-Target-1"
                }
            }
        },
```

```
        "stopConditions": [
            {
                "source": "aws:cloudwatch:alarm",
                "value": "arn:aws:cloudwatch:us-west-2:123456789012:alarm:alarmName"
            }
        ],
        "creationTime": 1616434850.659,
        "lastUpdateTime": 1616434850.659,
        "roleArn": "arn:aws:iam::123456789012:role/myRole",
        "tags": {}
    }
}
```

Para obtener más información, consulte Create an experiment template en la Guía del usuario de AWS Fault Injection Simulator.

- Para obtener información sobre la API, consulte CreateExperimentTemplate en la Referencia de comandos de la AWS CLI.

`delete-experiment-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-experiment-template`.

AWS CLI

Para eliminar una plantilla de experimento

En el siguiente ejemplo de `delete-experiment-template`, se elimina la plantilla de experimento especificada.

```
aws fis delete-experiment-template \
    --id ABCDE1fgHIJkLmNop
```

Salida:

```
{
    "experimentTemplate": {
        "id": "ABCDE1fgHIJkLmNop",
        "description": "myExperimentTemplate",
        "targets": {
            "Instances-Target-1": {
                "resourceType": "aws:ec2:instance",
                "resourceArns": [
```

```
                    "arn:aws:ec2:us-west-2:123456789012:instance/
i-12a3b4c56d78e9012"
                ],
                "selectionMode": "ALL"
            }
        },
        "actions": {
            "testaction": {
                "actionId": "aws:ec2:stop-instances",
                "parameters": {},
                "targets": {
                    "Instances": "Instances-Target-1"
                }
            }
        },
        "stopConditions": [
            {
                "source": "none"
            }
        ],
        "creationTime": 1616017191.124,
        "lastUpdateTime": 1616017859.607,
        "roleArn": "arn:aws:iam::123456789012:role/FISRole"
    }
}
```

Para obtener más información, consulte Delete an experiment template en la Guía del usuario de AWS Fault Injection Simulator.

- Para obtener información sobre la API, consulte DeleteExperimentTemplate en la Referencia de comandos de la AWS CLI.

`get-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-action`.

AWS CLI

Para obtener los detalles de la acción

En el siguiente ejemplo de `get-action`, se obtienen los detalles de la acción especificada.

```
aws fis get-action \
```

```
    --id aws:ec2:stop-instances
```

Salida:

```
{
    "action": {
        "id": "aws:ec2:stop-instances",
        "description": "Stop the specified EC2 instances.",
        "parameters": {
            "startInstancesAfterDuration": {
                "description": "The time to wait before restarting the instances
 (ISO 8601 duration).",
                "required": false
            }
        },
        "targets": {
            "Instances": {
                "resourceType": "aws:ec2:instance"
            }
        },
        "tags": {}
    }
}
```

Para obtener más información, consulte Actions en la Guía del usuario de AWS Fault Injection Simulator.

- Para obtener información sobre la API, consulte GetAction en la Referencia de comandos de la AWS CLI.

`get-experiment-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-experiment-template`.

AWS CLI

Para obtener los detalles de la plantilla de experimento

En el siguiente ejemplo de `get-experiment-template`, se obtienen los detalles de la plantilla de experimento especificada.

```
aws fis get-experiment-template \
```

```
    --id ABCDE1fgHIJkLmNop
```

Salida:

```
{
    "experimentTemplate": {
        "id": "ABCDE1fgHIJkLmNop",
        "description": "myExperimentTemplate",
        "targets": {
            "Instances-Target-1": {
                "resourceType": "aws:ec2:instance",
                "resourceArns": [
                    "arn:aws:ec2:us-west-2:123456789012:instance/
i-12a3b4c56d78e9012"
                ],
                "selectionMode": "ALL"
            }
        },
        "actions": {
            "testaction": {
                "actionId": "aws:ec2:stop-instances",
                "parameters": {},
                "targets": {
                    "Instances": "Instances-Target-1"
                }
            }
        },
        "stopConditions": [
            {
                "source": "none"
            }
        ],
        "creationTime": 1616017191.124,
        "lastUpdateTime": 1616017331.51,
        "roleArn": "arn:aws:iam::123456789012:role/FISRole",
        "tags": {
        "key: "value"
        }
    }
}
```

Para obtener más información, consulte Experiment templates en la Guía del usuario de AWS Fault Injection Simulator.

- Para obtener información sobre la API, consulte GetExperimentTemplate en la Referencia de comandos de la AWS CLI.

`get-experiment`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-experiment`.

AWS CLI

Para obtener los detalles del experimento

En el siguiente ejemplo de `get-experiment`, se obtienen los detalles del experimento especificado.

```
aws fis get-experiment \
    --id ABC12DeFGhI3jKLMNOP
```

Salida:

```
{
    "experiment": {
        "id": "ABC12DeFGhI3jKLMNOP",
        "experimentTemplateId": "ABCDE1fgHIJkLmNop",
        "roleArn": "arn:aws:iam::123456789012:role/myRole",
        "state": {
            "status": "completed",
            "reason": "Experiment completed."
        },
        "targets": {
            "Instances-Target-1": {
                "resourceType": "aws:ec2:instance",
                "resourceArns": [
                    "arn:aws:ec2:us-west-2:123456789012:instance/
i-12a3b4c56d78e9012"
                ],
                "selectionMode": "ALL"
            }
        },
        "actions": {
            "reboot": {
                "actionId": "aws:ec2:reboot-instances",
                "parameters": {},
```

```
                "targets": {
                    "Instances": "Instances-Target-1"
                },
                "state": {
                    "status": "completed",
                    "reason": "Action was completed."
                }
            }
        },
        "stopConditions": [
            {
                "source": "none"
            }
        ],
        "creationTime": 1616432509.662,
        "startTime": 1616432509.962,
        "endTime": 1616432522.307,
        "tags": {}
    }
}
```

Para obtener más información, consulte Experiments for AWS FIS en la Guía del usuario de AWS Fault Injection Simulator.

- Para obtener información sobre la API, consulte GetExperiment en la Referencia de comandos de la AWS CLI.

`list-actions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-actions`.

AWS CLI

Para enumerar las acciones

En el siguiente ejemplo de `list-actions`, se enumeran todas las acciones disponibles.

```
aws fis list-actions
```

Salida:

```
{
    "actions": [
```

```
        {
            "id": "aws:ec2:reboot-instances",
            "description": "Reboot the specified EC2 instances.",
            "targets": {
                "Instances": {
                    "resourceType": "aws:ec2:instance"
                }
            },
            "tags": {}
        },
        {
            "id": "aws:ec2:stop-instances",
            "description": "Stop the specified EC2 instances.",
            "targets": {
                "Instances": {
                    "resourceType": "aws:ec2:instance"
                }
            },
            "tags": {}
        },
        {
            "id": "aws:ec2:terminate-instances",
            "description": "Terminate the specified EC2 instances.",
            "targets": {
                "Instances": {
                    "resourceType": "aws:ec2:instance"
                }
            },
            "tags": {}
        },
        {
            "id": "aws:ecs:drain-container-instances",
            "description": "Drain percentage of underlying EC2 instances on an ECS
cluster.",
            "targets": {
                "Clusters": {
                    "resourceType": "aws:ecs:cluster"
                }
            },
            "tags": {}
        },
        {
            "id": "aws:eks:terminate-nodegroup-instances",
```

```
            "description": "Terminates a percentage of the underlying EC2 instances
in an EKS cluster.",
            "targets": {
                "Nodegroups": {
                    "resourceType": "aws:eks:nodegroup"
                }
            },
            "tags": {}
        },
        {
            "id": "aws:fis:inject-api-internal-error",
            "description": "Cause an AWS service to return internal error responses
for specific callers and operations.",
            "targets": {
                "Roles": {
                    "resourceType": "aws:iam:role"
                }
            },
            "tags": {}
        },
        {
            "id": "aws:fis:inject-api-throttle-error",
            "description": "Cause an AWS service to return throttled responses for
specific callers and operations.",
            "targets": {
                "Roles": {
                    "resourceType": "aws:iam:role"
                }
            },
            "tags": {}
        },
        {
        "id": "aws:fis:inject-api-unavailable-error",
            "description": "Cause an AWS service to return unavailable error
responses for specific callers and operations.",
            "targets": {
                "Roles": {
                    "resourceType": "aws:iam:role"
                }
            },
            "tags": {}
        },
        {
            "id": "aws:fis:wait",
```

```
            "description": "Wait for the specified duration. Stop condition
 monitoring will continue during this time.",
            "tags": {}
        },
        {
            "id": "aws:rds:failover-db-cluster",
            "description": "Failover a DB Cluster to one of the replicas.",
            "targets": {
                "Clusters": {
                    "resourceType": "aws:rds:cluster"
                }
            },
            "tags": {}
        },
        {
            "id": "aws:rds:reboot-db-instances",
            "description": "Reboot the specified DB instances.",
            "targets": {
                "DBInstances": {
                    "resourceType": "aws:rds:db"
                }
            },
            "tags": {}
        },
        {
            "id": "aws:ssm:send-command",
            "description": "Run the specified SSM document.",
            "targets": {
                "Instances": {
                    "resourceType": "aws:ec2:instance"
                }
            },
            "tags": {}
        }
    ]
}
```

Para obtener más información, consulte Actions en la Guía del usuario de AWS Fault Injection Simulator.

- Para obtener información sobre la API, consulte ListActions en la Referencia de comandos de la AWS CLI.

`list-experiment-templates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-experiment-templates`.

AWS CLI

Para enumerar plantillas de experimentos

En el siguiente ejemplo de `list-experiment-templates`, se muestran las plantillas de experimentos de su cuenta de AWS.

```
aws fis list-experiment-templates
```

Salida:

```
{
    "experimentTemplates": [
        {
            "id": "ABCDE1fgHIJkLmNop",
            "description": "myExperimentTemplate",
            "creationTime": 1616017191.124,
            "lastUpdateTime": 1616017191.124,
            "tags": {
                "key": "value"
            }
        }
    ]
}
```

Para obtener más información, consulte Experiment templates en la Guía del usuario de AWS Fault Injection Simulator.

- Para obtener información sobre la API, consulte ListExperimentTemplates en la Referencia de comandos de la AWS CLI.

`list-experiments`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-experiments`.

AWS CLI

Para enumerar experimentos

En el siguiente ejemplo de `list-experiments`, se enumeran los experimentos de su cuenta de AWS.

```
aws fis list-experiments
```

Salida:

```
{
    "experiments": [
        {
            "id": "ABCdeF1GHiJkLM23NO",
            "experimentTemplateId": "ABCDE1fgHIJkLmNop",
            "state": {
                "status": "running",
                "reason": "Experiment is running."
            },
            "creationTime": 1616017341.197,
            "tags": {
            "key": "value"
            }
        }
    ]
}
```

Para obtener más información, consulte Experiments en la Guía del usuario de AWS Fault Injection Simulator.

- Para obtener información sobre la API, consulte ListExperiments en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran las etiquetas para el recurso especificado.

```
aws fis list-tags-for-resource \
```

```
    --resource-arn arn:aws:fis:us-west-2:123456789012:experiment/ABC12DeFGhI3jKLMNOP
```

Salida:

```
{
    "tags": {
        "key1": "value1",
        "key2": "value2"
    }
}
```

Para obtener más información, consulte Tag your AWS FIS resources en la Guía del usuario de AWS Fault Injection Simulator.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`start-experiment`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-experiment`.

AWS CLI

Para iniciar un experimento

En el siguiente ejemplo de `start-experiment`, se inicia el experimento especificado.

```
aws fis start-experiment \
    --experiment-template-id ABCDE1fgHIJkLmNop
```

Salida:

```
{
    "experiment": {
        "id": "ABC12DeFGhI3jKLMNOP",
        "experimentTemplateId": "ABCDE1fgHIJkLmNop",
        "roleArn": "arn:aws:iam::123456789012:role/myRole",
        "state": {
            "status": "initiating",
            "reason": "Experiment is initiating."
        },
```

```
        "targets": {
            "Instances-Target-1": {
                "resourceType": "aws:ec2:instance",
                "resourceArns": [
                    "arn:aws:ec2:us-west-2:123456789012:instance/
i-12a3b4c56d78e9012"
                ],
                "selectionMode": "ALL"
            }
        },
        "actions": {
            "reboot": {
                "actionId": "aws:ec2:reboot-instances",
                "parameters": {},
                "targets": {
                    "Instances": "Instances-Target-1"
                },
                "state": {
                    "status": "pending",
                    "reason": "Initial state"
                }
            }
        },
        "stopConditions": [
            {
                "source": "none"
            }
        ],
        "creationTime": 1616432464.025,
        "startTime": 1616432464.374,
        "tags": {}
    }
}
```

Para obtener más información, consulte Experiments for AWS FIS en la Guía del usuario de AWS Fault Injection Simulator.

- Para obtener información sobre la API, consulte StartExperiment en la Referencia de comandos de AWS CLI.

`stop-experiment`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-experiment`.

AWS CLI

Para detener un experimento

En el siguiente ejemplo de `stop-experiment`, se detiene la ejecución del experimento especificado.

```
aws fis stop-experiment \
    --id ABC12DeFGhI3jKLMNOP
```

Salida:

```
{
    "experiment": {
        "id": "ABC12DeFGhI3jKLMNOP",
        "experimentTemplateId": "ABCDE1fgHIJkLmNop",
        "roleArn": "arn:aws:iam::123456789012:role/myRole",
        "state": {
            "status": "stopping",
            "reason": "Stopping Experiment."
        },
        "targets": {
            "Instances-Target-1": {
                "resourceType": "aws:ec2:instance",
                "resourceArns": [
                    "arn:aws:ec2:us-west-2:123456789012:instance/
i-12a3b4c56d78e9012"
                ],
                "selectionMode": "ALL"
            }
        },
        "actions": {
            "reboot": {
                "actionId": "aws:ec2:reboot-instances",
                "parameters": {},
                "targets": {
                    "Instances": "Instances-Target-1"
                },
                "startAfter": [
                    "wait"
                ],
                "state": {
                    "status": "pending",
```

```
                    "reason": "Initial state."
                }
            },
            "wait": {
                "actionId": "aws:fis:wait",
                "parameters": {
                    "duration": "PT5M"
                },
                "state": {
                    "status": "running",
                    "reason": ""
                }
            }
        },
        "stopConditions": [
            {
                "source": "none"
            }
        ],
        "creationTime": 1616432680.927,
        "startTime": 1616432681.177,
        "tags": {}
    }
}
```

Para obtener más información, consulte Experiments for AWS FIS en la Guía del usuario de AWS Fault Injection Simulator.

- Para obtener información sobre la API, consulte StopExperiment en la Referencia de comandos de AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para etiquetar un recurso

En el siguiente ejemplo de `tag-resource`, se etiqueta el recurso especificado.

```
aws fis tag-resource \
```

```
    --resource-arn arn:aws:fis:us-west-2:123456789012:experiment/ABC12DeFGhI3jKLMNOP
\
    --tags key1=value1,key2=value2
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tag your AWS FIS resources en la Guía del usuario de AWS Fault Injection Simulator.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para retirar la etiqueta de un recurso

En el siguiente ejemplo de `untag-resource`, se eliminan la etiquetas del recurso especificado.

```
aws fis untag-resource \
    --resource-arn arn:aws:fis:us-west-2:123456789012:experiment/ABC12DeFGhI3jKLMNOP
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tag your AWS FIS resources en la Guía del usuario de AWS Fault Injection Simulator.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-experiment-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-experiment-template`.

AWS CLI

Para actualizar una plantilla de experimento

En el siguiente ejemplo de `update-experiment-template`, se actualiza la descripción de la plantilla de experimento especificada.

```
aws fis update-experiment-template \
    --id ABCDE1fgHIJkLmNop \
    ---description myExperimentTemplate
```

Salida:

```
{
    "experimentTemplate": {
        "id": "ABCDE1fgHIJkLmNop",
        "description": "myExperimentTemplate",
        "targets": {
            "Instances-Target-1": {
                "resourceType": "aws:ec2:instance",
                "resourceArns": [
                    "arn:aws:ec2:us-west-2:123456789012:instance/
i-12a3b4c56d78e9012"
                ],
                "selectionMode": "ALL"
            }
        },
        "actions": {
            "testaction": {
                "actionId": "aws:ec2:stop-instances",
                "parameters": {},
                "targets": {
                    "Instances": "Instances-Target-1"
                }
            }
        },
        "stopConditions": [
            {
                "source": "none"
            }
        ],
        "creationTime": 1616017191.124,
        "lastUpdateTime": 1616017859.607,
        "roleArn": "arn:aws:iam::123456789012:role/FISRole",
        "tags": {
            "key": "value"
        }
```

```
    }
}
```

Para obtener más información, consulte Update an experiment template en la Guía del usuario de AWS Fault Injection Simulator.

- Para obtener información sobre la API, consulte UpdateExperimentTemplate en la Referencia de comandos de la AWS CLI.

Ejemplos de servidores de Amazon GameLift que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante AWS Command Line Interface con servidores de Amazon GameLift.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-build`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-build`.

AWS CLI

Ejemplo 1: creación de una compilación de juego a partir de los archivos de un bucket de S3

En el siguiente ejemplo de `create-build`, se crea un nuevo recurso de compilación de juego personalizado. Utiliza archivos comprimidos que se almacenan en una ubicación de S3 en una cuenta de AWS que usted controla. En este ejemplo, se supone que ya ha creado un rol de IAM que concede permiso a Amazon GameLift para acceder a la ubicación de S3. Puesto que la solicitud no especifica un sistema operativo, el nuevo recurso de compilación es WINDOWS_2012 de manera predeterminada.

```
aws gamelift create-build \
    --storage-location file://storage-loc.json \
    --name MegaFrogRaceServer.NA \
    --build-version 12345.678
```

Contenido de `storage-loc.json`:

```
{
    "Bucket":"MegaFrogRaceServer_NA_build_files"
    "Key":"MegaFrogRaceServer_build_123.zip"
    "RoleArn":"arn:aws:iam::123456789012:role/gamelift"
}
```

Salida:

```
{
    "Build": {
        "BuildArn": "arn:aws:gamelift:us-west-2::build/build-a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "BuildId": "build-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "CreationTime": 1496708916.18,
        "Name": "MegaFrogRaceServer.NA",
        "OperatingSystem": "WINDOWS_2012",
        "SizeOnDisk": 479303,
        "Status": "INITIALIZED",
        "Version": "12345.678"
    },
    "StorageLocation": {
        "Bucket": "MegaFrogRaceServer_NA_build_files",
        "Key": "MegaFrogRaceServer_build_123.zip"
    }
}
```

Ejemplo 2: creación de un recurso de compilación de juego para cargar archivos manualmente en GameLift

En el siguiente ejemplo de `create-build`, se crea un nuevo recurso de compilación. También obtiene una ubicación de almacenamiento y credenciales temporales que le permiten cargar manualmente la versión del juego a la ubicación de GameLift en Amazon S3. Una vez que haya cargado correctamente la compilación, el servicio de GameLift la valida y actualiza el estado de la nueva compilación.

```
aws gamelift create-build \
    --name MegaFrogRaceServer.NA \
    --build-version 12345.678 \
    --operating-system AMAZON_LINUX
```

Salida:

```
{
    "Build": {
        "BuildArn": "arn:aws:gamelift:us-west-2::build/build-a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "BuildId": "build-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "CreationTime": 1496708916.18,
        "Name": "MegaFrogRaceServer.NA",
        "OperatingSystem": "AMAZON_LINUX",
        "SizeOnDisk": 0,
        "Status": "INITIALIZED",
        "Version": "12345.678"
    },
    "StorageLocation": {
        "Bucket": "gamelift-builds-us-west-2",
        "Key": "123456789012/build-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    },
    "UploadCredentials": {
        "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
        "SessionToken": "AgoGb3JpZ2luENz...EXAMPLETOKEN=="
    }
}
```

Para obtener más información, consulte Upload a Custom Server Build to GameLift en la Guía para desarrolladores de Amazon GameLift.

- Para obtener más información sobre la API, consulte CreateBuild en la Referencia de comandos de la AWS CLI.

`create-fleet`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-fleet`.

AWS CLI

Ejemplo 1: creación de una flota de Linux básica

En el siguiente ejemplo de `create-fleet`, se crea una flota mínimamente configurada de instancias de Linux bajo demanda para alojar una compilación de servidor personalizada. Puede completar la configuración usando `update-fleet`.

```
aws gamelift create-fleet \
    --name MegaFrogRaceServer.NA.v2 \
    --description 'Hosts for v2 North America' \
    --build-id build-1111aaaa-22bb-33cc-44dd-5555eeee66ff \
    --certificate-configuration 'CertificateType=GENERATED' \
    --ec2-instance-type c4.large \
    --fleet-type ON_DEMAND \
    --runtime-configuration 'ServerProcesses=[{LaunchPath=/local/game/release-na/
MegaFrogRace_Server.exe,ConcurrentExecutions=1}]'
```

Salida:

```
{
    "FleetAttributes": {
        "BuildId": "build-1111aaaa-22bb-33cc-44dd-5555eeee66ff",
        "CertificateConfiguration": {
            "CertificateType": "GENERATED"
        },
        "CreationTime": 1496365885.44,
        "Description": "Hosts for v2 North America",
        "FleetArn": "arn:aws:gamelift:us-west-2:444455556666:fleet/
fleet-2222bbbb-33cc-44dd-55ee-6666ffff77aa",
        "FleetId": "fleet-2222bbbb-33cc-44dd-55ee-6666ffff77aa",
        "FleetType": "ON_DEMAND",
        "InstanceType": "c4.large",
        "MetricGroups": ["default"],
        "Name": "MegaFrogRace.NA.v2",
        "NewGameSessionProtectionPolicy": "NoProtection",
        "OperatingSystem": "AMAZON_LINUX",
        "ServerLaunchPath": "/local/game/release-na/MegaFrogRace_Server.exe",
        "Status": "NEW"
    }
}
```

Ejemplo 2: creación de una flota de Windows básica

En el siguiente ejemplo de `create-fleet`, se crea una flota mínimamente configurada de instancias de Windows de spot para alojar una compilación de servidor personalizada. Puede completar la configuración usando `update-fleet`.

```
aws gamelift create-fleet \
    --name MegaFrogRace.NA.v2 \
    --description 'Hosts for v2 North America' \
    --build-id build-2222aaaa-33bb-44cc-55dd-6666eeee77ff  \
    --certificate-configuration 'CertificateType=GENERATED' \
    --ec2-instance-type c4.large \
    --fleet-type SPOT \
    --runtime-configuration 'ServerProcesses=[{LaunchPath=C:\game
\Bin64.Release.Dedicated\MegaFrogRace_Server.exe,ConcurrentExecutions=1}]'
```

Salida:

```
{
    "FleetAttributes": {
        "BuildId": "build-2222aaaa-33bb-44cc-55dd-6666eeee77ff",
        "CertificateConfiguration": {
            "CertificateType": "GENERATED"
        },
        "CreationTime": 1496365885.44,
        "Description": "Hosts for v2 North America",
        "FleetArn": "arn:aws:gamelift:us-west-2:444455556666:fleet/
fleet-2222bbbb-33cc-44dd-55ee-6666ffff77aa",
        "FleetId": "fleet-2222bbbb-33cc-44dd-55ee-6666ffff77aa",
        "FleetType": "SPOT",
        "InstanceType": "c4.large",
        "MetricGroups": ["default"],
        "Name": "MegaFrogRace.NA.v2",
        "NewGameSessionProtectionPolicy": "NoProtection",
        "OperatingSystem": "WINDOWS_2012",
        "ServerLaunchPath": "C:\game\Bin64.Release.Dedicated
\MegaFrogRace_Server.exe",
        "Status": "NEW"
    }
}
```

Ejemplo 3: creación de una flota completamente configurada

En el siguiente ejemplo de `create-fleet`, se crea una flota de instancias de Windows de spot para una versión de servidor personalizada, con los ajustes de configuración más utilizados.

```
aws gamelift create-fleet \
    --name MegaFrogRace.NA.v2 \
    --description 'Hosts for v2 North America' \
    --build-id build-2222aaaa-33bb-44cc-55dd-6666eeee77ff \
    --certificate-configuration 'CertificateType=GENERATED' \
    --ec2-instance-type c4.large \
    --ec2-inbound-permissions
 'FromPort=33435,ToPort=33435,IpRange=10.24.34.0/23,Protocol=UDP' \
    --fleet-type SPOT \
    --new-game-session-protection-policy FullProtection \
    --runtime-configuration file://runtime-config.json \
    --metric-groups default \
    --instance-role-arn 'arn:aws:iam::444455556666:role/GameLiftS3Access'
```

Contenido de `runtime-config.json`:

```
GameSessionActivationTimeoutSeconds=300,
 MaxConcurrentGameSessionActivations=2,
 ServerProcesses=[
   {LaunchPath=C:\game\Bin64.Release.Dedicated\MegaFrogRace_Server.exe,Parameters=-
debug,ConcurrentExecutions=1},
   {LaunchPath=C:\game\Bin64.Release.Dedicated
\MegaFrogRace_Server.exe,ConcurrentExecutions=1}]
```

Salida:

```
{
    "FleetAttributes": {
        "InstanceRoleArn": "arn:aws:iam::444455556666:role/GameLiftS3Access",
        "Status": "NEW",
        "InstanceType": "c4.large",
        "FleetArn": "arn:aws:gamelift:us-west-2:444455556666:fleet/
fleet-2222bbbb-33cc-44dd-55ee-6666ffff77aa",
        "FleetId": "fleet-2222bbbb-33cc-44dd-55ee-6666ffff77aa",
        "Description": "Hosts for v2 North America",
        "FleetType": "SPOT",
        "OperatingSystem": "WINDOWS_2012",
        "Name": "MegaFrogRace.NA.v2",
        "CreationTime": 1569309011.11,
```

```
        "MetricGroups": [
            "default"
        ],
        "BuildId": "build-2222aaaa-33bb-44cc-55dd-6666eeee77ff",
        "ServerLaunchParameters": "abc",
        "ServerLaunchPath": "C:\\game\\Bin64.Release.Dedicated\
\MegaFrogRace_Server.exe",
        "NewGameSessionProtectionPolicy": "FullProtection",
        "CertificateConfiguration": {
            "CertificateType": "GENERATED"
        }
    }
}
```

Ejemplo 4: creación de una flota de Servidores en tiempo real

En el siguiente ejemplo de `create-fleet`, se crea una flota de instancias de spot con un script de configuración en tiempo real que se ha cargado en Amazon GameLift. Todos los Servidores en tiempo real se implementan en máquinas Linux. Para este ejemplo, supongamos que el script de Realtime cargado incluye varios archivos de script y que la función `Init()` se encuentra en el archivo de script llamado `MainScript.js`. Como se muestra, este archivo se identifica como el script de inicio en la configuración de tiempo de ejecución.

```
aws gamelift create-fleet \
    --name MegaFrogRace.NA.realtime \
    --description 'Mega Frog Race Realtime fleet' \
    --script-id script-1111aaaa-22bb-33cc-44dd-5555eeee66ff \
    --ec2-instance-type c4.large \
    --fleet-type SPOT \
    --certificate-configuration 'CertificateType=GENERATED' --runtime-configuration
 'ServerProcesses=[{LaunchPath=/local/game/MainScript.js,Parameters=+map
 Winter444,ConcurrentExecutions=5}]'
```

Salida:

```
{
    "FleetAttributes": {
        "FleetId": "fleet-2222bbbb-33cc-44dd-55ee-6666ffff77aa",
        "Status": "NEW",
        "CreationTime": 1569310745.212,
        "InstanceType": "c4.large",
        "NewGameSessionProtectionPolicy": "NoProtection",
```

```
        "CertificateConfiguration": {
            "CertificateType": "GENERATED"
        },
        "Name": "MegaFrogRace.NA.realtime",
        "ScriptId": "script-1111aaaa-22bb-33cc-44dd-5555eeee66ff",
        "FleetArn": "arn:aws:gamelift:us-west-2:444455556666:fleet/
fleet-2222bbbb-33cc-44dd-55ee-6666ffff77aa",
        "FleetType": "SPOT",
        "MetricGroups": [
            "default"
        ],
        "Description": "Mega Frog Race Realtime fleet",
        "OperatingSystem": "AMAZON_LINUX"
    }
}
```

- Para obtener información sobre la API, consulte CreateFleet en la Referencia de comandos de la AWS CLI.

`create-game-session-queue`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-game-session-queue`.

AWS CLI

Ejemplo 1: configuración de una cola de sesiones de juego ordenada

En el siguiente ejemplo de `create-game-session-queue`, se crea una nueva cola de sesiones de juego con destinos en dos regiones. También configura la cola para que las sesiones de juego soliciten tiempo de espera después de esperar 10 minutos para ser colocadas. Puesto que no se definen políticas de latencia, GameLift intenta colocar todas las sesiones de juego en el primer destino de la lista.

```
aws gamelift create-game-session-queue \
    --name MegaFrogRaceServer-NA \
    --destinations file://destinations.json \
    --timeout-in-seconds 600
```

Contenido de `destinations.json`:

```
{
```

```
    "Destinations": [
        {"DestinationArn": "arn:aws:gamelift:us-west-2::fleet/fleet-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" },
        {"DestinationArn": "arn:aws:gamelift:us-west-1::fleet/fleet-
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222" }
    ]
}
```

Salida:

```
{
    "GameSessionQueues": [
        {
            "Name": "MegaFrogRaceServer-NA",
            "GameSessionQueueArn": "arn:aws:gamelift:us-
west-2:123456789012:gamesessionqueue/MegaFrogRaceServer-NA",
            "TimeoutInSeconds": 600,
            "Destinations": [
                {"DestinationArn": "arn:aws:gamelift:us-west-2::fleet/fleet-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"},
                {"DestinationArn": "arn:aws:gamelift:us-west-1::fleet/fleet-
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"}
            ]
        }
    ]
}
```

Ejemplo 2: configuración de una cola de sesiones de juego con políticas de latencia de jugadores

En el siguiente ejemplo de `create-game-session-queue`, se crea una nueva cola de sesiones de juego con políticas de latencia para dos jugadores. La primera política establece un límite de latencia de 100 ms que se aplica durante el primer minuto de un intento de ubicación de una sesión de juego. La segunda política aumenta el límite de latencia a 200 ms hasta que se agoten los tiempos de espera de la solicitud de ubicación, que es de 3 minutos.

```
aws gamelift create-game-session-queue \
    --name MegaFrogRaceServer-NA \
    --destinations file://destinations.json \
    --player-latency-policies file://latency-policies.json \
    --timeout-in-seconds 180
```

Contenido de `destinations.json`:

```
{
    "Destinations": [
        { "DestinationArn": "arn:aws:gamelift:us-west-2::fleet/fleet-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" },
        { "DestinationArn": "arn:aws:gamelift:us-east-1::fleet/fleet-
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222" }
    ]
}
```

Contenido de `latency-policies.json`:

```
{
    "PlayerLatencyPolicies": [
        {"MaximumIndividualPlayerLatencyMilliseconds": 200},
        {"MaximumIndividualPlayerLatencyMilliseconds": 100, "PolicyDurationSeconds":
 60}
    ]
}
```

Salida:

```
{
    "GameSessionQueue": {
        "Name": "MegaFrogRaceServer-NA",
        "GameSessionQueueArn": "arn:aws:gamelift:us-
west-2:111122223333:gamesessionqueue/MegaFrogRaceServer-NA",
        "TimeoutInSeconds": 600,
        "PlayerLatencyPolicies": [
            {
                "MaximumIndividualPlayerLatencyMilliseconds": 100,
                "PolicyDurationSeconds": 60
            },
            {
                "MaximumIndividualPlayerLatencyMilliseconds": 200
            }
        ]
        "Destinations": [
            {"DestinationArn": "arn:aws:gamelift:us-west-2::fleet/fleet-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"},
            {"DestinationArn": "arn:aws:gamelift:us-east-1::fleet/fleet-
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"}
        ],
```

```
    }
}
```

Para obtener más información, consulte Create a Queue en la Guía para desarrolladores de Amazon GameLift.

- Para obtener información sobre la API, consulte CreateGameSessionQueue en la Referencia de comandos de la AWS CLI.

`delete-build`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-build`.

AWS CLI

Para eliminar una compilación de juego personalizada

En el siguiente ejemplo de `delete-build`, se elimina una compilación de su cuenta de Amazon GameLift. Una vez eliminada la compilación, no podrá usarla para crear nuevas flotas. Esta operación no se puede deshacer.

```
aws gamelift delete-build \
   --build-id build-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Este comando no genera ninguna salida.

- Para obtener más información sobre la API, consulte DeleteBuild en la Referencia de comandos de la AWS CLI.

`delete-fleet`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-fleet`.

AWS CLI

Para eliminar una flota que ya no está en uso

En el siguiente ejemplo de `delete-fleet`, se elimina una flota que se ha reducido a cero instancias. Si la capacidad de la flota es superior a cero, se produce un error HTTP 400 en la solicitud.

```
aws gamelift delete-fleet \
```

```
    --fleet-id fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Manage GameLift Fleets en la Guía para desarrolladores de Amazon GameLift.

- Para obtener información sobre la API, consulte DeleteFleet en la Referencia de comandos de la AWS CLI.

`delete-game-session-queue`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-game-session-queue`.

AWS CLI

Para eliminar una cola de sesión de juego

En el siguiente ejemplo de `delete-game-session-queue`, se elimina una cola de sesiones de juego especificada.

```
aws gamelift delete-game-session-queue \
    --name MegaFrogRace-NA
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteGameSessionQueue en la Referencia de comandos de la AWS CLI.

`describe-build`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-build`.

AWS CLI

Para obtener información sobre una compilación de juego personalizada

En el siguiente ejemplo de `describe-build`, se recuperan las propiedades de un recurso de compilación de un servidor de juegos.

```
aws gamelift describe-build \
    --build-id build-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "Build": {
        "BuildArn": "arn:aws:gamelift:us-west-2::build/build-a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "BuildId": "build-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "CreationTime": 1496708916.18,
        "Name": "My_Game_Server_Build_One",
        "OperatingSystem": "AMAZON_LINUX",
        "SizeOnDisk": 1304924,
        "Status": "READY",
        "Version": "12345.678"
    }
}
```

Para obtener más información, consulte Upload a Custom Server Build to GameLift en la Guía para desarrolladores de Amazon GameLift.

- Para obtener más información sobre la API, consulte DescribeBuild en la Referencia de comandos de la AWS CLI.

`describe-ec2-instance-limits`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-ec2-instance-limits`.

AWS CLI

Para recuperar los límites de servicio para un tipo de instancia de EC2

En el siguiente ejemplo de `describe-ec2-instance-limits`, se muestran las instancias máximas permitidas y las instancias actuales que se utilizan para el tipo de instancia de EC2 especificado en la región actual. El resultado indica que solo se utilizan cinco de las veinte instancias permitidas.

```
aws gamelift describe-ec2-instance-limits \
    --ec2-instance-type m5.large
```

Salida:

```
{
    "EC2InstanceLimits": [
```

```
        {
            "EC2InstanceType": ""m5.large",
            "CurrentInstances": 5,
            "InstanceLimit": 20
        }
    ]
}
```

Para obtener más información, consulte Choose Computing Resources en la Guía para desarrolladores de Amazon GameLift.

- Para obtener información sobre la API, consulte DescribeEc2InstanceLimits en la Referencia de comandos de la AWS CLI.

`describe-fleet-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fleet-attributes`.

AWS CLI

Ejemplo 1: visualización de los atributos para una lista de flotas

En el siguiente ejemplo de `describe-fleet-attributes`, se recuperan los atributos de flota para dos flotas especificadas. Como se muestra, las flotas solicitadas se implementan con la misma compilación, una para las instancias bajo demanda y otra para las instancias de spot, con algunas pequeñas diferencias de configuración.

```
aws gamelift describe-fleet-attributes \
    --fleet-ids arn:aws:gamelift:us-west-2::fleet/fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

Salida:

```
{
    "FleetAttributes": [
        {
            "FleetId": "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "FleetArn": "arn:aws:gamelift:us-west-2::fleet/fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "FleetType": "ON_DEMAND",
            "InstanceType": "c4.large",
            "Description": "On-demand hosts for v2 North America",
```

```
            "Name": "MegaFrogRaceServer.NA.v2-od",
            "CreationTime": 1568836191.995,
            "Status": "ACTIVE",
            "BuildId": "build-a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "BuildArn": "arn:aws:gamelift:us-west-2::build/build-a1b2c3d4-5678-90ab-
cdef-EXAMPLE33333",
            "ServerLaunchPath": "C:\\game\\MegaFrogRace_Server.exe",
            "ServerLaunchParameters": "+gamelift_start_server",
            "NewGameSessionProtectionPolicy": "NoProtection",
            "OperatingSystem": "WINDOWS_2012",
            "MetricGroups": [
                "default"
            ],
            "CertificateConfiguration": {
                "CertificateType": "DISABLED"
            }
        },
        {
            "FleetId": "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "FleetArn": "arn:aws:gamelift:us-west-2::fleet/fleet-a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222",
            "FleetType": "SPOT",
            "InstanceType": "c4.large",
            "Description": "On-demand hosts for v2 North America",
            "Name": "MegaFrogRaceServer.NA.v2-spot",
            "CreationTime": 1568838275.379,
            "Status": "ACTIVATING",
            "BuildId": "build-a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "BuildArn": "arn:aws:gamelift:us-west-2::build/build-a1b2c3d4-5678-90ab-
cdef-EXAMPLE33333",
            "ServerLaunchPath": "C:\\game\\MegaFrogRace_Server.exe",
            "NewGameSessionProtectionPolicy": "NoProtection",
            "OperatingSystem": "WINDOWS_2012",
                "MetricGroups": [
                "default"
            ],
            "CertificateConfiguration": {
                "CertificateType": "GENERATED"
            }
        }
    ]
}
```

Ejemplo 2: solicitud de atributos para todas las flotas

En el siguiente `describe-fleet-attributes`, se devuelven los atributos de flota de todas las flotas con cualquier estado. En este ejemplo, se muestra el uso de parámetros de paginación para devolver una flota a la vez.

```
aws gamelift describe-fleet-attributes \
    --limit 1
```

Salida:

```
{
    "FleetAttributes": [
        {
            "FleetId": "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "FleetArn": "arn:aws:gamelift:us-west-2::fleet/fleet-a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222",
            "FleetType": "SPOT",
            "InstanceType": "c4.large",
            "Description": "On-demand hosts for v2 North America",
            "Name": "MegaFrogRaceServer.NA.v2-spot",
            "CreationTime": 1568838275.379,
            "Status": "ACTIVATING",
            "BuildId": "build-a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "BuildArn": "arn:aws:gamelift:us-west-2::build/build-a1b2c3d4-5678-90ab-
cdef-EXAMPLE33333",
            "ServerLaunchPath": "C:\\game\\MegaFrogRace_Server.exe",
            "NewGameSessionProtectionPolicy": "NoProtection",
            "OperatingSystem": "WINDOWS_2012",
            "MetricGroups": [
                "default"
            ],
            "CertificateConfiguration": {
                "CertificateType": "GENERATED"
            }
        }
    ],
    "NextToken":
 "eyJhd3NBY2NvdW50SWQiOnsicyI6IjMwMjc3NjAxNjM5OCJ9LCJidWlsZElkIjp7InMiOiJidWlsZC01NWYxZTZmMS
}
```

El resultado incluye un valor de `NextToken` que puede utilizar al llamar al comando por segunda vez. Pase el valor al parámetro `--next-token` para especificar dónde recoger la salida. El siguiente comando devuelve el segundo resultado en la salida:

```
aws gamelift describe-fleet-attributes \
    --limit 1 \
    --next-
token eyJhd3NBY2NvdW50SWQiOnsicyI6IjMwMjc3NjAxNjM5OCJ9LCJidWlsZElkIjp7InMiOiJidWlsZC01NWYxZT
```

Repita el proceso hasta que la respuesta no incluya un valor de `NextToken`.

Para obtener más información, consulte Setting Up GameLift Fleets en la Guía para desarrolladores de Amazon GameLift.

- Para obtener información sobre la API, consulte DescribeFleetAttributes en la Referencia de comandos de la AWS CLI.

`describe-fleet-capacity`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fleet-capacity`.

AWS CLI

Para ver el estado de la capacidad para una lista de flotas

En el siguiente ejemplo de `describe-fleet-capacity`, se recupera la capacidad actual para dos flotas especificadas.

```
aws gamelift describe-fleet-capacity \
    --fleet-ids arn:aws:gamelift:us-west-2::fleet/fleet-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111 fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

Salida:

```
{
    "FleetCapacity": [
        {
            "FleetId": "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "InstanceType": "c5.large",
            "InstanceCounts": {
                "DESIRED": 10,
```

```
                "MINIMUM": 1,
                "MAXIMUM": 20,
                "PENDING": 0,
                "ACTIVE": 10,
                "IDLE": 3,
                "TERMINATING": 0
            }
        },
        {
            "FleetId": "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "InstanceType": "c5.large",
            "InstanceCounts": {
                "DESIRED": 13,
                "MINIMUM": 1,
                "MAXIMUM": 20,
                "PENDING": 0,
                "ACTIVE": 15,
                "IDLE": 2,
                "TERMINATING": 2
            }
        }

    ]
}
```

Para obtener más información, consulte GameLift Metrics for Fleets en la Guía para desarrolladores de Amazon GameLift.

- Para obtener información sobre la API, consulte DescribeFleetCapacity en la Referencia de comandos de la AWS CLI.

`describe-fleet-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fleet-events`.

AWS CLI

Para solicitar eventos durante un período de tiempo específico

En el siguiente ejemplo de `describe-fleet-events`, se muestran los detalles de todos los eventos relacionados con la flota que se produjeron durante el período de tiempo especificado.

```
aws gamelift describe-fleet-events \
```

```
    --fleet-id arn:aws:gamelift:us-west-2::fleet/fleet-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111 \
    --start-time 1579647600 \
    --end-time 1579649400 \
    --limit 5
```

Salida:

```
{
    "Events": [
        {
            "EventId": "a37b6892-5d07-4d3b-8b47-80244ecf66b9",
            "ResourceId": "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "EventCode": "FLEET_STATE_ACTIVE",
            "Message": "Fleet fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 changed
 state to ACTIVE",
            "EventTime": 1579649342.191
        },
        {
            "EventId": "67da4ec9-92a3-4d95-886a-5d6772c24063",
            "ResourceId": "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "EventCode": "FLEET_STATE_ACTIVATING",
            "Message": "Fleet fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 changed
 state to ACTIVATING",
            "EventTime": 1579649321.427
        },
        {
            "EventId": "23813a46-a9e6-4a53-8847-f12e6a8381ac",
            "ResourceId": "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "EventCode": "FLEET_STATE_BUILDING",
            "Message": "Fleet fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 changed
 state to BUILDING",
            "EventTime": 1579649321.243
        },
        {
            "EventId": "3bf217d0-1d44-42f9-9202-433ed475d2e8",
            "ResourceId": "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "EventCode": "FLEET_STATE_VALIDATING",
            "Message": "Fleet fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 changed
 state to VALIDATING",
            "EventTime": 1579649197.449
        },
        {
```

```
            "EventId": "2ecd0130-5986-44eb-99a7-62df27741084",
            "ResourceId": "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "EventCode": "FLEET_VALIDATION_LAUNCH_PATH_NOT_FOUND",
            "Message": "Failed to find a valid path",
            "EventTime": 1569319075.839,
            "PreSignedLogUrl": "https://gamelift-event-logs-prod-
us-west-2.s3.us-west-2.amazonaws.com/logs/fleet-83422059-8329-42a2-
a4d6-c4444386a6f8/events/2ecd0130-5986-44eb-99a7-62df27741084/
FLEET_VALIDATION_LAUNCH_PATH_NOT_FOUND.txt?X-Amz-Security-
Token=IQoJb3JpZ2luX2VjEB8aCXVzLXdlc3QtMiJHMEUCIHV5K%2FLPx8h310D
%2FAvx0%2FZxsDy5XA3cJOwPdu3T0eBa%2FAiEA1yovokcZYy%2FV4CWW6l26aFyiSHO
%2Bxz%2FBMAhEHYHMQNcqkQMImP%2F%2F%2F%2F%2F%2F%2F%2F%2F
%2FARAAGgw3NDEwNjE1OTIxNzEiDI8rsZtzLzlwEDQhXSrlAtl5Ae
%2Fgo6FCIzqXPbXfBOnSvFYqeDlriZarEpKqKrUt8mXQv9iqHResqCph9AKo49lwgSYTT2QoSxnrD7%2FUgv
%2BZm2pVuczvuKtUA0fcx6s0GxpjIAzdIE%2F5P%2FB7B9M%2BVZ
%2F9KF82hbJi0HTE6Y7BjKsEgFCvk4UXILhfjtan9iQl8%2F21ZTurAcJbm7Y5tuLF9SWSK3%2BEa7VXOcCK4D4O1sMj
%2FIaXoHkNvg0RVTa0hIqdvpaDQlsSBNdqTXbjHTu6fETE9Y9Ky%2BiJK5KiUG
%2F59GjCpDcvS1FqKeLUEmKT7wysGmvjMc2n%2Fr
%2F9VxQfte7w9srXwlLAQuwhiXAAyI5ICMZ5JvzjzQwTqD4CHTVKUUDwL
%2BRZzbuuqkJObZml02CkRGp%2B74RTAzLbWptVqZTIfzctiCTmWxb
%2FmKyELRYsVLrwNJ%2BGJ7%2BCrN0RC%2FjlgfLYIZyeAqjPgAu5HjgX
%2BM7jCo9M7wBTrnAXKOFQuf9dvA84SuwXOJFp17LYGjrHMKv0qC3GfbTMrZ6kzeNV9awKCpXB2Gnx9z2KvIlJdqirWV
%2F9C6%2B4jIZPME3jXmZcEHqqw5uvAVF7aeIavtUZU8pxpDIWT0YE4p3Kriy2AA7ziCRKtVfjV839InyLk8LUjsioWK
%2BYUq8%2FDTlLxqj1S%2Fi04TI0Wo7ilAo%2FKKWWF4guuNDexj8EOOynSp1yImB
%2BZf2Fua3O44W4eEXAMPLE33333&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Date=20170621T231808Z&X-Amz-SignedHeaders=host&X-Amz-Expires=900&X-Amz-
Credential=AKIAIOSFODNN7EXAMPLE%2F20170621%2Fus-west-2%2Fs3%2Faws4_request&X-Amz-
Signature=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
        }
    ],
    "NextToken":
 "eyJhd3NBY2NvdW50SWQiOnsicyI6IjMwMjc3NjAxNjM5OCJ9LCJidWlsZElkIjp7InMiOiJidWlsZC01NWYxZTZmMS
}
```


Para obtener más información, consulte Debug GameLift Fleet Issues en la Guía para desarrolladores de Amazon GameLift.

- Para obtener información sobre la API, consulte DescribeFleetEvents en la Referencia de comandos de la AWS CLI.

`describe-fleet-port-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fleet-port-settings`.

AWS CLI

Para ver los permisos de conexión de entrada para una flota

En el siguiente ejemplo de `describe-fleet-port-settings`, se recupera la configuración de conexión para una flota especificada.

```
aws gamelift describe-fleet-port-settings \
    --fleet-id arn:aws:gamelift:us-west-2::fleet/fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "InboundPermissions": [
        {
            "FromPort": 33400,
            "ToPort": 33500,
            "IpRange": "0.0.0.0/0",
            "Protocol": "UDP"
        },
        {
            "FromPort": 1900,
            "ToPort": 2000,
            "IpRange": "0.0.0.0/0",
            "Protocol": "TCP"
        }
    ]
}
```

Para obtener más información, consulte Setting Up GameLift Fleets en la Guía para desarrolladores de Amazon GameLift.

- Para obtener información sobre la API, consulte DescribeFleetPortSettings en la Referencia de comandos de la AWS CLI.

`describe-fleet-utilization`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fleet-utilization`.

AWS CLI

Ejemplo 1: visualización de los datos de uso de una lista de flotas

En el siguiente ejemplo de `describe-fleet-utilization`, se recupera la información de uso actual para una flota especificada.

```
aws gamelift describe-fleet-utilization \
    --fleet-ids arn:aws:gamelift:us-west-2::fleet/fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "FleetUtilization": [
        {
        "FleetId": "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "ActiveServerProcessCount": 100,
        "ActiveGameSessionCount": 62,
        "CurrentPlayerSessionCount": 329,
        "MaximumPlayerSessionCount": 1000
        }
    ]
}
```

Ejemplo 2: solicitud de los datos de uso para todas las flotas

En el siguiente `describe-fleet-utilization`, se devuelven los datos de uso de la flota de todas las flotas con cualquier estado. En este ejemplo, se utilizan parámetros de paginación para devolver datos de dos flotas a la vez.

```
aws gamelift describe-fleet-utilization \
    --limit 2
```

Salida:

```
{
    "FleetUtilization": [
        {
            "FleetId": "fleet-1111aaaa-22bb-33cc-44dd-5555eeee66ff",
            "ActiveServerProcessCount": 100,
```

```
            "ActiveGameSessionCount": 13,
            "CurrentPlayerSessionCount": 98,
            "MaximumPlayerSessionCount": 1000
        },
        {
            "FleetId": "fleet-2222bbbb-33cc-44dd-55ee-6666ffff77aa",
            "ActiveServerProcessCount": 100,
            "ActiveGameSessionCount": 62,
            "CurrentPlayerSessionCount": 329,
            "MaximumPlayerSessionCount": 1000
        }
    ],
    "NextToken":
 "eyJhd3NBY2NvdW50SWQiOnsicyI6IjMwMjc3NjAxNjM5OCJ9LCJidWlsZElkIjp7InMiOiJidWlsZC01NWYxZTZmMS
}
```

Llame al comando por segunda vez y pase el valor de `NextToken` como argumento al parámetro `--next-token` para ver los dos siguientes resultados.

```
aws gamelift describe-fleet-utilization \
    --limit 2 \
    --next-
token eyJhd3NBY2NvdW50SWQiOnsicyI6IjMwMjc3NjAxNjM5OCJ9LCJidWlsZElkIjp7InMiOiJidWlsZC01NWYxZT
```

Repita el proceso hasta que la respuesta deje de incluir un valor `NextToken` en la salida.

Para obtener más información, consulte GameLift Metrics for Fleets en la Guía para desarrolladores de Amazon GameLift.

- Para obtener información sobre la API, consulte DescribeFleetUtilization en la Referencia de comandos de la AWS CLI.

`describe-game-session-queues`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-game-session-queues`.

AWS CLI

Para ver las colas de sesiones de juego

En el siguiente ejemplo de `describe-game-session-queues`, se recuperan las propiedades de dos colas especificadas.

```
aws gamelift describe-game-session-queues \
    --names MegaFrogRace-NA MegaFrogRace-EU
```

Salida:

```
{
    "GameSessionQueues": [{
            "Destinations": [{
                    "DestinationArn": "arn:aws:gamelift:us-west-2::fleet/fleet-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                {
                    "DestinationArn": "arn:aws:gamelift:us-west-2::fleet/fleet-
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
                }
            ],
            "Name": "MegaFrogRace-NA",
            "TimeoutInSeconds": 600,
            "GameSessionQueueArn": "arn:aws:gamelift:us-west-2::gamesessionqueue/
MegaFrogRace-NA",
            "PlayerLatencyPolicies": [{
                    "MaximumIndividualPlayerLatencyMilliseconds": 200
                },
                {
                    "MaximumIndividualPlayerLatencyMilliseconds": 100,
                    "PolicyDurationSeconds": 60
                }
            ],
            "FilterConfiguration": {
                "AllowedLocations": ["us-west-2", "ap-south-1", "us-east-1"]
            },
            "PriorityConfiguration": {
                "PriorityOrder": ["LOCATION", "FLEET_TYPE", "DESTINATION"],
                "LocationOrder": ["us-west-2", "ap-south-1", "us-east-1"]
            }
        },
        {
            "Destinations": [{
                "DestinationArn": "arn:aws:gamelift:eu-west-3::fleet/fleet-
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
            }],
            "Name": "MegaFrogRace-EU",
            "TimeoutInSeconds": 600,
```

```
            "GameSessionQueueArn": "arn:aws:gamelift:us-west-2::gamesessionqueue/
MegaFrogRace-EU"
        }
    ]
}
```

Para obtener más información, consulte Using Multi-Region Queues en la Guía para desarrolladores de Amazon GameLift.

- Para obtener información sobre la API, consulte DescribeGameSessionQueues en la Referencia de comandos de la AWS CLI.

`describe-runtime-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-runtime-configuration`.

AWS CLI

Para solicitar la configuración de tiempo de ejecución para una flota

En el siguiente ejemplo de `describe-runtime-configuration`, se recuperan detalles sobre la configuración actual de tiempo de ejecución para una flota específica.

```
aws gamelift describe-runtime-configuration \
    --fleet-id fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "RuntimeConfiguration": {
        "ServerProcesses": [
            {
                "LaunchPath": "C:\game\Bin64.Release.Dedicated
\MegaFrogRace_Server.exe",
                "Parameters": "+gamelift_start_server",
                "ConcurrentExecutions": 3
            },
            {
                "LaunchPath": "C:\game\Bin64.Release.Dedicated
\MegaFrogRace_Server.exe",
                "Parameters": "+gamelift_start_server +debug",
                "ConcurrentExecutions": 1
```

```
            }
        ],
        "MaxConcurrentGameSessionActivations": 2147483647,
        "GameSessionActivationTimeoutSeconds": 300
    }
}
```

Para obtener más información, consulte Run Multiple Processes on a Fleet en la Guía para desarrolladores de Amazon GameLift.

- Para obtener información sobre la API, consulte DescribeRuntimeConfiguration en la Referencia de comandos de la AWS CLI.

`list-builds`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-builds`.

AWS CLI

Ejemplo 1: obtención de una lista de compilaciones de juegos personalizadas

En el siguiente ejemplo de `list-builds`, se recuperan las propiedades de todas las versiones de servidores de juegos de la región actual. La solicitud de ejemplo muestra cómo utilizar los parámetros de paginación, `Limit` y `NextToken`, para recuperar los resultados en conjuntos secuenciales. El primer comando recupera las dos primeras compilaciones. Como hay más de dos disponibles, la respuesta incluye un `NextToken` para indicar que hay más resultados disponibles.

```
aws gamelift list-builds \
    --limit 2
```

Salida:

```
{
    "Builds": [
        {
            "BuildArn": "arn:aws:gamelift:us-west-2::build/build-a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
            "BuildId": "build-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "CreationTime": 1495664528.723,
            "Name": "My_Game_Server_Build_One",
```

```
            "OperatingSystem": "WINDOWS_2012",
            "SizeOnDisk": 8567781,
            "Status": "READY",
            "Version": "12345.678"
        },
        {
            "BuildArn": "arn:aws:gamelift:us-west-2::build/build-a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222",
            "BuildId": "build-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "CreationTime": 1495528748.555,
            "Name": "My_Game_Server_Build_Two",
            "OperatingSystem": "AMAZON_LINUX_2",
            "SizeOnDisk": 8567781,
            "Status": "FAILED",
            "Version": "23456.789"
        }
    ],
    "NextToken":
 "eyJhd3NBY2NvdW50SWQiOnsicyI6IjMwMjc3NjAxNjM5OCJ9LCJidWlsZElkIjp7InMiOiJidWlsZC01NWYxZTZmMS
}
```

A continuación, puede volver a llamar al comando con el parámetro `--next-token` de la siguiente manera para ver las dos compilaciones siguientes.

```
aws gamelift list-builds \
    --limit 2
    --next-
token eyJhd3NBY2NvdW50SWQiOnsicyI6IjMwMjc3NjAxNjM5OCJ9LCJidWlsZElkIjp7InMiOiJidWlsZC01NWYxZT
```

Repita el proceso hasta que la respuesta no incluya un valor de `NextToken`.

Ejemplo 2: obtención de una lista de compilaciones de juegos personalizadas en estado de error

En el siguiente ejemplo de `list-builds`, se recuperan las propiedades de todas las compilaciones de servidores de juegos de la región actual que actualmente tienen el estado FAILED.

```
aws gamelift list-builds \
    --status FAILED
```

Salida:

```
{
    "Builds": [
        {
            "BuildArn": "arn:aws:gamelift:us-west-2::build/build-a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222",
            "BuildId": "build-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "CreationTime": 1495528748.555,
            "Name": "My_Game_Server_Build_Two",
            "OperatingSystem": "AMAZON_LINUX_2",
            "SizeOnDisk": 8567781,
            "Status": "FAILED",
            "Version": "23456.789"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListBuilds en la Referencia de comandos de la AWS CLI.

`list-fleets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-fleets`.

AWS CLI

Ejemplo 1: obtención de una lista de todas las flotas de una región

En el siguiente ejemplo de `list-fleets`, se muestran los ID de flota de todas las flotas de la región actual. En este ejemplo, se utilizan parámetros de paginación para recuperar dos ID de flota a la vez. La respuesta incluye un atributo `next-token`, que indica que hay más resultados que recuperar.

```
aws gamelift list-fleets \
    --limit 2
```

Salida:

```
{
    "FleetIds": [
        "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
```

```
    ],
    "NextToken":
 "eyJhd3NBY2NvdW50SWQiOnsicyI6IjMwMjc3NjAxNjM5OCJ9LCJidWlsZElkIjp7InMiOiJidWlsZC01NWYxZTZmMS
}
```

Puede pasar el valor `NextToken` de la respuesta anterior al siguiente comando, como se muestra aquí, para obtener los siguientes dos resultados.

```
aws gamelift list-fleets \
    --limit 2 \
    --next-
token eyJhd3NBY2NvdW50SWQiOnsicyI6IjMwMjc3NjAxNjM5OCJ9LCJidWlsZElkIjp7InMiOiJidWlsZC00NDRlZj
```

Ejemplo 2: obtención de una lista de todas las flotas de una región con un script o una compilación específicos

En el siguiente ejemplo de `list-builds`, se recuperan los ID de las flotas que se implementan con la compilación de juego especificada. Si trabaja con Servidores en tiempo real, puede proporcionar un ID de script en lugar de un ID de compilación. Dado que este ejemplo no especifica el parámetro de límite, los resultados pueden incluir hasta 16 ID de flota.

```
aws gamelift list-fleets \
    --build-id build-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "FleetIds": [
        "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
        "fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE44444"
    ]
}
```

- Para obtener información sobre la API, consulte ListFleets en la Referencia de comandos de la AWS CLI.

`request-upload-credentials`

En el siguiente ejemplo de código, se muestra cómo utilizar `request-upload-credentials`.

AWS CLI

Para actualizar las credenciales de acceso para cargar una compilación

En el siguiente ejemplo de `create-build`, se obtienen credenciales de acceso nuevas y válidas para cargar un archivo de compilación de GameLift en una ubicación de Amazon S3. Las credenciales tienen una vida útil limitada. El ID de compilación se obtiene de la respuesta a la solicitud de `CreateBuild` original.

```
aws gamelift request-upload-credentials \
    --build-id build-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "StorageLocation": {
        "Bucket": "gamelift-builds-us-west-2",
        "Key": "123456789012/build-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    },
    "UploadCredentials": {
        "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
        "SessionToken": "AgoGb3JpZ2luENz...EXAMPLETOKEN=="
    }
}
```

Para obtener más información, consulte Upload a Custom Server Build to GameLift en la Guía para desarrolladores de Amazon GameLift.

- Para obtener información sobre la API, consulte RequestUploadCredentials en la Referencia de comandos de la AWS CLI.

`start-fleet-actions`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-fleet-actions`.

AWS CLI

Para reiniciar la actividad de escalado automático de la flota

En el siguiente ejemplo de `start-fleet-actions`, se reanuda el uso de todas las políticas de escalado que se definen para la flota especificada, pero que se detuvieron al llamar a stop-

fleet-actions. Tras empezar, las políticas de escalado comienzan de inmediato a realizar un seguimiento de sus métricas respectivas.

```
aws gamelift start-fleet-actions \
    --fleet-id fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --actions AUTO_SCALING
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte StartFleetActions en la Referencia de comandos de la AWS CLI.

`stop-fleet-actions`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-fleet-actions`.

AWS CLI

Para detener la actividad de escalado automático de una flota

En el siguiente ejemplo de `stop-fleet-actions`, se detiene el uso de todas las políticas de escalado definidas para la flota especificada. Una vez suspendidas las políticas, la capacidad de la flota permanece con el mismo número de instancias activas, a menos que lo ajuste manualmente.

```
aws gamelift start-fleet-actions \
    --fleet-id fleet-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --actions AUTO_SCALING
```

Este comando no genera ninguna salida.

- Para obtener detalles sobre la API, consulte StopFleetActions en la Referencia de comandos de la AWS CLI.

`update-build`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-build`.

AWS CLI

Para actualizar una compilación de juego personalizada

En el siguiente ejemplo de `update-build`, se cambia el nombre y la información de versión asociada a un recurso de compilación especificado. El objeto de compilación devuelto comprueba que los cambios se hayan realizado correctamente.

```
aws gamelift update-build \
    --build-id build-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --name MegaFrogRaceServer.NA.east \
    --build-version 12345.east
```

Salida:

```
{
    "Build": {
        "BuildArn": "arn:aws:gamelift:us-west-2::build/build-a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "BuildId": "build-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "CreationTime": 1496708916.18,
        "Name": "MegaFrogRaceServer.NA.east",
        "OperatingSystem": "AMAZON_LINUX_2",
        "SizeOnDisk": 1304924,
        "Status": "READY",
        "Version": "12345.east"
    }
}
```

Para obtener más información, consulte Update Your Build Files en la Guía para desarrolladores de Amazon GameLift.

- Para obtener información sobre la API, consulte UpdateBuild en la Referencia de comandos de la AWS CLI.

update-game-session-queue

En el siguiente ejemplo de código, se muestra cómo utilizar `update-game-session-queue`.

AWS CLI

Para actualizar una configuración de cola de sesión de juego

En el siguiente ejemplo de `update-game-session-queue`, se agrega un nuevo destino y se actualizan las políticas de latencia de los jugadores para una cola de sesiones de juego existente.

```
aws gamelift update-game-session-queue \
    --name MegaFrogRace-NA \
    --destinations file://destinations.json \
    --player-latency-policies file://latency-policies.json
```

Contenido de `destinations.json`:

```
{
    "Destinations": [
        {"DestinationArn": "arn:aws:gamelift:us-west-2::fleet/
fleet-1a2b3c4d-5e6f-7a8b-9c0d-1e2f3a4b5c6d"},
        {"DestinationArn": "arn:aws:gamelift:us-east-1::fleet/
fleet-5c6d3c4d-5e6f-7a8b-9c0d-1e2f3a4b5a2b"},
        {"DestinationArn": "arn:aws:gamelift:us-east-1::alias/
alias-11aa22bb-3c4d-5e6f-000a-1111aaaa22bb"}
    ]
}
```

Contenido de `latency-policies.json`:

```
{
    "PlayerLatencyPolicies": [
        {"MaximumIndividualPlayerLatencyMilliseconds": 200},
        {"MaximumIndividualPlayerLatencyMilliseconds": 150, "PolicyDurationSeconds":
 120},
        {"MaximumIndividualPlayerLatencyMilliseconds": 100, "PolicyDurationSeconds":
 120}
    ]
}
```

Salida:

```
{
    "GameSessionQueue": {
        "Destinations": [
            {"DestinationArn": "arn:aws:gamelift:us-west-2::fleet/
fleet-1a2b3c4d-5e6f-7a8b-9c0d-1e2f3a4b5c6d"},
            {"DestinationArn": "arn:aws:gamelift:us-east-1::fleet/
fleet-5c6d3c4d-5e6f-7a8b-9c0d-1e2f3a4b5a2b"},
            {"DestinationArn": "arn:aws:gamelift:us-east-1::alias/
alias-11aa22bb-3c4d-5e6f-000a-1111aaaa22bb"}
```

```
        ],
        "GameSessionQueueArn": "arn:aws:gamelift:us-
west-2:111122223333:gamesessionqueue/MegaFrogRace-NA",
        "Name": "MegaFrogRace-NA",
        "TimeoutInSeconds": 600,
        "PlayerLatencyPolicies": [
            {"MaximumIndividualPlayerLatencyMilliseconds": 200},
            {"MaximumIndividualPlayerLatencyMilliseconds": 150,
 "PolicyDurationSeconds": 120},
            {"MaximumIndividualPlayerLatencyMilliseconds": 100,
 "PolicyDurationSeconds": 120}
        ]
    }
}
```

Para obtener más información, consulte Using Multi-Region Queues en la Guía para desarrolladores de Amazon GameLift.

- Para obtener más información sobre la API, consulte UpdateGameSessionQueue en la Referencia de comandos de la AWS CLI.

`upload-build`

En el siguiente ejemplo de código, se muestra cómo utilizar `upload-build`.

AWS CLI

Ejemplo 1: carga de una compilación de servidor de juegos de Linux

En el siguiente ejemplo de `upload-build`, se cargan los archivos de compilación del servidor de juegos de Linux desde un directorio de archivos al servicio GameLift y se crea un recurso de compilación.

```
aws gamelift upload-build \
    --name MegaFrogRaceServer.NA \
    --build-version 2.0.1 \
    --build-root ~/MegaFrogRace_Server/release-na \
    --operating-system AMAZON_LINUX_2
    --server-sdk-version 4.0.2
```

Salida:

```
Uploading ~/MegaFrogRace_Server/release-na:  16.0 KiB / 74.6 KiB (21.45%)
Uploading ~/MegaFrogRace_Server/release-na:  32.0 KiB / 74.6 KiB (42.89%)
Uploading ~/MegaFrogRace_Server/release-na:  48.0 KiB / 74.6 KiB (64.34%)
Uploading ~/MegaFrogRace_Server/release-na:  64.0 KiB / 74.6 KiB (85.79%)
Uploading ~/MegaFrogRace_Server/release-na:  74.6 KiB / 74.6 KiB (100.00%)
Successfully uploaded ~/MegaFrogRace_Server/release-na to AWS GameLift
Build ID: build-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Ejemplo 2: carga de una compilación de servidor de juegos de Windows

En el siguiente ejemplo de `upload-build`, se cargan los archivos de compilación del servidor de juegos de Windows desde un directorio al servicio GameLift y se crea un registro de compilación.

```
aws gamelift upload-build \
    --name MegaFrogRaceServer.NA \
    --build-version 2.0.1 \
    --build-root C:\MegaFrogRace_Server\release-na \
    --operating-system WINDOWS_2012
    --server-sdk-version 4.0.2
```

Salida:

```
Uploading C:\MegaFrogRace_Server\release-na:  16.0 KiB / 74.6 KiB (21.45%)
Uploading C:\MegaFrogRace_Server\release-na:  32.0 KiB / 74.6 KiB (42.89%)
Uploading C:\MegaFrogRace_Server\release-na:  48.0 KiB / 74.6 KiB (64.34%)
Uploading C:\MegaFrogRace_Server\release-na:  64.0 KiB / 74.6 KiB (85.79%)
Uploading C:\MegaFrogRace_Server\release-na:  74.6 KiB / 74.6 KiB (100.00%)
Successfully uploaded C:\MegaFrogRace_Server\release-na to AWS GameLift
Build ID: build-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Para obtener más información, consulte Upload a Custom Server Build to GameLift en la Guía para desarrolladores de Amazon GameLift.

- Para obtener información sobre la API, consulte UploadBuild en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon Glacier que utilizan AWS CLI

En el siguiente ejemplo de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon Glacier.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`abort-multipart-upload`

En el siguiente ejemplo de código, se muestra cómo utilizar `abort-multipart-upload`.

AWS CLI

El siguiente comando elimina una carga multiparte en curso en un almacén llamado `my-vault`:

```
aws glacier abort-multipart-upload --account-id - --vault-name my-vault
 --upload-id 19gaRezEXAMPLES6Ry5YYdqthHOC_kGRCT03L9yetr220UmPtBYKk-
OssZtLqyFu7sY1_lR7vgFuJV6NtcV5zpsJ
```

Este comando no produce ninguna salida. Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso. El comando `aws glacier initiate-multipart-upload` devuelve el ID de carga y también se puede obtener mediante `aws glacier list-multipart-uploads`.

Para obtener más información sobre las cargas de varias partes a Amazon Glacier mediante la CLI de AWS, consulte Uso de Amazon Glacier en la Guía del usuario de la CLI de AWS.

- Para obtener información sobre la API, consulte AbortMultipartUploads en la Referencia de comandos de la AWS CLI.

`abort-vault-lock`

En el siguiente ejemplo de código, se muestra cómo utilizar `abort-vault-lock`.

AWS CLI

Para anular un proceso de bloqueo de almacén en curso

En el siguiente ejemplo de `abort-vault-lock`, se elimina una política de bloqueo de almacenes del almacén especificado y se restablece el estado de bloqueo del almacén que se desbloqueará.

```
aws glacier abort-vault-lock \
    --account-id - \
    --vault-name MyVaultName
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Abort Vault Lock (DELETE lock-policy) en la Guía para desarrolladores de API de Amazon Glacier.

- Para obtener más información sobre la API, consulte AbortVaultLock en la Referencia de comandos de la AWS CLI.

`add-tags-to-vault`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-tags-to-vault`.

AWS CLI

El siguiente comando añade dos etiquetas a un almacén denominado `my-vault`:

```
aws glacier add-tags-to-vault --account-id - --vault-name my-vault --
tags id=1234,date=july2015
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

- Para obtener información sobre la API, consulte AddTagsToVault en la Referencia de comandos de la AWS CLI.

`complete-multipart-upload`

En el siguiente ejemplo de código, se muestra cómo utilizar `complete-multipart-upload`.

AWS CLI

El siguiente comando completa la carga multiparte de un archivo de 3 MiB:

```
aws glacier complete-multipart-upload --archive-size 3145728 --
checksum 9628195fcdbcbbe76cdde456d4646fa7de5f219fb39823836d81f0cc0e18aa67
 --upload-id 19gaRezEXAMPLES6Ry5YYdqthHOC_kGRCT03L9yetr220UmPtBYKk-
OssZtLqyFu7sY1_lR7vgFuJV6NtcV5zpsJ --account-id - --vault-name my-vault
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

El comando `aws glacier initiate-multipart-upload` devuelve el ID de carga y también se puede obtener mediante `aws glacier list-multipart-uploads`. El parámetro checksum toma un hash en árbol SHA-256 del archivo en hexadecimal.

Para obtener más información sobre las cargas de varias partes a Amazon Glacier mediante la CLI de AWS, como las instrucciones sobre el cálculo de un hash en árbol, consulte Uso de Amazon Glacier en la Guía del usuario de la CLI de AWS.

- Para obtener información sobre la API, consulte CompleteMultipartUpload en la Referencia de comandos de la AWS CLI.

`complete-vault-lock`

En el siguiente ejemplo de código, se muestra cómo utilizar `complete-vault-lock`.

AWS CLI

Para completar un proceso de bloqueo de almacén en curso

En el siguiente ejemplo de `complete-vault-lock`, se completa el progreso de bloqueo en curso del almacén especificado y se establece el estado de bloqueo del almacén en `Locked`. Obtiene el valor del parámetro `lock-id` al ejecutar `initiate-lock-process`.

```
aws glacier complete-vault-lock \
    --account-id - \
    --vault-name MyVaultName \
    --lock-id 9QZgEXAMPLEPhvL6xEXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Complete Vault Lock (POST lockId) en la Guía para desarrolladores de la API de Amazon Glacier.

- Para obtener información sobre la API, consulte CompleteVaultLock en la Referencia de comandos de la AWS CLI.

`create-vault`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-vault`.

AWS CLI

El comando siguiente crea un nuevo almacén llamado `my-vault`.

```
aws glacier create-vault --vault-name my-vault --account-id -
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

- Para obtener información sobre la API, consulte CreateVault en la Referencia de comandos de la AWS CLI.

`delete-archive`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-archive`.

AWS CLI

Eliminación de un archivo desde un almacén

En el siguiente ejemplo de `delete-archive` se elimina el archivo especificado de `example_vault`.

```
aws glacier delete-archive \
    --account-id 111122223333  \
    --vault-name example_vault \
    --archive-id Sc0u9ZP8yaWkmh-XGlIvAVprtLhaLCGnNwNl5I5x9HqPIkX5mjc0DrId3Ln-
Gi_k2HzmlIDZUz117KSdVMdMXLuFWi9PJUitxWO73edQ43eTlMWkH0pd9zVSAuV_XXZBVhKhyGhJ7w
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteArchive en la Referencia de comandos de la AWS CLI.

`delete-vault-access-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-vault-access-policy`.

AWS CLI

Para eliminar la política de acceso de un almacén

En el siguiente ejemplo de `delete-vault-access-policy`, se elimina la política de acceso del almacén especificado.

```
aws glacier delete-vault-access-policy \
    --account-id 111122223333 \
    --vault-name example_vault
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteVaultAccessPolicy en la Referencia de comandos de la AWS CLI.

`delete-vault-notifications`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-vault-notifications`.

AWS CLI

Para eliminar las notificaciones de SNS para un almacén

El siguiente ejemplo de `delete-vault-notifications` muestra las notificaciones enviadas por Amazon Simple Notification Service (Amazon SNS) para el almacén especificado.

```
aws glacier delete-vault-notifications \
    --account-id 111122223333 \
    --vault-name example_vault
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteVaultNotifications en la Referencia de comandos de la AWS CLI.

`delete-vault`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-vault`.

AWS CLI

El comando siguiente elimina un almacén llamado `my-vault`.

```
aws glacier delete-vault --vault-name my-vault --account-id -
```

Este comando no produce ninguna salida. Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

- Para obtener información sobre la API, consulte DeleteVault en la Referencia de comandos de la AWS CLI.

`describe-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-job`.

AWS CLI

El siguiente comando recupera información sobre un trabajo de recuperación de inventario en un almacén denominado `my-vault`:

```
aws glacier describe-job --account-id - --vault-name my-
vault --job-id zbxcm3Z_3z5UkoroF7SuZKrxgGoDc3RloGduS7Eg-
RO47Yc6FxsdGBgf_Q2DK5Ejh18CnTS5XW4_XqlNHS61dsO4CnMW
```

Salida:

```
{
    "InventoryRetrievalParameters": {
        "Format": "JSON"
    },
    "VaultARN": "arn:aws:glacier:us-west-2:0123456789012:vaults/my-vault",
    "Completed": false,
    "JobId": "zbxcm3Z_3z5UkoroF7SuZKrxgGoDc3RloGduS7Eg-
RO47Yc6FxsdGBgf_Q2DK5Ejh18CnTS5XW4_XqlNHS61dsO4CnMW",
    "Action": "InventoryRetrieval",
    "CreationDate": "2015-07-17T20:23:41.616Z",
    "StatusCode": "InProgress"
```

```
}
```

El ID del trabajo se encuentra en la salida de `aws glacier initiate-job` y `aws glacier list-jobs`. Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

- Para obtener información sobre la API, consulte DescribeJob en la Referencia de comandos de AWS CLI.

`describe-vault`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-vault`.

AWS CLI

El siguiente comando recupera datos sobre un almacén denominado `my-vault`:

```
aws glacier describe-vault --vault-name my-vault --account-id -
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

- Para obtener información de la API, consulte DescribeVault en la Referencia de comandos de AWS CLI.

`get-data-retrieval-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-data-retrieval-policy`.

AWS CLI

El siguiente comando obtiene la política de recuperación de datos de la cuenta en uso:

```
aws glacier get-data-retrieval-policy --account-id -
```

Salida:

```
{
    "Policy": {
        "Rules": [
```

```
            {
                "BytesPerHour": 10737418240,
                "Strategy": "BytesPerHour"
            }
        ]
    }
}
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

- Para obtener información sobre la API, consulte GetDataRetrievalPolicy en la Referencia de comandos de la AWS CLI.

`get-job-output`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-job-output`.

AWS CLI

El siguiente comando guarda el resultado de un trabajo de inventario de almacén en un archivo del directorio actual denominado `output.json`:

```
aws glacier get-job-output --account-id - --vault-name my-
vault --job-id zbxcm3Z_3z5UkoroF7SuZKrxgGoDc3RloGduS7Eg-
RO47Yc6FxsdGBgf_Q2DK5Ejh18CnTS5XW4_XqlNHS61ds04CnMW output.json
```

El `job-id` está disponible en la salida de `aws glacier list-jobs`. Tenga en cuenta que el nombre de archivo de salida es un argumento posicional que no va precedido de un nombre de opción. Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

Salida:

```
{
    "status": 200,
    "acceptRanges": "bytes",
    "contentType": "application/json"
}
```

`output.json`:

```
{"VaultARN":"arn:aws:glacier:us-west-2:0123456789012:vaults/
my-vault","InventoryDate":"2015-04-07T00:26:18Z","ArchiveList":
[{"ArchiveId":"kKB7ymWJVpPSwhGP6ycSOAekp9ZYe_--zM_mw6k76ZFGEIWQX-
ybtRDvc2VkPSDtfKmQrj0IRQLSGsNuDp-
AJVlu2ccmDSyDUmZwKbwbpAdGATGDiB3hHO0bjbGehXTcApVud_wyDw","ArchiveDescription":"multipart
 upload
 test","CreationDate":"2015-04-06T22:24:34Z","Size":3145728,"SHA256TreeHash":"9628195fcdbcbb
```

- Para obtener información sobre la API, consulte GetJobOutput en la Referencia de comandos de la AWS CLI.

`get-vault-access-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-vault-access-policy`.

AWS CLI

Para recuperar la política de acceso de un almacén

En el siguiente ejemplo de `get-vault-access-policy`, se recupera la política de acceso para el almacén especificado.

```
aws glacier get-vault-access-policy \
    --account-id 111122223333 \
    --vault-name example_vault
```

Salida:

```
{
    "policy": {
        "Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Principal\":{\"AWS\":\"arn:aws:iam::444455556666:root
\"},\"Action\":\"glacier:ListJobs\",\"Resource\":\"arn:aws:glacier:us-
east-1:111122223333:vaults/example_vault\"},{\"Effect\":\"Allow\",\"Principal\":
{\"AWS\":\"arn:aws:iam::444455556666:root\"},\"Action\":\"glacier:UploadArchive\",
\"Resource\":\"arn:aws:glacier:us-east-1:111122223333:vaults/example_vault\"}]}"
    }
}
```

- Para obtener información sobre la API, consulte GetVaultAccessPolicy en la Referencia de comandos de la AWS CLI.

`get-vault-lock`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-vault-lock`.

AWS CLI

Para obtener los detalles de un bloque de almacén

En el siguiente ejemplo de `get-vault-lock`, se recuperan los detalles sobre el almacén especificado.

```
aws glacier get-vault-lock \
    --account-id - \
    --vault-name MyVaultName
```

Salida:

```
{
    "Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":\"Define-vault-
lock\",\"Effect\":\"Deny\",\"Principal\":{\"AWS\":\"arn:aws:iam::999999999999:root
\"},\"Action\":\"glacier:DeleteArchive\",\"Resource\":\"arn:aws:glacier:us-
west-2:99999999999:vaults/MyVaultName\",\"Condition\":{\"NumericLessThanEquals\":
{\"glacier:ArchiveAgeinDays\":\"365\"}}}]}",
    "State": "Locked",
    "CreationDate": "2019-07-29T22:25:28.640Z"
}
```

Para obtener más información, consulte Get Vault Lock (GET lock-policy) en la Guía para desarrolladores de la API de Amazon Glacier.

- Para obtener información sobre la API, consulte GetVaultLock en la Referencia de comandos de la AWS CLI.

`get-vault-notifications`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-vault-notifications`.

AWS CLI

El siguiente comando obtiene una descripción de la configuración de notificaciones de un almacén denominado `my-vault`:

```
aws glacier get-vault-notifications --account-id - --vault-name my-vault
```

Salida:

```
{
    "vaultNotificationConfig": {
        "Events": [
            "InventoryRetrievalCompleted",
            "ArchiveRetrievalCompleted"
        ],
        "SNSTopic": "arn:aws:sns:us-west-2:0123456789012:my-vault"
    }
}
```

Si no se ha configurado ninguna notificación para el almacén, se devuelve un error. Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

- Para obtener información sobre la API, consulte GetVaultNotifications en la Referencia de comandos de la AWS CLI.

`initiate-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `initiate-job`.

AWS CLI

El siguiente comando inicia un trabajo para obtener un inventario del almacén `my-vault`:

```
aws glacier initiate-job --account-id - --vault-name my-vault --job-parameters
 '{"Type": "inventory-retrieval"}'
```

Salida:

```
{
    "location": "/0123456789012/vaults/my-vault/jobs/
zbxcm3Z_3z5UkoroF7SuZKrxgGoDc3RloGduS7Eg-
RO47Yc6FxsdGBgf_Q2DK5Ejh18CnTS5XW4_XqlNHS61dsO4CnMW",
    "jobId": "zbxcm3Z_3z5UkoroF7SuZKrxgGoDc3RloGduS7Eg-
RO47Yc6FxsdGBgf_Q2DK5Ejh18CnTS5XW4_XqlNHS61dsO4CnMW"
```

```
}
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

El siguiente comando inicia un trabajo para recuperar un archivo del almacén `my-vault`:

```
aws glacier initiate-job --account-id - --vault-name my-vault --job-
parameters file://job-archive-retrieval.json
```

`job-archive-retrieval.json` es un archivo JSON de la carpeta local que especifica el tipo de trabajo, el ID del archivo y algunos parámetros opcionales:

```
{
  "Type": "archive-retrieval",
  "ArchiveId": "kKB7ymWJVpPSwhGP6ycSOAekp9ZYe_--zM_mw6k76ZFGEIWQX-
ybtRDvc2VkPSDtfKmQrj0IRQLSGsNuDp-
AJVlu2ccmDSyDUmZwKbwbpAdGATGDiB3hHO0bjbGehXTcApVud_wyDw",
  "Description": "Retrieve archive on 2015-07-17",
  "SNSTopic": "arn:aws:sns:us-west-2:0123456789012:my-topic"
}
```

Los ID de archivo están disponibles en la salida de `aws glacier upload-archive` y `aws glacier get-job-output`.

Salida:

```
{
    "location": "/011685312445/vaults/mwunderl/jobs/l7IL5-
EkXyEY9Ws95fClzIbk2O5uLYaFdAYOi-
azsX_Z8V6NH4yERHzars8wTKYQMX6nBDI9cMNHzyZJO59-8N9aHWav",
    "jobId": "l7IL5-EkXy2O5uLYaFdAYOiEY9Ws95fClzIbk-
azsX_Z8V6NH4yERHzars8wTKYQMX6nBDI9cMNHzyZJO59-8N9aHWav"
}
```

Consulte Initiate Job en la referencia de la API de Amazon Glacier para obtener más información sobre el formato de los parámetros del trabajo.

- Para obtener información sobre la API, consulte InitiateJob en Referencia de comandos de la AWS CLI.

`initiate-multipart-upload`

En el siguiente ejemplo de código, se muestra cómo utilizar `initiate-multipart-upload`.

AWS CLI

El siguiente comando inicia una carga multiparte en un almacén llamado `my-vault` con un tamaño de parte de 1 MiB (1024 x 1024 bytes) por archivo:

```
aws glacier initiate-multipart-upload --account-id - --part-size 1048576 --vault-
name my-vault --archive-description "multipart upload test"
```

El parámetro de descripción del archivo es opcional. Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

Este comando genera un ID de carga si se realiza correctamente. Use el ID de carga al cargar cada parte de su archivo con `aws glacier upload-multipart-part`. Para obtener más información sobre las cargas de varias partes a Amazon Glacier mediante la CLI de AWS, consulte Uso de Amazon Glacier en la Guía del usuario de la CLI de AWS.

- Para obtener información sobre la API, consulte InitiateMultipartUpload en la Referencia de comandos de la AWS CLI.

`initiate-vault-lock`

En el siguiente ejemplo de código, se muestra cómo utilizar `initiate-vault-lock`.

AWS CLI

Para iniciar el proceso de bloqueo de almacenes

En el siguiente ejemplo de `initiate-vault-lock`, se instala una política de bloqueo de almacenes en el almacén especificado y se establece el estado de bloqueo del almacén en `InProgress`. Llame a `complete-vault-lock` en un plazo de 24 horas para completar el proceso con el fin de establecer el estado del bloqueo de almacén en `Locked`.

```
aws glacier initiate-vault-lock \
    --account-id - \
    --vault-name MyVaultName \
    --policy file://vault_lock_policy.json
```

Contenido de `vault_lock_policy.json`:

```
{"Policy":"{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":\"Define-vault-
lock\",\"Effect\":\"Deny\",\"Principal\":{\"AWS\":\"arn:aws:iam::999999999999:root
\"},\"Action\":\"glacier:DeleteArchive\",\"Resource\":\"arn:aws:glacier:us-
west-2:999999999999:vaults/examplevault\",\"Condition\":{\"NumericLessThanEquals\":
{\"glacier:ArchiveAgeinDays\":\"365\"}}}]}"}
```

La salida es el ID de bloqueo de almacén que puede utilizar para completar el proceso de bloqueo de almacenes.

```
{
    "lockId": "9QZgEXAMPLEPhvL6xEXAMPLE"
}
```

Para obtener más información, consulte Initiate Vault Lock (POST lock-policy) en la Guía para desarrolladores de la API de Amazon Glacier.

- Para obtener detalles de la API, consulte InitiateVaultLock en la Referencia de comandos de la AWS CLI.

`list-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-jobs`.

AWS CLI

El siguiente comando muestra los trabajos en curso y los que se han completado recientemente para un almacén denominado `my-vault`:

```
aws glacier list-jobs --account-id - --vault-name my-vault
```

Salida:

```
{
    "JobList": [
        {
            "VaultARN": "arn:aws:glacier:us-west-2:0123456789012:vaults/my-vault",
            "RetrievalByteRange": "0-3145727",
            "SNSTopic": "arn:aws:sns:us-west-2:0123456789012:my-vault",
            "Completed": false,
            "SHA256TreeHash":
 "9628195fcdbcbbe76cdde932d4646fa7de5f219fb39823836d81f0cc0e18aa67",
```

```
            "JobId": "l7IL5-EkXyEY9Ws95fClzIbk2O5uLYaFdAYOi-
azsX_Z8V6NH4yERHzars8wTKYQMX6nBDI9cMNHzyZJO59-8N9aHWav",
            "ArchiveId": "kKB7ymWJVpPSwhGP6ycSOAekp9ZYe_--zM_mw6k76ZFGEIWQX-
ybtRDvc2VkPSDtfKmQrj0IRQLSGsNuDp-
AJVlu2ccmDSyDUmZwKbwbpAdGATGDiB3hHO0bjbGehXTcApVud_wyDw",
            "JobDescription": "Retrieve archive on 2015-07-17",
            "ArchiveSizeInBytes": 3145728,
            "Action": "ArchiveRetrieval",
            "ArchiveSHA256TreeHash":
 "9628195fcdbcbbe76cdde932d4646fa7de5f219fb39823836d81f0cc0e18aa67",
            "CreationDate": "2015-07-17T21:16:13.840Z",
            "StatusCode": "InProgress"
        },
        {
            "InventoryRetrievalParameters": {
                "Format": "JSON"
            },
            "VaultARN": "arn:aws:glacier:us-west-2:0123456789012:vaults/my-vault",
            "Completed": false,
            "JobId": "zbxcm3Z_3z5UkoroF7SuZKrxgGoDc3RloGduS7Eg-
RO47Yc6FxsdGBgf_Q2DK5Ejh18CnTS5XW4_XqlNHS61dsO4CnMW",
            "Action": "InventoryRetrieval",
            "CreationDate": "2015-07-17T20:23:41.616Z",
            "StatusCode": ""InProgress""
        }
    ]
}
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

- Para obtener información sobre la API, consulte ListJobs en la Referencia de comandos de la AWS CLI.

`list-multipart-uploads`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-multipart-uploads`.

AWS CLI

El siguiente comando muestra todas las cargas multiparte en curso para un almacén llamado `my-vault`.

```
aws glacier list-multipart-uploads --account-id - --vault-name my-vault
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

Para obtener más información sobre las cargas de varias partes a Amazon Glacier mediante la CLI de AWS, consulte Uso de Amazon Glacier en la Guía del usuario de la CLI de AWS.

- Para obtener información sobre la API, consulte ListMultipartUploads en la Referencia de comandos de la AWS CLI.

`list-parts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-parts`.

AWS CLI

El siguiente comando muestra las partes cargadas para una carga multiparte a un almacén llamado `my-vault`.

```
aws glacier list-parts --account-id - --vault-name my-vault --upload-id "SYZi7qnL-YGqGwAm8Kn3BLP2ElNCvnB-5961R09CSaPmPwkYGHOqeN_nX3-Vhnd2yF0KfB5FkmbnBU9GubbdrCs8ut-D"
```

Salida:

```
{
    "MultipartUploadId": "SYZi7qnL-
YGqGwAm8Kn3BLP2ElNCvnB-5961R09CSaPmPwkYGHOqeN_nX3-Vhnd2yF0KfB5FkmbnBU9GubbdrCs8ut-
D",
    "Parts": [
        {
            "RangeInBytes": "0-1048575",
            "SHA256TreeHash":
 "e1f2a7cd6e047350f69b9f8cfa60fa606fe2f02802097a9a026360a7edc1f553"
        },
        {
            "RangeInBytes": "1048576-2097151",
            "SHA256TreeHash":
 "43cf3061fb95796aed99a11a6aa3cd8f839eed15e655ab0a597126210636aee6"
        }
```

```
    ],
    "VaultARN": "arn:aws:glacier:us-west-2:0123456789012:vaults/my-vault",
    "CreationDate": "2015-07-18T00:05:23.830Z",
    "PartSizeInBytes": 1048576
}
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

Para obtener más información sobre las cargas de varias partes a Amazon Glacier mediante la CLI de AWS, consulte Uso de Amazon Glacier en la Guía del usuario de la CLI de AWS.

- Para obtener información sobre la API, consulte ListParts en la Referencia de comandos de la AWS CLI.

`list-provisioned-capacity`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-provisioned-capacity`.

AWS CLI

Para recuperar las unidades de capacidad aprovisionadas

En el siguiente ejemplo de `list-provisioned-capacity`, se recuperan detalles de cualquier unidad de capacidad aprovisionada para la cuenta especificada.

```
aws glacier list-provisioned-capacity \
    --account-id 111122223333
```

Salida:

```
{
    "ProvisionedCapacityList": [
        {
            "CapacityId": "HpASAuvfRFiVDbOjMfEIcr8K",
            "ExpirationDate": "2020-03-18T19:59:24.000Z",
            "StartDate": "2020-02-18T19:59:24.912Z"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListProvisionedCapacity en la Referencia de comandos de la AWS CLI.

`list-tags-for-vault`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-vault`.

AWS CLI

El siguiente comando muestra las etiquetas aplicadas a un almacén denominado `my-vault`:

```
aws glacier list-tags-for-vault --account-id - --vault-name my-vault
```

Salida:

```
{
    "Tags": {
        "date": "july2015",
        "id": "1234"
    }
}
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

- Para obtener información sobre la API, consulte ListTagsForVault en la Referencia de comandos de la AWS CLI.

`list-vaults`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-vaults`.

AWS CLI

El siguiente comando muestra los almacenes de la cuenta y región predeterminadas:

```
aws glacier list-vaults --account-id -
```

Salida:

```
{
    "VaultList": [
        {
            "SizeInBytes": 3178496,
            "VaultARN": "arn:aws:glacier:us-west-2:0123456789012:vaults/my-vault",
            "LastInventoryDate": "2015-04-07T00:26:19.028Z",
            "VaultName": "my-vault",
            "NumberOfArchives": 1,
            "CreationDate": "2015-04-06T21:23:45.708Z"
        }
    ]
}
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

- Para obtener información sobre la API, consulte ListVaults en la Referencia de comandos de la AWS CLI.

`purchase-provisioned-capacity`

En el siguiente ejemplo de código, se muestra cómo utilizar `purchase-provisioned-capacity`.

AWS CLI

Para comprar una unidad de capacidad aprovisionada

En el siguiente ejemplo de `purchase-provisioned-capacity`, se compra una unidad de capacidad aprovisionada.

```
aws glacier purchase-provisioned-capacity \
    --account-id 111122223333
```

Salida:

```
{
    "capacityId": "HpASAuvfRFiVDbOjMfEIcr8K"
}
```

- Para obtener información sobre la API, consulte PurchaseProvisionedCapacity en la Referencia de comandos de la AWS CLI.

`remove-tags-from-vault`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-tags-from-vault`.

AWS CLI

El siguiente comando elimina una etiqueta con la clave `date` de un almacén llamado `my-vault`.

```
aws glacier remove-tags-from-vault --account-id - --vault-name my-vault --tag-keys date
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

- Para obtener información sobre la API, consulte RemoveTagsFromVault en la Referencia de comandos de la AWS CLI.

`set-data-retrieval-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-data-retrieval-policy`.

AWS CLI

El siguiente comando configura una política de recuperación de datos para la cuenta en uso:

```
aws glacier set-data-retrieval-policy --account-id - --policy file://data-retrieval-policy.json
```

`data-retrieval-policy.json` es un archivo JSON en la carpeta actual que especifica una política de recuperación de datos:

```
{
  "Rules":[
     {
         "Strategy":"BytesPerHour",
         "BytesPerHour":10737418240
      }
   ]
}
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

El siguiente comando establece la política de recuperación de datos para que `FreeTier` utilice JSON en línea:

```
aws glacier set-data-retrieval-policy --account-id - --policy '{"Rules":
[{"Strategy":"FreeTier"}]}'
```

Consulte Configuración de la política de recuperación de datos en la Referencia de la API de Amazon Glacier para obtener más información sobre el formato de la política.

- Para obtener información sobre la API, consulte SetDataRetrievalPolicy en la Referencia de comandos de la AWS CLI.

`set-vault-access-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-vault-access-policy`.

AWS CLI

Para establecer la política de acceso de un almacén

En el siguiente ejemplo de `set-vault-access-policy`, se asocia una política de permisos al almacén especificado.

```
aws glacier set-vault-access-policy \
    --account-id 111122223333 \
    --vault-name example_vault
    --policy '{"Policy": "{\"Version\":\"2012-10-17\",\"Statement\":
[{\"Effect\":\"Allow\",\"Principal\":{\"AWS\":\"arn:aws:iam::444455556666:root
\"},\"Action\":\"glacier:ListJobs\",\"Resource\":\"arn:aws:glacier:us-
east-1:111122223333:vaults/example_vault\"},{\"Effect\":\"Allow\",\"Principal\":
{\"AWS\":\"arn:aws:iam::444455556666:root\"},\"Action\":\"glacier:UploadArchive\",
\"Resource\":\"arn:aws:glacier:us-east-1:111122223333:vaults/example_vault\"}]}"}'
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte SetVaultAccessPolicy en la Referencia de comandos de la AWS CLI.

`set-vault-notifications`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-vault-notifications`.

AWS CLI

El siguiente comando configura las notificaciones de SNS para un almacén denominado `my-vault`:

```
aws glacier set-vault-notifications --account-id - --vault-name my-vault --vault-notification-config file://notificationconfig.json
```

`notificationconfig.json` es un archivo JSON de la carpeta actual que especifica un tema de SNS y los eventos que se van a publicar:

```
{
  "SNSTopic": "arn:aws:sns:us-west-2:0123456789012:my-vault",
  "Events": ["ArchiveRetrievalCompleted", "InventoryRetrievalCompleted"]
}
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

- Para obtener información sobre la API, consulte SetVaultNotifications en la Referencia de comandos de la AWS CLI.

`upload-archive`

En el siguiente ejemplo de código, se muestra cómo utilizar `upload-archive`.

AWS CLI

El siguiente comando carga un archivo de la carpeta actual denominado `archive.zip` en un almacén denominado `my-vault`:

```
aws glacier upload-archive --account-id - --vault-name my-vault --body archive.zip
```

Salida:

```
{
    "archiveId": "kKB7ymWJVpPSwhGP6ycSOAekp9ZYe_--zM_mw6k76ZFGEIWQX-
ybtRDvc2VkPSDtfKmQrj0IRQLSGsNuDp-
AJVlu2ccmDSyDUmZwKbwbpAdGATGDiB3hHO0bjbGehXTcApVud_wyDw",
```

```
    "checksum": "969fb39823836d81f0cc028195fcdbcbbe76cdde932d4646fa7de5f21e18aa67",
    "location": "/0123456789012/vaults/my-vault/archives/
kKB7ymWJVpPSwhGP6ycSOAekp9ZYe_--zM_mw6k76ZFGEIWQX-ybtRDvc2VkPSDtfKmQrj0IRQLSGsNuDp-
AJVlu2ccmDSyDUmZwKbwbpAdGATGDiB3hHO0bjbGehXTcApVud_wyDw"
}
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

Para recuperar un archivo cargado, inicie un trabajo de recuperación con el comando aws glacier initiate-job.

- Para obtener información sobre la API, consulte UploadArchive en la Referencia de comandos de la AWS CLI.

`upload-multipart-part`

En el siguiente ejemplo de código, se muestra cómo utilizar `upload-multipart-part`.

AWS CLI

El siguiente comando carga la primera parte de 1 MiB (1024 x 1024 bytes) de un archivo:

```
aws glacier upload-multipart-part --body part1 --range 'bytes
 0-1048575/*' --account-id - --vault-name my-vault --upload-
id 19gaRezEXAMPLES6Ry5YYdqthHOC_kGRCT03L9yetr220UmPtBYKk-
OssZtLqyFu7sY1_lR7vgFuJV6NtcV5zpsJ
```

Amazon Glacier requiere un argumento de ID de cuenta al realizar operaciones, pero puede usar un guion para especificar la cuenta en uso.

El parámetro body toma una ruta a un archivo de parte del sistema de archivos local. El parámetro range toma un rango de contenido HTTP que indica los bytes que ocupa la parte en el archivo completado. El comando `aws glacier initiate-multipart-upload` devuelve el ID de carga y también se puede obtener mediante `aws glacier list-multipart-uploads`.

Para obtener más información sobre las cargas de varias partes a Amazon Glacier mediante la CLI de AWS, consulte Uso de Amazon Glacier en la Guía del usuario de la CLI de AWS.

- Para obtener información sobre la API, consulte UploadMultipartPart en Referencia de comandos de la AWS CLI.

Ejemplos de Global Accelerator que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando la AWS Command Line Interface con Global Accelerator.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-custom-routing-endpoints`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-custom-routing-endpoints`.

AWS CLI

Para agregar un punto de conexión de subred de VPC a un grupo de puntos de conexión para un acelerador de enrutamiento personalizado

En el siguiente ejemplo de `add-custom-routing-endpoints`, se agrega un punto de conexión de subred de VPC a un grupo de puntos de conexión para un acelerador de enrutamiento personalizado.

```
aws globalaccelerator add-custom-routing-endpoints \
    --endpoint-group-
arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/0123vxyz/endpoint-group/4321abcd \
    --endpoint-configurations "EndpointId=subnet-1234567890abcdef0"
```

Salida:

```
{
    "EndpointDescriptions": [
```

```
        {
            "EndpointId": "subnet-1234567890abcdef0"
        }
    ],

 "EndpointGroupArn":"arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-
abcd-1234-abcd-1234abcdefgh/listener/0123vxyz/endpoint-group/4321abcd"
}
```

Para obtener más información, consulte Puntos de conexión de subred de Amazon VPC para aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte AddCustomRoutingEndpoints en la Referencia de comandos de la AWS CLI.

`advertise-byoip-cidr`

En el siguiente ejemplo de código, se muestra cómo utilizar `advertise-byoip-cidr`.

AWS CLI

Para anunciar un rango de direcciones

En el siguiente ejemplo de `advertise-byoip-cidr`, se solicita que AWS anuncie un rango de direcciones que haya aprovisionado para usarlo con sus recursos de AWS.

```
aws globalaccelerator advertise-byoip-cidr \
    --cidr 198.51.100.0/24
```

Salida:

```
{
    "ByoipCidr": {
        "Cidr": "198.51.100.0/24",
        "State": "PENDING_ADVERTISING"
    }
}
```

Para obtener más información, consulte Traiga sus propias direcciones IP (BYOIP) en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte AdvertiseByoipCidr en la Referencia de comandos de la AWS CLI.

`allow-custom-routing-traffic`

En el siguiente ejemplo de código, se muestra cómo utilizar `allow-custom-routing-traffic`.

AWS CLI

Para permitir el tráfico a destinos específicos de instancias de Amazon EC2 en una subred de VPC para un acelerador de enrutamiento personalizado

En el siguiente ejemplo de `allow-custom-routing-traffic`, se especifica que se permite el tráfico a determinadas direcciones IP (destino) de instancias de Amazon EC2 y que los puertos de un punto de conexión de subred de VPC en un acelerador de enrutamiento personalizado pueden recibir tráfico.

```
aws globalaccelerator allow-custom-routing-traffic \
    --endpoint-group-
arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/0123vxyz/endpoint-group/ab88888example \
    --endpoint-id subnet-abcd123example \
    --destination-addresses "172.31.200.6" "172.31.200.7" \
    --destination-ports 80 81
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Puntos de conexión de subred de Amazon VPC para aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener detalles sobre la API, consulte AllowCustomRoutingTraffic en la Referencia de comandos de la AWS CLI.

`create-accelerator`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-accelerator`.

AWS CLI

Para crear un acelerador

En el siguiente ejemplo de `create-accelerator`, se crea un acelerador con dos etiquetas con dos direcciones IP estáticas de BYOIP. Debe especificar la región `US-West-2 (Oregon)` para crear o actualizar un acelerador.

```
aws globalaccelerator create-accelerator \
    --name ExampleAccelerator \
    --tags Key="Name",Value="Example Name" Key="Project",Value="Example Project" \
    --ip-addresses 192.0.2.250 198.51.100.52
```

Salida:

```
{
    "Accelerator": {
        "AcceleratorArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh",
        "IpAddressType": "IPV4",
        "Name": "ExampleAccelerator",
        "Enabled": true,
        "Status": "IN_PROGRESS",
        "IpSets": [
            {
                "IpAddresses": [
                    "192.0.2.250",
                    "198.51.100.52"
                ],
                "IpFamily": "IPv4"
            }
        ],
        "DnsName":"a1234567890abcdef.awsglobalaccelerator.com",
        "CreatedTime": 1542394847.0,
        "LastModifiedTime": 1542394847.0
    }
}
```

Para obtener más información, consulte Aceleradores estándar de AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte CreateAccelerator en la Referencia de comandos de la AWS CLI.

`create-custom-routing-accelerator`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-custom-routing-accelerator`.

AWS CLI

Para crear un acelerador de enrutamiento personalizado

En el siguiente ejemplo de `create-custom-routing-accelerator`, se crea un acelerador de enrutamiento personalizado con las etiquetas `Name` y `Project`.

```
aws globalaccelerator create-custom-routing-accelerator \
    --name ExampleCustomRoutingAccelerator \
    --tags Key="Name",Value="Example Name" Key="Project",Value="Example Project" \
    --ip-addresses 192.0.2.250 198.51.100.52
```

Salida:

```
{
    "Accelerator": {
        "AcceleratorArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh",
        "IpAddressType": "IPV4",
        "Name": "ExampleCustomRoutingAccelerator",
        "Enabled": true,
        "Status": "IN_PROGRESS",
        "IpSets": [
            {
                "IpAddresses": [
                    "192.0.2.250",
                    "198.51.100.52"
                ],
                "IpFamily": "IPv4"
            }
        ],
        "DnsName":"a1234567890abcdef.awsglobalaccelerator.com",
        "CreatedTime": 1542394847.0,
        "LastModifiedTime": 1542394847.0
    }
}
```

Para obtener más información, consulte Aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte CreateCustomRoutingAccelerator en la Referencia de comandos de la AWS CLI.

`create-custom-routing-endpoint-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-custom-routing-endpoint-group`.

AWS CLI

Para crear un grupo de puntos de conexión para un acelerador de enrutamiento personalizado

En el siguiente ejemplo de `create-custom-routing-endpoint-group`, se crea un grupo de puntos de conexión para un acelerador de enrutamiento personalizado.

```
aws globalaccelerator create-custom-routing-endpoint-group \
    --listener-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123vxyz \
    --endpoint-group-region us-east-2 \
    --destination-configurations "FromPort=80,ToPort=81,Protocols=TCP,UDP"
```

Salida:

```
{
    "EndpointGroup": {
        "EndpointGroupArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123vxyz/endpoint-group/4321abcd",
        "EndpointGroupRegion": "us-east-2",
        "DestinationDescriptions": [
            {
                "FromPort": 80,
                "ToPort": 81,
                "Protocols": [
                    "TCP",
                    "UDP"
                ]
            }
        ],
```

```
        "EndpointDescriptions": []
    }
}
```

Para obtener más información, consulte Grupos de puntos de conexión para aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte CreateCustomRoutingEndpointGroup en la Referencia de comandos de la AWS CLI.

`create-custom-routing-listener`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-custom-routing-listener`.

AWS CLI

Para crear un oyente para un acelerador de enrutamiento personalizado

En el siguiente ejemplo de `create-custom-routing-listener`, se crea un oyente con un rango de puertos de entre 5000 y 10 000 para un acelerador de enrutamiento personalizado.

```
aws globalaccelerator create-custom-routing-listener \
    --accelerator-arn arn:aws:globalaccelerator::123456789012:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh \
    --port-ranges FromPort=5000,ToPort=10000
```

Salida:

```
{
    "Listener": {
        "PortRange": [
            "FromPort": 5000,
            "ToPort": 10000
        ],
        "ListenerArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123vxyz"
    }
}
```

Para obtener más información, consulte Oyentes para aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte CreateCustomRoutingListener en la Referencia de comandos de la AWS CLI.

`create-endpoint-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-endpoint-group`.

AWS CLI

Para crear un grupo de puntos de conexión

En el siguiente ejemplo de `create-endpoint-group` se crea un grupo de puntos de conexión con un punto de conexión.

```
aws globalaccelerator create-endpoint-group \
    --listener-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123vxyz \
    --endpoint-group-region us-east-1 \
    --endpoint-configurations EndpointId=i-1234567890abcdef0,Weight=128
```

Salida:

```
{
    "EndpointGroup": {
        "TrafficDialPercentage": 100.0,
        "EndpointDescriptions": [
            {
                "Weight": 128,
                "EndpointId": "i-1234567890abcdef0"
            }
        ],
        "EndpointGroupArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123vxyz/endpoint-group/098765zyxwvu",
        "EndpointGroupRegion": "us-east-1"
    }
}
```

Para obtener más información, consulte Grupos de puntos de conexión en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte CreateEndpointGroup en la Referencia de comandos de la AWS CLI.

`create-listener`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-listener`.

AWS CLI

Para crear un oyente

En el siguiente ejemplo de `create-listener`, se crea un oyente con dos puertos.

```
aws globalaccelerator create-listener \
    --accelerator-arn arn:aws:globalaccelerator::123456789012:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh \
    --port-ranges FromPort=80,ToPort=80 FromPort=81,ToPort=81 \
    --protocol TCP
```

Salida:

```
{
    "Listener": {
        "PortRanges": [
            {
                "ToPort": 80,
                "FromPort": 80
            },
            {
                "ToPort": 81,
                "FromPort": 81
            }
        ],
        "ClientAffinity": "NONE",
        "Protocol": "TCP",
        "ListenerArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123vxyz"
    }
```

```
}
```

Para obtener más información, consulte Oyentes para aceleradores estándar en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte CreateListener en la Referencia de comandos de la AWS CLI.

`deny-custom-routing-traffic`

En el siguiente ejemplo de código, se muestra cómo utilizar `deny-custom-routing-traffic`.

AWS CLI

Para especificar una dirección de destino que no pueda recibir tráfico en un acelerador de enrutamiento personalizado

En el siguiente ejemplo de `deny-custom-routing-traffic`, se especifican las direcciones de destino de un punto de conexión de subred que no pueden recibir tráfico para un acelerador de enrutamiento personalizado. Para especificar más de una dirección de destino, separe las direcciones con un espacio. No hay respuesta para una llamada a deny-custom-routing-traffic correcta.

```
aws globalaccelerator deny-custom-routing-traffic \
    --endpoint-group-
arn "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/0123vxyz/endpoint-group/ab88888example" \
    --endpoint-id "subnet-abcd123example" \
    --destination-addresses "198.51.100.52"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Puntos de conexión de subred de Amazon VPC para aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte DenyCustomRoutingTraffic en la Referencia de comandos de la AWS CLI.

`deprovision-byoip-cidr`

En el siguiente ejemplo de código, se muestra cómo utilizar `deprovision-byoip-cidr`.

AWS CLI

Para desaprovisionar un rango de direcciones

En el siguiente ejemplo de `deprovision-byoip-cidr`, se publica el rango de direcciones especificado que ha aprovisionado para usarlo con sus recursos de AWS.

```
aws globalaccelerator deprovision-byoip-cidr \
    --cidr "198.51.100.0/24"
```

Salida:

```
{
    "ByoipCidr": {
        "Cidr": "198.51.100.0/24",
        "State": "PENDING_DEPROVISIONING"
    }
}
```

Para obtener más información, consulte Traiga sus propias direcciones IP (BYOIP) en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte DeprovisionByoipCidr en la Referencia de comandos de la AWS CLI.

`describe-accelerator-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-accelerator-attributes`.

AWS CLI

Para describir los atributos de un acelerador

En el siguiente ejemplo de `describe-accelerator-attributes`, se recuperan los detalles de atributos para un acelerador.

```
aws globalaccelerator describe-accelerator-attributes \
```

```
    --accelerator-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh
```

Salida:

```
{
    "AcceleratorAttributes": {
        "FlowLogsEnabled": true
        "FlowLogsS3Bucket": flowlogs-abc
        "FlowLogsS3Prefix": bucketprefix-abc
    }
}
```

Para obtener más información, consulte Aceleradores estándar de AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte DescribeAcceleratorAttributes en la Referencia de comandos de la AWS CLI.

`describe-accelerator`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-accelerator`.

AWS CLI

Para describir un acelerador

En el siguiente ejemplo de `describe-accelerator` se recuperan los detalles sobre el acelerador especificado.

```
aws globalaccelerator describe-accelerator \
    --accelerator-arn arn:aws:globalaccelerator::123456789012:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh
```

Salida:

```
{
    "Accelerator": {
        "AcceleratorArn":
 "arn:aws:globalaccelerator::123456789012:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh",
```

```
        "IpAddressType": "IPV4",
        "Name": "ExampleAccelerator",
        "Enabled": true,
        "Status": "IN_PROGRESS",
        "IpSets": [
            {
                "IpAddresses": [
                    "192.0.2.250",
                    "198.51.100.52"
                ],
                "IpFamily": "IPv4"
            }
        ],
        "DnsName":"a1234567890abcdef.awsglobalaccelerator.com",
        "CreatedTime": 1542394847,
        "LastModifiedTime": 1542395013
    }
}
```

Para obtener más información, consulte Aceleradores estándar de AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte DescribeAccelerator en la Referencia de comandos de la AWS CLI.

`describe-custom-routing-accelerator-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-custom-routing-accelerator-attributes`.

AWS CLI

Para describir los atributos de un acelerador de enrutamiento personalizado

En el siguiente ejemplo de `describe-custom-routing-accelerator-attributes`, se describen los atributos de un acelerador de enrutamiento personalizado.

```
aws globalaccelerator describe-custom-routing-accelerator-attributes \
   --accelerator-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh
```

Salida:

```
{
    "AcceleratorAttributes": {
    "FlowLogsEnabled": false
    }
}
```

Para obtener más información, consulte Aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte DescribeCustomRoutingAcceleratorAttributes en la Referencia de comandos de la AWS CLI.

`describe-custom-routing-accelerator`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-custom-routing-accelerator`.

AWS CLI

Para describir un acelerador de enrutamiento personalizado

En el siguiente ejemplo de `describe-custom-routing-accelerator`, se recuperan los detalles sobre el acelerador de enrutamiento personalizado especificado.

```
aws globalaccelerator describe-custom-routing-accelerator \
    --accelerator-arn arn:aws:globalaccelerator::123456789012:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh
```

Salida:

```
{
    "Accelerator": {
        "AcceleratorArn":
 "arn:aws:globalaccelerator::123456789012:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh",
        "IpAddressType": "IPV4",
        "Name": "ExampleCustomRoutingAccelerator",
        "Enabled": true,
        "Status": "IN_PROGRESS",
        "IpSets": [
            {
                "IpAddresses": [
```

```
                    "192.0.2.250",
                    "198.51.100.52"
                ],
                "IpFamily": "IPv4"
            }
        ],
        "DnsName":"a1234567890abcdef.awsglobalaccelerator.com",
        "CreatedTime": 1542394847,
        "LastModifiedTime": 1542395013
    }
}
```

Para obtener más información, consulte Aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte DescribeCustomRoutingAccelerator en la Referencia de comandos de la AWS CLI.

`describe-custom-routing-endpoint-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-custom-routing-endpoint-group`.

AWS CLI

Para describir un grupo de puntos de conexión para un acelerador de enrutamiento personalizado

En el siguiente ejemplo de `describe-custom-routing-endpoint-group`, se describe un grupo de puntos de conexión para un acelerador de enrutamiento personalizado.

```
aws globalaccelerator describe-custom-routing-endpoint-group \
    --endpoint-group-
arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/6789vxyz/endpoint-group/ab88888example
```

Salida:

```
{
    "EndpointGroup": {
        "EndpointGroupArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/6789vxyz/endpoint-group/ab88888example",
```

```
        "EndpointGroupRegion": "us-east-2",
        "DestinationDescriptions": [
            {
                "FromPort": 5000,
                "ToPort": 10000,
                "Protocols": [
                    "UDP"
                ]
            }
        ],
        "EndpointDescriptions": [
            {
                "EndpointId": "subnet-1234567890abcdef0"
            }
        ]
    }
}
```

Para obtener más información, consulte Grupos de puntos de conexión para aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte DescribeCustomRoutingEndpointGroup en la Referencia de comandos de la AWS CLI.

`describe-custom-routing-listener`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-custom-routing-listener`.

AWS CLI

Para describir un oyente para un acelerador de enrutamiento personalizado

En el siguiente ejemplo de `describe-custom-routing-listener`, se describe un oyente para un acelerador de enrutamiento personalizado.

```
aws globalaccelerator describe-custom-routing-listener \
    --listener-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/abcdef1234
```

Salida:

```
{
    "Listener": {
        "PortRanges": [
            "FromPort": 5000,
            "ToPort": 10000
        ],
        "ListenerArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/abcdef1234"
    }
}
```

Para obtener más información, consulte Oyentes para aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte DescribeCustomRoutingListener en la Referencia de comandos de la AWS CLI.

`describe-endpoint-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-endpoint-group`.

AWS CLI

Para describir un grupo de puntos de conexión

En el siguiente ejemplo de `describe-endpoint-group`, se recuperan detalles sobre un grupo de puntos de conexión con los siguientes puntos de conexión: una instancia de Amazon EC2, un ALB y un NLB.

```
aws globalaccelerator describe-endpoint-group \
    --endpoint-group-
arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/6789vxyz-vxyz-6789-vxyz-6789lmnopqrs/endpoint-group/
ab88888example
```

Salida:

```
{
    "EndpointGroup": {
        "TrafficDialPercentage": 100.0,
```

```
        "EndpointDescriptions": [
        {
            "Weight": 128,
            "EndpointId": "i-1234567890abcdef0"
        },
        {
            "Weight": 128,
            "EndpointId": "arn:aws:elasticloadbalancing:us-
east-1:000123456789:loadbalancer/app/ALBTesting/alb01234567890xyz"
        },
        {
            "Weight": 128,
            "EndpointId": "arn:aws:elasticloadbalancing:us-
east-1:000123456789:loadbalancer/net/NLBTesting/alb01234567890qrs"
        }
        ],
        "EndpointGroupArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/6789vxyz-vxyz-6789-vxyz-6789lmnopqrs/endpoint-
group/4321abcd-abcd-4321-abcd-4321abcdefg",
        "EndpointGroupRegion": "us-east-1"
    }
}
```

Para obtener más información, consulte Grupos de puntos de conexión en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte DescribeEndpointGroup en la Referencia de comandos de la AWS CLI.

`describe-listener`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-listener`.

AWS CLI

Para describir un oyente

En el siguiente ejemplo de `describe-listener`, se describe un oyente:

```
aws globalaccelerator describe-listener \
    --listener-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-
abcd-1234-abcd-1234abcdefgh/listener/abcdef1234
```

Salida:

```
{
    "Listener": {
        "ListenerArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/abcdef1234",
        "PortRanges": [
            {
                "FromPort": 80,
                "ToPort": 80
            }
        ],
        "Protocol": "TCP",
        "ClientAffinity": "NONE"
    }
}
```

Para obtener más información, consulte Oyentes para aceleradores estándar en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte DescribeListener en la Referencia de comandos de la AWS CLI.

`list-accelerators`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-accelerators`.

AWS CLI

Para describir de los aceleradores

En el siguiente ejemplo de `list-accelerators`, se muestran los aceleradores en su cuenta de AWS. Esta cuenta tiene dos aceleradores.

```
aws globalaccelerator list-accelerators
```

Salida:

```
{
    "Accelerators": [
        {
```

```
            "AcceleratorArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/5555abcd-abcd-5555-
abcd-5555EXAMPLE1",
            "Name": "TestAccelerator",
            "IpAddressType": "IPV4",
            "Enabled": true,
            "IpSets": [
                {
                    "IpFamily": "IPv4",
                    "IpAddresses": [
                        "192.0.2.250",
                        "198.51.100.52"
                    ]
                }
            ],
            "DnsName": "5a5a5a5a5a5a5a5a.awsglobalaccelerator.com",
            "Status": "DEPLOYED",
            "CreatedTime": 1552424416.0,
            "LastModifiedTime": 1569375641.0
        },
        {
            "AcceleratorArn":
 "arn:aws:globalaccelerator::888888888888:accelerator/8888abcd-abcd-8888-
abcd-8888EXAMPLE2",
            "Name": "ExampleAccelerator",
            "IpAddressType": "IPV4",
            "Enabled": true,
            "IpSets": [
                {
                    "IpFamily": "IPv4",
                    "IpAddresses": [
                        "192.0.2.100",
                        "198.51.100.10"
                    ]
                }
            ],
            "DnsName": "6a6a6a6a6a6a6a6a.awsglobalaccelerator.com",
            "Status": "DEPLOYED",
            "CreatedTime": 1575585564.0,
            "LastModifiedTime": 1579809243.0
        },
    ]
}
```

Para obtener más información, consulte Aceleradores estándar de AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte ListAccelerators en la Referencia de comandos de la AWS CLI.

`list-byoip-cidr`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-byoip-cidr`.

AWS CLI

Para enumerar los rangos de direcciones

En el siguiente ejemplo de `list-byoip-cidr`, se enumeran los rangos de direcciones IP (BYOIP) que ha aprovisionado para su uso con Global Accelerator.

```
aws globalaccelerator list-byoip-cidrs
```

Salida:

```
{
    "ByoipCidrs": [
        {
            "Cidr": "198.51.100.0/24",
            "State": "READY"
        }
        {
            "Cidr": "203.0.113.25/24",
            "State": "READY"
        }
    ]
}
```

Para obtener más información, consulte Traiga sus propias direcciones IP (BYOIP) en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte ListByoipCidr en la Referencia de comandos de la AWS CLI.

`list-custom-routing-accelerators`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-custom-routing-accelerators`.

AWS CLI

Para enumerar sus aceleradores de enrutamiento personalizados

En el siguiente ejemplo de `list-custom-routing-accelerators`, se muestran los aceleradores de enrutamiento personalizados en su cuenta de AWS.

```
aws globalaccelerator list-custom-routing-accelerators
```

Salida:

```
{
    "Accelerators": [
        {
            "AcceleratorArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/5555abcd-abcd-5555-
abcd-5555EXAMPLE1",
            "Name": "TestCustomRoutingAccelerator",
            "IpAddressType": "IPV4",
            "Enabled": true,
            "IpSets": [
                {
                    "IpFamily": "IPv4",
                    "IpAddresses": [
                        "192.0.2.250",
                        "198.51.100.52"
                    ]
                }
            ],
            "DnsName": "5a5a5a5a5a5a5a5a.awsglobalaccelerator.com",
            "Status": "DEPLOYED",
            "CreatedTime": 1552424416.0,
            "LastModifiedTime": 1569375641.0
        },
        {
            "AcceleratorArn":
 "arn:aws:globalaccelerator::888888888888:accelerator/8888abcd-abcd-8888-
abcd-8888EXAMPLE2",
```

```
            "Name": "ExampleCustomRoutingAccelerator",
            "IpAddressType": "IPV4",
            "Enabled": true,
            "IpSets": [
                {
                    "IpFamily": "IPv4",
                    "IpAddresses": [
                        "192.0.2.100",
                        "198.51.100.10"
                    ]
                }
            ],
            "DnsName": "6a6a6a6a6a6a6a.awsglobalaccelerator.com",
            "Status": "DEPLOYED",
            "CreatedTime": 1575585564.0,
            "LastModifiedTime": 1579809243.0
        },
    ]
}
```

Para obtener más información, consulte Aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte ListCustomRoutingAccelerators en la Referencia de comandos de la AWS CLI.

`list-custom-routing-endpoint-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-custom-routing-endpoint-groups`.

AWS CLI

Para enumerar los grupos de puntos de conexión para un oyente de un acelerador de enrutamiento personalizado

En el siguiente ejemplo de `list-custom-routing-endpoint-groups`, se muestran los grupos de puntos de conexión para un oyente en acelerador de enrutamiento personalizado.

```
aws globalaccelerator list-custom-routing-endpoint-groups \
    --listener-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/abcdef1234
```

Salida:

```
{
    "EndpointGroups": [
        {
            "EndpointGroupArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/abcdef1234/endpoint-group/ab88888example",
            "EndpointGroupRegion": "eu-central-1",
            "DestinationDescriptions": [
                {
                    "FromPort": 80,
                    "ToPort": 80,
                    "Protocols": [
                        "TCP",
                        "UDP"
                    ]
                }
            ]
            "EndpointDescriptions": [
                {
                    "EndpointId": "subnet-abcd123example"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Grupos de puntos de conexión para aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte ListCustomRoutingEndpointGroups en la Referencia de comandos de la AWS CLI.

`list-custom-routing-listeners`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-custom-routing-listeners`.

AWS CLI

Para enumerar los oyentes de los aceleradores de enrutamiento personalizados

En el siguiente ejemplo de `list-custom-routing-listeners`, se enumeran los oyentes para un acelerador de enrutamiento personalizado.

```
aws globalaccelerator list-custom-routing-listeners \
    --accelerator-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh
```

Salida:

```
{
    "Listeners": [
        {
            "ListenerArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/abcdef1234",
            "PortRanges": [
                {
                    "FromPort": 5000,
                    "ToPort": 10000
                }
            ],
            "Protocol": "TCP"
        }
    ]
}
```

Para obtener más información, consulte Oyentes para aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte ListCustomRoutingListeners en la Referencia de comandos de la AWS CLI.

`list-custom-routing-port-mappings-by-destination`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-custom-routing-port-mappings-by-destination`.

AWS CLI

Para enumerar una lista de las asignaciones de puertos para un destino de acelerador de enrutamiento personalizado

En el siguiente ejemplo de `list-custom-routing-port-mappings-by-destination`, se proporcionan las asignaciones de puertos para un servidor EC2 de destino específico (en la dirección de destino) para un acelerador de enrutamiento personalizado.

```
aws globalaccelerator list-custom-routing-port-mappings-by-destination \
    --endpoint-id subnet-abcd123example \
    --destination-address 198.51.100.52
```

Salida:

```
{
    "DestinationPortMappings": [
        {
            "AcceleratorArn":
 "arn:aws:globalaccelerator::402092451327:accelerator/24ea29b8-
d750-4489-8919-3095f3c4b0a7",
                "AcceleratorSocketAddresses": [
                    {
                        "IpAddress": "192.0.2.250",
                        "Port": 65514
                    },
                    {
                        "IpAddress": "192.10.100.99",
                        "Port": 65514
                    }
                ],
                "EndpointGroupArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/0123vxyz/endpoint-group/ab88888example",
                "EndpointId": "subnet-abcd123example",
                "EndpointGroupRegion": "us-west-2",
                "DestinationSocketAddress": {
                    "IpAddress": "198.51.100.52",
                    "Port": 80
                },
                "IpAddressType": "IPv4",
                "DestinationTrafficState": "ALLOW"
        }
    ]
}
```

Para obtener más información, consulte Cómo funcionan los aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte ListCustomRoutingPortMappingsByDestination en la Referencia de comandos de la AWS CLI.

`list-custom-routing-port-mappings`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-custom-routing-port-mappings`.

AWS CLI

Para enumerar las asignaciones de puertos en un acelerador de enrutamiento personalizado

En el siguiente ejemplo de `list-custom-routing-port-mappings`, se proporciona una lista parcial de las asignaciones de puertos en un acelerador de enrutamiento personalizado.

```
aws globalaccelerator list-custom-routing-port-mappings \
    --accelerator-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh
```

Salida:

```
{
    "PortMappings": [
        {
            "AcceleratorPort": 40480,
            "EndpointGroupArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123vxyz/endpoint-group/098765zyxwvu",
            "EndpointId": "subnet-1234567890abcdef0",
            "DestinationSocketAddress": {
                "IpAddress": "192.0.2.250",
                "Port": 80
            },
            "Protocols": [
                "TCP",
                "UDP"
            ],
            "DestinationTrafficState": "ALLOW"
```

```
        }
        {
            "AcceleratorPort": 40481,
            "EndpointGroupArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/0123vxyz/endpoint-group/098765zyxwvu",
            "EndpointId": "subnet-1234567890abcdef0",
            "DestinationSocketAddress": {
               "IpAddress": "192.0.2.251",
              "Port": 80
            },
            "Protocols": [
                "TCP",
                "UDP"
            ],
            "DestinationTrafficState": "ALLOW"
        }
    ]
}
```

Para obtener más información, consulte Cómo funcionan los aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte ListCustomRoutingPortMappings en la Referencia de comandos de la AWS CLI.

`list-endpoint-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-endpoint-groups`.

AWS CLI

Para enumerar grupos de puntos de conexión

En el siguiente ejemplo de `list-endpoint-groups`, se muestran los grupos de puntos de conexión para un oyente. Este oyente tiene dos grupos de puntos de conexión.

```
aws globalaccelerator --region us-west-2 list-endpoint-groups \
    --listener-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-
abcd-1234-abcd-1234abcdefgh/listener/abcdef1234
```

Salida:

```
{
    "EndpointGroups": [
        {
            "EndpointGroupArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/abcdef1234/endpoint-group/ab88888example",
            "EndpointGroupRegion": "eu-central-1",
            "EndpointDescriptions": [],
            "TrafficDialPercentage": 100.0,
            "HealthCheckPort": 80,
            "HealthCheckProtocol": "TCP",
            "HealthCheckIntervalSeconds": 30,
            "ThresholdCount": 3
        }
        {
            "EndpointGroupArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/abcdef1234/endpoint-group/ab99999example",
            "EndpointGroupRegion": "us-east-1",
            "EndpointDescriptions": [],
            "TrafficDialPercentage": 50.0,
            "HealthCheckPort": 80,
            "HealthCheckProtocol": "TCP",
            "HealthCheckIntervalSeconds": 30,
            "ThresholdCount": 3
        }
    ]
}
```

Para obtener más información, consulte Grupos de puntos de conexión en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte ListEndpointGroups en la Referencia de comandos de la AWS CLI.

`list-listeners`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-listeners`.

AWS CLI

Para enumerar los oyentes

En el siguiente ejemplo de `list-listeners`, se enumeran los oyentes para un acelerador.

```
aws globalaccelerator list-listeners \
    --accelerator-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh
```

Salida:

```
{
    "Listeners": [
        {
            "ListenerArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/abcdef1234",
            "PortRanges": [
                {
                    "FromPort": 80,
                    "ToPort": 80
                }
            ],
            "Protocol": "TCP",
            "ClientAffinity": "NONE"
        }
    ]
}
```

Para obtener más información, consulte Oyentes para aceleradores estándar en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte ListListeners en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un acelerador

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran las etiquetas para un acelerador específico.

```
aws globalaccelerator list-tags-for-resource \
    --accelerator-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh
```

Salida:

```
{
    "Tags": [
        {
            "Key": "Project",
            "Value": "A123456"
        }
    ]
}
```

Para obtener más información, consulte Etiquetado en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`provision-byoip-cidr`

En el siguiente ejemplo de código, se muestra cómo utilizar `provision-byoip-cidr`.

AWS CLI

Para aprovisionar un rango de direcciones

En el siguiente ejemplo de `provision-byoip-cidr`, se aprovisiona el rango de direcciones especificado para usarlo con los recursos de AWS.

```
aws globalaccelerator provision-byoip-cidr \
    --cidr 192.0.2.250/24 \
    --cidr-authorization-context Message="$text_message",Signature="$signed_message"
```

Salida:

```
{
    "ByoipCidr": {
        "Cidr": "192.0.2.250/24",
        "State": "PENDING_PROVISIONING"
    }
}
```

Para obtener más información, consulte Traiga sus propias direcciones IP (BYOIP) en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre de la API, consulte ProvisionByoipCidr en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para etiquetar un acelerador

En el siguiente ejemplo de `tag-resource`, se agregan las etiquetas Name y Project a un acelerador, junto con los valores correspondientes a cada una de ellas.

```
aws globalaccelerator tag-resource \
    --resource-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh \
    --tags Key="Name",Value="Example Name" Key="Project",Value="Example Project"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar una etiqueta de un acelerador

En el siguiente ejemplo de `untag-resource`, se eliminan las etiquetas Name y Project de un acelerador.

```
aws globalaccelerator untag-resource \
    --resource-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh \
    --tag-keys Key="Name" Key="Project"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-accelerator-attributes

En el siguiente ejemplo de código, se muestra cómo utilizar `update-accelerator-attributes`.

AWS CLI

Para actualizar los atributos de un acelerador

En el siguiente ejemplo de `update-accelerator-attributes`, se actualiza un acelerador para habilitar los registros de flujo. Debe especificar la región `US-West-2 (Oregon)` para crear o actualizar los atributos del acelerador.

```
aws globalaccelerator update-accelerator-attributes \
    --accelerator-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh \
    --flow-logs-enabled \
    --flow-logs-s3-bucket flowlogs-abc \
    --flow-logs-s3-prefix bucketprefix-abc
```

Salida:

```
{
```

```
    "AcceleratorAttributes": {
        "FlowLogsEnabled": true
        "FlowLogsS3Bucket": flowlogs-abc
        "FlowLogsS3Prefix": bucketprefix-abc
    }
}
```

Para obtener más información, consulte Aceleradores estándar de AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte UpdateAcceleratorAttributes en la Referencia de comandos de la AWS CLI.

`update-accelerator`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-accelerator`.

AWS CLI

Para actualizar un acelerador

En el siguiente ejemplo de `update-accelerator`, se modifica un acelerador para cambiarle el nombre a `ExampleAcceleratorNew`. Debe especificar la región `US-West-2 (Oregon)` para crear o actualizar los aceleradores.

```
aws globalaccelerator update-accelerator \
    --accelerator-arn arn:aws:globalaccelerator::123456789012:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh \
    --name ExampleAcceleratorNew
```

Salida:

```
{
    "Accelerator": {
        "AcceleratorArn":
 "arn:aws:globalaccelerator::123456789012:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh",
        "IpAddressType": "IPV4",
        "Name": "ExampleAcceleratorNew",
        "Enabled": true,
        "Status": "IN_PROGRESS",
        "IpSets": [
```

```
            {
                "IpAddresses": [
                    "192.0.2.250",
                    "198.51.100.52"
                ],
                "IpFamily": "IPv4"
            }
        ],
        "DnsName":"a1234567890abcdef.awsglobalaccelerator.com",
        "CreatedTime": 1232394847,
        "LastModifiedTime": 1232395654
    }
}
```

Para obtener más información, consulte Aceleradores estándar de AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte UpdateAccelerator en la Referencia de comandos de la AWS CLI.

`update-custom-routing-accelerator-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-custom-routing-accelerator-attributes`.

AWS CLI

Para actualizar los atributos de un acelerador de enrutamiento personalizado

En el siguiente ejemplo de `update-custom-routing-accelerator-attributes`, se actualiza un acelerador de enrutamiento personalizado para habilitar los registros de flujo.

```
aws globalaccelerator update-custom-routing-accelerator-attributes \
    --accelerator-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh \
    --flow-logs-enabled \
    --flow-logs-s3-bucket flowlogs-abc \
    --flow-logs-s3-prefix bucketprefix-abc
```

Salida:

```
{
```

```
    "AcceleratorAttributes": {
        "FlowLogsEnabled": true
        "FlowLogsS3Bucket": flowlogs-abc
        "FlowLogsS3Prefix": bucketprefix-abc
    }
}
```

Para obtener más información, consulte Aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre de la API, consulte UpdateCustomRoutingAcceleratorAttributes en la Referencia de comandos de la AWS CLI.

`update-custom-routing-accelerator`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-custom-routing-accelerator`.

AWS CLI

Para actualizar un acelerador de enrutamiento personalizado

En el siguiente ejemplo de `update-custom-routing-accelerator`, se modifica un acelerador de enrutamiento personalizado para cambiarle el nombre.

```
aws globalaccelerator --region us-west-2 update-custom-routing-accelerator \
    --accelerator-arn arn:aws:globalaccelerator::123456789012:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh \
    --name ExampleCustomRoutingAcceleratorNew
```

Salida:

```
{
    "Accelerator": {
        "AcceleratorArn":
 "arn:aws:globalaccelerator::123456789012:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh",
        "IpAddressType": "IPV4",
        "Name": "ExampleCustomRoutingAcceleratorNew",
        "Enabled": true,
        "Status": "IN_PROGRESS",
        "IpSets": [
```

```
            {
                "IpAddresses": [
                    "192.0.2.250",
                    "198.51.100.52"
                ],
                "IpFamily": "IPv4"
            }
        ],
        "DnsName":"a1234567890abcdef.awsglobalaccelerator.com",
        "CreatedTime": 1232394847,
        "LastModifiedTime": 1232395654
    }
}
```

Para obtener más información, consulte Aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte UpdateCustomRoutingAccelerator en la Referencia de comandos de la AWS CLI.

`update-custom-routing-listener`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-custom-routing-listener`.

AWS CLI

Para actualizar un oyente de un acelerador de enrutamiento personalizado

En el siguiente ejemplo de `update-custom-routing-listener`, se actualiza un oyente para cambiar el rango de puertos.

```
aws globalaccelerator update-custom-routing-listener \
    --listener-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123vxyz \
    --port-ranges FromPort=10000,ToPort=20000
```

Salida:

```
{
    "Listener": {
        "ListenerArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123vxyz
```

```
        "PortRanges": [
            {
                "FromPort": 10000,
                "ToPort": 20000
            }
        ],
        "Protocol": "TCP"
    }
}
```

Para obtener más información, consulte Oyentes para aceleradores de enrutamiento personalizados en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte UpdateCustomRoutingListener en la Referencia de comandos de la AWS CLI.

`update-endpoint-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-endpoint-group`.

AWS CLI

Para actualizar un grupo de puntos de conexión

En el siguiente ejemplo de `update-endpoint-group`, se agregan tres puntos de conexión a un grupo de puntos de conexión: una dirección IP elástica, un ALB y un NLB.

```
aws globalaccelerator update-endpoint-group \
    --endpoint-group-
arn arn:aws:globalaccelerator::123456789012:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/6789vxyz-vxyz-6789-vxyz-6789lmnopqrs/endpoint-group/
ab88888example \
    --endpoint-configurations \
        EndpointId=eipalloc-eip01234567890abc,Weight=128 \
        EndpointId=arn:aws:elasticloadbalancing:us-east-1:000123456789:loadbalancer/
app/ALBTesting/alb01234567890xyz,Weight=128 \
        EndpointId=arn:aws:elasticloadbalancing:us-east-1:000123456789:loadbalancer/
net/NLBTesting/alb01234567890qrs,Weight=128
```

Salida:

```
{
    "EndpointGroup": {
        "TrafficDialPercentage": 100,
        "EndpointDescriptions": [
            {
                "Weight": 128,
                "EndpointId": "eip01234567890abc"
            },
            {
                "Weight": 128,
                "EndpointId": "arn:aws:elasticloadbalancing:us-
east-1:000123456789:loadbalancer/app/ALBTesting/alb01234567890xyz"
            },
            {
                "Weight": 128,
                "EndpointId": "arn:aws:elasticloadbalancing:us-
east-1:000123456789:loadbalancer/net/NLBTesting/alb01234567890qrs"
            }
        ],
        "EndpointGroupArn":
 "arn:aws:globalaccelerator::123456789012:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh/listener/6789vxyz-vxyz-6789-vxyz-6789lmnopqrs/endpoint-
group/4321abcd-abcd-4321-abcd-4321abcdefg",
        "EndpointGroupRegion": "us-east-1"
    }
}
```

Para obtener más información, consulte Grupos de puntos de conexión en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte UpdateEndpointGroup en la Referencia de comandos de la AWS CLI.

`update-listener`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-listener`.

AWS CLI

Para actualizar un oyente

En el siguiente ejemplo de `update-listener`, se actualiza un oyente para cambiar el puerto a 100.

```
aws globalaccelerator update-listener \
    --listener-arn arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123vxyz \
    --port-ranges FromPort=100,ToPort=100
```

Salida:

```
{
    "Listener": {
        "ListenerArn":
 "arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123vxyz
        "PortRanges": [
            {
                "FromPort": 100,
                "ToPort": 100
            }
        ],
        "Protocol": "TCP",
        "ClientAffinity": "NONE"
    }
}
```

Para obtener más información, consulte Oyentes para aceleradores estándar en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte UpdateListener en la Referencia de comandos de la AWS CLI.

`withdraw-byoip-cidr`

En el siguiente ejemplo de código, se muestra cómo utilizar `withdraw-byoip-cidr`.

AWS CLI

Para retirar un rango de direcciones

En el siguiente ejemplo de `withdraw-byoip-cidr`, se retira un rango de direcciones de AWS Global Accelerator que ha anunciado anteriormente para usarlo con los recursos de AWS.

```
aws globalaccelerator withdraw-byoip-cidr \
```

```
    --cidr 192.0.2.250/24
```

Salida:

```
{
    "ByoipCidr": {
        "Cidr": "192.0.2.250/24",
        "State": "PENDING_WITHDRAWING"
    }
}
```

Para obtener más información, consulte Traiga sus propias direcciones IP (BYOIP) en AWS Global Accelerator en la Guía para desarrolladores de AWS Global Accelerator.

- Para obtener información sobre la API, consulte WithdrawByoipCidr en la Referencia de comandos de la AWS CLI.

AWS Glue Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS Glue.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`batch-stop-job-run`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-stop-job-run`.

AWS CLI

Para detener las ejecuciones de trabajos

En el siguiente ejemplo de `batch-stop-job-run`, se detienen las ejecuciones de un trabajo.

```
aws glue batch-stop-job-run \
    --job-name "my-testing-job" \
    --job-run-id jr_852f1de1f29fb62e0ba4166c33970803935d87f14f96cfdee5089d5274a61d3f
```

Salida:

```
{
    "SuccessfulSubmissions": [
        {
            "JobName": "my-testing-job",
            "JobRunId":
 "jr_852f1de1f29fb62e0ba4166c33970803935d87f14f96cfdee5089d5274a61d3f"
        }
    ],
    "Errors": [],
    "ResponseMetadata": {
        "RequestId": "66bd6b90-01db-44ab-95b9-6aeff0e73d88",
        "HTTPStatusCode": 200,
        "HTTPHeaders": {
            "date": "Fri, 16 Oct 2020 20:54:51 GMT",
            "content-type": "application/x-amz-json-1.1",
            "content-length": "148",
            "connection": "keep-alive",
            "x-amzn-requestid": "66bd6b90-01db-44ab-95b9-6aeff0e73d88"
        },
        "RetryAttempts": 0
    }
}
```

Para obtener más información, consulte Ejecuciones de trabajo en la Guía para desarrolladores de AWS Glue.

- Para obtener más información sobre la API, consulte BatchStopJobRun en la Referencia de comandos de la AWS CLI.

`create-connection`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-connection`.

AWS CLI

Para crear una conexión para los almacenes de datos de AWS Glue

En el siguiente ejemplo de `create-connection`, se crea una conexión en el catálogo de datos de AWS Glue que proporciona información de conexión para un almacén de datos de Kafka.

```
aws glue create-connection \
    --connection-input '{ \
        "Name":"conn-kafka-custom", \
        "Description":"kafka connection with ssl to custom kafka", \
        "ConnectionType":"KAFKA",  \
        "ConnectionProperties":{  \
            "KAFKA_BOOTSTRAP_SERVERS":"<Kafka-broker-server-url>:<SSL-Port>", \
            "KAFKA_SSL_ENABLED":"true", \
            "KAFKA_CUSTOM_CERT": "s3://bucket/prefix/cert-file.pem" \
        }, \
        "PhysicalConnectionRequirements":{ \
            "SubnetId":"subnet-1234", \
            "SecurityGroupIdList":["sg-1234"], \
            "AvailabilityZone":"us-east-1a"} \
    }' \
    --region us-east-1
    --endpoint https://glue.us-east-1.amazonaws.com
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Defining Connections in the AWS Glue Data Catalog en la Guía del desarrollador de AWS Glue.

- Para obtener más información sobre la API, consulte CreateConnection en la Referencia de comandos de la AWS CLI.

`create-database`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-database`.

AWS CLI

Para crear una base de datos

En el siguiente ejemplo de `create-database`, se crea una base de datos en el catálogo de datos de AWS Glue.

```
aws glue create-database \
    --database-input "{\"Name\":\"tempdb\"}" \
    --profile my_profile \
    --endpoint https://glue.us-east-1.amazonaws.com
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Definición de una base de datos en su Catálogo de datos en la Guía para desarrolladores de AWS Glue.

- Para obtener información sobre la API, consulte CreateDatabase en la Referencia de comandos de la AWS CLI.

`create-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-job`.

AWS CLI

Creación de un trabajo a fin de transformar datos

El siguiente ejemplo de `create-job` crea un trabajo de streaming que ejecuta un script almacenado en S3.

```
aws glue create-job \
    --name my-testing-job \
    --role AWSGlueServiceRoleDefault \
    --command '{ \
        "Name": "gluestreaming", \
        "ScriptLocation": "s3://amzn-s3-demo-bucket/folder/" \
    }' \
    --region us-east-1 \
    --output json \
    --default-arguments '{ \
        "--job-language":"scala", \
        "--class":"GlueApp" \
    }' \
    --profile my-profile \
    --endpoint https://glue.us-east-1.amazonaws.com
```

Contenido de `test_script.scala`:

```
import com.amazonaws.services.glue.ChoiceOption
import com.amazonaws.services.glue.GlueContext
import com.amazonaws.services.glue.MappingSpec
import com.amazonaws.services.glue.ResolveSpec
import com.amazonaws.services.glue.errors.CallSite
import com.amazonaws.services.glue.util.GlueArgParser
import com.amazonaws.services.glue.util.Job
import com.amazonaws.services.glue.util.JsonOptions
import org.apache.spark.SparkContext
import scala.collection.JavaConverters._

object GlueApp {
    def main(sysArgs: Array[String]) {
        val spark: SparkContext = new SparkContext()
        val glueContext: GlueContext = new GlueContext(spark)
        // @params: [JOB_NAME]
        val args = GlueArgParser.getResolvedOptions(sysArgs,
 Seq("JOB_NAME").toArray)
        Job.init(args("JOB_NAME"), glueContext, args.asJava)
        // @type: DataSource
        // @args: [database = "tempdb", table_name = "s3-source", transformation_ctx
 = "datasource0"]
        // @return: datasource0
        // @inputs: []
        val datasource0 = glueContext.getCatalogSource(database = "tempdb",
 tableName = "s3-source", redshiftTmpDir = "", transformationContext =
 "datasource0").getDynamicFrame()
        // @type: ApplyMapping
        // @args: [mapping = [("sensorid", "int", "sensorid", "int"),
 ("currenttemperature", "int", "currenttemperature", "int"), ("status", "string",
 "status", "string")], transformation_ctx = "applymapping1"]
        // @return: applymapping1
        // @inputs: [frame = datasource0]
        val applymapping1 = datasource0.applyMapping(mappings = Seq(("sensorid",
 "int", "sensorid", "int"), ("currenttemperature", "int", "currenttemperature",
 "int"), ("status", "string", "status", "string")), caseSensitive = false,
 transformationContext = "applymapping1")
        // @type: SelectFields
        // @args: [paths = ["sensorid", "currenttemperature", "status"],
 transformation_ctx = "selectfields2"]
        // @return: selectfields2
        // @inputs: [frame = applymapping1]
```

```
        val selectfields2 = applymapping1.selectFields(paths = Seq("sensorid",
 "currenttemperature", "status"), transformationContext = "selectfields2")
        // @type: ResolveChoice
        // @args: [choice = "MATCH_CATALOG", database = "tempdb", table_name = "my-
s3-sink", transformation_ctx = "resolvechoice3"]
        // @return: resolvechoice3
        // @inputs: [frame = selectfields2]
        val resolvechoice3 = selectfields2.resolveChoice(choiceOption =
 Some(ChoiceOption("MATCH_CATALOG")), database = Some("tempdb"), tableName =
 Some("my-s3-sink"), transformationContext = "resolvechoice3")
        // @type: DataSink
        // @args: [database = "tempdb", table_name = "my-s3-sink",
 transformation_ctx = "datasink4"]
        // @return: datasink4
        // @inputs: [frame = resolvechoice3]
        val datasink4 = glueContext.getCatalogSink(database = "tempdb",
 tableName = "my-s3-sink", redshiftTmpDir = "", transformationContext =
 "datasink4").writeDynamicFrame(resolvechoice3)
        Job.commit()
    }
}
```

Salida:

```
{
    "Name": "my-testing-job"
}
```

Para obtener más información, consulte Creación de trabajos en AWS Glue en la Guía para desarrolladores de AWS Glue.

- Para obtener más información sobre la API, consulte CreateJob en la Referencia de comandos de la AWS CLI.

`create-table`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-table`.

AWS CLI

Ejemplo 1: creación de una tabla para un flujo de datos de Kinesis

En el siguiente ejemplo de `create-table`, se crea una tabla en el catálogo de datos de AWS Glue que describe un flujo de datos de Kinesis.

```
aws glue create-table \
    --database-name tempdb \
    --table-input  '{"Name":"test-kinesis-input", "StorageDescriptor":{ \
            "Columns":[ \
                {"Name":"sensorid", "Type":"int"}, \
                {"Name":"currenttemperature", "Type":"int"}, \
                {"Name":"status", "Type":"string"} \
            ], \
            "Location":"my-testing-stream", \
            "Parameters":{ \
                "typeOfData":"kinesis","streamName":"my-testing-stream", \
                "kinesisUrl":"https://kinesis.us-east-1.amazonaws.com" \
            }, \
            "SerdeInfo":{ \
                "SerializationLibrary":"org.openx.data.jsonserde.JsonSerDe"} \
        }, \
        "Parameters":{ \
            "classification":"json"} \
        }' \
    --profile my-profile \
    --endpoint https://glue.us-east-1.amazonaws.com
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Definición de tablas en el Catálogo de datos de AWS Glue en la Guía para desarrolladores de AWS Glue.

Ejemplo 2: creación de una tabla para un almacén de datos de Kafka

En el siguiente ejemplo de `create-table`, se crea una tabla en el catálogo de datos de AWS Glue que describe un almacén de datos de Kafka.

```
aws glue create-table \
    --database-name tempdb \
    --table-input  '{"Name":"test-kafka-input", "StorageDescriptor":{ \
            "Columns":[ \
                {"Name":"sensorid", "Type":"int"}, \
                {"Name":"currenttemperature", "Type":"int"}, \
                {"Name":"status", "Type":"string"}
```

```
            ], \
            "Location":"glue-topic", \
            "Parameters":{ \
                "typeOfData":"kafka","topicName":"glue-topic", \
                "connectionName":"my-kafka-connection"
            }, \
            "SerdeInfo":{ \
                "SerializationLibrary":"org.apache.hadoop.hive.serde2.OpenCSVSerde"}
 \
        }, \
        "Parameters":{ \
            "separatorChar":","} \
        }' \
    --profile my-profile \
    --endpoint https://glue.us-east-1.amazonaws.com
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Definición de tablas en el Catálogo de datos de AWS Glue en la Guía para desarrolladores de AWS Glue.

Ejemplo 3: creación de una tabla para un almacén de datos de AWS S3

En el siguiente ejemplo de `create-table`, se crea una tabla en el catálogo de datos de AWS Glue que describe un almacén de datos de AWS Simple Storage Service (AWS S3).

```
aws glue create-table \
    --database-name tempdb \
    --table-input  '{"Name":"s3-output", "StorageDescriptor":{ \
            "Columns":[ \
                {"Name":"s1", "Type":"string"}, \
                {"Name":"s2", "Type":"int"}, \
                {"Name":"s3", "Type":"string"}
            ], \
            "Location":"s3://bucket-path/", \
            "SerdeInfo":{ \
                "SerializationLibrary":"org.openx.data.jsonserde.JsonSerDe"} \
        }, \
        "Parameters":{ \
            "classification":"json"} \
        }' \
    --profile my-profile \
    --endpoint https://glue.us-east-1.amazonaws.com
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Definición de tablas en el Catálogo de datos de AWS Glue en la Guía para desarrolladores de AWS Glue.

- Para obtener información sobre la API, consulte CreateTable en la Referencia de comandos de la AWS CLI.

`delete-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-job`.

AWS CLI

Eliminación de un trabajo

En el siguiente ejemplo de `delete-job`, se elimina un trabajo que ya no necesite.

```
aws glue delete-job \
    --job-name my-testing-job
```

Salida:

```
{
    "JobName": "my-testing-job"
}
```

Para obtener más información, consulte Uso de trabajos en la consola de AWS Glue en la Guía para desarrolladores de AWS Glue.

- Para obtener más información sobre la API, consulte DeleteJob en la Referencia de comandos de la AWS CLI.

`get-databases`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-databases`.

AWS CLI

Enumeración de las definiciones de algunas o todas las bases de datos del Catálogo de datos de AWS Glue

El siguiente ejemplo de `get-databases` devuelve información sobre las bases de datos del Catálogo de datos.

```
aws glue get-databases
```

Salida:

```
{
    "DatabaseList": [
        {
            "Name": "default",
            "Description": "Default Hive database",
            "LocationUri": "file:/spark-warehouse",
            "CreateTime": 1602084052.0,
            "CreateTableDefaultPermissions": [
                {
                    "Principal": {
                        "DataLakePrincipalIdentifier": "IAM_ALLOWED_PRINCIPALS"
                    },
                    "Permissions": [
                        "ALL"
                    ]
                }
            ],
            "CatalogId": "111122223333"
        },
        {
            "Name": "flights-db",
            "CreateTime": 1587072847.0,
            "CreateTableDefaultPermissions": [
                {
                    "Principal": {
                        "DataLakePrincipalIdentifier": "IAM_ALLOWED_PRINCIPALS"
                    },
                    "Permissions": [
                        "ALL"
                    ]
                }
            ],
            "CatalogId": "111122223333"
        },
        {
            "Name": "legislators",
```

```
            "CreateTime": 1601415625.0,
            "CreateTableDefaultPermissions": [
                {
                    "Principal": {
                        "DataLakePrincipalIdentifier": "IAM_ALLOWED_PRINCIPALS"
                    },
                    "Permissions": [
                        "ALL"
                    ]
                }
            ],
            "CatalogId": "111122223333"
        },
        {
            "Name": "tempdb",
            "CreateTime": 1601498566.0,
            "CreateTableDefaultPermissions": [
                {
                    "Principal": {
                        "DataLakePrincipalIdentifier": "IAM_ALLOWED_PRINCIPALS"
                    },
                    "Permissions": [
                        "ALL"
                    ]
                }
            ],
            "CatalogId": "111122223333"
        }
    ]
}
```

Para obtener más información, consulte Definición de una base de datos en su Catálogo de datos en la Guía para desarrolladores de AWS Glue.

- Para obtener más información sobre la API, consulte GetDatabases en la Referencia de comandos de la AWS CLI.

`get-job-run`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-job-run`.

AWS CLI

Obtención de información sobre una ejecución de trabajo

El siguiente ejemplo de `get-job-run` recupera información sobre una ejecución de trabajo.

```
aws glue get-job-run \
    --job-name "Combine legistators data" \
    --run-id jr_012e176506505074d94d761755e5c62538ee1aad6f17d39f527e9140cf0c9a5e
```

Salida:

```
{
    "JobRun": {
        "Id": "jr_012e176506505074d94d761755e5c62538ee1aad6f17d39f527e9140cf0c9a5e",
        "Attempt": 0,
        "JobName": "Combine legistators data",
        "StartedOn": 1602873931.255,
        "LastModifiedOn": 1602874075.985,
        "CompletedOn": 1602874075.985,
        "JobRunState": "SUCCEEDED",
        "Arguments": {
            "--enable-continuous-cloudwatch-log": "true",
            "--enable-metrics": "",
            "--enable-spark-ui": "true",
            "--job-bookmark-option": "job-bookmark-enable",
            "--spark-event-logs-path": "s3://aws-glue-assets-111122223333-us-east-1/
sparkHistoryLogs/"
        },
        "PredecessorRuns": [],
        "AllocatedCapacity": 10,
        "ExecutionTime": 117,
        "Timeout": 2880,
        "MaxCapacity": 10.0,
        "WorkerType": "G.1X",
        "NumberOfWorkers": 10,
        "LogGroupName": "/aws-glue/jobs",
        "GlueVersion": "2.0"
    }
}
```

Para obtener más información, consulte Ejecuciones de trabajo en la Guía para desarrolladores de AWS Glue.

- Para obtener más información sobre la API, consulte GetJobRuns en la Referencia de comandos de la AWS CLI.

`get-job-runs`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-job-runs`.

AWS CLI

Obtención de información sobre todas las ejecuciones de trabajo para un trabajo

El siguiente ejemplo de `get-job-runs` recupera información acerca de las ejecuciones de flujo de trabajo para una tarea.

```
aws glue get-job-runs \
    --job-name "my-testing-job"
```

Salida:

```
{
    "JobRuns": [
        {
            "Id":
 "jr_012e176506505074d94d761755e5c62538ee1aad6f17d39f527e9140cf0c9a5e",
            "Attempt": 0,
            "JobName": "my-testing-job",
            "StartedOn": 1602873931.255,
            "LastModifiedOn": 1602874075.985,
            "CompletedOn": 1602874075.985,
            "JobRunState": "SUCCEEDED",
            "Arguments": {
                "--enable-continuous-cloudwatch-log": "true",
                "--enable-metrics": "",
                "--enable-spark-ui": "true",
                "--job-bookmark-option": "job-bookmark-enable",
                "--spark-event-logs-path": "s3://aws-glue-assets-111122223333-us-
east-1/sparkHistoryLogs/"
            },
            "PredecessorRuns": [],
            "AllocatedCapacity": 10,
            "ExecutionTime": 117,
            "Timeout": 2880,
```

```
            "MaxCapacity": 10.0,
            "WorkerType": "G.1X",
            "NumberOfWorkers": 10,
            "LogGroupName": "/aws-glue/jobs",
            "GlueVersion": "2.0"
        },
        {
            "Id":
 "jr_03cc19ddab11c4e244d3f735567de74ff93b0b3ef468a713ffe73e53d1aec08f_attempt_2",
            "Attempt": 2,
            "PreviousRunId":
 "jr_03cc19ddab11c4e244d3f735567de74ff93b0b3ef468a713ffe73e53d1aec08f_attempt_1",
            "JobName": "my-testing-job",
            "StartedOn": 1602811168.496,
            "LastModifiedOn": 1602811282.39,
            "CompletedOn": 1602811282.39,
            "JobRunState": "FAILED",
            "ErrorMessage": "An error occurred while calling
 o122.pyWriteDynamicFrame.
                Access Denied (Service: Amazon S3; Status Code: 403; Error Code:
 AccessDenied;
                Request ID: 021AAB703DB20A2D;
                S3 Extended Request ID: teZk24Y09TkXzBvMPG502L5VJBhe9DJuWA9/
TXtuGOqfByajkfL/Tlqt5JBGdEGpigAqzdMDM/U=)",
            "PredecessorRuns": [],
            "AllocatedCapacity": 10,
            "ExecutionTime": 110,
            "Timeout": 2880,
            "MaxCapacity": 10.0,
            "WorkerType": "G.1X",
            "NumberOfWorkers": 10,
            "LogGroupName": "/aws-glue/jobs",
            "GlueVersion": "2.0"
        },
        {
            "Id":
 "jr_03cc19ddab11c4e244d3f735567de74ff93b0b3ef468a713ffe73e53d1aec08f_attempt_1",
            "Attempt": 1,
            "PreviousRunId":
 "jr_03cc19ddab11c4e244d3f735567de74ff93b0b3ef468a713ffe73e53d1aec08f",
            "JobName": "my-testing-job",
            "StartedOn": 1602811020.518,
            "LastModifiedOn": 1602811138.364,
            "CompletedOn": 1602811138.364,
```

```
            "JobRunState": "FAILED",
            "ErrorMessage": "An error occurred while calling
 o122.pyWriteDynamicFrame.
                Access Denied (Service: Amazon S3; Status Code: 403; Error Code:
 AccessDenied;
                Request ID: 2671D37856AE7ABB;
                S3 Extended Request ID: RLJCJw20brV
+PpC6GpORahyF2fp9flB5SSb2bTGPnUSPVizLXRl1PN3QZldb+v1o9qRVktNYbW8=)",
            "PredecessorRuns": [],
            "AllocatedCapacity": 10,
            "ExecutionTime": 113,
            "Timeout": 2880,
            "MaxCapacity": 10.0,
            "WorkerType": "G.1X",
            "NumberOfWorkers": 10,
            "LogGroupName": "/aws-glue/jobs",
            "GlueVersion": "2.0"
        }
    ]
}
```

Para obtener más información, consulte Ejecuciones de trabajo en la Guía para desarrolladores de AWS Glue.

- Para obtener detalles de la API, consulte GetJobRuns en la Referencia de comandos de AWS CLI.

`get-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-job`.

AWS CLI

Recuperación de información sobre un trabajo

El siguiente ejemplo de `get-job` recupera información sobre un trabajo.

```
aws glue get-job \
    --job-name my-testing-job
```

Salida:

```
{
```

```
    "Job": {
        "Name": "my-testing-job",
        "Role": "Glue_DefaultRole",
        "CreatedOn": 1602805698.167,
        "LastModifiedOn": 1602805698.167,
        "ExecutionProperty": {
            "MaxConcurrentRuns": 1
        },
        "Command": {
            "Name": "gluestreaming",
            "ScriptLocation": "s3://janetst-bucket-01/Scripts/test_script.scala",
            "PythonVersion": "2"
        },
        "DefaultArguments": {
            "--class": "GlueApp",
            "--job-language": "scala"
        },
        "MaxRetries": 0,
        "AllocatedCapacity": 10,
        "MaxCapacity": 10.0,
        "GlueVersion": "1.0"
    }
}
```

Para obtener más información, consulte Trabajos en la Guía para desarrolladores de AWS Glue.

- Para obtener más información sobre la API, consulte GetJob en la Referencia de comandos de la AWS CLI.

`get-plan`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-plan`.

AWS CLI

Para obtener el código generado para asignar datos de las tablas de origen a las tablas de destino

En el siguiente `get-plan`, se recupera el código generado para asignar columnas del origen de datos al destino de datos.

```
aws glue get-plan --mapping '[ \
    { \
```

```
        "SourcePath":"sensorid", \
        "SourceTable":"anything", \
        "SourceType":"int", \
        "TargetPath":"sensorid", \
        "TargetTable":"anything", \
        "TargetType":"int" \
    }, \
    { \
        "SourcePath":"currenttemperature", \
        "SourceTable":"anything", \
        "SourceType":"int", \
        "TargetPath":"currenttemperature", \
        "TargetTable":"anything", \
        "TargetType":"int" \
    }, \
    { \
        "SourcePath":"status", \
        "SourceTable":"anything", \
        "SourceType":"string", \
        "TargetPath":"status", \
        "TargetTable":"anything", \
        "TargetType":"string" \
    }]' \
    --source '{ \
        "DatabaseName":"tempdb", \
        "TableName":"s3-source" \
    }' \
    --sinks '[ \
        { \
            "DatabaseName":"tempdb", \
            "TableName":"my-s3-sink" \
        }]' 
    --language "scala"
    --endpoint https://glue.us-east-1.amazonaws.com
    --output "text"
```

Salida:

```
import com.amazonaws.services.glue.ChoiceOption
import com.amazonaws.services.glue.GlueContext
import com.amazonaws.services.glue.MappingSpec
import com.amazonaws.services.glue.ResolveSpec
import com.amazonaws.services.glue.errors.CallSite
```

```
import com.amazonaws.services.glue.util.GlueArgParser
import com.amazonaws.services.glue.util.Job
import com.amazonaws.services.glue.util.JsonOptions
import org.apache.spark.SparkContext
import scala.collection.JavaConverters._

object GlueApp {
  def main(sysArgs: Array[String]) {
    val spark: SparkContext = new SparkContext()
    val glueContext: GlueContext = new GlueContext(spark)
    // @params: [JOB_NAME]
    val args = GlueArgParser.getResolvedOptions(sysArgs, Seq("JOB_NAME").toArray)
    Job.init(args("JOB_NAME"), glueContext, args.asJava)
    // @type: DataSource
    // @args: [database = "tempdb", table_name = "s3-source", transformation_ctx =
 "datasource0"]
    // @return: datasource0
    // @inputs: []
    val datasource0 = glueContext.getCatalogSource(database = "tempdb",
 tableName = "s3-source", redshiftTmpDir = "", transformationContext =
 "datasource0").getDynamicFrame()
    // @type: ApplyMapping
    // @args: [mapping = [("sensorid", "int", "sensorid", "int"),
 ("currenttemperature", "int", "currenttemperature", "int"), ("status", "string",
 "status", "string")], transformation_ctx = "applymapping1"]
    // @return: applymapping1
    // @inputs: [frame = datasource0]
    val applymapping1 = datasource0.applyMapping(mappings = Seq(("sensorid",
 "int", "sensorid", "int"), ("currenttemperature", "int", "currenttemperature",
 "int"), ("status", "string", "status", "string")), caseSensitive = false,
 transformationContext = "applymapping1")
    // @type: SelectFields
    // @args: [paths = ["sensorid", "currenttemperature", "status"],
 transformation_ctx = "selectfields2"]
    // @return: selectfields2
    // @inputs: [frame = applymapping1]
    val selectfields2 = applymapping1.selectFields(paths = Seq("sensorid",
 "currenttemperature", "status"), transformationContext = "selectfields2")
    // @type: ResolveChoice
    // @args: [choice = "MATCH_CATALOG", database = "tempdb", table_name = "my-s3-
sink", transformation_ctx = "resolvechoice3"]
    // @return: resolvechoice3
    // @inputs: [frame = selectfields2]
```

```
    val resolvechoice3 = selectfields2.resolveChoice(choiceOption =
 Some(ChoiceOption("MATCH_CATALOG")), database = Some("tempdb"), tableName =
 Some("my-s3-sink"), transformationContext = "resolvechoice3")
    // @type: DataSink
    // @args: [database = "tempdb", table_name = "my-s3-sink", transformation_ctx =
 "datasink4"]
    // @return: datasink4
    // @inputs: [frame = resolvechoice3]
    val datasink4 = glueContext.getCatalogSink(database = "tempdb",
 tableName = "my-s3-sink", redshiftTmpDir = "", transformationContext =
 "datasink4").writeDynamicFrame(resolvechoice3)
    Job.commit()
  }
}
```

Para obtener más información, consulte Editing Scripts in AWS Glue en la Guía para desarrolladores de AWS Glue.

- Para obtener información sobre la API, consulte GetPlan en la Referencia de comandos de la AWS CLI.

`get-tables`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-tables`.

AWS CLI

Enumeración de las definiciones de algunas o todas las tablas de la base de datos especificada

El siguiente ejemplo de `get-tables` devuelve información sobre las tablas de la base de datos especificada.

```
aws glue get-tables --database-name 'tempdb'
```

Salida:

```
{
    "TableList": [
        {
            "Name": "my-s3-sink",
            "DatabaseName": "tempdb",
            "CreateTime": 1602730539.0,
            "UpdateTime": 1602730539.0,
```

```
            "Retention": 0,
            "StorageDescriptor": {
                "Columns": [
                    {
                        "Name": "sensorid",
                        "Type": "int"
                    },
                    {
                        "Name": "currenttemperature",
                        "Type": "int"
                    },
                    {
                        "Name": "status",
                        "Type": "string"
                    }
                ],
                "Location": "s3://janetst-bucket-01/test-s3-output/",
                "Compressed": false,
                "NumberOfBuckets": 0,
                "SerdeInfo": {
                    "SerializationLibrary": "org.openx.data.jsonserde.JsonSerDe"
                },
                "SortColumns": [],
                "StoredAsSubDirectories": false
            },
            "Parameters": {
                "classification": "json"
            },
            "CreatedBy": "arn:aws:iam::007436865787:user/JRSTERN",
            "IsRegisteredWithLakeFormation": false,
            "CatalogId": "007436865787"
        },
        {
            "Name": "s3-source",
            "DatabaseName": "tempdb",
            "CreateTime": 1602730658.0,
            "UpdateTime": 1602730658.0,
            "Retention": 0,
            "StorageDescriptor": {
                "Columns": [
                    {
                        "Name": "sensorid",
                        "Type": "int"
                    },
```

```
                {
                    "Name": "currenttemperature",
                    "Type": "int"
                },
                {
                    "Name": "status",
                    "Type": "string"
                }
            ],
            "Location": "s3://janetst-bucket-01/",
            "Compressed": false,
            "NumberOfBuckets": 0,
            "SortColumns": [],
            "StoredAsSubDirectories": false
        },
        "Parameters": {
            "classification": "json"
        },
        "CreatedBy": "arn:aws:iam::007436865787:user/JRSTERN",
        "IsRegisteredWithLakeFormation": false,
        "CatalogId": "007436865787"
    },
    {
        "Name": "test-kinesis-input",
        "DatabaseName": "tempdb",
        "CreateTime": 1601507001.0,
        "UpdateTime": 1601507001.0,
        "Retention": 0,
        "StorageDescriptor": {
            "Columns": [
                {
                    "Name": "sensorid",
                    "Type": "int"
                },
                {
                    "Name": "currenttemperature",
                    "Type": "int"
                },
                {
                    "Name": "status",
                    "Type": "string"
                }
            ],
            "Location": "my-testing-stream",
```

```
                "Compressed": false,
                "NumberOfBuckets": 0,
                "SerdeInfo": {
                    "SerializationLibrary": "org.openx.data.jsonserde.JsonSerDe"
                },
                "SortColumns": [],
                "Parameters": {
                    "kinesisUrl": "https://kinesis.us-east-1.amazonaws.com",
                    "streamName": "my-testing-stream",
                    "typeOfData": "kinesis"
                },
                "StoredAsSubDirectories": false
            },
            "Parameters": {
                "classification": "json"
            },
            "CreatedBy": "arn:aws:iam::007436865787:user/JRSTERN",
            "IsRegisteredWithLakeFormation": false,
            "CatalogId": "007436865787"
        }
    ]
}
```

Para obtener más información, consulte Definición de tablas en el Catálogo de datos de AWS Glue en la Guía para desarrolladores de AWS Glue.

- Para obtener más información sobre la API, consulte GetTables en la Referencia de comandos de laAWS CLI.

`start-crawler`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-crawler`.

AWS CLI

Inicio de un rastreador

El siguiente ejemplo de `start-crawler` inicia un rastreador.

```
aws glue start-crawler --name my-crawler
```

Salida:

```
None
```

Para obtener más información, consulte Definición de rastreadores en la Guía para desarrolladores de AWS Glue.

- Para obtener más información sobre la API, consulte StartCrawler en la Referencia de comandos de la AWS CLI.

`start-job-run`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-job-run`.

AWS CLI

Inicio de la ejecución de un trabajo

El siguiente ejemplo de `start-job-run` inicia un trabajo.

```
aws glue start-job-run \
    --job-name my-job
```

Salida:

```
{
    "JobRunId":
 "jr_22208b1f44eb5376a60569d4b21dd20fcb8621e1a366b4e7b2494af764b82ded"
}
```

Para obtener más información, consulte Creación de trabajos en la Guía para desarrolladores de AWS Glue.

- Para obtener información sobre la API, consulte StartJobRun en la Referencia de comandos de la AWS CLI.

Ejemplos de GuardDuty que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios habituales mediante AWS Command Line Interface con GuardDuty.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`accept-invitation`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-invitation`.

AWS CLI

Para aceptar una invitación para convertirse en una cuenta de miembro de GuardDuty en la región actual

En el siguiente ejemplo de `accept-invitation`, se muestra cómo aceptar una invitación para convertirse en una cuenta de miembro de GuardDuty en la región actual.

```
aws guardduty accept-invitation  \
    --detector-id 12abc34d567e8fa901bc2d34eexample \
    --master-id 123456789111 \
    --invitation-id d6b94fb03a66ff665f7db8764example
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing GuardDuty accounts by invitation en la Guía del usuario de GuardDuty.

- Para obtener detalles sobre la API, consulte AcceptInvitation en la Referencia de comandos de la AWS CLI.

`archive-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `archive-findings`.

AWS CLI

Para archivar los resultados de la región actual

En este ejemplo de `archive-findings`, se muestra cómo archivar los resultados en la región actual.

```
aws guardduty archive-findings \
    --detector-id 12abc34d567e8fa901bc2d34eexample \
    --finding-ids d6b94fb03a66ff665f7db8764example 3eb970e0de00c16ec14e6910fexample
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación de reglas de supresión en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte ArchiveFindings en la Referencia de comandos de la AWS CLI.

`create-detector`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-detector`.

AWS CLI

Para habilitar GuardDuty en la región actual

En este ejemplo, se muestra cómo crear un detector, que habilita GuardDuty, en la región actual:

```
aws guardduty create-detector \
    --enable
```

Salida:

```
{
    "DetectorId": "b6b992d6d2f48e64bc59180bfexample"
}
```

Para obtener más información, consulte Enable Amazon GuardDuty en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte CreateDetector en la Referencia de comandos de la AWS CLI.

`create-filter`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-filter`.

AWS CLI

Ejemplo 1: creación de un filtro nuevo en la región actual

En este ejemplo de `create-filter`, se crea un filtro que coincide con todos los resultados de la exploración de puertos, por ejemplo, los creados a partir de una imagen específica. Esto no suprime esos resultados.

```
aws guardduty create-filter \
    --detector-id b6b992d6d2f48e64bc59180bfexample \
    --name myFilterExample \
    --finding-criteria '{"Criterion": {"type": {"Eq": ["Recon:EC2/
Portscan"]},"resource.instanceDetails.imageId": {"Eq": ["ami-0a7a207083example"]}}}'
```

Salida:

```
{
    "Name": "myFilterExample"
}
```

Para obtener más información, consulte Filtrado de resultados de GuardDuty en la Guía del usuario de GuardDuty.

Ejemplo 2: creación de un filtro nuevo y supresión de resultados en la región actual

En este ejemplo de `create-filter`, se crea un filtro que coincide con todos los resultados de la exploración de puertos, por ejemplo, los creados a partir de una imagen específica. Este filtro archiva esos resultados para que no aparezcan en los resultados actuales.

```
aws guardduty create-filter \
    --detector-id b6b992d6d2f48e64bc59180bfexample \
    --action ARCHIVE \
    --name myFilterSecondExample \
```

```
    --finding-criteria '{"Criterion": {"type": {"Eq": ["Recon:EC2/
Portscan"]},"resource.instanceDetails.imageId": {"Eq": ["ami-0a7a207083example"]}}}'
```

Salida:

```
{
    "Name": "myFilterSecondExample"
}
```

Para obtener más información, consulte Filtrado de resultados de GuardDuty en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte CreateFilter en la Referencia de comandos de la AWS CLI.

`create-ip-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-ip-set`.

AWS CLI

Creación y activación de un conjunto de IP de confianza

En el siguiente ejemplo de `create-ip-set`, se crea y activa un conjunto de IP de confianza en la región actual.

```
aws guardduty create-ip-set \
    --detector-id 12abc34d567e8fa901bc2d34eexample \
    --name new-ip-set-example \
    --format TXT \
    --location s3://amzn-s3-demo-bucket/customtrustlist.csv \
    --activate
```

Salida:

```
{
    "IpSetId": "d4b94fc952d6912b8f3060768example"
}
```

Para obtener más información, consulte Working with Trusted IP Lists and Threat Lists en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte CreateIpSet en la Referencia de comandos de la AWS CLI.

`create-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-members`.

AWS CLI

Para asociar un nuevo miembro a su cuenta maestra de GuardDuty en la región actual.

En este ejemplo, se muestra cómo asociar las cuentas de los miembros para que las administre la cuenta actual como la maestra de GuardDuty.

```
aws guardduty create-members
    --detector-id b6b992d6d2f48e64bc59180bfexample \
    --account-details AccountId=111122223333,Email=first
+member@example.com AccountId=111111111111 ,Email=another+member@example.com
```

Salida:

```
{
   "UnprocessedAccounts": []
}
```

Para obtener más información, consulte Managing multiple accounts en la Guía del usuario de GuardDuty.

- Para obtener detalles sobre la API, consulte CreateMembers en la Referencia de comandos de la AWS CLI.

`create-publishing-destination`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-publishing-destination`.

AWS CLI

Para crear un destino de publicación al que exportar los resultados de GuardDuty en la región actual.

En el siguiente ejemplo de `create-publishing-destination`, se muestra cómo configurar un destino de publicación para exportar los resultados actuales (no archivados) de GuardDuty a fin de realizar un seguimiento de los datos de resultados históricos.

```
aws guardduty create-publishing-destination \
    --detector-id b6b992d6d2f48e64bc59180bfexample \
    --destination-type S3 \
    --destination-properties 'DestinationArn=arn:aws:s3:::amzn-s3-demo-bucket,KmsKeyArn=arn:aws:kms:us-west-1:111122223333:key/84cee9c5-dea1-401a-ab6d-e1de7example'
```

Salida:

```
{
    "DestinationId": "46b99823849e1bbc242dfbe3cexample"
}
```

Para obtener más información, consulte Exportación de los resultados de GuardDuty generados a buckets de Amazon S3 en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte CreatePublishingDestination en la Referencia de comandos de la AWS CLI.

`create-sample-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-sample-findings`.

AWS CLI

Para crear resultados de GuardDuty de ejemplo en la región actual.

En este ejemplo, se muestra cómo crear un resultado de ejemplo de los tipos proporcionados.

```
aws guardduty create-sample-findings \
    --detector-id b6b992d6d2f48e64bc59180bfexample \
    --finding-types UnauthorizedAccess:EC2/TorClient UnauthorizedAccess:EC2/TorRelay
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Sample findings en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte CreateSampleFindings en la Referencia de comandos de la AWS CLI.

`create-threat-intel-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-threat-intel-set`.

AWS CLI

Creación y activación de un nuevo conjunto de información sobre amenazas

En el siguiente ejemplo de `create-threat-intel-set`, se crea y activa un conjunto de información sobre amenazas en la región actual.

```
aws guardduty create-threat-intel-set \
    --detector-id b6b992d6d2f48e64bc59180bfexample \
    --name myThreatSet-example \
    --format TXT \
    --location s3://amzn-s3-demo-bucket/threatlist.csv \
    --activate
```

Salida:

```
{
    "ThreatIntelSetId": "20b9a4691aeb33506b808878cexample"
}
```

Para obtener más información, consulte Working with Trusted IP Lists and Threat Lists en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte CreateThreatIntelSet en la Referencia de comandos de la AWS CLI.

`decline-invitations`

En el siguiente ejemplo de código, se muestra cómo utilizar `decline-invitations`.

AWS CLI

Para rechazar una invitación para que Guardduty administre otra cuenta de la región actual.

En este ejemplo, se muestra cómo rechazar una invitación a una suscripción.

```
aws guardduty decline-invitations \
    --account-ids 111122223333
```

Salida:

```
{
    "UnprocessedAccounts": []
}
```

Para obtener más información, consulte Managing GuardDuty accounts by invitation en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte DeclineInvitations en la Referencia de comandos de la AWS CLI.

`delete-detector`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-detector`.

AWS CLI

Para eliminar un detector y deshabilitar GuardDuty en la región actual.

En este ejemplo, se muestra cómo eliminar un detector. Si se elimina correctamente, se deshabilitará GuardDuty en la región asociada a ese detector.

```
aws guardduty delete-detector \
    --detector-id b6b992d6d2f48e64bc59180bfexample
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Suspending or disabling GuardDuty en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte DeleteDetector en la Referencia de comandos de la AWS CLI.

`delete-filter`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-filter`.

AWS CLI

Para eliminar un filtro existente en la región actual

En este ejemplo, se muestra cómo crear y eliminar un filtro.

```
aws guardduty delete-filter \
    --detector-id b6b992d6d2f48e64bc59180bfexample \
    --filter-name byebyeFilter
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Filtering findings en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte DeleteFilter en la Referencia de comandos de la AWS CLI.

`disable-organization-admin-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-organization-admin-account`.

AWS CLI

Para eliminar una cuenta como administrador delegado de GuardDuty en su organización

En este ejemplo, se muestra cómo quitar una cuenta como administrador delegado para GuardDuty.

```
aws guardduty disable-organization-admin-account \
    --admin-account-id 111122223333
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing accounts with AWS organizations en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte DisableOrganizationAdminAccount en la Referencia de comandos de la AWS CLI.

`disassociate-from-master-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-from-master-account`.

AWS CLI

Desasociación de la cuenta de administrador actual en la región actual

En el siguiente ejemplo de `disassociate-from-master-account`, se desasocia la cuenta de la cuenta de administrador de GuardDuty actual en la región de AWS actual.

```
aws guardduty disassociate-from-master-account \
    --detector-id d4b040365221be2b54a6264dcexample
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Comprender la relación entre la cuenta de administrador de GuardDuty y las cuentas de miembro en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte DisassociateFromMasterAccount en la Referencia de comandos de la AWS CLI.

`get-detector`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-detector`.

AWS CLI

Para recuperar los detalles de un detector específico

En el siguiente ejemplo de `get-detector`, se muestran los detalles de configuración del detector especificado.

```
aws guardduty get-detector \
    --detector-id 12abc34d567e8fa901bc2d34eexample
```

Salida:

```
{
    "Status": "ENABLED",
```

```
    "ServiceRole": "arn:aws:iam::111122223333:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Tags": {},
    "FindingPublishingFrequency": "SIX_HOURS",
    "UpdatedAt": "2018-11-07T03:24:22.938Z",
    "CreatedAt": "2017-12-22T22:51:31.940Z"
}
```

Para obtener más información, consulte Concepts and Terminology en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte GetDetector en la Referencia de comandos de la AWS CLI.

`get-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-findings`.

AWS CLI

Ejemplo 1: recuperación de los detalles de un resultado específico

En el siguiente ejemplo de `get-findings`, se recuperan los detalles de resultados JSON completos del resultado especificado.

```
aws guardduty get-findings \
    --detector-id 12abc34d567e8fa901bc2d34eexample \
    --finding-id 1ab92989eaf0e742df4a014d5example
```

Salida:

```
{
    "Findings": [
        {
            "Resource": {
                "ResourceType": "AccessKey",
                "AccessKeyDetails": {
                    "UserName": "testuser",
                    "UserType": "IAMUser",
                    "PrincipalId": "AIDACKCEVSQ6C2EXAMPLE",
                    "AccessKeyId": "ASIASZ4SI7REEEXAMPLE"
                }
            },
```

```
            "Description": "APIs commonly used to discover the users, groups,
 policies and permissions in an account, was invoked by IAM principal testuser under
 unusual circumstances. Such activity is not typically seen from this principal.",
            "Service": {
                "Count": 5,
                "Archived": false,
                "ServiceName": "guardduty",
                "EventFirstSeen": "2020-05-26T22:02:24Z",
                "ResourceRole": "TARGET",
                "EventLastSeen": "2020-05-26T22:33:55Z",
                "DetectorId": "d4b040365221be2b54a6264dcexample",
                "Action": {
                    "ActionType": "AWS_API_CALL",
                    "AwsApiCallAction": {
                        "RemoteIpDetails": {
                            "GeoLocation": {
                                "Lat": 51.5164,
                                "Lon": -0.093
                            },
                            "City": {
                                "CityName": "London"
                            },
                            "IpAddressV4": "52.94.36.7",
                            "Organization": {
                                "Org": "Amazon.com",
                                "Isp": "Amazon.com",
                                "Asn": "16509",
                                "AsnOrg": "AMAZON-02"
                            },
                            "Country": {
                                "CountryName": "United Kingdom"
                            }
                        },
                        "Api": "ListPolicyVersions",
                        "ServiceName": "iam.amazonaws.com",
                        "CallerType": "Remote IP"
                    }
                }
            },
            "Title": "Unusual user permission reconnaissance activity by testuser.",
            "Type": "Recon:IAMUser/UserPermissions",
            "Region": "us-east-1",
            "Partition": "aws",
```

```
            "Arn": "arn:aws:guardduty:us-east-1:111122223333:detector/
d4b040365221be2b54a6264dcexample/finding/1ab92989eaf0e742df4a014d5example",
            "UpdatedAt": "2020-05-26T22:55:21.703Z",
            "SchemaVersion": "2.0",
            "Severity": 5,
            "Id": "1ab92989eaf0e742df4a014d5example",
            "CreatedAt": "2020-05-26T22:21:48.385Z",
            "AccountId": "111122223333"
        }
    ]
}
```

Para obtener más información, consulte Findings en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte GetFindings en la Referencia de comandos de la AWS CLI.

`get-ip-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ip-set`.

AWS CLI

Para enumerar los detalles de un conjunto de IP de confianza especificado

En el siguiente ejemplo de `get-ip-set`, se muestran el estado y los detalles del conjunto de direcciones IP de confianza especificado.

```
aws guardduty get-ip-set \
    --detector-id 12abc34d567e8fa901bc2d34eexample \
    --ip-set-id d4b94fc952d6912b8f3060768example
```

Salida:

```
{
    "Status": "ACTIVE",
    "Location": "s3://amzn-s3-demo-bucket.s3-us-west-2.amazonaws.com/
customlist.csv",
    "Tags": {},
    "Format": "TXT",
    "Name": "test-ip-set-example"
}
```

Para obtener más información, consulte Working with Trusted IP Lists and Threat Lists en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte GetIpSet en la Referencia de comandos de la AWS CLI.

`get-master-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-master-account`.

AWS CLI

Para recuperar detalles sobre su cuenta maestra en la región actual

En el siguiente ejemplo de `get-master-account`, se muestran el estado y los detalles de la cuenta maestra asociada a su detector en la región actual.

```
aws guardduty get-master-account \
    --detector-id 12abc34d567e8fa901bc2d34eexample
```

Salida:

```
{
    "Master": {
        "InvitationId": "04b94d9704854a73f94e061e8example",
        "InvitedAt": "2020-06-09T22:23:04.970Z",
        "RelationshipStatus": "Enabled",
        "AccountId": "111122223333"
    }
}
```

Para obtener más información, consulte Comprender la relación entre la cuenta de administrador de GuardDuty y la cuenta de miembro en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte GetMasterAccount en la Referencia de comandos de la AWS CLI.

`list-detectors`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-detectors`.

AWS CLI

Para enumerar los detectores disponibles en la región actual

En el siguiente ejemplo de `list-detectors`, se enumeran los detectores disponibles en la región de AWS actual.

```
aws guardduty list-detectors
```

Salida:

```
{
    "DetectorIds": [
        "12abc34d567e8fa901bc2d34eexample"
    ]
}
```

Para obtener más información, consulte Concepts and Terminology en la Guía del usuario de GuardDuty.

- Para obtener más información sobre la API, consulte ListDetectors en la Referencia de comandos de la AWS CLI.

`list-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-findings`.

AWS CLI

Ejemplo 1: enumeración de todos los resultados de la región actual

En el siguiente ejemplo de `list-findings`, se muestra una lista de todos los findingIds para la región actual ordenados por gravedad, de la mayor a la menor.

```
aws guardduty list-findings \
    --detector-id 12abc34d567e8fa901bc2d34eexample \
    --sort-criteria '{"AttributeName": "severity","OrderBy":"DESC"}'
```

Salida:

```
{
```

```
    "FindingIds": [
        "04b8ab50fd29c64fc771b232dexample",
        "5ab8ab50fd21373735c826d3aexample",
        "90b93de7aba69107f05bbe60bexample",
        ...
    ]
}
```

Para obtener más información, consulte Findings en la Guía del usuario de GuardDuty.

Ejemplo 2: enumeración de los resultados de la región actual que coinciden con un criterio de resultado específico

En el siguiente ejemplo de `list-findings`, se muestra una lista de todos los findingIds que coinciden con un tipo de resultado especificado.

```
aws guardduty list-findings \
    --detector-id 12abc34d567e8fa901bc2d34eexample \
    --finding-criteria  '{"Criterion":{"type": {"Eq":["UnauthorizedAccess:EC2/
SSHBruteForce"]}}}'
```

Salida:

```
{
    "FindingIds": [
        "90b93de7aba69107f05bbe60bexample",
        "6eb9430d7023d30774d6f05e3example",
        "2eb91a2d060ac9a21963a5848example",
        "44b8ab50fd2b0039a9e48f570example",
        "9eb8ab4cd2b7e5b66ba4f5e96example",
        "e0b8ab3a38e9b0312cc390ceeexample"
    ]
}
```

Para obtener más información, consulte Findings en la Guía del usuario de GuardDuty.

Ejemplo 3: enumeración de los resultados de la región actual que coinciden con un conjunto específico de criterios de resultados definidos en un archivo JSON

En el siguiente ejemplo de `list-findings`, se muestra una lista de todos los findingIds que no están archivados e incluyen al usuario de IAM llamado testuser, tal y como se especifica en un archivo JSON.

```
aws guardduty list-findings \
    --detector-id 12abc34d567e8fa901bc2d34eexample \
    --finding-criteria  file://myfile.json
```

Contenidos de `myfile.json`:

```
{"Criterion": {
    "resource.accessKeyDetails.userName":{
                "Eq":[
                    "testuser"
                    ]
                },
    "service.archived": {
                "Eq": [
                    "false"
                ]
            }
        }
}
```

Salida:

```
{
    "FindingIds": [
        "1ab92989eaf0e742df4a014d5example"
    ]
}
```

Para obtener más información, consulte Findings en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte ListFindings en la Referencia de comandos de la AWS CLI.

`list-invitations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-invitations`.

AWS CLI

Para enumerar los detalles de sus invitaciones para convertirse en una cuenta de miembro en la región actual

En el siguiente ejemplo de `list-invitations` se enumeran los detalles y estados de sus invitaciones para convertirse en una cuenta de miembro de GuardDuty en la región actual.

```
aws guardduty list-invitations
```

Salida:

```
{
    "Invitations": [
        {
            "InvitationId": "d6b94fb03a66ff665f7db8764example",
            "InvitedAt": "2020-06-10T17:56:38.221Z",
            "RelationshipStatus": "Invited",
            "AccountId": "123456789111"
        }
    ]
}
```

Para obtener más información, consulte Managing GuardDuty Accounts by Invitation en la Guía del usuario de GuardDuty.

- Para obtener detalles sobre la API, consulte ListInvitations en la Referencia de comandos de la AWS CLI.

`list-ip-sets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-ip-sets`.

AWS CLI

Para enumerar los conjuntos de dirección IP de confianza de la región actual

En el siguiente ejemplo de `list-ip-sets`, se enumeran los conjuntos de direcciones IP de confianza en la región de AWS actual.

```
aws guardduty list-ip-sets \
    --detector-id 12abc34d567e8fa901bc2d34eexample
```

Salida:

```
{
```

```
    "IpSetIds": [
        "d4b94fc952d6912b8f3060768example"
    ]
}
```

Para obtener más información, consulte Working with Trusted IP Lists and Threat Lists en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte ListIpSets en la Referencia de comandos de la AWS CLI.

`list-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-members`.

AWS CLI

Ejemplo 1: muestra exclusiva de los miembros actuales de la región actual

En el siguiente ejemplo de `list-members`, se muestran y proporcionan detalles solo de las cuentas de los miembros actuales asociadas a la cuenta de administrador de GuardDuty, en la región actual.

```
aws guardduty list-members \
    --detector-id 12abc34d567e8fa901bc2d34eexample \
    --only-associated="true"
```

Salida:

```
{
    "Members": [
        {
            "RelationshipStatus": "Enabled",
            "InvitedAt": "2020-06-09T22:49:00.910Z",
            "MasterId": "111122223333",
            "DetectorId": "7ab8b2f61b256c87f793f6a86example",
            "UpdatedAt": "2020-06-09T23:08:22.512Z",
            "Email": "your+member@example.com",
            "AccountId": "123456789012"
        }
    ]
}
```

Para obtener más información, consulte Comprender la relación entre la cuenta de administrador de GuardDuty y las cuentas de miembro en la Guía del usuario de GuardDuty.

Ejemplo 2: muestra de todos los miembros de la región actual

En el siguiente ejemplo de `list-members`, se muestran y proporcionan detalles de todas las cuentas de los miembros de la región actual, incluidas las que se han disociado o que aún no han aceptado la invitación del administrador de GuardDuty.

```
aws guardduty list-members \
    --detector-id 12abc34d567e8fa901bc2d34eexample \
    --only-associated="false"
```

Salida:

```
{
    "Members": [
        {
            "RelationshipStatus": "Enabled",
            "InvitedAt": "2020-06-09T22:49:00.910Z",
            "MasterId": "111122223333",
            "DetectorId": "7ab8b2f61b256c87f793f6a86example",
            "UpdatedAt": "2020-06-09T23:08:22.512Z",
            "Email": "your+other+member@example.com",
            "AccountId": "555555555555"
        }
    ]
}
```

Para obtener más información, consulte Comprender la relación entre la cuenta de administrador de GuardDuty y las cuentas de miembro en la Guía del usuario de GuardDuty.

- Para obtener detalles sobre la API, consulte ListMembers en la Referencia de comandos de la AWS CLI.

update-ip-set

En el siguiente ejemplo de código, se muestra cómo utilizar `update-ip-set`.

AWS CLI

Para actualizar un conjunto de direcciones IP de confianza

En el siguiente ejemplo de `update-ip-set`, se muestra cómo actualizar los detalles de un conjunto de direcciones IP de confianza.

```
aws guardduty update-ip-set \
    --detector-id 12abc34d567e8fa901bc2d34eexample \
    --ip-set-id d4b94fc952d6912b8f3060768example \
    --location https://amzn-s3-demo-bucket.s3-us-west-2.amazonaws.com/
customtrustlist2.csv
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with Trusted IP Lists and Threat Lists en la Guía del usuario de GuardDuty.

- Para obtener información sobre la API, consulte UpdateIpSet en la Referencia de comandos de la AWS CLI.

AWS Health Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS Health.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`describe-affected-entities`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-affected-entities`.

AWS CLI

Para enumerar las entidades que se ven afectadas por un evento de AWS Health específico

En el siguiente ejemplo de `describe-affected-entities`, se enumeran las entidades que se ven afectadas por el evento AWS Health especificado. Este evento es una notificación de facturación para la cuenta de AWS.

```
aws health describe-affected-entities \
    --filter "eventArns=arn:aws:health:global::event/BILLING/
AWS_BILLING_NOTIFICATION/AWS_BILLING_NOTIFICATION_6ce1d874-e995-40e2-99cd-
EXAMPLE11145" \
    --region us-east-1
```

Salida:

```
{
    "entities": [
        {
            "entityArn": "arn:aws:health:global:123456789012:entity/
EXAMPLEimSMoULmWHpb",
            "eventArn": "arn:aws:health:global::event/BILLING/
AWS_BILLING_NOTIFICATION/AWS_BILLING_NOTIFICATION_6ce1d874-e995-40e2-99cd-
EXAMPLE11145",
            "entityValue": "AWS_ACCOUNT",
            "awsAccountId": "123456789012",
            "lastUpdatedTime": 1588356454.08
        }
    ]
}
```

Para obtener más información, consulte Event log en la Guía del usuario de AWS Health.

- Para obtener información sobre la API, consulte DescribeAffectedEntities en la Referencia de comandos de la AWS CLI.

`describe-event-details`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-event-details`.

AWS CLI

Inclusión de información sobre un evento de AWS Health

En el siguiente ejemplo de `describe-event-details`, se muestra información sobre el evento AWS Health especificado.

```
aws health describe-event-details \
    --event-arns "arn:aws:health:us-east-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE/
AWS_EC2_OPERATIONAL_ISSUE_VKTXI_EXAMPLE111" \
    --region us-east-1
```

Salida:

```
{
    "successfulSet": [
        {
            "event": {
                "arn": "arn:aws:health:us-east-1::event/EC2/
AWS_EC2_OPERATIONAL_ISSUE/AWS_EC2_OPERATIONAL_ISSUE_VKTXI_EXAMPLE111",
                "service": "EC2",
                "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
                "eventTypeCategory": "issue",
                "region": "us-east-1",
                "startTime": 1587462325.096,
                "endTime": 1587464204.774,
                "lastUpdatedTime": 1587464204.865,
                "statusCode": "closed"
            },
            "eventDescription": {
                "latestDescription": "[RESOLVED] Increased API Error Rates and
 Latencies\n\n[02:45 AM PDT] We are investigating increased API error rates and
 latencies in the US-EAST-1 Region.\n\n[03:16 AM PDT] Between 2:10 AM and 2:59 AM
 PDT we experienced increased API error rates and latencies in the US-EAST-1 Region.
 The issue has been resolved and the service is operating normally."
            }
        }
    ],
    "failedSet": []
}
```

Para obtener más información, consulte Event details pane en la Guía del usuario de AWS Health.

- Para obtener información sobre la API, consulte DescribeEventDetails en la Referencia de comandos de la AWS CLI.

`describe-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-events`.

AWS CLI

Ejemplo 1: enumeración de eventos AWS Health

En el siguiente ejemplo de `describe-events`, se enumeran los eventos de AWS Health recientes.

```
aws health describe-events \
    --region us-east-1
```

Salida:

```
{
    "events": [
        {
            "arn": "arn:aws:health:us-west-1::event/ECS/AWS_ECS_OPERATIONAL_ISSUE/
AWS_ECS_OPERATIONAL_ISSUE_KWQPY_EXAMPLE111",
            "service": "ECS",
            "eventTypeCode": "AWS_ECS_OPERATIONAL_ISSUE",
            "eventTypeCategory": "issue",
            "region": "us-west-1",
            "startTime": 1589077890.53,
            "endTime": 1589086345.597,
            "lastUpdatedTime": 1589086345.905,
            "statusCode": "closed",
            "eventScopeCode": "PUBLIC"
        },
        {
            "arn": "arn:aws:health:global::event/BILLING/AWS_BILLING_NOTIFICATION/
AWS_BILLING_NOTIFICATION_6ce1d874-e995-40e2-99cd-EXAMPLE1118b",
            "service": "BILLING",
            "eventTypeCode": "AWS_BILLING_NOTIFICATION",
            "eventTypeCategory": "accountNotification",
            "region": "global",
            "startTime": 1588356000.0,
            "lastUpdatedTime": 1588356524.358,
            "statusCode": "open",
            "eventScopeCode": "ACCOUNT_SPECIFIC"
        },
```

```
        {
            "arn": "arn:aws:health:us-west-2::event/
CLOUDFORMATION/AWS_CLOUDFORMATION_OPERATIONAL_ISSUE/
AWS_CLOUDFORMATION_OPERATIONAL_ISSUE_OHTWY_EXAMPLE111",
            "service": "CLOUDFORMATION",
            "eventTypeCode": "AWS_CLOUDFORMATION_OPERATIONAL_ISSUE",
            "eventTypeCategory": "issue",
            "region": "us-west-2",
            "startTime": 1588279630.761,
            "endTime": 1588284650.0,
            "lastUpdatedTime": 1588284691.941,
            "statusCode": "closed",
            "eventScopeCode": "PUBLIC"
        },
        {
            "arn": "arn:aws:health:ap-northeast-1::event/LAMBDA/
AWS_LAMBDA_OPERATIONAL_ISSUE/AWS_LAMBDA_OPERATIONAL_ISSUE_JZDND_EXAMPLE111",
            "service": "LAMBDA",
            "eventTypeCode": "AWS_LAMBDA_OPERATIONAL_ISSUE",
            "eventTypeCategory": "issue",
            "region": "ap-northeast-1",
            "startTime": 1587379534.08,
            "endTime": 1587391771.0,
            "lastUpdatedTime": 1587395689.316,
            "statusCode": "closed",
            "eventScopeCode": "PUBLIC"
        },
        {
            "arn": "arn:aws:health:us-east-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE/
AWS_EC2_OPERATIONAL_ISSUE_COBXJ_EXAMPLE111",
            "service": "EC2",
            "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
            "eventTypeCategory": "issue",
            "region": "us-east-1",
            "startTime": 1586473044.284,
            "endTime": 1586479706.091,
            "lastUpdatedTime": 1586479706.153,
            "statusCode": "closed",
            "eventScopeCode": "PUBLIC"
        },
        {
            "arn": "arn:aws:health:global::event/SECURITY/AWS_SECURITY_NOTIFICATION/
AWS_SECURITY_NOTIFICATION_42007387-8129-42da-8c88-EXAMPLE11139",
            "service": "SECURITY",
```

```
            "eventTypeCode": "AWS_SECURITY_NOTIFICATION",
            "eventTypeCategory": "accountNotification",
            "region": "global",
            "startTime": 1585674000.0,
            "lastUpdatedTime": 1585674004.132,
            "statusCode": "open",
            "eventScopeCode": "PUBLIC"
        },
        {
            "arn": "arn:aws:health:global::event/CLOUDFRONT/
AWS_CLOUDFRONT_OPERATIONAL_ISSUE/AWS_CLOUDFRONT_OPERATIONAL_ISSUE_FRQXG_EXAMPLE111",
            "service": "CLOUDFRONT",
            "eventTypeCode": "AWS_CLOUDFRONT_OPERATIONAL_ISSUE",
            "eventTypeCategory": "issue",
            "region": "global",
            "startTime": 1585610898.589,
            "endTime": 1585617671.0,
            "lastUpdatedTime": 1585620638.869,
            "statusCode": "closed",
            "eventScopeCode": "PUBLIC"
        },
        {
            "arn": "arn:aws:health:us-east-1::event/SES/AWS_SES_OPERATIONAL_ISSUE/
AWS_SES_OPERATIONAL_ISSUE_URNDF_EXAMPLE111",
            "service": "SES",
            "eventTypeCode": "AWS_SES_OPERATIONAL_ISSUE",
            "eventTypeCategory": "issue",
            "region": "us-east-1",
            "startTime": 1585342008.46,
            "endTime": 1585344017.0,
            "lastUpdatedTime": 1585344355.989,
            "statusCode": "closed",
            "eventScopeCode": "PUBLIC"
        },
        {
            "arn": "arn:aws:health:global::event/IAM/
AWS_IAM_OPERATIONAL_NOTIFICATION/
AWS_IAM_OPERATIONAL_NOTIFICATION_b6771c34-6ecd-4aea-9d3e-EXAMPLE1117e",
            "service": "IAM",
            "eventTypeCode": "AWS_IAM_OPERATIONAL_NOTIFICATION",
            "eventTypeCategory": "accountNotification",
            "region": "global",
            "startTime": 1584978300.0,
            "lastUpdatedTime": 1584978553.572,
```

```
            "statusCode": "open",
            "eventScopeCode": "ACCOUNT_SPECIFIC"
        },
        {
            "arn": "arn:aws:health:ap-southeast-2::event/EC2/
AWS_EC2_OPERATIONAL_ISSUE/AWS_EC2_OPERATIONAL_ISSUE_HNGHE_EXAMPLE111",
            "service": "EC2",
            "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
            "eventTypeCategory": "issue",
            "region": "ap-southeast-2",
            "startTime": 1583881487.483,
            "endTime": 1583885056.785,
            "lastUpdatedTime": 1583885057.052,
            "statusCode": "closed",
            "eventScopeCode": "PUBLIC"
        }
    ]
}
```

Para obtener más información, consulte Getting started with your AWS Health Dashboard en la Guía del usuario de AWS Health.

Ejemplo 2: enumeración de los eventos de AWS Health por servicio y código de estado del evento

En el siguiente ejemplo de `describe-events`, se muestra una lista de los eventos de AWS Health para Amazon Elastic Compute Cloud (Amazon EC2) en los que el estado del evento es Cerrado.

```
aws health describe-events \
    --filter "services=EC2,eventStatusCodes=closed"
```

Salida:

```
{
    "events": [
        {
            "arn": "arn:aws:health:us-east-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE/
AWS_EC2_OPERATIONAL_ISSUE_VKTXI_EXAMPLE111",
            "service": "EC2",
            "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
            "eventTypeCategory": "issue",
```

```
            "region": "us-east-1",
            "startTime": 1587462325.096,
            "endTime": 1587464204.774,
            "lastUpdatedTime": 1587464204.865,
            "statusCode": "closed",
            "eventScopeCode": "PUBLIC"
        },
        {
            "arn": "arn:aws:health:us-east-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE/
AWS_EC2_OPERATIONAL_ISSUE_COBXJ_EXAMPLE111",
            "service": "EC2",
            "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
            "eventTypeCategory": "issue",
            "region": "us-east-1",
            "startTime": 1586473044.284,
            "endTime": 1586479706.091,
            "lastUpdatedTime": 1586479706.153,
            "statusCode": "closed",
            "eventScopeCode": "PUBLIC"
        },
        {
            "arn": "arn:aws:health:ap-southeast-2::event/EC2/
AWS_EC2_OPERATIONAL_ISSUE/AWS_EC2_OPERATIONAL_ISSUE_HNGHE_EXAMPLE111",
            "service": "EC2",
            "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
            "eventTypeCategory": "issue",
            "region": "ap-southeast-2",
            "startTime": 1583881487.483,
            "endTime": 1583885056.785,
            "lastUpdatedTime": 1583885057.052,
            "statusCode": "closed",
            "eventScopeCode": "PUBLIC"
        }
    ]
}
```

Para obtener más información, consulte Getting started with your AWS Health Dashboard en la Guía del usuario de AWS Health.

- Para obtener detalles sobre la API, consulte DescribeEvents en la Referencia de comandos de la AWS CLI.

Ejemplos de HealthImaging que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con HealthImaging.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`copy-image-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-image-set`.

AWS CLI

Ejemplo 1: copia de un conjunto de imágenes sin un destino.

El siguiente ejemplo de `copy-image-set` crea una copia duplicada de un conjunto de imágenes sin un destino.

```
aws medical-imaging copy-image-set \
    --datastore-id 12345678901234567890123456789012 \
    --source-image-set-id ea92b0d8838c72a3f25d00d13616f87e \
    --copy-image-set-information '{"sourceImageSet": {"latestVersionId": "1" } }'
```

Salida:

```
{
    "destinationImageSetProperties": {
        "latestVersionId": "2",
        "imageSetWorkflowStatus": "COPYING",
        "updatedAt": 1680042357.432,
```

```
        "imageSetId": "b9a06fef182a5f992842f77f8e0868e5",
        "imageSetState": "LOCKED",
        "createdAt": 1680042357.432
    },
    "sourceImageSetProperties": {
        "latestVersionId": "1",
        "imageSetWorkflowStatus": "COPYING_WITH_READ_ONLY_ACCESS",
        "updatedAt": 1680042357.432,
        "imageSetId": "ea92b0d8838c72a3f25d00d13616f87e",
        "imageSetState": "LOCKED",
        "createdAt": 1680027126.436
    },
    "datastoreId": "12345678901234567890123456789012"
}
```

Ejemplo 2: copia de un conjunto de imágenes con un destino.

El siguiente ejemplo de `copy-image-set` crea una copia duplicada de un conjunto de imágenes con un destino.

```
aws medical-imaging copy-image-set \
    --datastore-id 12345678901234567890123456789012 \
    --source-image-set-id ea92b0d8838c72a3f25d00d13616f87e \
    --copy-image-set-information '{"sourceImageSet": {"latestVersionId": "1" },
 "destinationImageSet": { "imageSetId": "b9a06fef182a5f992842f77f8e0868e5",
 "latestVersionId": "1"} }'
```

Salida:

```
{
    "destinationImageSetProperties": {
        "latestVersionId": "2",
        "imageSetWorkflowStatus": "COPYING",
        "updatedAt": 1680042505.135,
        "imageSetId": "b9a06fef182a5f992842f77f8e0868e5",
        "imageSetState": "LOCKED",
        "createdAt": 1680042357.432
    },
    "sourceImageSetProperties": {
        "latestVersionId": "1",
        "imageSetWorkflowStatus": "COPYING_WITH_READ_ONLY_ACCESS",
        "updatedAt": 1680042505.135,
        "imageSetId": "ea92b0d8838c72a3f25d00d13616f87e",
```

```
        "imageSetState": "LOCKED",
        "createdAt": 1680027126.436
    },
    "datastoreId": "12345678901234567890123456789012"
}
```

Ejemplo 3: copiar un subconjunto de instancias de un conjunto de imágenes de origen a un conjunto de imágenes de destino.

El siguiente ejemplo de `copy-image-set` copia una instancia de DICOM del conjunto de imágenes de origen al conjunto de imágenes de destino. El parámetro force se proporciona para anular las incoherencias en los atributos de nivel de paciente, estudio y serie.

```
aws medical-imaging copy-image-set \
    --datastore-id 12345678901234567890123456789012 \
    --source-image-set-id ea92b0d8838c72a3f25d00d13616f87e \
    --copy-image-set-information '{"sourceImageSet": {"latestVersionId":
 "1","DICOMCopies": {"copiableAttributes": "{\"SchemaVersion\":\"1.1\",\"Study\":
{\"Series\":{\"1.3.6.1.4.1.5962.99.1.3673257865.2104868982.1369432891697.3666.0\":
{\"Instances\":
{\"1.3.6.1.4.1.5962.99.1.3673257865.2104868982.1369432891697.3669.0\":
{}}}}}}"}},"destinationImageSet": {"imageSetId":
 "b9eb50d8ee682eb9fcf4acbf92f62bb7","latestVersionId": "1"}}' \
    --force
```

Salida:

```
{
    "destinationImageSetProperties": {
        "latestVersionId": "2",
        "imageSetWorkflowStatus": "COPYING",
        "updatedAt": 1680042505.135,
        "imageSetId": "b9eb50d8ee682eb9fcf4acbf92f62bb7",
        "imageSetState": "LOCKED",
        "createdAt": 1680042357.432
    },
    "sourceImageSetProperties": {
        "latestVersionId": "1",
        "imageSetWorkflowStatus": "COPYING_WITH_READ_ONLY_ACCESS",
        "updatedAt": 1680042505.135,
        "imageSetId": "ea92b0d8838c72a3f25d00d13616f87e",
        "imageSetState": "LOCKED",
```

```
        "createdAt": 1680027126.436
    },
    "datastoreId": "12345678901234567890123456789012"
}
```

Para obtener más información, consulte Copying an image set en la Guía para desarrolladores de AWS HealthImaging.

- Para obtener información sobre la API, consulte CopyImageSet en la Referencia de comandos de la AWS CLI.

`create-datastore`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-datastore`.

AWS CLI

Ejemplo 1: Creación de un almacén de datos

En el siguiente ejemplo de código `create-datastore` se crea un almacén de datos con el nombre `my-datastore`. Al crear un almacén de datos sin especificar un `--lossless-storage-format`, AWS HealthImaging toma como valor predeterminado HTJ2K (JPEG 2000 de alto rendimiento).

```
aws medical-imaging create-datastore \
    --datastore-name "my-datastore"
```

Salida:

```
{
    "datastoreId": "12345678901234567890123456789012",
    "datastoreStatus": "CREATING"
}
```

Ejemplo 2: Creación de un almacén de datos con el formato de almacenamiento JPEG 2000 sin pérdidas

Un almacén de datos configurado con el formato de almacenamiento JPEG 2000 sin pérdidas transcodificará y conservará los fotogramas de imagen sin pérdidas en formato JPEG 2000. A continuación, los fotogramas de imagen se pueden recuperar en JPEG 2000 sin pérdidas sin

necesidad de transcodificación. En el ejemplo de código `create-datastore` siguiente, se crea un almacén de datos configurado para el formato de almacenamiento JPEG 2000 sin pérdidas con el nombre `my-datastore`.

```
aws medical-imaging create-datastore \
    --datastore-name "my-datastore" \
    --lossless-storage-format JPEG_2000_LOSSLESS
```

Salida:

```
{
    "datastoreId": "12345678901234567890123456789012",
    "datastoreStatus": "CREATING"
}
```

Para obtener más información, consulte Creating a data store en la Guía para desarrolladores de AWS HealthImaging.

- Para obtener información sobre la API, consulte CreateDatastore en la Referencia de comandos de la AWS CLI.

`delete-datastore`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-datastore`.

AWS CLI

Eliminación de un almacén de datos

En el siguiente ejemplo de código `delete-datastore` se elimina un almacén de datos.

```
aws medical-imaging delete-datastore \
    --datastore-id "12345678901234567890123456789012"
```

Salida:

```
{
    "datastoreId": "12345678901234567890123456789012",
    "datastoreStatus": "DELETING"
}
```

Para obtener más información, consulte Deleting a data store en la Guía para desarrolladores de AWS HealthImaging.

- Para obtener información sobre la API, consulte DeleteDatastore en la Referencia de comandos de la AWS CLI.

`delete-image-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-image-set`.

AWS CLI

Eliminación de un conjunto de imágenes

En el siguiente ejemplo de código `delete-image-set` se elimina un conjunto de imágenes.

```
aws medical-imaging delete-image-set \
    --datastore-id 12345678901234567890123456789012 \
    --image-set-id ea92b0d8838c72a3f25d00d13616f87e
```

Salida:

```
{
    "imageSetWorkflowStatus": "DELETING",
    "imageSetId": "ea92b0d8838c72a3f25d00d13616f87e",
    "imageSetState": "LOCKED",
    "datastoreId": "12345678901234567890123456789012"
}
```

Para obtener más información, consulte Deleting an image set en la Guía para desarrolladores de AWS HealthImaging.

- Para obtener información sobre la API, consulte DeleteImageSet en la Referencia de comandos de la AWS CLI.

`get-datastore`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-datastore`.

AWS CLI

Ejemplo 1: Obtención de las propiedades de un almacén de datos

En el siguiente ejemplo de código `get-datastore` se obtienen las propiedades de un almacén de datos.

```
aws medical-imaging get-datastore \
    --datastore-id 12345678901234567890123456789012
```

Salida:

```
{
    "datastoreProperties": {
        "datastoreId": "12345678901234567890123456789012",
        "datastoreName": "TestDatastore123",
        "datastoreStatus": "ACTIVE",
        "losslessStorageFormat": "HTJ2K"
        "datastoreArn": "arn:aws:medical-imaging:us-
east-1:123456789012:datastore/12345678901234567890123456789012",
        "createdAt": "2022-11-15T23:33:09.643000+00:00",
        "updatedAt": "2022-11-15T23:33:09.643000+00:00"
    }
}
```

Ejemplo 2: Obtención de las propiedades del almacén de datos configuradas para JPEG2000

En el ejemplo de código `get-datastore` siguiente, se obtienen las propiedades de un almacén de datos configurado para el formato de almacenamiento JPEG 2000 sin pérdidas.

```
aws medical-imaging get-datastore \
    --datastore-id 12345678901234567890123456789012
```

Salida:

```
{
    "datastoreProperties": {
        "datastoreId": "12345678901234567890123456789012",
        "datastoreName": "TestDatastore123",
        "datastoreStatus": "ACTIVE",
        "losslessStorageFormat": "JPEG_2000_LOSSLESS",
        "datastoreArn": "arn:aws:medical-imaging:us-
east-1:123456789012:datastore/12345678901234567890123456789012",
        "createdAt": "2022-11-15T23:33:09.643000+00:00",
        "updatedAt": "2022-11-15T23:33:09.643000+00:00"
```

```
    }
}
```

Para obtener más información, consulte Getting data store properties en la Guía para desarrolladores de AWS HealthImaging.

- Para obtener información sobre la API, consulte GetDatastore en la Referencia de comandos de la AWS CLI.

`get-dicom-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-dicom-import-job`.

AWS CLI

Obtención de las propiedades de un trabajo de importación DICOM

En el siguiente ejemplo de código `get-dicom-import-job` se obtienen las propiedades de un trabajo de importación DICOM.

```
aws medical-imaging get-dicom-import-job \
    --datastore-id "12345678901234567890123456789012" \
    --job-id "09876543210987654321098765432109"
```

Salida:

```
{
    "jobProperties": {
        "jobId": "09876543210987654321098765432109",
        "jobName": "my-job",
        "jobStatus": "COMPLETED",
        "datastoreId": "12345678901234567890123456789012",
        "dataAccessRoleArn": "arn:aws:iam::123456789012:role/
ImportJobDataAccessRole",
        "endedAt": "2022-08-12T11:29:42.285000+00:00",
        "submittedAt": "2022-08-12T11:28:11.152000+00:00",
        "inputS3Uri": "s3://medical-imaging-dicom-input/dicom_input/",
        "outputS3Uri": "s3://medical-imaging-output/
job_output/12345678901234567890123456789012-
DicomImport-09876543210987654321098765432109/"
    }
```

```
}
```

Para obtener más información, consulte Getting import job properties en la Guía para desarrolladores de AWS HealthImaging.

- Para obtener información sobre la API, consulte GetDICOMImportJob en la Referencia de comandos de la AWS CLI.

`get-image-frame`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-image-frame`.

AWS CLI

Obtención de datos de píxeles de un conjunto de imágenes

En el siguiente ejemplo de código `get-image-frame` se obtiene un marco de una imagen.

```
aws medical-imaging get-image-frame \
    --datastore-id "12345678901234567890123456789012" \
    --image-set-id "98765412345612345678907890789012" \
    --image-frame-information imageFrameId=3abf5d5d7ae72f80a0ec81b2c0de3ef4 \
    imageframe.jph
```

Nota: Este código de ejemplo no incluye la salida porque la acción GetImageFrame devuelve un flujo de datos de píxeles al archivo imageframe.jph. Para obtener información sobre la decodificación y la visualización de marcos de imágenes, consulte las bibliotecas de decodificación HTJ2K.

Para obtener más información, consulte Getting image set pixel data en la Guía para desarrolladores de AWS HealthImaging.

- Para obtener información sobre la API, consulte GetImageFrame en la Referencia de comandos de la AWS CLI.

`get-image-set-metadata`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-image-set-metadata`.

AWS CLI

Ejemplo 1: obtención de los metadatos de un conjunto de imágenes sin versión

En el siguiente ejemplo de código `get-image-set-metadata` se obtienen los metadatos de un conjunto de imágenes sin especificar una versión.

Nota: El parámetro `outfile` es obligatorio

```
aws medical-imaging get-image-set-metadata \
    --datastore-id 12345678901234567890123456789012 \
    --image-set-id ea92b0d8838c72a3f25d00d13616f87e \
    studymetadata.json.gz
```

Los metadatos devueltos se comprimen con gzip y se almacenan en el archivo studymetadata.json.gz. Para ver el contenido del objeto JSON devuelto, primero debe descomprimirlo.

Salida:

```
{
    "contentType": "application/json",
    "contentEncoding": "gzip"
}
```

Ejemplo 2: obtención de los metadatos de un conjunto de imágenes con versión

En el siguiente ejemplo de código `get-image-set-metadata` se obtienen los metadatos de un conjunto de imágenes con una versión especificada.

Nota: El parámetro `outfile` es obligatorio

```
aws medical-imaging get-image-set-metadata \
    --datastore-id 12345678901234567890123456789012 \
    --image-set-id ea92b0d8838c72a3f25d00d13616f87e \
    --version-id 1 \
    studymetadata.json.gz
```

Los metadatos devueltos se comprimen con gzip y se almacenan en el archivo studymetadata.json.gz. Para ver el contenido del objeto JSON devuelto, primero debe descomprimirlo.

Salida:

```
{
    "contentType": "application/json",
```

```
    "contentEncoding": "gzip"
}
```

Para obtener más información, consulte Getting image set metadata en la Guía para desarrolladores de AWS HealthImaging.

- Para obtener información sobre la API, consulte GetImageSetMetadata en la Referencia de comandos de la AWS CLI.

`get-image-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-image-set`.

AWS CLI

Obtención de las propiedades de un conjunto de imágenes

En el siguiente ejemplo de código `get-image-set` se obtienen las propiedades de un conjunto de imágenes.

```
aws medical-imaging get-image-set \
    --datastore-id 12345678901234567890123456789012 \
    --image-set-id 18f88ac7870584f58d56256646b4d92b \
    --version-id 1
```

Salida:

```
{
    "versionId": "1",
    "imageSetWorkflowStatus": "COPIED",
    "updatedAt": 1680027253.471,
    "imageSetId": "18f88ac7870584f58d56256646b4d92b",
    "imageSetState": "ACTIVE",
    "createdAt": 1679592510.753,
    "datastoreId": "12345678901234567890123456789012"
}
```

Para obtener más información, consulte Getting image set properties en la Guía para desarrolladores de AWS HealthImaging.

- Para obtener información sobre la API, consulte GetImageSet en la Referencia de comandos de la AWS CLI.

`list-datastores`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-datastores`.

AWS CLI

Enumeración de almacenes de datos

En el siguiente ejemplo de código `list-datastores` se enumeran los almacenes de datos disponibles.

```
aws medical-imaging list-datastores
```

Salida:

```
{
    "datastoreSummaries": [
        {
            "datastoreId": "12345678901234567890123456789012",
            "datastoreName": "TestDatastore123",
            "datastoreStatus": "ACTIVE",
            "datastoreArn": "arn:aws:medical-imaging:us-
east-1:123456789012:datastore/12345678901234567890123456789012",
            "createdAt": "2022-11-15T23:33:09.643000+00:00",
            "updatedAt": "2022-11-15T23:33:09.643000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Listing data stores en la Guía para desarrolladores de AWS HealthImaging.

- Para obtener información sobre la API, consulte ListDatastores en la Referencia de comandos de la AWS CLI.

`list-dicom-import-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-dicom-import-jobs`.

AWS CLI

Enumeración de los trabajos de importación DICOM

En el siguiente ejemplo de código `list-dicom-import-jobs` se enumeran los trabajos de importación DICOM.

```
aws medical-imaging list-dicom-import-jobs \
    --datastore-id "12345678901234567890123456789012"
```

Salida:

```
{
    "jobSummaries": [
        {
            "jobId": "09876543210987654321098765432109",
            "jobName": "my-job",
            "jobStatus": "COMPLETED",
            "datastoreId": "12345678901234567890123456789012",
            "dataAccessRoleArn": "arn:aws:iam::123456789012:role/
ImportJobDataAccessRole",
            "endedAt": "2022-08-12T11:21:56.504000+00:00",
            "submittedAt": "2022-08-12T11:20:21.734000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Listing import jobs en la Guía para desarrolladores de AWS HealthImaging.

- Para obtener información sobre la API, consulte ListDICOMImportJobs en la Referencia de comandos de la AWS CLI.

`list-image-set-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-image-set-versions`.

AWS CLI

Enumeración de las versiones de un conjunto de imágenes

En el siguiente ejemplo de código `list-image-set-versions` se enumera el historial de versiones de un conjunto de imágenes.

```
aws medical-imaging list-image-set-versions \
```

```
    --datastore-id 12345678901234567890123456789012 \
    --image-set-id ea92b0d8838c72a3f25d00d13616f87e
```

Salida:

```
{
    "imageSetPropertiesList": [
        {
            "ImageSetWorkflowStatus": "UPDATED",
            "versionId": "4",
            "updatedAt": 1680029436.304,
            "imageSetId": "ea92b0d8838c72a3f25d00d13616f87e",
            "imageSetState": "ACTIVE",
            "createdAt": 1680027126.436
        },
        {
            "ImageSetWorkflowStatus": "UPDATED",
            "versionId": "3",
            "updatedAt": 1680029163.325,
            "imageSetId": "ea92b0d8838c72a3f25d00d13616f87e",
            "imageSetState": "ACTIVE",
            "createdAt": 1680027126.436
        },
        {
            "ImageSetWorkflowStatus": "COPY_FAILED",
            "versionId": "2",
            "updatedAt": 1680027455.944,
            "imageSetId": "ea92b0d8838c72a3f25d00d13616f87e",
            "imageSetState": "ACTIVE",
            "message": "INVALID_REQUEST:  Series of SourceImageSet and
 DestinationImageSet don't match.",
            "createdAt": 1680027126.436
        },
        {
            "imageSetId": "ea92b0d8838c72a3f25d00d13616f87e",
            "imageSetState": "ACTIVE",
            "versionId": "1",
            "ImageSetWorkflowStatus": "COPIED",
            "createdAt": 1680027126.436
        }
    ]
}
```

Para obtener más información, consulte Listing image set versions en la Guía para desarrolladores de AWS HealthImaging.

- Para obtener información sobre la API, consulte ListImageSetVersions en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Ejemplo 1: enumeración de las etiquetas de recursos de un almacén de datos

En el siguiente ejemplo de código `list-tags-for-resource` se enumeran las etiquetas de un almacén de datos.

```
aws medical-imaging list-tags-for-resource \
    --resource-arn "arn:aws:medical-imaging:us-
east-1:123456789012:datastore/12345678901234567890123456789012"
```

Salida:

```
{
    "tags":{
        "Deployment":"Development"
    }
}
```

Ejemplo 2: enumeración de las etiquetas de recursos de un conjunto de imágenes

En el siguiente ejemplo de código `list-tags-for-resource` se enumeran las etiquetas de un conjunto de imágenes.

```
aws medical-imaging list-tags-for-resource \
    --resource-arn "arn:aws:medical-imaging:us-
east-1:123456789012:datastore/12345678901234567890123456789012/
imageset/18f88ac7870584f58d56256646b4d92b"
```

Salida:

```
{
    "tags":{
        "Deployment":"Development"
    }
}
```

Para obtener más información, consulte Tagging resources with AWS HealthImaging en la Guía para desarrolladores de AWS HealthImaging.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`search-image-sets`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-image-sets`.

AWS CLI

Ejemplo 1: búsqueda de conjuntos de imágenes con un operador EQUAL

En el siguiente ejemplo de código `search-image-sets` se usa el operador EQUAL para buscar conjuntos de imágenes en función de un valor específico.

```
aws medical-imaging search-image-sets \
    --datastore-id 12345678901234567890123456789012 \
    --search-criteria file://search-criteria.json
```

Contenido de `search-criteria.json`

```
{
    "filters": [{
        "values": [{"DICOMPatientId" : "SUBJECT08701"}],
        "operator": "EQUAL"
    }]
}
```

Salida:

```
{
    "imageSetsMetadataSummaries": [{
```

```
        "imageSetId": "09876543210987654321098765432109",
        "createdAt": "2022-12-06T21:40:59.429000+00:00",
        "version": 1,
        "DICOMTags": {
            "DICOMStudyId": "2011201407",
            "DICOMStudyDate": "19991122",
             "DICOMPatientSex": "F",
             "DICOMStudyInstanceUID": "1.2.840.99999999.84710745.943275268089",
             "DICOMPatientBirthDate": "19201120",
             "DICOMStudyDescription": "UNKNOWN",
             "DICOMPatientId": "SUBJECT08701",
             "DICOMPatientName": "Melissa844 Huel628",
             "DICOMNumberOfStudyRelatedInstances": 1,
             "DICOMStudyTime": "140728",
             "DICOMNumberOfStudyRelatedSeries": 1
            },
        "updatedAt": "2022-12-06T21:40:59.429000+00:00"
    }]
}
```

Ejemplo 2: búsqueda de conjuntos de imágenes con un operador BETWEEN mediante DICOMStudyDate y DICOMStudyTime

En el siguiente ejemplo de código `search-image-sets` se buscan conjuntos de imágenes con estudios DICOM generados entre el 1 de enero de 1990 (00:00 h) y el 1 de enero de 2023 (00:00 h).

Nota: DICOMStudyTime es opcional. Si no está presente, el valor de hora de las fechas indicado para el filtrado es a las 00:00 h (inicio del día).

```
aws medical-imaging search-image-sets \
    --datastore-id 12345678901234567890123456789012 \
    --search-criteria file://search-criteria.json
```

Contenido de `search-criteria.json`

```
{
    "filters": [{
        "values": [{
            "DICOMStudyDateAndTime": {
                "DICOMStudyDate": "19900101",
                "DICOMStudyTime": "000000"
```

```
            }
        },
        {
            "DICOMStudyDateAndTime": {
                "DICOMStudyDate": "20230101",
                "DICOMStudyTime": "000000"
            }
        }],
        "operator": "BETWEEN"
    }]
}
```

Salida:

```
{
    "imageSetsMetadataSummaries": [{
        "imageSetId": "09876543210987654321098765432109",
        "createdAt": "2022-12-06T21:40:59.429000+00:00",
        "version": 1,
        "DICOMTags": {
            "DICOMStudyId": "2011201407",
            "DICOMStudyDate": "19991122",
            "DICOMPatientSex": "F",
            "DICOMStudyInstanceUID": "1.2.840.99999999.84710745.943275268089",
            "DICOMPatientBirthDate": "19201120",
            "DICOMStudyDescription": "UNKNOWN",
            "DICOMPatientId": "SUBJECT08701",
            "DICOMPatientName": "Melissa844 Huel628",
            "DICOMNumberOfStudyRelatedInstances": 1,
            "DICOMStudyTime": "140728",
            "DICOMNumberOfStudyRelatedSeries": 1
        },
        "updatedAt": "2022-12-06T21:40:59.429000+00:00"
    }]
}
```

Ejemplo 3: búsqueda de conjuntos de imágenes con un operador BETWEEN mediante createdAt (los estudios de tiempo se conservaban previamente)

En el siguiente ejemplo de código `search-image-sets` se buscan conjuntos de imágenes con estudios DICOM que se conservan en HealthImaging entre los periodos de tiempo de la zona horaria UTC.

Nota: Ingrese createdAt en el formato de ejemplo (“1985-04-12T23:20:50.52Z”).

```
aws medical-imaging search-image-sets \
    --datastore-id 12345678901234567890123456789012 \
    --search-criteria  file://search-criteria.json
```

Contenido de `search-criteria.json`

```
{
    "filters": [{
        "values": [{
            "createdAt": "1985-04-12T23:20:50.52Z"
        },
        {
            "createdAt": "2022-04-12T23:20:50.52Z"
        }],
        "operator": "BETWEEN"
    }]
}
```

Salida:

```
{
    "imageSetsMetadataSummaries": [{
        "imageSetId": "09876543210987654321098765432109",
        "createdAt": "2022-12-06T21:40:59.429000+00:00",
        "version": 1,
        "DICOMTags": {
            "DICOMStudyId": "2011201407",
            "DICOMStudyDate": "19991122",
            "DICOMPatientSex": "F",
            "DICOMStudyInstanceUID": "1.2.840.99999999.84710745.943275268089",
            "DICOMPatientBirthDate": "19201120",
            "DICOMStudyDescription": "UNKNOWN",
            "DICOMPatientId": "SUBJECT08701",
            "DICOMPatientName": "Melissa844 Huel628",
            "DICOMNumberOfStudyRelatedInstances": 1,
            "DICOMStudyTime": "140728",
            "DICOMNumberOfStudyRelatedSeries": 1
        },
        "lastUpdatedAt": "2022-12-06T21:40:59.429000+00:00"
    }]
```

```
}
```

Ejemplo 4: buscar conjuntos de imágenes con un operador EQUAL en DICOMSeriesInstanceUID y BETWEEN en updatedAt y ordenar la respuesta en orden ASC en el campo updatedAt

El siguiente código `search-image-sets` busca conjuntos de imágenes con un operador EQUAL en DICOMSeriesInstanceUID y BETWEEN en updatedAt y ordena la respuesta en orden ASC en el campo updatedAt.

Nota: Introduzca updatedAt en el formato de ejemplo ("1985-04-12T23:20:50.52Z").

```
aws medical-imaging search-image-sets \
    --datastore-id 12345678901234567890123456789012 \
    --search-criteria  file://search-criteria.json
```

Contenido de `search-criteria.json`

```
{
    "filters": [{
        "values": [{
            "updatedAt": "2024-03-11T15:00:05.074000-07:00"
        }, {
            "updatedAt": "2024-03-11T16:00:05.074000-07:00"
        }],
        "operator": "BETWEEN"
    }, {
        "values": [{
            "DICOMSeriesInstanceUID": "1.2.840.99999999.84710745.943275268089"
        }],
        "operator": "EQUAL"
    }],
    "sort": {
        "sortField": "updatedAt",
        "sortOrder": "ASC"
    }
}
```

Salida:

```
{
    "imageSetsMetadataSummaries": [{
        "imageSetId": "09876543210987654321098765432109",
```

```
        "createdAt": "2022-12-06T21:40:59.429000+00:00",
        "version": 1,
        "DICOMTags": {
            "DICOMStudyId": "2011201407",
            "DICOMStudyDate": "19991122",
            "DICOMPatientSex": "F",
            "DICOMStudyInstanceUID": "1.2.840.99999999.84710745.943275268089",
            "DICOMPatientBirthDate": "19201120",
            "DICOMStudyDescription": "UNKNOWN",
            "DICOMPatientId": "SUBJECT08701",
            "DICOMPatientName": "Melissa844 Huel628",
            "DICOMNumberOfStudyRelatedInstances": 1,
            "DICOMStudyTime": "140728",
            "DICOMNumberOfStudyRelatedSeries": 1
        },
        "lastUpdatedAt": "2022-12-06T21:40:59.429000+00:00"
    }]
}
```

Para obtener más información, consulte Searching image sets en la Guía para desarrolladores de AWS HealthImaging.

- Para obtener información sobre la API, consulte SearchImageSets en la Referencia de comandos de la AWS CLI.

`start-dicom-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-dicom-import-job`.

AWS CLI

Inicio de un trabajo de importación DICOM

En el siguiente ejemplo de código `start-dicom-import-job` se inicia un trabajo de importación DICOM.

```
aws medical-imaging start-dicom-import-job \
    --job-name "my-job" \
    --datastore-id "12345678901234567890123456789012" \
    --input-s3-uri "s3://medical-imaging-dicom-input/dicom_input/" \
    --output-s3-uri "s3://medical-imaging-output/job_output/" \
    --data-access-role-arn "arn:aws:iam::123456789012:role/ImportJobDataAccessRole"
```

Salida:

```
{
    "datastoreId": "12345678901234567890123456789012",
    "jobId": "09876543210987654321098765432109",
    "jobStatus": "SUBMITTED",
    "submittedAt": "2022-08-12T11:28:11.152000+00:00"
}
```

Para obtener más información, consulte Starting an import job en la Guía para desarrolladores de AWS HealthImaging.

- Para obtener información sobre la API, consulte StartDICOMImportJob en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Ejemplo 1: etiquetado de un almacén de datos

En los siguientes ejemplos de código `tag-resource` se etiqueta un almacén de datos.

```
aws medical-imaging tag-resource \
  --resource-arn "arn:aws:medical-imaging:us-
east-1:123456789012:datastore/12345678901234567890123456789012" \
  --tags '{"Deployment":"Development"}'
```

Este comando no genera ninguna salida.

Ejemplo 2: etiquetado de un conjunto de imágenes

En los siguientes ejemplos de código `tag-resource` se etiqueta un conjunto de imágenes.

```
aws medical-imaging tag-resource \
    --resource-arn "arn:aws:medical-imaging:us-
east-1:123456789012:datastore/12345678901234567890123456789012/
imageset/18f88ac7870584f58d56256646b4d92b" \
    --tags '{"Deployment":"Development"}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging resources with AWS HealthImaging en la Guía para desarrolladores de AWS HealthImaging.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Ejemplo 1: eliminación de las etiquetas de un almacén de datos

En el siguiente ejemplo de código `untag-resource` se eliminan las etiquetas de un almacén de datos.

```
aws medical-imaging untag-resource \
    --resource-arn "arn:aws:medical-imaging:us-
east-1:123456789012:datastore/12345678901234567890123456789012" \
    --tag-keys '["Deployment"]'
```

Este comando no genera ninguna salida.

Ejemplo 2: eliminación de las etiquetas de un conjunto de imágenes

En el siguiente ejemplo de código `untag-resource` se eliminan las etiquetas de un conjunto de imágenes.

```
aws medical-imaging untag-resource \
    --resource-arn "arn:aws:medical-imaging:us-
east-1:123456789012:datastore/12345678901234567890123456789012/
imageset/18f88ac7870584f58d56256646b4d92b" \
    --tag-keys '["Deployment"]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging resources with AWS HealthImaging en la Guía para desarrolladores de AWS HealthImaging.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-image-set-metadata`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-image-set-metadata`.

AWS CLI

Ejemplo 1: insertar o actualizar un atributo en los metadatos del conjunto de imágenes

El siguiente ejemplo de `update-image-set-metadata` inserta o actualiza un atributo en los metadatos del conjunto de imágenes

```
aws medical-imaging update-image-set-metadata \
    --datastore-id 12345678901234567890123456789012 \
    --image-set-id ea92b0d8838c72a3f25d00d13616f87e \
    --latest-version-id 1 \
    --cli-binary-format raw-in-base64-out \
    --update-image-set-metadata-updates file://metadata-updates.json
```

Contenido de `metadata-updates.json`

```
{
    "DICOMUpdates": {
        "updatableAttributes": "{\"SchemaVersion\":1.1,\"Patient\":{\"DICOM\":
{\"PatientName\":\"MX^MX\"}}}"
    }
}
```

Salida:

```
{
    "latestVersionId": "2",
    "imageSetWorkflowStatus": "UPDATING",
    "updatedAt": 1680042257.908,
    "imageSetId": "ea92b0d8838c72a3f25d00d13616f87e",
    "imageSetState": "LOCKED",
    "createdAt": 1680027126.436,
    "datastoreId": "12345678901234567890123456789012"
}
```

Ejemplo 2: eliminar un atributo de los metadatos del conjunto de imágenes

El siguiente ejemplo de `update-image-set-metadata` elimina un atributo de los metadatos del conjunto de imágenes

```
aws medical-imaging update-image-set-metadata \
    --datastore-id 12345678901234567890123456789012 \
    --image-set-id ea92b0d8838c72a3f25d00d13616f87e \
    --latest-version-id 1 \
    --cli-binary-format raw-in-base64-out \
    --update-image-set-metadata-updates file://metadata-updates.json
```

Contenido de `metadata-updates.json`

```
{
    "DICOMUpdates": {
        "removableAttributes": "{\"SchemaVersion\":1.1,\"Study\":{\"DICOM\":
{\"StudyDescription\":\"CHEST\"}}}"
    }
}
```

Salida:

```
{
    "latestVersionId": "2",
    "imageSetWorkflowStatus": "UPDATING",
    "updatedAt": 1680042257.908,
    "imageSetId": "ea92b0d8838c72a3f25d00d13616f87e",
    "imageSetState": "LOCKED",
    "createdAt": 1680027126.436,
    "datastoreId": "12345678901234567890123456789012"
}
```

Ejemplo 3: eliminar una instancia de los metadatos del conjunto de imágenes

El siguiente ejemplo de `update-image-set-metadata` elimina una instancia de los metadatos del conjunto de imágenes

```
aws medical-imaging update-image-set-metadata \
    --datastore-id 12345678901234567890123456789012 \
    --image-set-id ea92b0d8838c72a3f25d00d13616f87e \
```

```
    --latest-version-id 1 \
    --cli-binary-format raw-in-base64-out \
    --update-image-set-metadata-updates file://metadata-updates.json
```

Contenido de `metadata-updates.json`

```
{
    "DICOMUpdates": {
        "removableAttributes": "{\"SchemaVersion\": 1.1,\"Study\": {\"Series
\": {\"1.1.1.1.1.1.12345.123456789012.123.12345678901234.1\": {\"Instances\":
 {\"1.1.1.1.1.1.12345.123456789012.123.12345678901234.1\": {}}}}}}"
    }
}
```

Salida:

```
{
    "latestVersionId": "2",
    "imageSetWorkflowStatus": "UPDATING",
    "updatedAt": 1680042257.908,
    "imageSetId": "ea92b0d8838c72a3f25d00d13616f87e",
    "imageSetState": "LOCKED",
    "createdAt": 1680027126.436,
    "datastoreId": "12345678901234567890123456789012"
}
```

Ejemplo 4: revertir un conjunto de imágenes a una versión anterior

El siguiente ejemplo de `update-image-set-metadata` muestra cómo revertir un conjunto de imágenes a una versión anterior. Las acciones CopyImageSet y UpdateImageSetMetadata crean nuevas versiones de los conjuntos de imágenes.

```
aws medical-imaging update-image-set-metadata \
    --datastore-id 12345678901234567890123456789012 \
    --image-set-id 53d5fdb05ca4d46ac7ca64b06545c66e \
    --latest-version-id 3 \
    --cli-binary-format raw-in-base64-out \
    --update-image-set-metadata-updates '{"revertToVersionId": "1"}'
```

Salida:

```
{
    "datastoreId": "12345678901234567890123456789012",
    "imageSetId": "53d5fdb05ca4d46ac7ca64b06545c66e",
    "latestVersionId": "4",
    "imageSetState": "LOCKED",
    "imageSetWorkflowStatus": "UPDATING",
    "createdAt": 1680027126.436,
    "updatedAt": 1680042257.908
}
```

Ejemplo 5: añadir un elemento de datos DICOM privado a una instancia

El siguiente ejemplo de `update-image-set-metadata` muestra cómo añadir un elemento privado a una instancia específica en un conjunto de imágenes. El estándar DICOM permite que los elementos de datos privados comuniquen información que no puede estar contenida en elementos de datos estándar. Puede crear, actualizar y eliminar elementos de datos privados con la acción UpdateImageSetMetadata.

```
aws medical-imaging update-image-set-metadata \
    --datastore-id 12345678901234567890123456789012 \
    --image-set-id 53d5fdb05ca4d46ac7ca64b06545c66e \
    --latest-version-id 1 \
    --cli-binary-format raw-in-base64-out \
    --force \
    --update-image-set-metadata-updates file://metadata-updates.json
```

Contenido de `metadata-updates.json`

```
{
    "DICOMUpdates": {
        "updatableAttributes": "{\"SchemaVersion\": 1.1,\"Study\": {\"Series
\": {\"1.1.1.1.1.1.12345.123456789012.123.12345678901234.1\": {\"Instances
\": {\"1.1.1.1.1.1.12345.123456789012.123.12345678901234.1\": {\"DICOM\":
 {\"001910F9\": \"97\"},\"DICOMVRs\": {\"001910F9\": \"DS\"}}}}}}"
    }
}
```

Salida:

```
{
```

```
    "latestVersionId": "2",
    "imageSetWorkflowStatus": "UPDATING",
    "updatedAt": 1680042257.908,
    "imageSetId": "53d5fdb05ca4d46ac7ca64b06545c66e",
    "imageSetState": "LOCKED",
    "createdAt": 1680027126.436,
    "datastoreId": "12345678901234567890123456789012"
}
```

Ejemplo 6: actualizar un elemento de datos DICOM privado a una instancia

El siguiente ejemplo de `update-image-set-metadata` muestra cómo actualizar el valor de un elemento de datos privado que pertenece a una instancia en un conjunto de imágenes.

```
aws medical-imaging update-image-set-metadata \
    --datastore-id 12345678901234567890123456789012 \
    --image-set-id 53d5fdb05ca4d46ac7ca64b06545c66e \
    --latest-version-id 1 \
    --cli-binary-format raw-in-base64-out \
    --force \
    --update-image-set-metadata-updates file://metadata-updates.json
```

Contenido de `metadata-updates.json`

```
{
    "DICOMUpdates": {
        "updatableAttributes": "{\"SchemaVersion\": 1.1,\"Study\": {\"Series
\": {\"1.1.1.1.1.1.12345.123456789012.123.12345678901234.1\": {\"Instances
\": {\"1.1.1.1.1.1.12345.123456789012.123.12345678901234.1\": {\"DICOM\":
 {\"00091001\": \"GE_GENESIS_DD\"}}}}}}"
    }
}
```

Salida:

```
{
    "latestVersionId": "2",
    "imageSetWorkflowStatus": "UPDATING",
    "updatedAt": 1680042257.908,
    "imageSetId": "53d5fdb05ca4d46ac7ca64b06545c66e",
    "imageSetState": "LOCKED",
```

```
    "createdAt": 1680027126.436,
    "datastoreId": "12345678901234567890123456789012"
}
```

Ejemplo 7: actualizar un SOPInstanceUID con el parámetro force

En el siguiente ejemplo de `update-image-set-metadata`, se muestra cómo actualizar un SOPInstanceUID mediante el parámetro force para anular las restricciones de metadatos de DICOM.

```
aws medical-imaging update-image-set-metadata \
        --datastore-id 12345678901234567890123456789012 \
        --image-set-id 53d5fdb05ca4d46ac7ca64b06545c66e \
        --latest-version-id 1 \
        --cli-binary-format raw-in-base64-out \
        --force \
        --update-image-set-metadata-updates file://metadata-updates.json
```

Contenido de `metadata-updates.json`

```
{
    "DICOMUpdates": {
        "updatableAttributes": "{\"SchemaVersion\":1.1,\"Study\":{\"Series\":
{\"1.3.6.1.4.1.5962.99.1.3633258862.2104868982.1369432891697.3656.0\":{\"Instances
\":{\"1.3.6.1.4.1.5962.99.1.3633258862.2104868982.1369432891697.3659.0\":{\"DICOM\":
{\"SOPInstanceUID\":
\"1.3.6.1.4.1.5962.99.1.3633258862.2104868982.1369432891697.3659.9\"}}}}}}"
    }
}
```

Salida:

```
{
    "latestVersionId": "2",
    "imageSetWorkflowStatus": "UPDATING",
    "updatedAt": 1680042257.908,
    "imageSetId": "53d5fdb05ca4d46ac7ca64b06545c66e",
    "imageSetState": "LOCKED",
    "createdAt": 1680027126.436,
    "datastoreId": "12345678901234567890123456789012"
}
```

Para obtener más información, consulte Updating image set metadata en la Guía para desarrolladores de AWS HealthImaging.

- Para obtener información sobre la API, consulte UpdateImageSetMetadata en la Referencia de comandos de la AWS CLI.

Ejemplos de HealthLake que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con HealthLake.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-fhir-datastore`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-fhir-datastore`.

AWS CLI

Ejemplo 1: creación de un almacén de datos de HealthLake compatible con SigV4

En el siguiente ejemplo de `create-fhir-datastore`, se muestra cómo crear un nuevo almacén de datos en AWS HealthLake.

```
aws healthlake create-fhir-datastore \
    --datastore-type-version R4 \
    --datastore-name "FhirTestDatastore"
```

Salida:

```
{
    "DatastoreEndpoint": "https://healthlake.us-east-1.amazonaws.com/datastore/(Data
 store ID)/r4/",
    "DatastoreArn": "arn:aws:healthlake:us-east-1:(AWS Account ID):datastore/(Data
 store ID)",
    "DatastoreStatus": "CREATING",
    "DatastoreId": "(Data store ID)"
}
```

Ejemplo 2: creación de SMART en un almacén de datos de HealthLake compatible con FHIR

En el siguiente ejemplo de `create-fhir-datastore`, se muestra cómo crear un nuevo SMART en el almacén de datos habilitado por FHIR en AWS HealthLake.

```
aws healthlake create-fhir-datastore \
    --datastore-name "your-data-store-name" \
    --datastore-type-version R4 \
    --preload-data-config PreloadDataType="SYNTHEA" \
    --sse-configuration '{ "KmsEncryptionConfig": {  "CmkType":
 "CUSTOMER_MANAGED_KMS_KEY", "KmsKeyId": "arn:aws:kms:us-east-1:your-account-id:key/
your-key-id" } }' \
    --identity-provider-configuration  file://identity_provider_configuration.json
```

Contenido de `identity_provider_configuration.json`:

```
{
    "AuthorizationStrategy": "SMART_ON_FHIR_V1",
    "FineGrainedAuthorizationEnabled": true,
    "IdpLambdaArn": "arn:aws:lambda:your-region:your-account-id:function:your-
lambda-name",
    "Metadata": "{\"issuer\":\"https://ehr.example.com\", \"jwks_uri\":\"https://
ehr.example.com/.well-known/jwks.json\",\"authorization_endpoint\":\"https://
ehr.example.com/auth/authorize\",\"token_endpoint\":\"https://ehr.token.com/auth/
token\",\"token_endpoint_auth_methods_supported\":[\"client_secret_basic\",\"foo\"],
\"grant_types_supported\":[\"client_credential\",\"foo\"],\"registration_endpoint\":
\"https://ehr.example.com/auth/register\",\"scopes_supported\":[\"openId\",\"profile
\",\"launch\"],\"response_types_supported\":[\"code\"],\"management_endpoint\":
\"https://ehr.example.com/user/manage\",\"introspection_endpoint\":\"https://
ehr.example.com/user/introspect\",\"revocation_endpoint\":\"https://ehr.example.com/
user/revoke\",\"code_challenge_methods_supported\":[\"S256\"],\"capabilities\":
[\"launch-ehr\",\"sso-openid-connect\",\"client-public\"]}"
}
```

Salida:

```
{
    "DatastoreEndpoint": "https://healthlake.us-east-1.amazonaws.com/datastore/(Data
 store ID)/r4/",
    "DatastoreArn": "arn:aws:healthlake:us-east-1:(AWS Account ID):datastore/(Data
 store ID)",
    "DatastoreStatus": "CREATING",
    "DatastoreId": "(Data store ID)"
}
```

Para obtener más información, consulte Creación y supervisión de un almacén de datos de FHIR en la Guía para desarrolladores de AWS HealthLake.

- Para obtener información sobre la API, consulte CreateFHIRDatastore en la Referencia de comandos de la AWS CLI.

`delete-fhir-datastore`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-fhir-datastore`.

AWS CLI

Eliminación de un almacén de datos de FHIR

En el siguiente ejemplo de `delete-fhir-datastore`, se muestra cómo eliminar un almacén de datos y todo su contenido en AWS HealthLake.

```
aws healthlake delete-fhir-datastore \
    --datastore-id (Data store ID)
```

Salida:

```
{
    "DatastoreEndpoint": "https://healthlake.us-east-1.amazonaws.com/datastore/(Data
 store ID)/r4/",
    "DatastoreArn": "arn:aws:healthlake:us-east-1:(AWS Account ID):datastore/(Data
 store ID)",
    "DatastoreStatus": "DELETING",
    "DatastoreId": "(Data store ID)"
}
```

Para obtener más información, consulte Creación y supervisión de un almacén de datos de FHIR <https://docs.aws.amazon.com/healthlake/latest/devguide/working-with-FHIR-healthlake.html> en la Guía para desarrolladores de AWS HealthLake.

- Para obtener información sobre la API, consulte DeleteFHIRDatastore en la Referencia de comandos de la AWS CLI.

`describe-fhir-datastore`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fhir-datastore`.

AWS CLI

Descripción de un almacén de datos de FHIR

En el siguiente ejemplo de `describe-fhir-datastore`, se muestra cómo encontrar las propiedades de un almacén de datos en AWS HealthLake.

```
aws healthlake describe-fhir-datastore \
    --datastore-id "1f2f459836ac6c513ce899f9e4f66a59"
```

Salida:

```
{
    "DatastoreProperties": {
        "PreloadDataConfig": {
            "PreloadDataType": "SYNTHEA"
        },
        "SseConfiguration": {
            "KmsEncryptionConfig": {
                "CmkType": "CUSTOMER_MANAGED_KMS_KEY",
                "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            }
        },
        "DatastoreName": "Demo",
        "DatastoreArn": "arn:aws:healthlake:us-east-1:<AWS Account ID>:datastore/
<Data store ID>",
        "DatastoreEndpoint": "https://healthlake.us-east-1.amazonaws.com/datastore/
<Data store ID>/r4/",
        "DatastoreStatus": "ACTIVE",
        "DatastoreTypeVersion": "R4",
```

```
        "CreatedAt": 1603761064.881,
        "DatastoreId": "<Data store ID>",
        "IdentityProviderConfiguration": {
            "AuthorizationStrategy": "AWS_AUTH",
            "FineGrainedAuthorizationEnabled": false
        }
    }
}
```

Para obtener más información, consulte Creación y supervisión de un almacén de datos de FHIR en la Guía para desarrolladores de AWS HealthLake.

- Para obtener información sobre la API, consulte DescribeFHIRDatastore en la Referencia de comandos de la AWS CLI.

`describe-fhir-export-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fhir-export-job`.

AWS CLI

Para describir un trabajo de exportación de FHIR

En el siguiente ejemplo de `describe-fhir-export-job`, se muestra cómo encontrar las propiedades de un trabajo de exportación de FHIR en AWS HealthLake.

```
aws healthlake describe-fhir-export-job \
    --datastore-id (Data store ID) \
    --job-id 9b9a51943afaedd0a8c0c26c49135a31
```

Salida:

```
{
    "ExportJobProperties": {
        "DataAccessRoleArn": "arn:aws:iam::(AWS Account ID):role/(Role Name)",
        "JobStatus": "IN_PROGRESS",
        "JobId": "9009813e9d69ba7cf79bcb3468780f16",
        "SubmitTime": "2024-11-20T11:31:46.672000-05:00",
        "EndTime": "2024-11-20T11:34:01.636000-05:00",
        "OutputDataConfig": {
            "S3Configuration": {
            "S3Uri": "s3://(Bucket Name)/(Prefix Name)/",
```

```
            "KmsKeyId": "arn:aws:kms:us-east-1:012345678910:key/d330e7fc-b56c-4216-
a250-f4c43ef46e83"
        }

        },
        "DatastoreId": "(Data store ID)"
    }
}
```

Para obtener más información, consulte Exportación de archivos de un almacén de datos de FHIR en la Guía para desarrolladores de AWS HealthLake.

- Para obtener información sobre la API, consulte DescribeFHIRExportJob en la Referencia de comandos de la AWS CLI.

`describe-fhir-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-fhir-import-job`.

AWS CLI

Para describir un trabajo de importación de FHIR

En el siguiente ejemplo de `describe-fhir-import-job`, se muestra cómo obtener información sobre las propiedades de un trabajo de importación de FHIR mediante AWS HealthLake.

```
aws healthlake describe-fhir-import-job \
    --datastore-id (Data store ID) \
    --job-id c145fbb27b192af392f8ce6e7838e34f
```

Salida:

```
{
    "ImportJobProperties": {
    "InputDataConfig": {
        "S3Uri": "s3://(Bucket Name)/(Prefix Name)/"
        { "arrayitem2": 2 }
    },
    "DataAccessRoleArn": "arn:aws:iam::(AWS Account ID):role/(Role Name)",
    "JobStatus": "COMPLETED",
```

```
    "JobId": "c145fbb27b192af392f8ce6e7838e34f",
    "SubmitTime": 1606272542.161,
    "EndTime": 1606272609.497,
    "DatastoreId": "(Data store ID)"
    }
}
```

Para obtener más información, consulte Importación de archivos a un almacén de datos de FHIR en la Guía para desarrolladores de AWS HealthLake.

- Para obtener información sobre la API, consulte DescribeFHIRImportJob en la Referencia de comandos de la AWS CLI.

`list-fhir-datastores`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-fhir-datastores`.

AWS CLI

Muestra de los almacenes de datos de FHIR

En el siguiente ejemplo de `list-fhir-datastores`, se muestra cómo utilizar el comando y de qué manera los usuarios pueden filtrar los resultados en función del estado del almacén de datos en AWS HealthLake.

```
aws healthlake list-fhir-datastores \
    --filter DatastoreStatus=ACTIVE
```

Salida:

```
{
    "DatastorePropertiesList": [
    {
        "PreloadDataConfig": {
            "PreloadDataType": "SYNTHEA"
        },
        "SseConfiguration": {
            "KmsEncryptionConfig": {
                "CmkType": "CUSTOMER_MANAGED_KMS_KEY",
                "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            }
```

```
        },
        "DatastoreName": "Demo",
        "DatastoreArn": "arn:aws:healthlake:us-east-1:<AWS Account ID>:datastore/
<Data store ID>",
        "DatastoreEndpoint": "https://healthlake.us-east-1.amazonaws.com/datastore/
<Data store ID>/r4/",
        "DatastoreStatus": "ACTIVE",
        "DatastoreTypeVersion": "R4",
        "CreatedAt": 1603761064.881,
        "DatastoreId": "<Data store ID>",
        "IdentityProviderConfiguration": {
            "AuthorizationStrategy": "AWS_AUTH",
            "FineGrainedAuthorizationEnabled": false
        }
    }
    ]
}
```

Para obtener más información, consulte Creación y supervisión de un almacén de datos de FHIR en la Guía para desarrolladores de AWS HealthLake.

- Para obtener información sobre la API, consulte ListFHIRDatastores en la Referencia de comandos de la AWS CLI.

`list-fhir-export-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-fhir-export-jobs`.

AWS CLI

Para enumerar todos los trabajos de exportación de FHIR

En el siguiente ejemplo de `list-fhir-export-jobs`, se muestra cómo utilizar el comando para ver una lista de trabajos de exportación asociados a una cuenta.

```
aws healthlake list-fhir-export-jobs \
    --datastore-id (Data store ID) \
    --submitted-before (DATE like 2024-10-13T19:00:00Z)\
    --submitted-after (DATE like 2020-10-13T19:00:00Z )\
    --job-name "FHIR-EXPORT" \
    --job-status SUBMITTED  \
    --max-results (Integer between 1 and 500)
```

Salida:

```
{
    "ExportJobPropertiesList": [
        {
            "ExportJobProperties": {
                "OutputDataConfig": {
                    "S3Uri": "s3://(Bucket Name)/(Prefix Name)/",
                    "S3Configuration": {
                        "S3Uri": "s3://(Bucket Name)/(Prefix Name)/",
                        "KmsKeyId": "(KmsKey Id)"
                    }
                },
                "DataAccessRoleArn": "arn:aws:iam::(AWS Account ID):role/(Role
 Name)",
                "JobStatus": "COMPLETED",
                "JobId": "c145fbb27b192af392f8ce6e7838e34f",
                "JobName": "FHIR-EXPORT",
                "SubmitTime": "2024-11-20T11:31:46.672000-05:00",
                "EndTime": "2024-11-20T11:34:01.636000-05:00",
                "DatastoreId": "(Data store ID)"
            }
        }
    ]
}
```

Para obtener más información, consulte Exportación de archivos de un almacén de datos de FHIR en la Guía para desarrolladores de AWS HealthLake.

- Para obtener información sobre la API, consulte ListFHIRExportJobs en la Referencia de comandos de la AWS CLI.

`list-fhir-import-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-fhir-import-jobs`.

AWS CLI

Para enumerar todos los trabajos de importación de FHIR

En el siguiente ejemplo de `list-fhir-import-jobs`, se muestra cómo utilizar el comando para ver una lista de todos los trabajos de importación asociados a una cuenta.

```
aws healthlake list-fhir-import-jobs \
    --datastore-id (Data store ID) \
    --submitted-before (DATE like 2024-10-13T19:00:00Z) \
    --submitted-after (DATE like 2020-10-13T19:00:00Z ) \
    --job-name "FHIR-IMPORT" \
    --job-status SUBMITTED  \
    -max-results (Integer between 1 and 500)
```

Salida:

```
{
    "ImportJobPropertiesList": [
        {
            "JobId": "c0fddbf76f238297632d4aebdbfc9ddf",
            "JobStatus": "COMPLETED",
            "SubmitTime": "2024-11-20T10:08:46.813000-05:00",
            "EndTime": "2024-11-20T10:10:09.093000-05:00",
            "DatastoreId": "(Data store ID)",
            "InputDataConfig": {
                "S3Uri": "s3://(Bucket Name)/(Prefix Name)/"
            },
            "JobOutputDataConfig": {
                "S3Configuration": {
                    "S3Uri": "s3://(Bucket Name)/
import/6407b9ae4c2def3cb6f1a46a0c599ec0-FHIR_IMPORT-
c0fddbf76f238297632d4aebdbfc9ddf/",
                    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/b7f645cb-
e564-4981-8672-9e012d1ff1a0"
                }
            },
            "JobProgressReport": {
                "TotalNumberOfScannedFiles": 1,
                "TotalSizeOfScannedFilesInMB": 0.001798,
                "TotalNumberOfImportedFiles": 1,
                "TotalNumberOfResourcesScanned": 1,
                "TotalNumberOfResourcesImported": 1,
                "TotalNumberOfResourcesWithCustomerError": 0,
                "TotalNumberOfFilesReadWithCustomerError": 0,
                "Throughput": 0.0
            },
            "DataAccessRoleArn": "arn:aws:iam::(AWS Account ID):role/(Role Name)"
        }
    ]
```

```
}
```

Para obtener más información, consulte Importación de archivos a un almacén de datos de FHIR en la Guía para desarrolladores de AWS HealthLake.

- Para obtener información sobre la API, consulte ListFHIRImportJobs en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Muestra de las etiquetas para un almacén de datos

En el siguiente ejemplo de `list-tags-for-resource`, se muestran las etiquetas asociadas al almacén de datos especificado:

```
aws healthlake list-tags-for-resource \
    --resource-arn "arn:aws:healthlake:us-east-1:123456789012:datastore/
fhir/0725c83f4307f263e16fd56b6d8ebdbe"
```

Salida:

```
{
    "tags": {
        "key": "value",
        "key1": "value1"
    }
}
```

Para obtener más información, consulte Etiquetado de recursos en AWS HealthLake en la Guía para desarrolladores de AWS HealthLake.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`start-fhir-export-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-fhir-export-job`.

AWS CLI

Para iniciar un trabajo de exportación de FHIR

En el siguiente ejemplo de `start-fhir-export-job`, se muestra cómo empezar un trabajo de exportación de FHIR con AWS HealthLake.

```
aws healthlake start-fhir-export-job \
    --output-data-config '{"S3Configuration": {"S3Uri":"s3://(Bucket Name)/(Prefix Name)/","KmsKeyId":"arn:aws:kms:us-east-1:012345678910:key/d330e7fc-b56c-4216-a250-f4c43ef46e83"}}' \
    --datastore-id (Data store ID) \
    --data-access-role-arn arn:aws:iam::(AWS Account ID):role/(Role Name)
```

Salida:

```
{
    "DatastoreId": "(Data store ID)",
    "JobStatus": "SUBMITTED",
    "JobId": "9b9a51943afaedd0a8c0c26c49135a31"
}
```

Para obtener más información, consulte Exportación de archivos de un almacén de datos de FHIR en la Guía para desarrolladores de AWS HealthLake.

- Para obtener información sobre la API, consulte StartFHIRExportJob en la Referencia de comandos de la AWS CLI.

`start-fhir-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-fhir-import-job`.

AWS CLI

Para iniciar un trabajo de importación de FHIR

En el siguiente ejemplo de `start-fhir-import-job`, se muestra cómo empezar un trabajo de importación de FHIR con AWS HealthLake.

```
aws healthlake start-fhir-import-job \
    --input-data-config S3Uri="s3://(Bucket Name)/(Prefix Name)/" \
```

```
    --job-output-data-config '{"S3Configuration": {"S3Uri":"s3://(Bucket Name)/
(Prefix Name)/","KmsKeyId":"arn:aws:kms:us-east-1:012345678910:key/d330e7fc-
b56c-4216-a250-f4c43ef46e83"}}' \
    --datastore-id (Data store ID) \
    --data-access-role-arn "arn:aws:iam::(AWS Account ID):role/(Role Name)"
```

Salida:

```
{
    "DatastoreId": "(Data store ID)",
    "JobStatus": "SUBMITTED",
    "JobId": "c145fbb27b192af392f8ce6e7838e34f"
}
```

Para obtener más información, consulte Importación de archivos a un almacén de datos de FHIR en la Guía para desarrolladores de AWS HealthLake.

- Para obtener información sobre la API, consulte StartFHIRImportJob en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Agregación de una etiqueta al almacén de datos

En el siguiente ejemplo de `tag-resource`, se muestra cómo agregar una etiqueta a un almacén de datos.

```
aws healthlake tag-resource \
    --resource-arn "arn:aws:healthlake:us-east-1:123456789012:datastore/
fhir/0725c83f4307f263e16fd56b6d8ebdbe" \
    --tags '[{"Key": "key1", "Value": "value1"}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Agregación de una etiqueta a un almacén de datos en la Guía para desarrolladores de AWS HealthLake.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de etiquetas de un almacén de datos.

En el siguiente ejemplo de `untag-resource`, se muestra cómo eliminar etiquetas de un almacén de datos.

```
aws healthlake untag-resource \
    --resource-arn "arn:aws:healthlake:us-east-1:123456789012:datastore/fhir/
b91723d65c6fdeb1d26543a49d2ed1fa" \
    --tag-keys '["key1"]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de etiquetas de un almacén de datos en la Guía para desarrolladores de AWS HealthLake.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

Ejemplos de HealthOmics que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con HealthOmics.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`abort-multipart-read-set-upload`

En el siguiente ejemplo de código, se muestra cómo utilizar `abort-multipart-read-set-upload`.

AWS CLI

Para detener la carga de conjunto de lectura de varias partes

En el siguiente ejemplo de `abort-multipart-read-set-upload` se detiene la carga de conjunto de lectura de varias partes en el almacén de secuencias de HealthOmics.

```
aws omics abort-multipart-read-set-upload \
    --sequence-store-id 0123456789 \
    --upload-id 1122334455
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Direct upload to a sequence store en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte AbortMultipartReadSetUpload en la Referencia de comandos de la AWS CLI.

`accept-share`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-share`.

AWS CLI

Para aceptar un recurso compartido de los datos del almacén de análisis

El siguiente ejemplo de `accept-share` acepta un recurso compartido de los datos del almacén de análisis de HealthOmics.

```
aws omics accept-share \
    ----share-id "495c21bedc889d07d0ab69d710a6841e-dd75ab7a1a9c384fa848b5bd8e5a7e0a"
```

Salida:

```
{
    "status": "ACTIVATING"
}
```

Para obtener más información, consulte Cross-account sharing en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte AcceptShare en la Referencia de comandos de la AWS CLI.

`batch-delete-read-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-delete-read-set`.

AWS CLI

Para eliminar varios conjuntos de lectura

En el siguiente ejemplo de `batch-delete-read-set` se eliminan dos conjuntos de lectura.

```
aws omics batch-delete-read-set \
    --sequence-store-id 1234567890 \
    --ids 1234567890 0123456789
```

Si se produce un error al eliminar alguno de los conjuntos de lectura especificados, el servicio devuelve una lista de errores.

```
{
    "errors": [
        {
            "code": "",
            "id": "0123456789",
            "message": "The specified readset does not exist."
        }
    ]
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte BatchDeleteReadSet en la Referencia de comandos de la AWS CLI.

`cancel-annotation-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-annotation-import-job`.

AWS CLI

Para cancelar un trabajo de importación de anotaciones

En el siguiente ejemplo de `cancel-annotation-import-job` se cancela un trabajo de importación de anotaciones con un ID `04f57618-xmpl-4fd0-9349-e5a85aefb997`.

```
aws omics cancel-annotation-import-job \
    --job-id 04f57618-xmpl-4fd0-9349-e5a85aefb997
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte CancelAnnotationImportJob en la Referencia de comandos de la AWS CLI.

`cancel-run`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-run`.

AWS CLI

Para cancelar una ejecución

En el siguiente ejemplo de `cancel-run` se cancela una ejecución con el ID `1234567`.

```
aws omics cancel-run \
    --id 1234567
```

Para obtener más información, consulte Ejecución del ciclo de vida en un flujo de trabajo en la Guía del usuario de AWS HealthOmics.

- Para obtener más información sobre la API, consulte CancelRun en la Referencia de comandos de la AWS CLI.

`cancel-variant-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-variant-import-job`.

AWS CLI

Para cancelar un trabajo de importación de variantes

En el siguiente ejemplo de `cancel-variant-import-job` se cancela un trabajo de importación de variantes con el ID `69cb65d6-xmpl-4a4a-9025-4565794b684e`.

```
aws omics cancel-variant-import-job \
    --job-id 69cb65d6-xmpl-4a4a-9025-4565794b684e
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte CancelVariantImportJob en la Referencia de comandos de la AWS CLI.

`complete-multipart-read-set-upload`

En el siguiente ejemplo de código, se muestra cómo utilizar `complete-multipart-read-set-upload`.

AWS CLI

Para concluir una carga de varias partes una vez que ha cargado todos los componentes.

En el siguiente ejemplo de `complete-multipart-read-set-upload` se concluye una carga de varias partes en un almacén de secuencias una vez que se han cargado todos los componentes.

```
aws omics complete-multipart-read-set-upload \
    --sequence-store-id 0123456789 \
    --upload-id 1122334455 \
    --parts '[{"checksum":"gaCBQMe+rpCFZxLpoP6gydBoXaKKDA/
Vobh5zBDb4W4=","partNumber":1,"partSource":"SOURCE1"}]'
```

Salida:

```
{
    "readSetId": "0000000001"
    "readSetId": "0000000002"
```

```
    "readSetId": "0000000003"
}
```

Para obtener más información, consulte Direct upload to a sequence store en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte CompleteMultipartReadSetUpload en la Referencia de comandos de la AWS CLI.

`create-annotation-store-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-annotation-store-version`.

AWS CLI

Para crear una nueva versión de un almacén de anotaciones

En el siguiente ejemplo de `create-annotation-store-version` se crea una nueva versión de un almacén de anotaciones.

```
aws omics create-annotation-store-version \
    --name my_annotation_store \
    --version-name my_version
```

Salida:

```
{
    "creationTime": "2023-07-21T17:15:49.251040+00:00",
    "id": "3b93cdef69d2",
    "name": "my_annotation_store",
    "reference": {
        "referenceArn": "arn:aws:omics:us-
west-2:555555555555:referenceStore/6505293348/reference/5987565360"
    },
    "status": "CREATING",
    "versionName": "my_version"
}
```

Para obtener más información, consulte Creating new versions of annotation stores en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte CreateAnnotationStoreVersion en la Referencia de comandos de la AWS CLI.

`create-annotation-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-annotation-store`.

AWS CLI

Ejemplo 1: crear un almacén de anotaciones VCF

En el siguiente ejemplo de `create-annotation-store` se crea un almacén de anotaciones en formato VCF.

```
aws omics create-annotation-store \
    --name my_ann_store \
    --store-format VCF \
    --reference referenceArn=arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890
```

Salida:

```
{
    "creationTime": "2022-11-23T22:48:39.226492Z",
    "id": "0a91xmplc71f",
    "name": "my_ann_store",
    "reference": {
        "referenceArn": "arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890"
    },
    "status": "CREATING",
    "storeFormat": "VCF"
}
```

Ejemplo 2: crear un almacén de anotaciones TSV

En el siguiente ejemplo de `create-annotation-store` se crea un almacén de anotaciones en formato TSV.

```
aws omics create-annotation-store \
    --name tsv_ann_store \
    --store-format TSV \
```

```
    --reference referenceArn=arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890 \
    --store-options file://tsv-store-options.json
```

`tsv-store-options.json` configura las opciones de formato para anotaciones.

```
{
    "tsvStoreOptions": {
        "annotationType": "CHR_START_END_ZERO_BASE",
        "formatToHeader": {
            "CHR": "chromosome",
            "START": "start",
            "END": "end"
        },
        "schema": [
            {
                "chromosome": "STRING"
            },
            {
                "start": "LONG"
            },
            {
                "end": "LONG"
            },
            {
                "name": "STRING"
            }
        ]
    }
}
```

Salida:

```
{
    "creationTime": "2022-11-30T01:28:08.525586Z",
    "id": "861cxmpl96b0",
    "name": "tsv_ann_store",
    "reference": {
        "referenceArn": "arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890"
    },
    "status": "CREATING",
    "storeFormat": "TSV",
```

```
    "storeOptions": {
        "tsvStoreOptions": {
            "annotationType": "CHR_START_END_ZERO_BASE",
            "formatToHeader": {
                "CHR": "chromosome",
                "END": "end",
                "START": "start"
            },
            "schema": [
                {
                    "chromosome": "STRING"
                },
                {
                    "start": "LONG"
                },
                {
                    "end": "LONG"
                },
                {
                    "name": "STRING"
                }
            ]
        }
    }
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte CreateAnnotationStore en la Referencia de comandos de la AWS CLI.

`create-multipart-read-set-upload`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-multipart-read-set-upload`.

AWS CLI

Para comenzar una carga de conjunto de lectura de varias partes.

En el siguiente ejemplo de `create-multipart-read-set-upload` se inicia una carga de conjunto de lectura de varias partes.

```
aws omics create-multipart-read-set-upload \
    --sequence-store-id 0123456789 \
    --name HG00146 \
    --source-file-type FASTQ \
    --subject-id mySubject\
    --sample-id mySample\
    --description "FASTQ for HG00146"\
    --generated-from "1000 Genomes"
```

Salida:

```
{
    "creationTime": "2022-07-13T23:25:20Z",
    "description": "FASTQ for HG00146",
    "generatedFrom": "1000 Genomes",
    "name": "HG00146",
    "sampleId": "mySample",
    "sequenceStoreId": "0123456789",
    "sourceFileType": "FASTQ",
    "subjectId": "mySubject",
    "uploadId": "1122334455"
}
```

Para obtener más información, consulte Direct upload to a sequence store en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte CreateMultipartReadSetUpload en la Referencia de comandos de la AWS CLI.

`create-reference-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-reference-store`.

AWS CLI

Para crear un almacén de referencia

En el siguiente ejemplo de `create-reference-store` se crea un almacén de referencias `my-ref-store`.

```
aws omics create-reference-store \
```

```
    --name my-ref-store
```

Salida:

```
{
    "arn": "arn:aws:omics:us-west-2:123456789012:referenceStore/1234567890",
    "creationTime": "2022-11-22T22:13:25.947Z",
    "id": "1234567890",
    "name": "my-ref-store"
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte CreateReferenceStore en la Referencia de comandos de la AWS CLI.

`create-run-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-run-group`.

AWS CLI

Para crear un grupo de ejecución

En el siguiente ejemplo de `create-run-group` se crea un grupo de ejecución llamado `cram-converter`.

```
aws omics create-run-group \
    --name cram-converter \
    --max-cpus 20 \
    --max-gpus 10 \
    --max-duration 600 \
    --max-runs 5
```

Salida:

```
{
    "arn": "arn:aws:omics:us-west-2:123456789012:runGroup/1234567",
    "id": "1234567",
```

```
    "tags": {}
}
```

Para obtener más información, consulte Creación de grupos de ejecución en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte CreateRunGroup en la Referencia de comandos de la AWS CLI.

`create-sequence-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-sequence-store`.

AWS CLI

Para crear un almacén de secuencias

En el siguiente ejemplo de `create-sequence-store` se crea un almacén de secuencias.

```
aws omics create-sequence-store \
    --name my-seq-store
```

Salida:

```
{
    "arn": "arn:aws:omics:us-west-2:123456789012:sequenceStore/1234567890",
    "creationTime": "2022-11-23T01:24:33.629Z",
    "id": "1234567890",
    "name": "my-seq-store"
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte CreateSequenceStore en la Referencia de comandos de la AWS CLI.

`create-share`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-share`.

AWS CLI

Para crear un recurso compartido de un almacén de análisis de HealthOmics

El siguiente ejemplo de `create-share` muestra cómo crear un recurso compartido de un almacén de análisis de HealthOmics que pueda ser aceptado por un suscriptor ajeno a la cuenta.

```
aws omics create-share \
    --resource-arn "arn:aws:omics:us-west-2:555555555555:variantStore/
omics_dev_var_store" \
    --principal-subscriber "123456789012" \
    --name "my_Share-123"
```

Salida:

```
{
    "shareId": "495c21bedc889d07d0ab69d710a6841e-dd75ab7a1a9c384fa848b5bd8e5a7e0a",
    "name": "my_Share-123",
    "status": "PENDING"
}
```

Para obtener más información, consulte Cross-account sharing en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte CreateShare en la Referencia de comandos de la AWS CLI.

`create-variant-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-variant-store`.

AWS CLI

Para crear un almacén de variantes

En el siguiente ejemplo de `create-variant-store` se crea un almacén de variantes llamado `my_var_store`.

```
aws omics create-variant-store \
    --name my_var_store \
    --reference referenceArn=arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890
```

Salida:

```
{
    "creationTime": "2022-11-23T22:09:07.534499Z",
    "id": "02dexmplcfdd",
    "name": "my_var_store",
    "reference": {
        "referenceArn": "arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890"
    },
    "status": "CREATING"
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte CreateVariantStore en la Referencia de comandos de la AWS CLI.

`create-workflow`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-workflow`.

AWS CLI

Para crear un flujo de trabajo

En el siguiente ejemplo de `create-workflow` se crea un flujo de trabajo WDL.

```
aws omics create-workflow \
    --name cram-converter \
    --engine WDL \
    --definition-zip fileb://workflow-crambam.zip \
    --parameter-template file://workflow-params.json
```

`workflow-crambam.zip` es un archivo ZIP que contiene una definición de flujo de trabajo. `workflow-params.json` define los parámetros de tiempo de ejecución del flujo de trabajo.

```
{
    "ref_fasta" : {
        "description": "Reference genome fasta file",
        "optional": false
```

```
    },
    "ref_fasta_index" : {
        "description": "Index of the reference genome fasta file",
        "optional": false
    },
    "ref_dict" : {
        "description": "dictionary file for 'ref_fasta'",
        "optional": false
    },
    "input_cram" : {
        "description": "The Cram file to convert to BAM",
        "optional": false
    },
    "sample_name" : {
        "description": "The name of the input sample, used to name the output BAM",
        "optional": false
    }
}
```

Salida:

```
{
    "arn": "arn:aws:omics:us-west-2:123456789012:workflow/1234567",
    "id": "1234567",
    "status": "CREATING",
    "tags": {}
}
```

Para obtener más información, consulte Creación de flujos de trabajo privados en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte CreateWorkflow en la Referencia de comandos de la AWS CLI.

`delete-annotation-store-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-annotation-store-versions`.

AWS CLI

Para eliminar una versión del almacén de anotaciones

En el siguiente ejemplo de `delete-annotation-store-versions` se elimina una versión del almacén de anotaciones.

```
aws omics delete-annotation-store-versions \
    --name my_annotation_store \
    --versions my_version
```

Salida:

```
{
    "errors": []
}
```

Para obtener más información, consulte Creating new versions of annotation stores en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte DeleteAnnotationStoreVersions en la Referencia de comandos de la AWS CLI.

`delete-annotation-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-annotation-store`.

AWS CLI

Para eliminar un almacén de anotaciones

En el siguiente ejemplo de `delete-annotation-store` se elimina un almacén de anotaciones llamado `my_vcf_store`.

```
aws omics delete-annotation-store \
    --name my_vcf_store
```

Salida:

```
{
    "status": "DELETING"
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte DeleteAnnotationStore en la Referencia de comandos de la AWS CLI.

`delete-reference-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-reference-store`.

AWS CLI

Para eliminar un almacén de referencias

En el siguiente ejemplo de `delete-reference-store` se elimina un almacén de referencia con el ID `1234567890`.

```
aws omics delete-reference-store \
    --id 1234567890
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte DeleteReferenceStore en la Referencia de comandos de la AWS CLI.

`delete-reference`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-reference`.

AWS CLI

Para eliminar una referencia

En el siguiente ejemplo de `delete-reference` se elimina una referencia.

```
aws omics delete-reference \
    --reference-store-id 1234567890 \
    --id 1234567890
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte DeleteReference en la Referencia de comandos de la AWS CLI.

`delete-run-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-run-group`.

AWS CLI

Para eliminar un grupo de ejecución

En el siguiente ejemplo de `delete-run-group` se elimina un grupo de ejecución con el ID `1234567`.

```
aws omics delete-run-group \
    --id 1234567
```

Para obtener más información, consulte Eliminación de ejecuciones y grupos de ejecuciones en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte DeleteRunGroup en la Referencia de comandos de la AWS CLI.

`delete-run`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-run`.

AWS CLI

Para eliminar una ejecución de flujo de trabajo

En el siguiente ejemplo de `delete-run` se elimina una ejecución con el ID `1234567`.

```
aws omics delete-run \
    --id 1234567
```

Para obtener más información, consulte Eliminación de ejecuciones y grupos de ejecuciones en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte DeleteRun en la Referencia de comandos de la AWS CLI.

`delete-sequence-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-sequence-store`.

AWS CLI

Para eliminar un almacén de secuencias

En el siguiente ejemplo de `delete-sequence-store` se elimina un almacén de secuencias con el ID `1234567890`.

```
aws omics delete-sequence-store \
    --id 1234567890
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte DeleteSequenceStore en la Referencia de comandos de la AWS CLI.

`delete-share`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-share`.

AWS CLI

Para eliminar un recurso compartido de los datos de análisis de HealthOmics

En el siguiente ejemplo de `delete-share` se elimina un recurso compartido entre cuentas de datos de análisis.

```
aws omics delete-share \
    --share-id "495c21bedc889d07d0ab69d710a6841e-dd75ab7a1a9c384fa848b5bd8e5a7e0a"
```

Salida:

```
{
    "status": "DELETING"
}
```

Para obtener más información, consulte Cross-account sharing en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte DeleteShare en la Referencia de comandos de la AWS CLI.

`delete-variant-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-variant-store`.

AWS CLI

Para eliminar un almacén de variantes

En el siguiente ejemplo de `delete-variant-store` se elimina un almacén de variantes llamado `my_var_store`.

```
aws omics delete-variant-store \
    --name my_var_store
```

Salida:

```
{
    "status": "DELETING"
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte DeleteVariantStore en la Referencia de comandos de la AWS CLI.

`delete-workflow`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-workflow`.

AWS CLI

Para eliminar un flujo de trabajo

En el siguiente ejemplo de `delete-workflow` se elimina un flujo de trabajo con el ID `1234567`.

```
aws omics delete-workflow \
    --id 1234567
```

Para obtener más información, consulte Eliminación de un flujo de trabajo privado en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte DeleteWorkflow en la Referencia de comandos de la AWS CLI.

`get-annotation-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-annotation-import-job`.

AWS CLI

Para ver un trabajo de importación de anotaciones

En el siguiente ejemplo de `get-annotation-import-job` se obtienen detalles sobre un trabajo de importación de anotaciones.

```
aws omics get-annotation-import-job \
    --job-id 984162c7-xmpl-4d23-ab47-286f7950bfbf
```

Salida:

```
{
    "creationTime": "2022-11-30T01:40:11.017746Z",
    "destinationName": "tsv_ann_store",
    "id": "984162c7-xmpl-4d23-ab47-286f7950bfbf",
    "items": [
        {
            "jobStatus": "COMPLETED",
            "source": "s3://omics-artifacts-01d6xmpl4e72dd32/targetedregions.bed.gz"
        }
    ],
    "roleArn": "arn:aws:iam::123456789012:role/omics-service-role-serviceRole-
W8O1XMPL7QZ",
    "runLeftNormalization": false,
    "status": "COMPLETED",
    "updateTime": "2022-11-30T01:42:39.134009Z"
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte GetAnnotationImportJob en la Referencia de comandos de la AWS CLI.

`get-annotation-store-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-annotation-store-version`.

AWS CLI

Para recuperar los metadatos de una versión del almacén de anotaciones

En el siguiente ejemplo de `get-annotation-store-version` se recuperan los metadatos de la versión del almacén de anotaciones solicitada.

```
aws omics get-annotation-store-version \
    --name my_annotation_store \
    --version-name my_version
```

Salida:

```
{
    "storeId": "4934045d1c6d",
    "id": "2a3f4a44aa7b",
    "status": "ACTIVE",
    "versionArn": "arn:aws:omics:us-west-2:555555555555:annotationStore/
my_annotation_store/version/my_version",
    "name": "my_annotation_store",
    "versionName": "my_version",
    "creationTime": "2023-07-21T17:15:49.251040+00:00",
    "updateTime": "2023-07-21T17:15:56.434223+00:00",
    "statusMessage": "",
    "versionSizeBytes": 0
}
```

Para obtener más información, consulte Creating new versions of annotation stores en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte GetAnnotationStoreVersion en la Referencia de comandos de la AWS CLI.

`get-annotation-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-annotation-store`.

AWS CLI

Para ver un almacén de anotaciones

En el siguiente ejemplo de `get-annotation-store` se obtienen detalles sobre un almacén de anotaciones llamado `my_ann_store`.

```
aws omics get-annotation-store \
    --name my_ann_store
```

Salida:

```
{
    "creationTime": "2022-11-23T22:48:39.226492Z",
    "id": "0a91xmplc71f",
    "name": "my_ann_store",
    "reference": {
        "referenceArn": "arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890"
    },
    "status": "CREATING",
    "storeArn": "arn:aws:omics:us-west-2:123456789012:annotationStore/my_ann_store",
    "storeFormat": "VCF",
    "storeSizeBytes": 0,
    "tags": {}
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte GetAnnotationStore en la Referencia de comandos de la AWS CLI.

`get-read-set-activation-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-read-set-activation-job`.

AWS CLI

Para ver un trabajo de activación de conjunto de lectura

En el siguiente ejemplo de `get-read-set-activation-job` se obtienen detalles sobre un trabajo de activación de conjunto de lectura.

```
aws omics get-read-set-activation-job \
    --sequence-store-id 1234567890 \
    --id 1234567890
```

Salida:

```
{
    "completionTime": "2022-12-06T22:33:42.828Z",
    "creationTime": "2022-12-06T22:32:45.213Z",
    "id": "1234567890",
    "sequenceStoreId": "1234567890",
    "sources": [
        {
            "readSetId": "1234567890",
            "status": "FINISHED",
            "statusMessage": "No activation needed as read set is already in
 ACTIVATING or ACTIVE state."
        }
    ],
    "status": "COMPLETED",
    "statusMessage": "The job completed successfully."
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte GetReadSetActivationJob en la Referencia de comandos de la AWS CLI.

`get-read-set-export-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-read-set-export-job`.

AWS CLI

Para ver un trabajo de exportación de conjunto de lectura

En el siguiente ejemplo de `get-read-set-export-job` se obtienen detalles sobre un trabajo de exportación de conjunto de lectura.

```
aws omics get-read-set-export-job \
    --sequence-store-id 1234567890 \
    --id 1234567890
```

Salida:

```
{
    "completionTime": "2022-12-06T22:39:14.491Z",
    "creationTime": "2022-12-06T22:37:18.612Z",
    "destination": "s3://omics-artifacts-01d6xmpl4e72dd32/read-set-export/",
    "id": "1234567890",
    "sequenceStoreId": "1234567890",
    "status": "COMPLETED",
    "statusMessage": "The job is submitted and will start soon."
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte GetReadSetExportJob en la Referencia de comandos de la AWS CLI.

`get-read-set-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-read-set-import-job`.

AWS CLI

Para ver un trabajo de importación de conjunto de lectura

En el siguiente ejemplo de `get-read-set-import-job` se obtienen detalles sobre un trabajo de importación de conjunto de lectura.

```
aws omics get-read-set-import-job \
    --sequence-store-id 1234567890 \
    --id 1234567890
```

Salida:

```
{
    "creationTime": "2022-11-23T01:36:38.158Z",
    "id": "1234567890",
```

```
    "roleArn": "arn:aws:iam::123456789012:role/omics-service-role-serviceRole-
W8O1XMPL7QZ",
    "sequenceStoreId": "1234567890",
    "sources": [
        {
            "name": "HG00100",
            "referenceArn": "arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890",
            "sampleId": "bam-sample",
            "sourceFileType": "BAM",
            "sourceFiles": {
                "source1": "s3://omics-artifacts-01d6xmpl4e72dd32/
HG00100.chrom20.ILLUMINA.bwa.GBR.low_coverage.20101123.bam",
                "source2": ""
            },
            "status": "IN_PROGRESS",
            "statusMessage": "The source job is currently in progress.",
            "subjectId": "bam-subject",
            "tags": {
                "aws:omics:sampleId": "bam-sample",
                "aws:omics:subjectId": "bam-subject"
            }
        },
        {
            "name": "HG00146",
            "referenceArn": "arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890",
            "sampleId": "fastq-sample",
            "sourceFileType": "FASTQ",
            "sourceFiles": {
                "source1": "s3://omics-artifacts-01d6xmpl4e72dd32/
SRR233106_1.filt.fastq.gz",
                "source2": "s3://omics-artifacts-01d6xmpl4e72dd32/
SRR233106_2.filt.fastq.gz"
            },
            "status": "IN_PROGRESS",
            "statusMessage": "The source job is currently in progress.",
            "subjectId": "fastq-subject",
            "tags": {
                "aws:omics:sampleId": "fastq-sample",
                "aws:omics:subjectId": "fastq-subject"
            }
        },
        {
```

```
            "name": "HG00096",
            "referenceArn": "arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890",
            "sampleId": "cram-sample",
            "sourceFileType": "CRAM",
            "sourceFiles": {
                "source1": "s3://omics-artifacts-01d6xmpl4e72dd32/
HG00096.alt_bwamem_GRCh38DH.20150718.GBR.low_coverage.cram",
                "source2": ""
            },
            "status": "IN_PROGRESS",
            "statusMessage": "The source job is currently in progress.",
            "subjectId": "cram-subject",
            "tags": {
                "aws:omics:sampleId": "cram-sample",
                "aws:omics:subjectId": "cram-subject"
            }
        }
    ],
    "status": "IN_PROGRESS",
    "statusMessage": "The job is currently in progress."
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte GetReadSetImportJob en la Referencia de comandos de la AWS CLI.

`get-read-set-metadata`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-read-set-metadata`.

AWS CLI

Para ver un conjunto de lectura

En el siguiente ejemplo de `get-read-set-metadata` se obtienen detalles sobre archivos de un conjunto de lectura.

```
aws omics get-read-set-metadata \
    --sequence-store-id 1234567890 \
```

```
    --id 1234567890
```

Salida:

```
{
    "arn": "arn:aws:omics:us-west-2:123456789012:sequenceStore/1234567890/
readSet/1234567890",
    "creationTime": "2022-11-23T21:55:00.515Z",
    "fileType": "FASTQ",
    "files": {
        "source1": {
            "contentLength": 310054739,
            "partSize": 104857600,
            "totalParts": 3
        },
        "source2": {
            "contentLength": 307846621,
            "partSize": 104857600,
            "totalParts": 3
        }
    },
    "id": "1234567890",
    "name": "HG00146",
    "referenceArn": "arn:aws:omics:us-west-2:123456789012:referenceStore/1234567890/
reference/1234567890",
    "sampleId": "fastq-sample",
    "sequenceInformation": {
        "alignment": "UNALIGNED",
        "totalBaseCount": 677717384,
        "totalReadCount": 8917334
    },
    "sequenceStoreId": "1234567890",
    "status": "ACTIVE",
    "subjectId": "fastq-subject"
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte GetReadSetMetadata en la Referencia de comandos de la AWS CLI.

`get-read-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-read-set`.

AWS CLI

Para descargar un conjunto de lectura

En el siguiente ejemplo de `get-read-set` se descarga la parte 3 de un conjunto de lectura como `1234567890.3.bam`.

```
aws omics get-read-set \
    --sequence-store-id 1234567890 \
    --id 1234567890 \
    --part-number 3  1234567890.3.bam
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte GetReadSet en la Referencia de comandos de la AWS CLI.

`get-reference-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-reference-import-job`.

AWS CLI

Para ver un trabajo de importación de referencia

En el siguiente ejemplo de `get-reference-import-job` se obtienen detalles sobre un trabajo de importación de referencia.

```
aws omics get-reference-import-job \
    --reference-store-id 1234567890 \
    --id 1234567890
```

Salida:

```
{
```

```
    "creationTime": "2022-11-22T22:25:41.124Z",
    "id": "1234567890",
    "referenceStoreId": "1234567890",
    "roleArn": "arn:aws:iam::123456789012:role/omics-service-role-serviceRole-
W8O1XMPL7QZ",
    "sources": [
        {
            "name": "assembly-38",
            "sourceFile": "s3://omics-artifacts-01d6xmpl4e72dd32/
Homo_sapiens_assembly38.fasta",
            "status": "IN_PROGRESS",
            "statusMessage": "The source job is currently in progress."
        }
    ],
    "status": "IN_PROGRESS",
    "statusMessage": "The job is currently in progress."
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte GetReferenceImportJob en la Referencia de comandos de la AWS CLI.

`get-reference-metadata`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-reference-metadata`.

AWS CLI

Para ver una referencia

En el siguiente ejemplo de `get-reference-metadata` se obtienen detalles sobre una referencia.

```
aws omics get-reference-metadata \
    --reference-store-id 1234567890 \
    --id 1234567890
```

Salida:

```
{
```

```
    "arn": "arn:aws:omics:us-west-2:123456789012:referenceStore/1234567890/
reference/1234567890",
    "creationTime": "2022-11-22T22:27:09.033Z",
    "files": {
        "index": {
            "contentLength": 160928,
            "partSize": 104857600,
            "totalParts": 1
        },
        "source": {
            "contentLength": 3249912778,
            "partSize": 104857600,
            "totalParts": 31
        }
    },
    "id": "1234567890",
    "md5": "7ff134953dcca8c8997453bbb80b6b5e",
    "name": "assembly-38",
    "referenceStoreId": "1234567890",
    "status": "ACTIVE",
    "updateTime": "2022-11-22T22:27:09.033Z"
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte GetReferenceMetadata en la Referencia de comandos de la AWS CLI.

`get-reference-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-reference-store`.

AWS CLI

Para ver un almacén de referencias

En el siguiente ejemplo de `get-reference-store` se obtienen detalles sobre un almacén de referencias.

```
aws omics get-reference-store \
    --id 1234567890
```

Salida:

```
{
    "arn": "arn:aws:omics:us-west-2:123456789012:referenceStore/1234567890",
    "creationTime": "2022-09-23T23:27:20.364Z",
    "id": "1234567890",
    "name": "my-rstore-0"
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte GetReferenceStore en la Referencia de comandos de la AWS CLI.

`get-reference`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-reference`.

AWS CLI

Para descargar una referencia genómica

En el siguiente ejemplo de `get-reference` se descarga la parte 1 de un genoma como `hg38.1.fa`.

```
aws omics get-reference \
    --reference-store-id 1234567890 \
    --id 1234567890 \
    --part-number 1 hg38.1.fa
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte GetReference en la Referencia de comandos de la AWS CLI.

`get-run-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-run-group`.

AWS CLI

Para ver un grupo de ejecución

En el siguiente ejemplo de `get-run-group` se obtienen detalles sobre un grupo de ejecución.

```
aws omics get-run-group \
    --id 1234567
```

Salida:

```
{
    "arn": "arn:aws:omics:us-west-2:123456789012:runGroup/1234567",
    "creationTime": "2022-12-01T00:58:42.915219Z",
    "id": "1234567",
    "maxCpus": 20,
    "maxDuration": 600,
    "name": "cram-convert",
    "tags": {}
}
```

Para obtener más información, consulte Creación de grupos de ejecución en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte GetRunGroup en la Referencia de comandos de la AWS CLI.

`get-run-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-run-task`.

AWS CLI

Para ver una tarea

En el siguiente ejemplo de `get-run-task` se obtienen detalles sobre una tarea de flujo de trabajo.

```
aws omics get-run-task \
    --id 1234567 \
```

```
    --task-id 1234567
```

Salida:

```
{
    "cpus": 1,
    "creationTime": "2022-11-30T23:13:00.718651Z",
    "logStream": "arn:aws:logs:us-west-2:123456789012:log-group:/aws/omics/
WorkflowLog:log-stream:run/1234567/task/1234567",
    "memory": 15,
    "name": "CramToBamTask",
    "startTime": "2022-11-30T23:17:47.016Z",
    "status": "COMPLETED",
    "stopTime": "2022-11-30T23:18:21.503Z",
    "taskId": "1234567"
}
```

Para obtener más información, consulte Ciclo de vida de las tareas en una ejecución de HealthOmics en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte GetRunTask en la Referencia de comandos de la AWS CLI.

`get-run`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-run`.

AWS CLI

Para ver una ejecución de flujo de trabajo

En el siguiente ejemplo de `get-run` se obtienen detalles sobre una ejecución de flujo de trabajo.

```
aws omics get-run \
    --id 1234567
```

Salida:

```
{
    "arn": "arn:aws:omics:us-west-2:123456789012:run/1234567",
    "creationTime": "2022-11-30T22:58:22.615865Z",
```

```
    "digest":
 "sha256:c54bxmpl742dcc26f7fa1f10e37550ddd8f251f418277c0a58e895b801ed28cf",
    "id": "1234567",
    "name": "cram-to-bam",
    "outputUri": "s3://omics-artifacts-01d6xmpl4e72dd32/workflow-output/",
    "parameters": {
        "ref_dict": "s3://omics-artifacts-01d6xmpl4e72dd32/
Homo_sapiens_assembly38.dict",
        "ref_fasta_index": "s3://omics-artifacts-01d6xmpl4e72dd32/
Homo_sapiens_assembly38.fasta.fai",
        "ref_fasta": "s3://omics-artifacts-01d6xmpl4e72dd32/
Homo_sapiens_assembly38.fasta",
        "sample_name": "NA12878",
        "input_cram": "s3://omics-artifacts-01d6xmpl4e72dd32/NA12878.cram"
    },
    "resourceDigests": {
        "s3://omics-artifacts-01d6xmpl4e72dd32/Homo_sapiens_assembly38.fasta.fai":
 "etag:f76371b113734a56cde236bc0372de0a",
        "s3://omics-artifacts-01d6xmpl4e72dd32/Homo_sapiens_assembly38.dict":
 "etag:3884c62eb0e53fa92459ed9bff133ae6",
        "s3://omics-artifacts-01d6xmpl4e72dd32/Homo_sapiens_assembly38.fasta":
 "etag:e307d81c605fb91b7720a08f00276842-388",
        "s3://omics-artifacts-01d6xmpl4e72dd32/NA12878.cram":
 "etag:a9f52976381286c6143b5cc681671ec6"
    },
    "roleArn": "arn:aws:iam::123456789012:role/omics-service-role-serviceRole-
W8O1XMPL7QZ",
    "startedBy": "arn:aws:iam::123456789012:user/laptop-2020",
    "status": "STARTING",
    "tags": {},
    "workflowId": "1234567",
    "workflowType": "PRIVATE"
}
```

Para obtener más información, consulte Ejecución del ciclo de vida en un flujo de trabajo en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte GetRun en la Referencia de comandos de la AWS CLI.

`get-sequence-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-sequence-store`.

AWS CLI

Para ver un almacén de secuencias

En el siguiente ejemplo de `get-sequence-store` se obtienen detalles sobre un almacén de secuencias con el ID `1234567890`.

```
aws omics get-sequence-store \
    --id 1234567890
```

Salida:

```
{
    "arn": "arn:aws:omics:us-east-1:123456789012:sequenceStore/1234567890",
    "creationTime": "2022-11-23T19:55:48.376Z",
    "id": "1234567890",
    "name": "my-seq-store"
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte GetSequenceStore en la Referencia de comandos de la AWS CLI.

`get-share`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-share`.

AWS CLI

Para recuperar los metadatos sobre un recurso compartido de los datos de análisis de HealthOmics

En el siguiente ejemplo de `get-share` se recuperan los metadatos de un recurso compartido entre cuentas de datos de análisis.

```
aws omics get-share \
    --share-id "495c21bedc889d07d0ab69d710a6841e-dd75ab7a1a9c384fa848b5bd8e5a7e0a"
```

Salida:

```
{
    "share": {
        "shareId": "495c21bedc889d07d0ab69d710a6841e-
dd75ab7a1a9c384fa848b5bd8e5a7e0a",
        "name": "my_Share-123",
        "resourceArn": "arn:aws:omics:us-west-2:555555555555:variantStore/
omics_dev_var_store",
        "principalSubscriber": "123456789012",
        "ownerId": "555555555555",
        "status": "PENDING"
    }
}
```

Para obtener más información, consulte Cross-account sharing en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte GetShare en la Referencia de comandos de la AWS CLI.

`get-variant-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-variant-import-job`.

AWS CLI

Para ver un trabajo de importación de variantes

En el siguiente ejemplo de `get-variant-import-job` se obtienen detalles sobre un trabajo de importación de variantes.

```
aws omics get-variant-import-job \
    --job-id edd7b8ce-xmpl-47e2-bc99-258cac95a508
```

Salida:

```
{
    "creationTime": "2022-11-23T22:42:50.037812Z",
    "destinationName": "my_var_store",
    "id": "edd7b8ce-xmpl-47e2-bc99-258cac95a508",
    "items": [
        {
            "jobStatus": "IN_PROGRESS",
```

```
            "source": "s3://omics-artifacts-01d6xmpl4e72dd32/
Homo_sapiens_assembly38.known_indels.vcf.gz"
        }
    ],
    "roleArn": "arn:aws:iam::123456789012:role/omics-service-role-serviceRole-
W8O1XMPL7QZ",
    "runLeftNormalization": false,
    "status": "IN_PROGRESS",
    "updateTime": "2022-11-23T22:43:05.898309Z"
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte GetVariantImportJob en la Referencia de comandos de la AWS CLI.

`get-variant-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-variant-store`.

AWS CLI

Para ver un almacén de variantes

En el siguiente ejemplo de `get-variant-store` se obtienen detalles sobre un almacén de variantes.

```
aws omics get-variant-store \
    --name my_var_store
```

Salida:

```
{
    "creationTime": "2022-11-23T22:09:07.534499Z",
    "id": "02dexmplcfdd",
    "name": "my_var_store",
    "reference": {
        "referenceArn": "arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890"
    },
    "status": "CREATING",
    "storeArn": "arn:aws:omics:us-west-2:123456789012:variantStore/my_var_store",
```

```
    "storeSizeBytes": 0,
    "tags": {},
    "updateTime": "2022-11-23T22:09:24.931711Z"
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte GetVariantStore en la Referencia de comandos de la AWS CLI.

`get-workflow`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-workflow`.

AWS CLI

Para ver un flujo de trabajo

En el siguiente ejemplo de `get-workflow` se obtienen detalles sobre un flujo de trabajo con el ID 1234567.

```
aws omics get-workflow \
    --id 1234567
```

Salida:

```
{
    "arn": "arn:aws:omics:us-west-2:123456789012:workflow/1234567",
    "creationTime": "2022-11-30T22:33:16.225368Z",
    "digest":
 "sha256:c54bxmpl742dcc26f7fa1f10e37550ddd8f251f418277c0a58e895b801ed28cf",
    "engine": "WDL",
    "id": "1234567",
    "main": "workflow-crambam.wdl",
    "name": "cram-converter",
    "parameterTemplate": {
        "ref_dict": {
            "description": "dictionary file for 'ref_fasta'"
        },
        "ref_fasta_index": {
            "description": "Index of the reference genome fasta file"
```

```
        },
        "ref_fasta": {
            "description": "Reference genome fasta file"
        },
        "input_cram": {
            "description": "The Cram file to convert to BAM"
        },
        "sample_name": {
            "description": "The name of the input sample, used to name the output
 BAM"
        }
    },
    "status": "ACTIVE",
    "statusMessage": "workflow-crambam.wdl\n    workflow CramToBamFlow\n
 call CramToBamTask\n        call ValidateSamFile\n    task CramToBamTask\n    task
 ValidateSamFile\n",
    "tags": {},
    "type": "PRIVATE"
}
```

Para obtener más información, consulte Creación de flujos de trabajo privados en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte GetWorkflow en la Referencia de comandos de la AWS CLI.

`list-annotation-import-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-annotation-import-jobs`.

AWS CLI

Para obtener una lista de trabajos de importación de anotaciones

El siguiente `list-annotation-import-jobs` obtiene una lista de los trabajos de importación de anotaciones.

```
aws omics list-annotation-import-jobs
```

Salida:

```
{
```

```
    "annotationImportJobs": [
        {
            "creationTime": "2022-11-30T01:39:41.478294Z",
            "destinationName": "gff_ann_store",
            "id": "18a9e792-xmpl-4869-a105-e5b602900444",
            "roleArn": "arn:aws:iam::123456789012:role/omics-service-role-
serviceRole-W8O1XMPL7QZ",
            "runLeftNormalization": false,
            "status": "COMPLETED",
            "updateTime": "2022-11-30T01:47:09.145178Z"
        },
        {
            "creationTime": "2022-11-30T00:45:58.007838Z",
            "destinationName": "my_ann_store",
            "id": "4e9eafc8-xmpl-431e-a0b2-3bda27cb600a",
            "roleArn": "arn:aws:iam::123456789012:role/omics-service-role-
serviceRole-W8O1XMPL7QZ",
            "runLeftNormalization": false,
            "status": "FAILED",
            "updateTime": "2022-11-30T00:47:01.706325Z"
        }
    ]
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte ListAnnotationImportJobs en la Referencia de comandos de la AWS CLI.

`list-annotation-store-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-annotation-store-versions`.

AWS CLI

Para enumerar todas las versiones de un almacén de anotaciones.

En el siguiente ejemplo de `list-annotation-store-versions` se enumeran todas las versiones que existen de un almacén de anotaciones.

```
aws omics list-annotation-store-versions \
```

```
    --name my_annotation_store
```

Salida:

```
{
    "annotationStoreVersions": [
        {
        "storeId": "4934045d1c6d",
        "id": "2a3f4a44aa7b",
        "status": "CREATING",
        "versionArn": "arn:aws:omics:us-west-2:555555555555:annotationStore/
my_annotation_store/version/my_version_2",
        "name": "my_annotation_store",
        "versionName": "my_version_2",
        "creation Time": "2023-07-21T17:20:59.380043+00:00",
        "versionSizeBytes": 0
},
{
     "storeId": "4934045d1c6d",
     "id": "4934045d1c6d",
     "status": "ACTIVE",
     "versionArn": "arn:aws:omics:us-west-2:555555555555:annotationStore/
my_annotation_store/version/my_version_1",
     "name": "my_annotation_store",
     "versionName": "my_version_1",
     "creationTime": "2023-07-21T17:15:49.251040+00:00",
     "updateTime": "2023-07-21T17:15:56.434223+00:00",
     "statusMessage": "",
     "versionSizeBytes": 0
     }

}
```

Para obtener más información, consulte Creating new versions of annotation stores en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte ListAnnotationStoreVersions en la Referencia de comandos de la AWS CLI.

`list-annotation-stores`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-annotation-stores`.

AWS CLI

Para obtener una lista de almacenes de anotaciones

En el siguiente ejemplo de `list-annotation-stores` se obtiene una lista de almacenes de anotaciones.

```
aws omics list-annotation-stores
```

Salida:

```
{
    "annotationStores": [
        {
            "creationTime": "2022-11-23T22:48:39.226492Z",
            "id": "0a91xmplc71f",
            "name": "my_ann_store",
            "reference": {
                "referenceArn": "arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890"
            },
            "status": "ACTIVE",
            "statusMessage": "",
            "storeArn": "arn:aws:omics:us-west-2:123456789012:annotationStore/
my_ann_store",
            "storeFormat": "VCF",
            "storeSizeBytes": 0,
            "updateTime": "2022-11-23T22:53:27.372840Z"
        }
    ]
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte ListAnnotationStores en la Referencia de comandos de la AWS CLI.

`list-multipart-read-set-uploads`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-multipart-read-set-uploads`.

AWS CLI

Para enumerar todas las cargas de conjuntos de lectura de varias partes y sus estados.

En el siguiente ejemplo de `list-multipart-read-set-uploads` se enumeran todas las cargas de conjuntos de lectura de varias partes y sus estados.

```
aws omics list-multipart-read-set-uploads \
    --sequence-store-id 0123456789
```

Salida:

```
{
"uploads":
    [
        {
           "sequenceStoreId": "0123456789",
           "uploadId": "8749584421",
           "sourceFileType": "FASTQ",
            "subjectId": "mySubject",
            "sampleId": "mySample",
            "generatedFrom": "1000 Genomes",
            "name": "HG00146",
            "description": "FASTQ for HG00146",
            "creationTime": "2023-11-29T19:22:51.349298+00:00"
        },
        {
            "sequenceStoreId": "0123456789",
            "uploadId": "5290538638",
            "sourceFileType": "BAM",
            "subjectId": "mySubject",
            "sampleId": "mySample",
            "generatedFrom": "1000 Genomes",
            "referenceArn": "arn:aws:omics:us-
west-2:845448930428:referenceStore/8168613728/reference/2190697383",
            "name": "HG00146",
            "description": "BAM for HG00146",
            "creationTime": "2023-11-29T19:23:33.116516+00:00"
        },
        {
            "sequenceStoreId": "0123456789",
            "uploadId": "4174220862",
            "sourceFileType": "BAM",
```

```
            "subjectId": "mySubject",
            "sampleId": "mySample",
            "generatedFrom": "1000 Genomes",
            "referenceArn": "arn:aws:omics:us-
west-2:845448930428:referenceStore/8168613728/reference/2190697383",
            "name": "HG00147",
            "description": "BAM for HG00147",
            "creationTime": "2023-11-29T19:23:47.007866+00:00"
        }
    ]
}
```

Para obtener más información, consulte Direct upload to a sequence store en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte ListMultipartReadSetUploads en la Referencia de comandos de la AWS CLI.

`list-read-set-activation-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-read-set-activation-jobs`.

AWS CLI

Para obtener una lista de trabajos de activación de conjuntos de lectura

En el siguiente ejemplo de `list-read-set-activation-jobs` se obtiene una lista de trabajos de activación de un almacén de secuencias con el ID `1234567890`.

```
aws omics list-read-set-activation-jobs \
    --sequence-store-id 1234567890
```

Salida:

```
{
    "activationJobs": [
        {
            "completionTime": "2022-12-06T22:33:42.828Z",
            "creationTime": "2022-12-06T22:32:45.213Z",
            "id": "1234567890",
            "sequenceStoreId": "1234567890",
            "status": "COMPLETED"
```

```
        },
        {
            "creationTime": "2022-12-06T22:35:10.100Z",
            "id": "1234567890",
            "sequenceStoreId": "1234567890",
            "status": "IN_PROGRESS"
        }
    ]
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener detalles sobre la API, consulte ListReadSetActivationJobs en la Referencia de comandos de la AWS CLI.

`list-read-set-export-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-read-set-export-jobs`.

AWS CLI

Para obtener una lista de trabajos de exportación de conjuntos de lectura

En el siguiente ejemplo de `list-read-set-export-jobs` se obtiene una lista de trabajos de exportación de un almacén de secuencias con el ID `1234567890`.

```
aws omics list-read-set-export-jobs \
    --sequence-store-id 1234567890
```

Salida:

```
{
    "exportJobs": [
        {
            "completionTime": "2022-12-06T22:39:14.491Z",
            "creationTime": "2022-12-06T22:37:18.612Z",
            "destination": "s3://omics-artifacts-01d6xmpl4e72dd32/read-set-export/",
            "id": "1234567890",
            "sequenceStoreId": "1234567890",
            "status": "COMPLETED"
        },
```

```
        {
            "creationTime": "2022-12-06T22:38:04.871Z",
            "destination": "s3://omics-artifacts-01d6xmpl4e72dd32/read-set-export/",
            "id": "1234567890",
            "sequenceStoreId": "1234567890",
            "status": "IN_PROGRESS"
        }
    ]
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte ListReadSetExportJobs en la Referencia de comandos de la AWS CLI.

`list-read-set-import-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-read-set-import-jobs`.

AWS CLI

Para obtener una lista de trabajos de importación de conjuntos de lectura

En el siguiente ejemplo de `list-read-set-import-jobs` se obtiene una lista de trabajos de importación de un almacén de secuencias con el ID `1234567890`.

```
aws omics list-read-set-import-jobs \
    --sequence-store-id 1234567890
```

Salida:

```
{
    "importJobs": [
        {
            "completionTime": "2022-11-29T18:17:49.244Z",
            "creationTime": "2022-11-29T17:32:47.700Z",
            "id": "1234567890",
            "roleArn": "arn:aws:iam::123456789012:role/omics-service-role-
serviceRole-W8O1XMPL7QZ",
            "sequenceStoreId": "1234567890",
            "status": "COMPLETED"
```

```
        },
        {
            "completionTime": "2022-11-23T22:01:34.090Z",
            "creationTime": "2022-11-23T21:52:43.289Z",
            "id": "1234567890",
            "roleArn": "arn:aws:iam::123456789012:role/omics-service-role-
serviceRole-W8O1XMPL7QZ",
            "sequenceStoreId": "1234567890",
            "status": "COMPLETED_WITH_FAILURES"
        }
    ]
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte ListReadSetImportJobs en la Referencia de comandos de la AWS CLI.

`list-read-set-upload-parts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-read-set-upload-parts`.

AWS CLI

Para enumerar todas las partes de una carga de varias partes solicitada para un almacén de secuencias.

El siguiente ejemplo de `list-read-set-upload-parts` enumera todas las partes de una carga de varias partes solicitada para un almacén de secuencias.

```
aws omics list-read-set-upload-parts \
    --sequence-store-id 0123456789 \
    --upload-id 1122334455 \
    --part-source SOURCE1
```

Salida:

```
{
    "parts": [
        {
            "partNumber": 1,
```

```
            "partSize": 94371840,
            "file": "SOURCE1",
            "checksum":
 "984979b9928ae8d8622286c4a9cd8e99d964a22d59ed0f5722e1733eb280e635",
            "lastUpdatedTime": "2023-02-02T20:14:47.533000+00:00"
        }
        {
            "partNumber": 2,
            "partSize": 10471840,
            "file": "SOURCE1",
            "checksum":
 "984979b9928ae8d8622286c4a9cd8e99d964a22d59ed0f5722e1733eb280e635",
            "lastUpdatedTime": "2023-02-02T20:14:47.533000+00:00"
        }
      ]

}
```

Para obtener más información, consulte Direct upload to a sequence store en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte ListReadSetUploadParts en la Referencia de comandos de la AWS CLI.

`list-read-sets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-read-sets`.

AWS CLI

Para obtener una lista de conjuntos de lectura

En el siguiente ejemplo de `list-read-sets` se obtiene una lista de conjuntos de lectura de un almacén de secuencias con el ID `1234567890`.

```
aws omics list-read-sets \
    --sequence-store-id 1234567890
```

Salida:

```
{
    "readSets": [
```

```
        {
            "arn": "arn:aws:omics:us-west-2:123456789012:sequenceStore/1234567890/
readSet/1234567890",
            "creationTime": "2022-11-23T21:55:00.515Z",
            "fileType": "FASTQ",
            "id": "1234567890",
            "name": "HG00146",
            "referenceArn": "arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890",
            "sampleId": "fastq-sample",
            "sequenceStoreId": "1234567890",
            "status": "ACTIVE",
            "subjectId": "fastq-subject"
        }
    ]
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte ListReadSets en la Referencia de comandos de la AWS CLI.

`list-reference-import-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-reference-import-jobs`.

AWS CLI

Para obtener una lista de trabajos de importación de referencia

En el siguiente ejemplo de `list-reference-import-jobs` se obtiene una lista de trabajos de importación de referencia de un almacén de referencia con el ID `1234567890`.

```
aws omics list-reference-import-jobs \
    --reference-store-id 1234567890
```

Salida:

```
{
    "importJobs": [
        {
```

```
            "completionTime": "2022-11-23T19:54:58.204Z",
            "creationTime": "2022-11-23T19:53:20.729Z",
            "id": "1234567890",
            "referenceStoreId": "1234567890",
            "roleArn": "arn:aws:iam::123456789012:role/omics-service-role-
serviceRole-W8O1XMPL7QZ",
            "status": "COMPLETED"
        },
        {
            "creationTime": "2022-11-23T20:34:03.250Z",
            "id": "1234567890",
            "referenceStoreId": "1234567890",
            "roleArn": "arn:aws:iam::123456789012:role/omics-service-role-
serviceRole-W8O1XMPL7QZ",
            "status": "IN_PROGRESS"
        }
    ]
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte ListReferenceImportJobs en la Referencia de comandos de la AWS CLI.

`list-reference-stores`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-reference-stores`.

AWS CLI

Para obtener una lista de almacenes de referencias

En el siguiente ejemplo de `list-reference-stores` se obtiene una lista de almacenes de referencias.

```
aws omics list-reference-stores
```

Salida:

```
{
    "referenceStores": [
        {
```

```
            "arn": "arn:aws:omics:us-west-2:123456789012:referenceStore/1234567890",
            "creationTime": "2022-11-22T22:13:25.947Z",
            "id": "1234567890",
            "name": "my-ref-store"
        }
    ]
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte ListReferenceStores en la Referencia de comandos de la AWS CLI.

`list-references`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-references`.

AWS CLI

Para obtener una lista de referencias

En el siguiente ejemplo de `list-references` se obtiene una lista de referencias de genoma de un almacén de referencia con el ID `1234567890`.

```
aws omics list-references \
    --reference-store-id 1234567890
```

Salida:

```
{
    "references": [
        {
            "arn": "arn:aws:omics:us-west-2:123456789012:referenceStore/1234567890/
reference/1234567890",
            "creationTime": "2022-11-22T22:27:09.033Z",
            "id": "1234567890",
            "md5": "7ff134953dcca8c8997453bbb80b6b5e",
            "name": "assembly-38",
            "referenceStoreId": "1234567890",
            "status": "ACTIVE",
            "updateTime": "2022-11-22T22:27:09.033Z"
```

```
        }
    ]
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información de la API, consulte ListReferences en la Referencia de comandos de la AWS CLI.

`list-run-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-run-groups`.

AWS CLI

Para obtener una lista de grupos de ejecución

En el ejemplo siguiente de `list-run-groups` se obtiene una lista de grupos de ejecución.

```
aws omics list-run-groups
```

Salida:

```
{
    "items": [
        {
            "arn": "arn:aws:omics:us-west-2:123456789012:runGroup/1234567",
            "creationTime": "2022-12-01T00:58:42.915219Z",
            "id": "1234567",
            "maxCpus": 20,
            "maxDuration": 600,
            "name": "cram-convert"
        }
    ]
}
```

Para obtener más información, consulte Creación de grupos de ejecución en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte ListRunGroups en la Referencia de comandos de la AWS CLI.

`list-run-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-run-tasks`.

AWS CLI

Para obtener una lista de tareas

En el siguiente ejemplo de `list-run-tasks` se obtiene una lista de tareas para una ejecución de flujo de trabajo.

```
aws omics list-run-tasks \
    --id 1234567
```

Salida:

```
{
    "items": [
        {
            "cpus": 1,
            "creationTime": "2022-11-30T23:13:00.718651Z",
            "memory": 15,
            "name": "CramToBamTask",
            "startTime": "2022-11-30T23:17:47.016Z",
            "status": "COMPLETED",
            "stopTime": "2022-11-30T23:18:21.503Z",
            "taskId": "1234567"
        },
        {
            "cpus": 1,
            "creationTime": "2022-11-30T23:18:32.315606Z",
            "memory": 4,
            "name": "ValidateSamFile",
            "startTime": "2022-11-30T23:23:40.165Z",
            "status": "COMPLETED",
            "stopTime": "2022-11-30T23:24:14.766Z",
            "taskId": "1234567"
        }
    ]
}
```

Para obtener más información, consulte Ciclo de vida de las tareas en una ejecución de HealthOmics en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte ListRunTasks en la Referencia de comandos de la AWS CLI.

`list-runs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-runs`.

AWS CLI

Para obtener una lista de ejecuciones de flujo de trabajo

En el siguiente ejemplo de `list-runs` se obtiene una lista de ejecuciones de flujo de trabajo.

```
aws omics list-runs
```

Salida:

```
{
    "items": [
        {
            "arn": "arn:aws:omics:us-west-2:123456789012:run/1234567",
            "creationTime": "2022-12-02T23:20:01.202074Z",
            "id": "1234567",
            "name": "cram-to-bam",
            "priority": 1,
            "startTime": "2022-12-02T23:29:18.115Z",
            "status": "COMPLETED",
            "stopTime": "2022-12-02T23:57:54.428812Z",
            "storageCapacity": 10,
            "workflowId": "1234567"
        },
        {
            "arn": "arn:aws:omics:us-west-2:123456789012:run/1234567",
            "creationTime": "2022-12-03T00:16:57.180066Z",
            "id": "1234567",
            "name": "cram-to-bam",
            "priority": 1,
            "startTime": "2022-12-03T00:26:50.233Z",
            "status": "FAILED",
            "stopTime": "2022-12-03T00:37:21.451340Z",
            "storageCapacity": 10,
            "workflowId": "1234567"
        },
```

```
        {
            "arn": "arn:aws:omics:us-west-2:123456789012:run/1234567",
            "creationTime": "2022-12-05T17:57:08.444817Z",
            "id": "1234567",
            "name": "cram-to-bam",
            "status": "STARTING",
            "workflowId": "1234567"
        }
    ]
}
```

Para obtener más información, consulte Ejecución del ciclo de vida en un flujo de trabajo en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte ListRuns en la Referencia de comandos de AWS CLI.

`list-sequence-stores`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-sequence-stores`.

AWS CLI

Para obtener una lista de almacenes de secuencias

En el siguiente ejemplo de `list-sequence-stores` se obtiene una lista de almacenes de secuencias.

```
aws omics list-sequence-stores
```

Salida:

```
{
    "sequenceStores": [
        {
            "arn": "arn:aws:omics:us-west-2:123456789012:sequenceStore/1234567890",
            "creationTime": "2022-11-23T01:24:33.629Z",
            "id": "1234567890",
            "name": "my-seq-store"
        }
    ]
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte ListSequenceStores en la Referencia de comandos de la AWS CLI.

`list-shares`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-shares`.

AWS CLI

Para enumerar las acciones disponibles de los datos de análisis de HealthOmics

En el siguiente ejemplo de `list-shares` se enumeran todos los recursos compartidos que se han creado para un propietario de recursos.

```
aws omics list-shares \
    --resource-owner SELF
```

Salida:

```
{
    "shares": [
        {
            "shareId": "595c1cbd-a008-4eca-a887-954d30c91c6e",
            "name": "myShare",
            "resourceArn": "arn:aws:omics:us-west-2:555555555555:variantStore/
store_1",
            "principalSubscriber": "123456789012",
            "ownerId": "555555555555",
            "status": "PENDING"
        }
        {
            "shareId": "39b65d0d-4368-4a19-9814-b0e31d73c10a",
            "name": "myShare3456",
            "resourceArn": "arn:aws:omics:us-west-2:555555555555:variantStore/
store_2",
            "principalSubscriber": "123456789012",
            "ownerId": "555555555555",
            "status": "ACTIVE"
        },
```

```
        {
            "shareId": "203152f5-eef9-459d-a4e0-a691668d44ef",
            "name": "myShare4",
            "resourceArn": "arn:aws:omics:us-west-2:555555555555:variantStore/
store_3",
            "principalSubscriber": "123456789012",
            "ownerId": "555555555555",
            "status": "ACTIVE"
        }
    ]
}
```

Para obtener más información, consulte Cross-account sharing en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte ListShares en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para obtener una lista de etiquetas

En el siguiente ejemplo de `list-tags-for-resource` se obtiene una lista de etiquetas para un flujo de trabajo con el ID `1234567`.

```
aws omics list-tags-for-resource \
    --resource-arn arn:aws:omics:us-west-2:123456789012:workflow/1234567
```

Salida:

```
{
    "tags": {
        "department": "analytics"
    }
}
```

Para obtener más información, consulte Tagging resources in Amazon Omics en la Guía para desarrolladores de Amazon Omics.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-variant-import-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-variant-import-jobs`.

AWS CLI

Para obtener una lista de trabajos de importación de variantes

En el siguiente ejemplo de `list-variant-import-jobs` se obtiene una lista de trabajos de importación de variantes.

```
aws omics list-variant-import-jobs
```

Salida:

```
{
    "variantImportJobs": [
        {
            "creationTime": "2022-11-23T22:47:02.514002Z",
            "destinationName": "my_var_store",
            "id": "69cb65d6-xmpl-4a4a-9025-4565794b684e",
            "roleArn": "arn:aws:iam::123456789012:role/omics-service-role-
serviceRole-W8O1XMPL7QZ",
            "runLeftNormalization": false,
            "status": "COMPLETED",
            "updateTime": "2022-11-23T22:49:17.976597Z"
        },
        {
            "creationTime": "2022-11-23T22:42:50.037812Z",
            "destinationName": "my_var_store",
            "id": "edd7b8ce-xmpl-47e2-bc99-258cac95a508",
            "roleArn": "arn:aws:iam::123456789012:role/omics-service-role-
serviceRole-W8O1XMPL7QZ",
            "runLeftNormalization": false,
            "status": "COMPLETED",
            "updateTime": "2022-11-23T22:45:26.009880Z"
        }
    ]
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte ListVariantImportJobs en la Referencia de comandos de la AWS CLI.

`list-variant-stores`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-variant-stores`.

AWS CLI

Para obtener una lista de almacenes de variantes

En el siguiente ejemplo de `list-variant-stores` se obtiene una lista de almacenes de variantes.

```
aws omics list-variant-stores
```

Salida:

```
{
    "variantStores": [
        {
            "creationTime": "2022-11-23T22:09:07.534499Z",
            "id": "02dexmplcfdd",
            "name": "my_var_store",
            "reference": {
                "referenceArn": "arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890"
            },
            "status": "CREATING",
            "storeArn": "arn:aws:omics:us-west-2:123456789012:variantStore/
my_var_store",
            "storeSizeBytes": 0,
            "updateTime": "2022-11-23T22:09:24.931711Z"
        },
        {
            "creationTime": "2022-09-23T23:00:09.140265Z",
            "id": "8777xmpl1a24",
            "name": "myvstore0",
            "status": "ACTIVE",
```

```
            "storeArn": "arn:aws:omics:us-west-2:123456789012:variantStore/
myvstore0",
            "storeSizeBytes": 0,
            "updateTime": "2022-09-23T23:03:26.013220Z"
        }
    ]
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte ListVariantStores en la Referencia de comandos de la AWS CLI.

`list-workflows`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-workflows`.

AWS CLI

Para obtener una lista de flujos de trabajo

En el siguiente ejemplo de `list-workflows` se obtiene una lista de flujos de trabajo.

```
aws omics list-workflows
```

Salida:

```
{
    "items": [
        {
            "arn": "arn:aws:omics:us-west-2:123456789012:workflow/1234567",
            "creationTime": "2022-09-23T23:08:22.041227Z",
            "digest": "nSCNo/qMWFxmplXpUdokXJnwgneOaxyyc2YOxVxrJTE=",
            "id": "1234567",
            "name": "my-wkflow-0",
            "status": "ACTIVE",
            "type": "PRIVATE"
        },
        {
            "arn": "arn:aws:omics:us-west-2:123456789012:workflow/1234567",
            "creationTime": "2022-11-30T22:33:16.225368Z",
```

```
            "digest":
 "sha256:c54bxmpl742dcc26f7fa1f10e37550ddd8f251f418277c0a58e895b801ed28cf",
            "id": "1234567",
            "name": "cram-converter",
            "status": "ACTIVE",
            "type": "PRIVATE"
        }
    ]
}
```

Para obtener más información, consulte Creación de flujos de trabajo privados en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte ListWorkflows en la Referencia de comandos de la AWS CLI.

`start-annotation-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-annotation-import-job`.

AWS CLI

Para importar anotaciones

El siguiente ejemplo de `start-annotation-import-job` se importan anotaciones de Amazon S3.

```
aws omics start-annotation-import-job \
    --destination-name tsv_ann_store \
    --no-run-left-normalization \
    --role-arn arn:aws:iam::123456789012:role/omics-service-role-serviceRole-
W801XMPL7QZ \
    --items source=s3://omics-artifacts-01d6xmpl4e72dd32/targetedregions.bed.gz
```

Salida:

```
{
    "jobId": "984162c7-xmpl-4d23-ab47-286f7950bfbf"
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte StartAnnotationImportJob en la Referencia de comandos de la AWS CLI.

`start-read-set-activation-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-read-set-activation-job`.

AWS CLI

Para activar un conjunto de lectura archivado

En el siguiente ejemplo de `start-read-set-activation-job` se eliminan dos conjuntos de lectura.

```
aws omics start-read-set-activation-job \
    --sequence-store-id 1234567890 \
    --sources readSetId=1234567890 readSetId=1234567890
```

Salida:

```
{
    "creationTime": "2022-12-06T22:35:10.100Z",
    "id": "1234567890",
    "sequenceStoreId": "1234567890",
    "status": "SUBMITTED"
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener detalles sobre la API, consulte StartReadSetActivationJob en la Referencia de comandos de la AWS CLI.

`start-read-set-export-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-read-set-export-job`.

AWS CLI

Para exportar un conjunto de lectura

En el siguiente ejemplo de `start-read-set-export-job` se exportan dos conjuntos de lectura a Amazon S3.

```
   aws omics start-read-set-export-job \
       --sequence-store-id 1234567890 \
       --sources readSetId=1234567890 readSetId=1234567890 \
       --role-arn arn:aws:iam::123456789012:role/omics-service-role-serviceRole-
W8O1XMPL7QZ
\
       --destination s3://omics-artifacts-01d6xmpl4e72dd32/read-set-export/
```

Salida:

```
{
    "creationTime": "2022-12-06T22:37:18.612Z",
    "destination": "s3://omics-artifacts-01d6xmpl4e72dd32/read-set-export/",
    "id": "1234567890",
    "sequenceStoreId": "1234567890",
    "status": "SUBMITTED"
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte StartReadSetExportJob en la Referencia de comandos de la AWS CLI.

`start-read-set-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-read-set-import-job`.

AWS CLI

Para importar un conjunto de lectura

En el siguiente ejemplo de `start-read-set-import-job` se importa un conjunto de lectura.

```
aws omics start-read-set-import-job \
    --sequence-store-id 1234567890 \
    --role-arn arn:aws:iam::123456789012:role/omics-service-role-serviceRole-
W8O1XMPL7QZ \
    --sources file://readset-sources.json
```

readset-sources.json es un documento de JSON con el siguiente contenido.

```
[
    {
        "sourceFiles":
        {
            "source1": "s3://omics-artifacts-01d6xmpl4e72dd32/
HG00100.chrom20.ILLUMINA.bwa.GBR.low_coverage.20101123.bam"
        },
        "sourceFileType": "BAM",
        "subjectId": "bam-subject",
        "sampleId": "bam-sample",
        "referenceArn": "arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890",
        "name": "HG00100"
    }
]
```

Salida:

```
{
    "creationTime": "2022-11-23T01:36:38.158Z",
    "id": "1234567890",
    "roleArn": "arn:aws:iam::123456789012:role/omics-service-role-serviceRole-
W8O1XMPL7QZ",
    "sequenceStoreId": "1234567890",
    "status": "SUBMITTED"
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte StartReadSetImportJob en la Referencia de comandos de la AWS CLI.

`start-reference-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-reference-import-job`.

AWS CLI

Para importar un genoma de referencia

El siguiente ejemplo de `start-reference-import-job` importa un genoma de referencia de Amazon S3.

```
aws omics start-reference-import-job \
    --reference-store-id 1234567890 \
    --role-arn arn:aws:iam::123456789012:role/omics-service-role-serviceRole-W801XMPL7QZ \
    --sources sourceFile=s3://omics-artifacts-01d6xmpl4e72dd32/Homo_sapiens_assembly38.fasta,name=assembly-38
```

Salida:

```
{
    "creationTime": "2022-11-22T22:25:41.124Z",
    "id": "1234567890",
    "referenceStoreId": "1234567890",
    "roleArn": "arn:aws:iam::123456789012:role/omics-service-role-serviceRole-W801XMPL7QZ",
    "status": "SUBMITTED"
}
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte StartReferenceImportJob en la Referencia de comandos de la AWS CLI.

`start-run`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-run`.

AWS CLI

Para ejecutar un flujo de trabajo

En el siguiente ejemplo de `start-run` se ejecuta un flujo de trabajo con el ID 1234567.

```
aws omics start-run \
    --workflow-id 1234567 \
    --role-arn arn:aws:iam::123456789012:role/omics-service-role-serviceRole-W801XMPL7QZ \
    --name 'cram-to-bam' \
```

```
    --output-uri s3://omics-artifacts-01d6xmpl4e72dd32/workflow-output/ \
    --run-group-id 1234567 \
    --priority 1 \
    --storage-capacity 10 \
    --log-level ALL \
    --parameters file://workflow-inputs.json
```

workflow-inputs.json es un documento de JSON con el siguiente contenido.

```
{
    "sample_name": "NA12878",
    "input_cram": "s3://omics-artifacts-01d6xmpl4e72dd32/NA12878.cram",
    "ref_dict": "s3://omics-artifacts-01d6xmpl4e72dd32/
Homo_sapiens_assembly38.dict",
    "ref_fasta": "s3://omics-artifacts-01d6xmpl4e72dd32/
Homo_sapiens_assembly38.fasta",
    "ref_fasta_index": "omics-artifacts-01d6xmpl4e72dd32/
Homo_sapiens_assembly38.fasta.fai"
}
```

Salida:

```
{
    "arn": "arn:aws:omics:us-west-2:123456789012:run/1234567",
    "id": "1234567",
    "status": "PENDING",
    "tags": {}
}
```

Para obtener más información, consulte Inicio de una ejecución en la Guía del usuario de AWS HealthOmics.

Para cargar archivos de origen de Amazon Omics

También puede cargar archivos de origen desde el almacenamiento de Amazon Omics mediante URI específicos del servicio. El siguiente ejemplo de archivo workflow-inputs.json utiliza los URI de Amazon Omics para los orígenes del genoma de referencia y del conjunto de lectura.

```
{
    "sample_name": "NA12878",
    "input_cram": "omics://123456789012.storage.us-west-2.amazonaws.com/1234567890/
readSet/1234567890/source1",
```

```
    "ref_dict": "s3://omics-artifacts-01d6xmpl4e72dd32/
Homo_sapiens_assembly38.dict",
    "ref_fasta": "omics://123456789012.storage.us-west-2.amazonaws.com/1234567890/
reference/1234567890",
    "ref_fasta_index": "omics://123456789012.storage.us-
west-2.amazonaws.com/1234567890/reference/1234567890/index"
}
```

- Para obtener información sobre la API, consulte StartRun en la Referencia de comandos de la AWS CLI.

`start-variant-import-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-variant-import-job`.

AWS CLI

Para importar un archivo de variantes

En el siguiente ejemplo de `start-variant-import-job` se importa un archivo de variantes en formato VCF.

```
aws omics start-variant-import-job \
    --destination-name my_var_store \
    --no-run-left-normalization  \
    --role-arn arn:aws:iam::123456789012:role/omics-service-role-serviceRole-
W801XMPL7QZ \
    --items source=s3://omics-artifacts-01d6xmpl4e72dd32/
Homo_sapiens_assembly38.known_indels.vcf.gz
```

Salida:

```
{
    "jobId": "edd7b8ce-xmpl-47e2-bc99-258cac95a508"
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte StartVariantImportJob en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para etiquetar un recurso

En el siguiente ejemplo de `tag-resource` se añade una etiqueta `department` a un flujo de trabajo con el ID `1234567`.

```
aws omics tag-resource \
    --resource-arn arn:aws:omics:us-west-2:123456789012:workflow/1234567 \
    --tags department=analytics
```

Para obtener más información, consulte Tagging resources in Amazon Omics en la Guía para desarrolladores de Amazon Omics.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar una etiqueta de un recurso

En el ejemplo siguiente de `untag-resource` se elimina la etiqueta `department` de un flujo de trabajo.

```
aws omics untag-resource \
    --resource-arn arn:aws:omics:us-west-2:123456789012:workflow/1234567 \
    --tag-keys department
```

Para obtener más información, consulte Almacenamiento de Omics en la Guía para desarrolladores de Amazon Omics.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-annotation-store

En el siguiente ejemplo de código, se muestra cómo utilizar `update-annotation-store`.

AWS CLI

Para actualizar un almacén de anotaciones

En el siguiente ejemplo de `update-annotation-store` se actualiza la descripción de un almacén de anotaciones llamado `my_vcf_store`.

```
aws omics update-annotation-store \
    --name my_vcf_store \
    --description "VCF annotation store"
```

Salida:

```
{
    "creationTime": "2022-12-05T18:00:56.101860Z",
    "description": "VCF annotation store",
    "id": "bd6axmpl2444",
    "name": "my_vcf_store",
    "reference": {
        "referenceArn": "arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890"
    },
    "status": "ACTIVE",
    "storeFormat": "VCF",
    "updateTime": "2022-12-05T18:13:16.100051Z"
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte UpdateAnnotationStore en la Referencia de comandos de la AWS CLI.

update-run-group

En el siguiente ejemplo de código, se muestra cómo utilizar `update-run-group`.

AWS CLI

Para actualizar un grupo de ejecución

En el siguiente ejemplo de `update-run-group` se actualiza la configuración de un grupo de ejecución con el ID `1234567`.

```
aws omics update-run-group \
    --id 1234567 \
    --max-cpus 10
```

Salida:

```
{
    "arn": "arn:aws:omics:us-west-2:123456789012:runGroup/1234567",
    "creationTime": "2022-12-01T00:58:42.915219Z",
    "id": "1234567",
    "maxCpus": 10,
    "maxDuration": 600,
    "name": "cram-convert",
    "tags": {}
}
```

Para obtener más información, consulte Flujos de trabajo de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información sobre la API, consulte UpdateRunGroup en la Referencia de comandos de la AWS CLI.

`update-variant-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-variant-store`.

AWS CLI

Para actualizar un almacén de variantes

En el siguiente ejemplo de `update-variant-store` se actualiza la descripción de un almacén de variantes llamado `my_var_store`.

```
aws omics update-variant-store \
```

```
    --name my_var_store \
    --description "variant store"
```

Salida:

```
{
    "creationTime": "2022-11-23T22:09:07.534499Z",
    "description": "variant store",
    "id": "02dexmplcfdd",
    "name": "my_var_store",
    "reference": {
        "referenceArn": "arn:aws:omics:us-
west-2:123456789012:referenceStore/1234567890/reference/1234567890"
    },
    "status": "ACTIVE",
    "updateTime": "2022-12-05T18:23:37.686402Z"
}
```

Para obtener más información, consulte Análisis de Omics en la Guía para desarrolladores de Amazon Omics.

- Para obtener información acerca de la API, consulte UpdateVariantStore en la Referencia de comandos de la AWS CLI.

`update-workflow`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-workflow`.

AWS CLI

Para actualizar un flujo de trabajo

En el siguiente ejemplo de `update-workflow` se actualiza la descripción de un flujo de trabajo con el ID `1234567`.

```
aws omics update-workflow \
    --id 1234567 \
    --description "copy workflow"
```

Para obtener más información, consulte Creación o actualización de un flujo de trabajo en la Guía del usuario de AWS HealthOmics.

- Para obtener información sobre la API, consulte UpdateWorkflow en la Referencia de comandos de la AWS CLI.

`upload-read-set-part`

En el siguiente ejemplo de código, se muestra cómo utilizar `upload-read-set-part`.

AWS CLI

Para cargar una parte de conjunto de lectura.

En el siguiente ejemplo de `upload-read-set-part` se carga una parte específica de un conjunto de lectura.

```
aws omics upload-read-set-part \
    --sequence-store-id 0123456789 \
    --upload-id 1122334455 \
    --part-source SOURCE1 \
    --part-number 1 \
    --payload /path/to/file/read_1_part_1.fastq.gz
```

Salida:

```
{
    "checksum": "984979b9928ae8d8622286c4a9cd8e99d964a22d59ed0f5722e1733eb280e635"
}
```

Para obtener más información, consulte Direct upload to a sequence store en la Guía del usuario de AWS HealthOmics.

- Para obtener más información sobre la API, consulte UploadReadSetPart en la referencia de comandos de la AWS CLI.

Ejemplos de IAM que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con IAM.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-client-id-to-open-id-connect-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-client-id-to-open-id-connect-provider`.

AWS CLI

Cómo agregar una nueva ID de cliente (audiencia) a un proveedor de Open-ID Connect (OIDC

El siguiente comando `add-client-id-to-open-id-connect-provider` agrega el ID de cliente `my-application-ID` al proveedor OIDC denominado `server.example.com`.

```
aws iam add-client-id-to-open-id-connect-provider \
    --client-id my-application-ID \
    --open-id-connect-provider-arn arn:aws:iam::123456789012:oidc-provider/
server.example.com
```

Este comando no genera ninguna salida.

Para crear un proveedor de OIDC, utilice el comando `create-open-id-connect-provider`.

Para obtener más información, consulte Creación de proveedores de identidad OpenID Connect (OIDC) en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte AddClientIDToOpenIDConnectProvider en la Referencia de comandos de la AWS CLI.

`add-role-to-instance-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-role-to-instance-profile`.

AWS CLI

Cómo añadir un rol a un perfil de instancia

El siguiente comando `add-role-to-instance-profile` agrega el rol nombrado `S3Access` al perfil de instancia llamado `Webserver`.

```
aws iam add-role-to-instance-profile \
    --role-name S3Access \
    --instance-profile-name Webserver
```

Este comando no genera ninguna salida.

Para crear un perfil de instancia, utilice el comando `create-instance-profile`.

Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2 en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte AddRoleToInstanceProfile en la Referencia de comandos de la AWS CLI.

`add-user-to-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-user-to-group`.

AWS CLI

Cómo añadir un usuario a un grupo de IAM

El siguiente comando `add-user-to-group` añade un usuario de IAM denominado `Bob` al grupo de IAM denominado `Admins`.

```
aws iam add-user-to-group \
    --user-name Bob \
    --group-name Admins
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adición y eliminación de usuarios de un grupo de usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte AddUserToGroup en la Referencia de comandos de la AWS CLI.

`attach-group-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-group-policy`.

AWS CLI

Cómo asociar una política administrada a un usuario de IAM

El siguiente comando `attach-group-policy` asocia la política administrada de AWS denominada `ReadOnlyAccess` al usuario de IAM denominado `Finance`.

```
aws iam attach-group-policy \
    --policy-arn arn:aws:iam::aws:policy/ReadOnlyAccess \
    --group-name Finance
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Políticas administradas y políticas insertadas en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte AttachGroupPolicy en la Referencia de comandos de la AWS CLI.

`attach-role-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-role-policy`.

AWS CLI

Cómo asociar una política administrada a un rol de IAM

El siguiente comando `attach-role-policy` asocia la política administrada de AWS denominada `ReadOnlyAccess` al rol de IAM denominado `ReadOnlyRole`.

```
aws iam attach-role-policy \
    --policy-arn arn:aws:iam::aws:policy/ReadOnlyAccess \
    --role-name ReadOnlyRole
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Políticas administradas y políticas insertadas en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte AttachRolePolicy en la Referencia de comandos de la AWS CLI.

`attach-user-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-user-policy`.

AWS CLI

Cómo asociar una política administrada a un usuario de IAM

El siguiente comando `attach-user-policy` asocia la política administrada de AWS denominada `AdministratorAccess` al usuario de IAM denominado `Alice`.

```
aws iam attach-user-policy \
    --policy-arn arn:aws:iam::aws:policy/AdministratorAccess \
    --user-name Alice
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Políticas administradas y políticas insertadas en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte AttachUserPolicy en la Referencia de comandos de la AWS CLI.

`change-password`

En el siguiente ejemplo de código, se muestra cómo utilizar `change-password`.

AWS CLI

Cómo cambiar la contraseña de un usuario de IAM

Para cambiar la contraseña de su usuario de IAM, recomendamos utilizar el parámetro `--cli-input-json` para pasar un archivo JSON que contenga sus contraseñas antiguas y nuevas. Con este método, puede utilizar contraseñas seguras con caracteres no alfanuméricos. Puede resultar difícil utilizar contraseñas con caracteres no alfanuméricos al pasarlas como parámetros de la línea de comandos. Para usar el parámetro `--cli-input-json`, comience por usar el comando `change-password` con el parámetro `--generate-cli-skeleton`, como en el siguiente ejemplo.

```
aws iam change-password \
    --generate-cli-skeleton > change-password.json
```

El comando anterior crea un archivo JSON llamado change-password.json que puede usar para rellenar las contraseñas antiguas y nuevas. Por ejemplo, el rol podría tener el siguiente aspecto.

```
{
    "OldPassword": "3s0K_;xh4~8XXI",
    "NewPassword": "]35d/{pB9Fo9wJ"
}
```

A continuación, para cambiar la contraseña, vuelva a utilizar el comando `change-password`, esta vez pasando el parámetro `--cli-input-json` para especificar el archivo JSON. El siguiente comando `change-password` usa el parámetro `--cli-input-json` con un archivo JSON llamado change-password.json.

```
aws iam change-password \
    --cli-input-json file://change-password.json
```

Este comando no genera ninguna salida.

Solo los usuarios de IAM pueden llamar a este comando. Si se llama a este comando con las credenciales de la cuenta de AWS (raíz), el comando devuelve un error `InvalidUserType`.

Para obtener más información, consulte Cómo el usuario de IAM cambia su propia contraseña en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ChangePassword en la Referencia de comandos de la AWS CLI.

`create-access-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-access-key`.

AWS CLI

Cómo crear una clave de acceso para un usuario de IAM

El siguiente comando `create-access-key` crea una clave de acceso (un ID de clave de acceso y una clave de acceso secreta) para el usuario de IAM denominado Bob.

```
aws iam create-access-key \
    --user-name Bob
```

Salida:

```
{
    "AccessKey": {
        "UserName": "Bob",
        "Status": "Active",
        "CreateDate": "2015-03-09T18:39:23.411Z",
        "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYzEXAMPLEKEY",
        "AccessKeyId": "AKIAIOSFODNN7EXAMPLE"
    }
}
```

Almacene la clave de acceso secreta en un lugar seguro. Si se pierde, no se puede recuperar y debe crear una nueva clave de acceso.

Para obtener más información, consulte Administración de claves de acceso para usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreateAccessKey en la Referencia de comandos de la AWS CLI.

`create-account-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-account-alias`.

AWS CLI

Cómo crear un alias de una cuenta

El siguiente comando `create-account-alias` crea el alias `examplecorp` para su cuenta de AWS.

```
aws iam create-account-alias \
    --account-alias examplecorp
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Su ID de cuenta y alias de AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreateAccountAlias en la Referencia de comandos de la AWS CLI.

`create-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-group`.

AWS CLI

Cómo crear un grupo de IAM

El siguiente comando `create-group` crea un grupo de IAM denominado `Admins`.

```
aws iam create-group \
    --group-name Admins
```

Salida:

```
{
    "Group": {
        "Path": "/",
        "CreateDate": "2015-03-09T20:30:24.940Z",
        "GroupId": "AIDGPMS9RO4H3FEXAMPLE",
        "Arn": "arn:aws:iam::123456789012:group/Admins",
        "GroupName": "Admins"
    }
}
```

Para obtener más información, consulte Creación de grupos de usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreateGroup en la Referencia de comandos de la AWS CLI.

`create-instance-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-instance-profile`.

AWS CLI

Cómo crear un perfil de instancia

El siguiente comando `create-instance-profile` crea un perfil de instancia denominado `Webserver`.

```
aws iam create-instance-profile \
    --instance-profile-name Webserver
```

Salida:

```
{
    "InstanceProfile": {
        "InstanceProfileId": "AIPAJMBYC7DLSPEXAMPLE",
        "Roles": [],
        "CreateDate": "2015-03-09T20:33:19.626Z",
        "InstanceProfileName": "Webserver",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:instance-profile/Webserver"
    }
}
```

Para añadir un rol a un perfil de instancia, utilice el comando `add-role-to-instance-profile`.

Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2 en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreateInstanceProfile en la Referencia de comandos de la AWS CLI.

`create-login-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-login-profile`.

AWS CLI

Cómo crear una contraseña para un usuario de IAM

Para crear una contraseña para un usuario de IAM, recomendamos usar el parámetro `--cli-input-json` para pasar un archivo JSON que contenga la contraseña. Con este método, puede crear una contraseña segura con caracteres no alfanuméricos. Puede resultar difícil crear una contraseña con caracteres no alfanuméricos si la pasa como parámetro de la línea de comandos.

Para usar el parámetro `--cli-input-json`, comience por usar el comando `create-login-profile` con el parámetro `--generate-cli-skeleton`, como en el siguiente ejemplo.

```
aws iam create-login-profile \
    --generate-cli-skeleton > create-login-profile.json
```

El comando anterior crea un archivo JSON llamado create-login-profile.json que puede utilizar para rellenar la información de un comando posterior `create-login-profile`. Por ejemplo:

```
{
    "UserName": "Bob",
    "Password": "&1-3a6u:RA0djs",
    "PasswordResetRequired": true
}
```

A continuación, para crear una contraseña para un usuario de IAM, vuelva a utilizar el comando `create-login-profile`, esta vez pasando el parámetro `--cli-input-json` para especificar el archivo JSON. El siguiente comando `create-login-profile` usa el parámetro `--cli-input-json` con un archivo JSON llamado create-login-profile.json.

```
aws iam create-login-profile \
    --cli-input-json file://create-login-profile.json
```

Salida:

```
{
    "LoginProfile": {
        "UserName": "Bob",
        "CreateDate": "2015-03-10T20:55:40.274Z",
        "PasswordResetRequired": true
    }
}
```

Si la nueva contraseña infringe la política de contraseñas de la cuenta, el comando devuelve el error `PasswordPolicyViolation`.

Para cambiar la contraseña de un usuario que ya posee una, utilice `update-login-profile`. Para establecer una política de contraseñas para la cuenta, utilice el comando `update-account-password-policy`.

Si la política de contraseñas de la cuenta lo permite, los usuarios de IAM pueden cambiar sus propias contraseñas mediante el comando `change-password`.

Para obtener más información, consulte Gestión de contraseñas para usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreateLogin Profile en la Referencia de comandos de la AWS CLI.

`create-open-id-connect-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-open-id-connect-provider`.

AWS CLI

Cómo crear un proveedor de IAM OpenID Connect (OIDC

Para crear un proveedor de OpenID Connect (OIDC), se recomienda utilizar el parámetro `--cli-input-json` para pasar un archivo JSON que contenga los parámetros necesarios. Al crear un proveedor de OIDC, debe pasar la URL del proveedor y la URL debe empezar por `https://`. Puede resultar difícil pasar la URL como parámetro de la línea de comandos, ya que los dos puntos (:) y la barra inclinada (/) tienen un significado especial en algunos entornos de línea de comandos. El uso del parámetro `--cli-input-json` evita esta limitación.

Para usar el parámetro `--cli-input-json`, comience por usar el comando `create-open-id-connect-provider` con el parámetro `--generate-cli-skeleton`, como en el siguiente ejemplo.

```
aws iam create-open-id-connect-provider \
    --generate-cli-skeleton > create-open-id-connect-provider.json
```

El comando anterior crea un archivo JSON llamado create-open-id-connect-provider.json que puede utilizar para rellenar la información de un comando posterior `create-open-id-connect-provider`. Por ejemplo:

```
{
    "Url": "https://server.example.com",
    "ClientIDList": [
```

```
        "example-application-ID"
    ],
    "ThumbprintList": [
        "c3768084dfb3d2b68b7897bf5f565da8eEXAMPLE"
    ]
}
```

A continuación, para crear el proveedor de OpenID Connect (OIDC), vuelva a utilizar el comando `create-open-id-connect-provider`, esta vez pasando el parámetro `--cli-input-json` para especificar el archivo JSON. El siguiente comando `create-open-id-connect-provider` usa el parámetro `--cli-input-json` con un archivo JSON llamado create-open-id-connect-provider.json.

```
aws iam create-open-id-connect-provider \
    --cli-input-json file://create-open-id-connect-provider.json
```

Salida:

```
{
    "OpenIDConnectProviderArn": "arn:aws:iam::123456789012:oidc-provider/
server.example.com"
}
```

Para obtener más información acerca de cómo crear los proveedores OIDC, consulte Creación de proveedores de identidades de OpenID Connect (OIDC) en la Guía del usuario de AWS IAM.

Para obtener más información sobre la obtención de huellas digitales para un proveedor de OIDC, consulte Obtención de la huella digital de un proveedor de identidades de OpenID Connect en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreateDocumentClassifier en la Referencia de comandos de la AWS CLI.

`create-policy-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-policy-version`.

AWS CLI

Cómo crear una nueva versión de la política administrada

En este ejemplo, se crea una nueva versión v2 de la política de IAM cuyo ARN es `arn:aws:iam::123456789012:policy/MyPolicy` y se la convierte en la versión predeterminada.

```
aws iam create-policy-version \
    --policy-arn arn:aws:iam::123456789012:policy/MyPolicy \
    --policy-document file://NewPolicyVersion.json \
    --set-as-default
```

Salida:

```
{
    "PolicyVersion": {
        "CreateDate": "2015-06-16T18:56:03.721Z",
        "VersionId": "v2",
        "IsDefaultVersion": true
    }
}
```

Para obtener más información, consulte Control de versiones de políticas de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreatePolicyVersion en la Referencia de comandos de la AWS CLI.

`create-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-policy`.

AWS CLI

Ejemplo 1: cómo crear una política administrada por el cliente

El siguiente comando crea una política administrada por el cliente denominada `my-policy`. El archivo `policy.json` es un documento JSON de la carpeta actual que concede acceso de solo lectura a la carpeta `shared` de un bucket de Amazon S3 denominado `amzn-s3-demo-bucket`.

```
aws iam create-policy \
    --policy-name my-policy \
    --policy-document file://policy.json
```

Contenido de policy.json:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/shared/*"
            ]
        }
    ]
}
```

Salida:

```
{
    "Policy": {
        "PolicyName": "my-policy",
        "CreateDate": "2015-06-01T19:31:18.620Z",
        "AttachmentCount": 0,
        "IsAttachable": true,
        "PolicyId": "ZXR6A36LTYANPAI7NJ5UV",
        "DefaultVersionId": "v1",
        "Path": "/",
        "Arn": "arn:aws:iam::0123456789012:policy/my-policy",
        "UpdateDate": "2015-06-01T19:31:18.620Z"
    }
}
```

Para obtener más información sobre el uso de archivos como entrada para los parámetros de cadena, consulte Especificar valores de parámetros para la CLI de AWS en la Guía del usuario de la CLI de AWS.

Ejemplo 2: cómo crear una política administrada por el cliente con una descripción

El siguiente comando crea una política administrada por el cliente denominada `my-policy` con una descripción inmutable.

El archivo `policy.json` es un documento JSON de la carpeta actual que concede acceso a todas las acciones poner, enumerar y obtener de un bucket de Amazon S3 denominado `amzn-s3-demo-bucket`.

```
aws iam create-policy \
    --policy-name my-policy \
    --policy-document file://policy.json \
    --description "This policy grants access to all Put, Get, and List actions for
 amzn-s3-demo-bucket"
```

Contenido de policy.json:

```
{
   "Version":"2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
                "s3:ListBucket*",
                "s3:PutBucket*",
                "s3:GetBucket*"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        }
    ]
}
```

Salida:

```
{
    "Policy": {
        "PolicyName": "my-policy",
        "PolicyId": "ANPAWGSUGIDPEXAMPLE",
        "Arn": "arn:aws:iam::123456789012:policy/my-policy",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 0,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "CreateDate": "2023-05-24T22:38:47+00:00",
```

```
        "UpdateDate": "2023-05-24T22:38:47+00:00"
    }
}
```

Para obtener más información acerca de las políticas basadas en identidades, consulte Políticas basadas en identidades y políticas basadas en recursos en la Guía del usuario de AWS IAM.

Ejemplo 3: cómo crear una política administrada por el cliente con etiquetas

El siguiente comando crea una política administrada por el cliente denominada `my-policy` con etiquetas. En este ejemplo, se utiliza el parámetro `--tags` con las siguientes etiquetas con formato JSON: `'{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location", "Value": "Seattle"}'`. Alternativamente, el parámetro `--tags` se puede usar con etiquetas en formato abreviado: `'Key=Department,Value=Accounting Key=Location,Value=Seattle'`.

El archivo `policy.json` es un documento JSON de la carpeta actual que concede acceso a todas las acciones poner, enumerar y obtener de un bucket de Amazon S3 denominado `amzn-s3-demo-bucket`.

```
aws iam create-policy \
    --policy-name my-policy \
    --policy-document file://policy.json \
    --tags '{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location",
 "Value": "Seattle"}'
```

Contenido de policy.json:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket*",
                "s3:PutBucket*",
                "s3:GetBucket*"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
```

```
        }
    ]
}
```

Salida:

```
{
    "Policy": {
        "PolicyName": "my-policy",
        "PolicyId": "ANPAWGSUGIDPEXAMPLE",
        "Arn": "arn:aws:iam::12345678012:policy/my-policy",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 0,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "CreateDate": "2023-05-24T23:16:39+00:00",
        "UpdateDate": "2023-05-24T23:16:39+00:00",
        "Tags": [
            {
                "Key": "Department",
                "Value": "Accounting"
            },
                "Key": "Location",
                "Value": "Seattle"
            {
        ]
    }
}
```

Para obtener más información sobre las políticas de etiquetado, consulte Políticas de etiquetado administradas por el cliente en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreatePolicy en la Referencia de comandos de la AWS CLI.

`create-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-role`.

AWS CLI

Ejemplo 1: cómo crear un rol de IAM

El siguiente comando `create-role` crean un rol denominado `Test-Role` y le asocia una política de confianza.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json
```

Salida:

```
{
    "Role": {
        "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "CreateDate": "2013-06-07T20:43:32.821Z",
        "RoleName": "Test-Role",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role"
    }
}
```

La política de confianza se define como un documento JSON en el archivo Test-Role-Trust-Policy.json. (El nombre y la extensión del archivo no son significativos). La política de confianza debe especificar una entidad principal.

Utilice el comando `put-role-policy` para asociar una política de permisos a un rol.

Para más información, consulte Creación de roles de IAM en la Guía del usuario de IAM de AWS.

Ejemplo 2: cómo crear un rol de IAM con una duración máxima de sesión especificada

El siguiente comando `create-role` crea un rol denominado `Test-Role` y establece una duración máxima de sesión de 7200 segundos (2 horas).

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --max-session-duration 7200
```

Salida:

```
{
```

```
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:role/Test-Role",
        "CreateDate": "2023-05-24T23:50:25+00:00",
        "AssumeRolePolicyDocument": {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::12345678012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

Para obtener más información, consulte Modificación de la duración máxima de sesión (API de AWS) en la Guía del usuario de AWS IAM.

Ejemplo 3: cómo crear un rol de IAM con etiquetas

El siguiente comando crea un rol de IAM `Test-Role` con etiquetas. En este ejemplo, se utiliza el indicador de parámetro `--tags` con las siguientes etiquetas con formato JSON: `'{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location", "Value": "Seattle"}'`. Alternativamente, el indicador `--tags` se puede usar con etiquetas en formato abreviado: `'Key=Department,Value=Accounting Key=Location,Value=Seattle'`.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --tags '{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location",
 "Value": "Seattle"}'
```

Salida:

```
{
```

```
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role",
        "CreateDate": "2023-05-25T23:29:41+00:00",
        "AssumeRolePolicyDocument": {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::123456789012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        },
        "Tags": [
            {
                "Key": "Department",
                "Value": "Accounting"
            },
            {
                "Key": "Location",
                "Value": "Seattle"
            }
        ]
    }
}
```

Para obtener más información, consulte Etiquetado de roles de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreateRole en la Referencia de comandos de la AWS CLI.

`create-saml-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-saml-provider`.

AWS CLI

Cómo crear un proveedor SAML

En este ejemplo se crea un nuevo proveedor SAML en IAM denominado `MySAMLProvider`. Se describe en el documento de metadatos de SAML que se encuentra en el archivo `SAMLMetaData.xml`.

```
aws iam create-saml-provider \
    --saml-metadata-document file://SAMLMetaData.xml \
    --name MySAMLProvider
```

Salida:

```
{
    "SAMLProviderArn": "arn:aws:iam::123456789012:saml-provider/MySAMLProvider"
}
```

Para obtener más información, consulte Creación de proveedores de identidad SAML de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreateSAMLProvider en la Referencia de comandos de la AWS CLI.

`create-service-linked-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-service-linked-role`.

AWS CLI

Cómo crear un rol vinculado a un servicio

En el siguiente ejemplo de `create-service-linked-role` se crea un rol vinculado a servicios para el servicio de AWS especificado y se asocia la descripción especificada.

```
aws iam create-service-linked-role \
    --aws-service-name lex.amazonaws.com \
    --description "My service-linked role to support Lex"
```

Salida:

```
{
```

```
    "Role": {
        "Path": "/aws-service-role/lex.amazonaws.com/",
        "RoleName": "AWSServiceRoleForLexBots",
        "RoleId": "AROA1234567890EXAMPLE",
        "Arn": "arn:aws:iam::1234567890:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "CreateDate": "2019-04-17T20:34:14+00:00",
        "AssumeRolePolicyDocument": {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Action": [
                        "sts:AssumeRole"
                    ],
                    "Effect": "Allow",
                    "Principal": {
                        "Service": [
                            "lex.amazonaws.com"
                        ]
                    }
                }
            ]
        }
    }
}
```

Para obtener más información, consulte Uso de roles vinculados a servicios en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreateServiceLinkedRole en la Referencia de comandos de la AWS CLI.

`create-service-specific-credential`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-service-specific-credential`.

AWS CLI

Crear un conjunto de credenciales específicas de un servicio para un usuario

En el siguiente ejemplo de `create-service-specific-credential`, se crea un nombre de usuario y una contraseña que se pueden usar para acceder únicamente al servicio configurado.

```
aws iam create-service-specific-credential \
    --user-name sofia \
    --service-name codecommit.amazonaws.com
```

Salida:

```
{
    "ServiceSpecificCredential": {
        "CreateDate": "2019-04-18T20:45:36+00:00",
        "ServiceName": "codecommit.amazonaws.com",
        "ServiceUserName": "sofia-at-123456789012",
        "ServicePassword": "k1zPZM6uVxMQ3oxqgoYlNuJPyRTZ1vREs76zTQE3eJk=",
        "ServiceSpecificCredentialId": "ACCAEXAMPLE123EXAMPLE",
        "UserName": "sofia",
        "Status": "Active"
    }
}
```

Para obtener más información, consulte Crear credenciales de Git para las conexiones HTTPS a CodeCommit en la Guía del usuario de AWS CodeCommit.

- Para obtener más información sobre la API, consulte CreateServiceSpecificCredential en la Referencia de comandos de la AWS CLI.

`create-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-user`.

AWS CLI

Ejemplo 1: cómo crear un usuario de IAM

El siguiente comando `create-user` crea un usuario de IAM denominado Bob en la cuenta actual.

```
aws iam create-user \
    --user-name Bob
```

Salida:

```
{
```

```
    "User": {
        "UserName": "Bob",
        "Path": "/",
        "CreateDate": "2023-06-08T03:20:41.270Z",
        "UserId": "AIDAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:user/Bob"
    }
}
```

Para obtener más información, consulte Creación de un usuario de IAM en su cuenta de AWS en la Guía del usuario de AWS IAM.

Ejemplo 2: cómo crear un usuario de IAM en una ruta específica

El siguiente comando `create-user` crea un usuario de IAM denominado Bob en la ruta especificada.

```
aws iam create-user \
    --user-name Bob \
    --path /division_abc/subdivision_xyz/
```

Salida:

```
{
    "User": {
        "Path": "/division_abc/subdivision_xyz/",
        "UserName": "Bob",
        "UserId": "AIDAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:user/division_abc/subdivision_xyz/Bob",
        "CreateDate": "2023-05-24T18:20:17+00:00"
    }
}
```

Para obtener más información, consulte Identificadores de IAM en la Guía del usuario de AWS IAM.

Ejemplo 3: cómo crear un usuario de IAM con etiquetas

El siguiente comando `create-user` crea un usuario de IAM denominado Bob con etiquetas. En este ejemplo, se utiliza el indicador de parámetro `--tags` con las siguientes etiquetas con formato JSON: `'{"Key": "Department", "Value": "Accounting"}' '{"Key":`

`"Location", "Value": "Seattle"}'`. Alternativamente, el indicador `--tags` se puede usar con etiquetas en formato abreviado: `'Key=Department,Value=Accounting Key=Location,Value=Seattle'`.

```
aws iam create-user \
    --user-name Bob \
    --tags '{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location",
 "Value": "Seattle"}'
```

Salida:

```
{
    "User": {
        "Path": "/",
        "UserName": "Bob",
        "UserId": "AIDAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:user/Bob",
        "CreateDate": "2023-05-25T17:14:21+00:00",
        "Tags": [
            {
                "Key": "Department",
                "Value": "Accounting"
            },
            {
                "Key": "Location",
                "Value": "Seattle"
            }
        ]
    }
}
```

Para obtener más información, consulte Etiquetado de usuarios de IAM en la Guía del usuario de AWS.

Ejemplo 3: cómo crear un usuario de IAM con un límite de permisos establecido

El siguiente comando `create-user` crea un usuario de IAM denominado Bob con el límite de permisos de AmazonS3FullAccess.

```
aws iam create-user \
    --user-name Bob \
```

```
    --permissions-boundary arn:aws:iam::aws:policy/AmazonS3FullAccess
```

Salida:

```
{
    "User": {
        "Path": "/",
        "UserName": "Bob",
        "UserId": "AIDAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:user/Bob",
        "CreateDate": "2023-05-24T17:50:53+00:00",
        "PermissionsBoundary": {
        "PermissionsBoundaryType": "Policy",
        "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AmazonS3FullAccess"
        }
    }
}
```

Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreateUser en la Referencia de comandos de la AWS CLI.

`create-virtual-mfa-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-virtual-mfa-device`.

AWS CLI

Cómo etiquetar un dispositivo MFA virtual

En este ejemplo se crea un nuevo dispositivo MFA virtual denominado `BobsMFADevice`. Crea un archivo que contiene la información de arranque denominada `QRCode.png` y la coloca en el directorio `C:/`. El método de arranque utilizado en este ejemplo es `QRCodePNG`.

```
aws iam create-virtual-mfa-device \
    --virtual-mfa-device-name BobsMFADevice \
    --outfile C:/QRCode.png \
    --bootstrap-method QRCodePNG
```

Salida:

```
{
    "VirtualMFADevice": {
        "SerialNumber": "arn:aws:iam::210987654321:mfa/BobsMFADevice"
}
```

Para obtener más información, consulte Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreateVirtualMfaDevice en la Referencia de comandos de la AWS CLI.

`deactivate-mfa-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `deactivate-mfa-device`.

AWS CLI

Cómo desactivar un dispositivo

Este comando desactiva el dispositivo MFA virtual con el ARN `arn:aws:iam::210987654321:mfa/BobsMFADevice` asociado al usuario Bob.

```
aws iam deactivate-mfa-device \
    --user-name Bob \
    --serial-number arn:aws:iam::210987654321:mfa/BobsMFADevice
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeactivateMfaDevice en la Referencia de comandos de la AWS CLI.

`decode-authorization-message`

En el siguiente ejemplo de código, se muestra cómo utilizar `decode-authorization-message`.

AWS CLI

Para decodificar un mensaje de error de autorización

El siguiente ejemplo de `decode-authorization-message` decodifica el mensaje devuelto por la consola de EC2 al intentar lanzar una instancia sin los permisos necesarios.

```
aws sts decode-authorization-message \
    --encoded-message lxzA8VEjEvu-s0TTt3PgYCXik9YakOqsrFJGRZR98xNcyWAxwRq14xIvd-
npzbgTevuufCTbjeBAaDARg9cbTK1rJbg3awM33o-Vy3ebPErE2-
mWR9hVYdvX-0zKgVOWF9pWjZaJSMqxB-aLXo-I_8TTvBq88x8IFPbMArNdpu0IjxDjzf22PF3SOE3XvIQ-
_PEO0aUqHCCcsSrFtvxm6yQD1nbm6VTIVrfa0Bzy8lsoMo7SjIaJ2r5vph6SY5vCCwg6o2JKe3hIHTa8zRrDbZSFMkcX
Xx9AYAAIr6bhcis7C__bZh4dlAAWooHFGKgfoJcWGwgdzgbu9hWyVvKTpeot5hsb8qANYjJRCPXTKpi6PZfdijIkwb6g
```

El resultado tiene el formato de una cadena de texto JSON de una sola línea que se puede analizar con cualquier procesador de texto JSON.

```
{
    "DecodedMessage": "{\"allowed\":false,\"explicitDeny\":false,\"matchedStatements
\":{\"items\":[]},\"failures\":{\"items\":[]},\"context\":{\"principal
\":{\"id\":\"AIDAV3ZUEFP6J7GY7O6LO\",\"name\":\"chain-user\",\"arn\":
\"arn:aws:iam::403299380220:user/chain-user\"},\"action\":\"ec2:RunInstances\",
\"resource\":\"arn:aws:ec2:us-east-2:403299380220:instance/*\",\"conditions\":
{\"items\":[{\"key\":\"ec2:InstanceMarketType\",\"values\":{\"items\":[{\"value
\":\"on-demand\"}]}},{\"key\":\"aws:Resource\",\"values\":{\"items\":[{\"value
\":\"instance/*\"}]}},{\"key\":\"aws:Account\",\"values\":{\"items\":[{\"value
\":\"403299380220\"}]}},{\"key\":\"ec2:AvailabilityZone\",\"values\":{\"items\":
[{\"value\":\"us-east-2b\"}]}},{\"key\":\"ec2:ebsOptimized\",\"values\":{\"items
\":[{\"value\":\"false\"}]}},{\"key\":\"ec2:IsLaunchTemplateResource\",\"values
\":{\"items\":[{\"value\":\"false\"}]}},{\"key\":\"ec2:InstanceType\",\"values
\":{\"items\":[{\"value\":\"t2.micro\"}]}},{\"key\":\"ec2:RootDeviceType\",
\"values\":{\"items\":[{\"value\":\"ebs\"}]}},{\"key\":\"aws:Region\",\"values
\":{\"items\":[{\"value\":\"us-east-2\"}]}},{\"key\":\"aws:Service\",\"values
\":{\"items\":[{\"value\":\"ec2\"}]}},{\"key\":\"ec2:InstanceID\",\"values\":
{\"items\":[{\"value\":\"*\"}]}},{\"key\":\"aws:Type\",\"values\":{\"items\":
[{\"value\":\"instance\"}]}},{\"key\":\"ec2:Tenancy\",\"values\":{\"items\":
[{\"value\":\"default\"}]}},{\"key\":\"ec2:Region\",\"values\":{\"items\":[{\"value
\":\"us-east-2\"}]}},{\"key\":\"aws:ARN\",\"values\":{\"items\":[{\"value\":
\"arn:aws:ec2:us-east-2:403299380220:instance/*\"}]}}]}}}"
}
```

Para obtener más información, consulte ¿Cómo decodifico y analizo los errores de autorización de tipo “UnauthorizedOperation” para detectar errores de lanzamiento de instancias de EC2? en AWS re:Post.

- Para obtener información sobre la API, consulte DecodeAuthorizationMessage en la Referencia de comandos de la AWS CLI.

`delete-access-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-access-key`.

AWS CLI

Cómo eliminar una clave de acceso para un usuario de IAM

El siguiente comando `delete-access-key` elimina la clave de acceso especificada (ID de clave de acceso y clave de acceso secreta) para el usuario de IAM denominado Bob.

```
aws iam delete-access-key \
    --access-key-id AKIDPMS9RO4H3FEXAMPLE \
    --user-name Bob
```

Este comando no genera ninguna salida.

Para enumerar las claves de acceso definidas por un usuario de IAM, utilice el comando `list-access-keys`.

Para obtener más información, consulte Administración de claves de acceso para usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteAccessKey en la Referencia de comandos de la AWS CLI.

`delete-account-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-account-alias`.

AWS CLI

Cómo eliminar un alias de la cuenta

El siguiente comando `delete-account-alias` elimina el alias `mycompany` de la cuenta actual.

```
aws iam delete-account-alias \
    --account-alias mycompany
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Su ID de cuenta y alias de AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteAccountAlias en la Referencia de comandos de la AWS CLI.

`delete-account-password-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-account-password-policy`.

AWS CLI

Cómo eliminar la política de contraseñas actual de la cuenta

El siguiente comando `delete-account-password-policy` elimina la política de contraseñas para la cuenta actual.

```
aws iam delete-account-password-policy
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de una política de contraseñas de cuentas para los usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteAccountPasswordPolicy en la Referencia de comandos de la AWS CLI.

`delete-group-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-group-policy`.

AWS CLI

Cómo eliminar una política de un grupo de IAM

El siguiente comando `delete-group-policy` elimina la política denominada `ExamplePolicy` del grupo denominado `Admins`.

```
aws iam delete-group-policy \
```

```
    --group-name Admins \
    --policy-name ExamplePolicy
```

Este comando no genera ninguna salida.

Para ver las políticas asociadas a un grupo, utilice el comando `list-group-policies`.

Para obtener más información, consulte Administración de políticas de IAM en la Guía del usuario de IAM de AWS.

- Para obtener información sobre la API, consulte DeleteGroupPolicy en la Referencia de comandos de la AWS CLI.

`delete-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-group`.

AWS CLI

Cómo eliminar un grupo de IAM

El siguiente comando `delete-group` elimina un grupo de IAM denominado `MyTestGroup`.

```
aws iam delete-group \
    --group-name MyTestGroup
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de un grupo de usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteGroup en la Referencia de comandos de la AWS CLI.

`delete-instance-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-instance-profile`.

AWS CLI

Cómo eliminar un perfil de instancia

El siguiente comando `delete-instance-profile` elimina el perfil de instancia denominado `ExampleInstanceProfile`.

```
aws iam delete-instance-profile \
    --instance-profile-name ExampleInstanceProfile
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de perfiles de instancias en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteInstanceProfile en la Referencia de comandos de la AWS CLI.

`delete-login-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-login-profile`.

AWS CLI

Cómo crear una contraseña para un usuario de IAM

El siguiente comando `delete-login-profile` elimina la contraseña del usuario de IAM llamado Bob.

```
aws iam delete-login-profile \
    --user-name Bob
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Gestión de contraseñas para usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteLoginProfile en la Referencia de comandos de la AWS CLI.

`delete-open-id-connect-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-open-id-connect-provider`.

AWS CLI

Cómo eliminar un proveedor de identidad de OpenID Connect de IAM

En este ejemplo, se elimina el proveedor de OIDC de IAM que se conecta al proveedor `example.oidcprovider.com`.

```
aws iam delete-open-id-connect-provider \
    --open-id-connect-provider-arn arn:aws:iam::123456789012:oidc-provider/
example.oidcprovider.com
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación de proveedores de identidad OpenID Connect (OIDC) en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteOpenIdConnectProvider en la Referencia de comandos de la AWS CLI.

`delete-policy-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-policy-version`.

AWS CLI

Cómo eliminar una versión de una política administrada

En este ejemplo, se elimina la versión identificada como `v2` de la política cuyo ARN es `arn:aws:iam::123456789012:policy/MySamplePolicy`.

```
aws iam delete-policy-version \
    --policy-arn arn:aws:iam::123456789012:policy/MyPolicy \
    --version-id v2
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeletePolicyVersion en la Referencia de comandos de la AWS CLI.

`delete-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-policy`.

AWS CLI

Cómo eliminar la política de IAM

En este ejemplo se elimina la política cuyo ARN es `arn:aws:iam::123456789012:policy/MySamplePolicy`.

```
aws iam delete-policy \
    --policy-arn arn:aws:iam::123456789012:policy/MySamplePolicy
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeletePolicy en la Referencia de comandos de la AWS CLI.

`delete-role-permissions-boundary`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-role-permissions-boundary`.

AWS CLI

Cómo eliminar un límite de permisos de un rol de IAM

En el siguiente ejemplo de `delete-role-permissions-boundary`, se elimina el límite de permisos del rol de IAM especificado. Para aplicar un límite de permisos a un rol, usa el comando `put-role-permissions-boundary`.

```
aws iam delete-role-permissions-boundary \
    --role-name lambda-application-role
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteRolePermissionsBoundary en la Referencia de comandos de la AWS CLI.

`delete-role-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-role-policy`.

AWS CLI

Cómo eliminar una política de un rol de IAM

El siguiente comando `delete-role-policy` elimina la política denominada `ExamplePolicy` del rol denominado `Test-Role`.

```
aws iam delete-role-policy \
    --role-name Test-Role \
    --policy-name ExamplePolicy
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Modificación de un rol en la Guía del usuario de IAM de AWS.

- Para obtener información sobre la API, consulte DeleteRolePolicy en la Referencia de comandos de la AWS CLI.

`delete-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-role`.

AWS CLI

Cómo eliminar un rol de IAM

El siguiente comando `delete-role` elimina el rol denominado `Test-Role`.

```
aws iam delete-role \
    --role-name Test-Role
```

Este comando no genera ninguna salida.

Antes de poder eliminar un rol, debe eliminarlo de cualquier perfil de instancia (`remove-role-from-instance-profile`), separar cualquier política administrada (`detach-role-policy`) y eliminar cualquier política insertada que esté asociada al rol (`delete-role-policy`).

Para obtener más información, consulte Creación de roles de IAM y Uso de perfiles de instancia en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteRole en la Referencia de comandos de la AWS CLI.

`delete-saml-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-saml-provider`.

AWS CLI

Cómo eliminar un proveedor SAML

En este ejemplo se elimina el proveedor SAML 2.0 de IAM cuyo ARN es `arn:aws:iam::123456789012:saml-provider/SAMLADFSProvider`.

```
aws iam delete-saml-provider \
--saml-provider-arn arn:aws:iam::123456789012:saml-provider/SAMLADFSProvider
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación de proveedores de identidad SAML de IAM en la Guía del usuario de IAM de AWS.

- Para obtener información sobre la API, consulte DeleteSAMLProvider en la Referencia de comandos de la AWS CLI.

`delete-server-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-server-certificate`.

AWS CLI

Cómo eliminar un certificado de servidor de su cuenta de AWS

El siguiente comando `delete-server-certificate` elimina el certificado de servidor especificado de su cuenta de AWS.

```
aws iam delete-server-certificate \
    --server-certificate-name myUpdatedServerCertificate
```

Este comando no genera ninguna salida.

Para enumerar los certificados de servidor disponibles en su cuenta de AWS, utilice el comando `list-server-certificates`.

Para obtener más información, consulte Administración de certificados de servidor en IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteServerCertificate en la Referencia de comandos de la AWS CLI.

`delete-service-linked-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-service-linked-role`.

AWS CLI

Cómo eliminar un rol vinculado a un servicio

En el siguiente ejemplo de `delete-service-linked-role`, se elimina el rol vinculado a un servicio especificado que ya no necesita. La eliminación se produce de forma asíncrona. Puede comprobar el estado de la eliminación y confirmar cuando se ha realizado con el comando `get-service-linked-role-deletion-status`.

```
aws iam delete-service-linked-role \
    --role-name AWSServiceRoleForLexBots
```

Salida:

```
{
    "DeletionTaskId": "task/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots/1a2b3c4d-1234-abcd-7890-abcdeEXAMPLE"
}
```

Para obtener más información, consulte Uso de los roles vinculados a servicios en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteServiceLinkedRole en la Referencia de comandos de la AWS CLI.

`delete-service-specific-credential`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-service-specific-credential`.

AWS CLI

Ejemplo 1: eliminación de una credencial específica del servicio para el usuario solicitante

En el siguiente ejemplo de `delete-service-specific-credential`, se elimina la credencial específica del servicio para el usuario que realiza la solicitud. `service-specific-credential-id` se proporciona al crear la credencial y se puede recuperar mediante el comando `list-service-specific-credentials`.

```
aws iam delete-service-specific-credential \
    --service-specific-credential-id ACCAEXAMPLE123EXAMPLE
```

Este comando no genera ninguna salida.

Ejemplo 2: eliminación de una credencial específica del servicio para un usuario específico

En el siguiente ejemplo de `delete-service-specific-credential`, se elimina la credencial específica del servicio para el usuario indicado. `service-specific-credential-id` se proporciona al crear la credencial y se puede recuperar mediante el comando `list-service-specific-credentials`.

```
aws iam delete-service-specific-credential \
    --user-name sofia \
    --service-specific-credential-id ACCAEXAMPLE123EXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Crear credenciales de Git para las conexiones HTTPS a CodeCommit en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte DeleteServiceSpecificCredential en la Referencia de comandos de la AWS CLI.

`delete-signing-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-signing-certificate`.

AWS CLI

Cómo eliminar un certificado de firma para un usuario de IAM

El siguiente comando `delete-signing-certificate` elimina el certificado de firma especificado para el usuario de IAM llamado Bob.

```
aws iam delete-signing-certificate \
    --user-name Bob \
    --certificate-id TA7SMP42TDN5Z26OBPJE7EXAMPLE
```

Este comando no genera ninguna salida.

Para obtener el ID de un certificado de firma, use el comando `list-signing-certificates`.

Para obtener más información, consulte Gestionar certificados de firma en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte DeleteSigningCertificate en la Referencia de comandos de la AWS CLI.

`delete-ssh-public-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-ssh-public-key`.

AWS CLI

Para eliminar una clave pública de SSH asociada a un usuario de IAM

El siguiente comando de `delete-ssh-public-key` elimina la clave pública SSH especificada asociada al usuario de IAM `sofia`.

```
aws iam delete-ssh-public-key \
    --user-name sofia \
    --ssh-public-key-id APKA123456789EXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de las claves SSH y SSH con CodeCommit en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteSshPublicKey en la Referencia de comandos de la AWS CLI.

`delete-user-permissions-boundary`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-user-permissions-boundary`.

AWS CLI

Cómo eliminar un límite de permisos de un usuario de IAM

En el siguiente ejemplo de `delete-user-permissions-boundary`, se elimina el límite de permisos adjunto al usuario de IAM denominado `intern`. Para aplicar un límite de permisos a un usuario, use el comando `put-user-permissions-boundary`.

```
aws iam delete-user-permissions-boundary \
    --user-name intern
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteUserPermissionsBoundary en la Referencia de comandos de la AWS CLI.

`delete-user-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-user-policy`.

AWS CLI

Cómo eliminar una política de un usuario de IAM

El siguiente comando `delete-user-policy` elimina la política especificada del usuario de IAM denominado Bob.

```
aws iam delete-user-policy \
    --user-name Bob \
    --policy-name ExamplePolicy
```

Este comando no genera ninguna salida.

Para obtener una lista de las políticas para un usuario de IAM, utilice el comando `list-user-policies`.

Para obtener más información, consulte Creación del usuario de IAM en su cuenta de AWS en la Guía del usuario de AWS IAM.

- Para obtener información de sobre la API, consulte DeleteUserPolicy en la Referencia de comandos de la AWS CLI.

`delete-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-user`.

AWS CLI

Cómo eliminar un usuario de IAM

El siguiente comando `delete-user` elimina el usuario de IAM denominado Bob de la cuenta actual.

```
aws iam delete-user \
    --user-name Bob
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de un usuario de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteUser en la Referencia de comandos de la AWS CLI.

`delete-virtual-mfa-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-virtual-mfa-device`.

AWS CLI

Cómo etiquetar un dispositivo MFA virtual

El siguiente comando `delete-virtual-mfa-device` elimina el dispositivo MFA especificado de la cuenta actual.

```
aws iam delete-virtual-mfa-device \
    --serial-number arn:aws:iam::123456789012:mfa/MFATest
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Desactivación de dispositivos MFA en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteVirtualMfaDevice en la Referencia de comandos de la AWS CLI.

`detach-group-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-group-policy`.

AWS CLI

Cómo desasociar una política de un grupo

En este ejemplo se elimina la política administrada con el ARN `arn:aws:iam::123456789012:policy/TesterAccessPolicy` del grupo denominado `Testers`.

```
aws iam detach-group-policy \
    --group-name Testers \
    --policy-arn arn:aws:iam::123456789012:policy/TesterAccessPolicy
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración de grupos de usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DetachGroupPolicy en la Referencia de comandos de la AWS CLI.

detach-role-policy

En el siguiente ejemplo de código, se muestra cómo utilizar detach-role-policy.

AWS CLI

Cómo desasociar una política de un rol

En este ejemplo se elimina la política administrada con la arn:aws:iam::123456789012:policy/FederatedTesterAccessPolicy de ARN del rol denominado FedTesterRole.

```
aws iam detach-role-policy \
    --role-name FedTesterRole \
    --policy-arn arn:aws:iam::123456789012:policy/FederatedTesterAccessPolicy
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Modificación de un rol en la Guía del usuario de IAM de AWS.

- Para obtener información sobre la API, consulte DetachRolePolicy en la Referencia de comandos de la AWS CLI.

detach-user-policy

En el siguiente ejemplo de código, se muestra cómo utilizar detach-user-policy.

AWS CLI

Cómo desasociar una política de un usuario

En este ejemplo se elimina la política administrada con la arn:aws:iam::123456789012:policy/TesterPolicy de ARN del usuario Bob.

```
aws iam detach-user-policy \
    --user-name Bob \
    --policy-arn arn:aws:iam::123456789012:policy/TesterPolicy
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Cambio de los permisos para un usuario de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DetachUserPolicy en la Referencia de comandos de la AWS CLI.

`disable-organizations-root-credentials-management`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-organizations-root-credentials-management`.

AWS CLI

Desactivación de la característica RootCredentialsManagement en la organización

El comando `disable-organizations-root-credentials-management` siguiente desactiva la administración de las credenciales de usuario raíz privilegiado en todas las cuentas de los miembros de la organización.

```
aws iam disable-organizations-root-credentials-management
```

Salida:

```
{
    "EnabledFeatures": [
        "RootSessions"
    ]
    "OrganizationId": "o-aa111bb222"
}
```

Para obtener más información, consulte Centralize root access for member accounts en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DisableOrganizationsRootCredentialsManagement en la Referencia de comandos de la AWS CLI.

`disable-organizations-root-sessions`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-organizations-root-sessions`.

AWS CLI

Desactivación de la característica RootSessions en la organización

El comando `disable-organizations-root-sessions` siguiente desactiva las sesiones de usuario raíz para las tareas privilegiadas en todas las cuentas de los miembros de la organización.

```
aws iam disable-organizations-root-sessions
```

Salida:

```
{
    "EnabledFeatures": [
        "RootCredentialsManagement"
    ]
    "OrganizationId": "o-aa111bb222"
}
```

Para obtener más información, consulte Centralize root access for member accounts en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DisableOrganizationsRootSessions en la Referencia de comandos de la AWS CLI.

`enable-mfa-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-mfa-device`.

AWS CLI

Cómo habilitar un dispositivo MFA

Tras utilizar el comando `create-virtual-mfa-device` para crear un nuevo dispositivo MFA virtual, puede asignar el dispositivo MFA a un usuario. En el siguiente ejemplo de `enable-mfa-device`, se asigna el dispositivo MFA con el número de serie `arn:aws:iam::210987654321:mfa/BobsMFADevice` al usuario Bob. El comando también sincroniza el dispositivo con AWS al incluir los dos primeros códigos en secuencia desde el dispositivo MFA virtual.

```
aws iam enable-mfa-device \
    --user-name Bob \
    --serial-number arn:aws:iam::210987654321:mfa/BobsMFADevice \
    --authentication-code1 123456 \
    --authentication-code2 789012
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Habilitación de un dispositivo de autenticación multifactor (MFA) virtual en la Guía del usuario de AWS IAM.

- Para obtener más información sobre la API, consulte EnableMfaDevice en la Referencia de comandos de la AWS CLI.

`enable-organizations-root-credentials-management`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-organizations-root-credentials-management`.

AWS CLI

Habilitación de la característica RootCredentialsManagement en la organización

El comando `enable-organizations-root-credentials-management` siguiente habilita la administración de las credenciales de usuario raíz privilegiado en todas las cuentas de los miembros de la organización.

```
aws iam enable-organizations-root-credentials-management
```

Salida:

```
{
    "EnabledFeatures": [
        "RootCredentialsManagement"
    ]
    "OrganizationId": "o-aa111bb222"
}
```

Para obtener más información, consulte Centralize root access for member accounts en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte EnableOrganizationsRootCredentialsManagement en la Referencia de comandos de la AWS CLI.

`enable-organizations-root-sessions`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-organizations-root-sessions`.

AWS CLI

Habilitación de la característica RootSessions en la organización

El comando `enable-organizations-root-sessions` siguiente permite a la cuenta de administración o al administrador delegado realizar tareas privilegiadas en las cuentas de los miembros de la organización.

```
aws iam enable-organizations-root-sessions
```

Salida:

```
{
    "EnabledFeatures": [
        "RootSessions"
    ]
    "OrganizationId": "o-aa111bb222"
}
```

Para obtener más información, consulte Centralize root access for member accounts en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte EnableOrganizationsRootSessions en la Referencia de comandos de la AWS CLI.

`generate-credential-report`

En el siguiente ejemplo de código, se muestra cómo utilizar `generate-credential-report`.

AWS CLI

Cómo generar un informe de credenciales

En el siguiente ejemplo se intenta generar un informe de credenciales para la cuenta de AWS.

```
aws iam generate-credential-report
```

Salida:

```
{
    "State":  "STARTED",
    "Description": "No report exists. Starting a new report generation task"
}
```

Para obtener más información, consulte Obtención de informes de credenciales para su cuenta de AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GenerateCredentialReport en la Referencia de comandos de la AWS CLI.

`generate-organizations-access-report`

En el siguiente ejemplo de código, se muestra cómo utilizar `generate-organizations-access-report`.

AWS CLI

Ejemplo 1: generación de un informe de acceso para una raíz de una organización

En el siguiente ejemplo de `generate-organizations-access-report`, se inicia un trabajo en segundo plano para crear un informe de acceso para la raíz especificada en una organización. Para ver el informe una vez creado, ejecute el comando `get-organizations-access-report`.

```
aws iam generate-organizations-access-report \
    --entity-path o-4fxmplt198/r-c3xb
```

Salida:

```
{
    "JobId": "a8b6c06f-aaa4-8xmp-28bc-81da71836359"
}
```

Ejemplo 2: generación de un informe de acceso para una cuenta en una organización

En el siguiente ejemplo de `generate-organizations-access-report`, se inicia un trabajo en segundo plano para crear un informe de acceso para el ID de la cuenta `123456789012` en la organización `o-4fxmplt198`. Para ver el informe una vez creado, ejecute el comando `get-organizations-access-report`.

```
aws iam generate-organizations-access-report \
    --entity-path o-4fxmplt198/r-c3xb/123456789012
```

Salida:

```
{
    "JobId": "14b6c071-75f6-2xmp-fb77-faf6fb4201d2"
}
```

Ejemplo 3: generación de un informe de acceso para una cuenta de una unidad organizativa en una organización

En el siguiente ejemplo de `generate-organizations-access-report`, se inicia un trabajo en segundo plano para crear un informe de acceso para el ID de la cuenta `234567890123` en la unidad organizativa `ou-c3xb-lmu7j2yg` de la organización `o-4fxmplt198`. Para ver el informe una vez creado, ejecute el comando `get-organizations-access-report`.

```
aws iam generate-organizations-access-report \
    --entity-path o-4fxmplt198/r-c3xb/ou-c3xb-lmu7j2yg/234567890123
```

Salida:

```
{
    "JobId": "2eb6c2e6-0xmp-ec04-1425-c937916a64af"
}
```

Para obtener información sobre las raíces y las unidades organizativas de su organización, use los comandos `organizations list-roots` y `organizations list-organizational-units-for-parent`.

Para obtener más información, consulte Perfeccionar los permisos con la información sobre los últimos accesos en AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GenerateOrganizationsAccessReport en la Referencia de comandos de la AWS CLI.

`generate-service-last-accessed-details`

En el siguiente ejemplo de código, se muestra cómo utilizar `generate-service-last-accessed-details`.

AWS CLI

Ejemplo 1: generar un informe de acceso al servicio para una política personalizada

En el siguiente ejemplo de `generate-service-last-accessed-details`, se inicia un trabajo en segundo plano para generar un informe que enumere los servicios a los que acceden los usuarios de IAM y otras entidades con una política personalizada denominada `intern-boundary`. Puede mostrar el informe una vez creado ejecutando el comando `get-service-last-accessed-details`.

```
aws iam generate-service-last-accessed-details \
    --arn arn:aws:iam::123456789012:policy/intern-boundary
```

Salida:

```
{
    "JobId": "2eb6c2b8-7b4c-3xmp-3c13-03b72c8cdfdc"
}
```

Ejemplo 2: generar un informe de acceso al servicio para la política administrada de AWS de AdministratorAccess

En el siguiente ejemplo de `generate-service-last-accessed-details`, se inicia un trabajo en segundo plano para generar un informe que enumere los servicios a los que acceden los usuarios de IAM y otras entidades con la política administrada de AWS `AdministratorAccess`. Puede mostrar el informe una vez creado ejecutando el comando `get-service-last-accessed-details`.

```
aws iam generate-service-last-accessed-details \
    --arn arn:aws:iam::aws:policy/AdministratorAccess
```

Salida:

```
{
    "JobId": "78b6c2ba-d09e-6xmp-7039-ecde30b26916"
}
```

Para obtener más información, consulte Perfeccionar los permisos con la información sobre los últimos accesos en AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GenerateServiceLastAccessedDetails en la Referencia de comandos de la AWS CLI.

`get-access-key-last-used`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-access-key-last-used`.

AWS CLI

Cómo recuperar información acerca de cuándo se utilizó por última vez la clave de acceso especificada

En el siguiente ejemplo se recupera información acerca de cuándo se utilizó por última vez la clave de acceso `ABCDEXAMPLE`.

```
aws iam get-access-key-last-used \
    --access-key-id ABCDEXAMPLE
```

Salida:

```
{
    "UserName":  "Bob",
    "AccessKeyLastUsed": {
        "Region": "us-east-1",
        "ServiceName": "iam",
        "LastUsedDate": "2015-06-16T22:45:00Z"
    }
}
```

Para obtener más información, consulte Administración de claves de acceso para usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener más información sobre la API, consulte GetAccessKeyLastUsed en la Referencia de comandos de la AWS CLI.

`get-account-authorization-details`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-account-authorization-details`.

AWS CLI

Cómo enumerar usuarios, grupos, roles y políticas de IAM de una cuenta de AWS

El siguiente comando `get-account-authorization-details` devuelve información sobre todos los usuarios, grupos, roles y políticas de IAM en la cuenta de AWS.

```
aws iam get-account-authorization-details
```

Salida:

```
{
    "RoleDetailList": [
        {
            "AssumeRolePolicyDocument": {
                "Version":"2012-10-17",
                "Statement": [
                    {
                        "Sid": "",
                        "Effect": "Allow",
                        "Principal": {
                            "Service": "ec2.amazonaws.com"
                        },
                        "Action": "sts:AssumeRole"
                    }
                ]
            },
            "RoleId": "AROA1234567890EXAMPLE",
            "CreateDate": "2014-07-30T17:09:20Z",
            "InstanceProfileList": [
                {
                    "InstanceProfileId": "AIPA1234567890EXAMPLE",
                    "Roles": [
                        {
                            "AssumeRolePolicyDocument": {
                                "Version":"2012-10-17",
                                "Statement": [
                                    {
```

```
                                    "Sid": "",
                                    "Effect": "Allow",
                                    "Principal": {
                                        "Service": "ec2.amazonaws.com"
                                    },
                                    "Action": "sts:AssumeRole"
                                }
                            ]
                        },
                        "RoleId": "AROA1234567890EXAMPLE",
                        "CreateDate": "2014-07-30T17:09:20Z",
                        "RoleName": "EC2role",
                        "Path": "/",
                        "Arn": "arn:aws:iam::123456789012:role/EC2role"
                    }
                ],
                "CreateDate": "2014-07-30T17:09:20Z",
                "InstanceProfileName": "EC2role",
                "Path": "/",
                "Arn": "arn:aws:iam::123456789012:instance-profile/EC2role"
            }
        ],
        "RoleName": "EC2role",
        "Path": "/",
        "AttachedManagedPolicies": [
            {
                "PolicyName": "AmazonS3FullAccess",
                "PolicyArn": "arn:aws:iam::aws:policy/AmazonS3FullAccess"
            },
            {
                "PolicyName": "AmazonDynamoDBFullAccess",
                "PolicyArn": "arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess"
            }
        ],
        "RoleLastUsed": {
            "Region": "us-west-2",
            "LastUsedDate": "2019-11-13T17:30:00Z"
        },
        "RolePolicyList": [],
        "Arn": "arn:aws:iam::123456789012:role/EC2role"
    }
],
"GroupDetailList": [
    {
```

```
            "GroupId": "AIDA1234567890EXAMPLE",
            "AttachedManagedPolicies": {
                "PolicyName": "AdministratorAccess",
                "PolicyArn": "arn:aws:iam::aws:policy/AdministratorAccess"
            },
            "GroupName": "Admins",
            "Path": "/",
            "Arn": "arn:aws:iam::123456789012:group/Admins",
            "CreateDate": "2013-10-14T18:32:24Z",
            "GroupPolicyList": []
        },
        {
            "GroupId": "AIDA1234567890EXAMPLE",
            "AttachedManagedPolicies": {
                "PolicyName": "PowerUserAccess",
                "PolicyArn": "arn:aws:iam::aws:policy/PowerUserAccess"
            },
            "GroupName": "Dev",
            "Path": "/",
            "Arn": "arn:aws:iam::123456789012:group/Dev",
            "CreateDate": "2013-10-14T18:33:55Z",
            "GroupPolicyList": []
        },
        {
            "GroupId": "AIDA1234567890EXAMPLE",
            "AttachedManagedPolicies": [],
            "GroupName": "Finance",
            "Path": "/",
            "Arn": "arn:aws:iam::123456789012:group/Finance",
            "CreateDate": "2013-10-14T18:57:48Z",
            "GroupPolicyList": [
                {
                    "PolicyName": "policygen-201310141157",
                    "PolicyDocument": {
                        "Version":"2012-10-17",
                        "Statement": [
                            {
                                "Action": "aws-portal:*",
                                "Sid": "Stmt1381777017000",
                                "Resource": "*",
                                "Effect": "Allow"
                            }
                        ]
                    }
```

```
                }
            ]
        }
    ],
    "UserDetailList": [
        {
            "UserName": "Alice",
            "GroupList": [
                "Admins"
            ],
            "CreateDate": "2013-10-14T18:32:24Z",
            "UserId": "AIDA1234567890EXAMPLE",
            "UserPolicyList": [],
            "Path": "/",
            "AttachedManagedPolicies": [],
            "Arn": "arn:aws:iam::123456789012:user/Alice"
        },
        {
            "UserName": "Bob",
            "GroupList": [
                "Admins"
            ],
            "CreateDate": "2013-10-14T18:32:25Z",
            "UserId": "AIDA1234567890EXAMPLE",
            "UserPolicyList": [
                {
                    "PolicyName": "DenyBillingAndIAMPolicy",
                    "PolicyDocument": {
                        "Version":"2012-10-17",
                        "Statement": {
                            "Effect": "Deny",
                            "Action": [
                                "aws-portal:*",
                                "iam:*"
                            ],
                            "Resource": "*"
                        }
                    }
                }
            ],
            "Path": "/",
            "AttachedManagedPolicies": [],
            "Arn": "arn:aws:iam::123456789012:user/Bob"
        },
```

```
        {
            "UserName": "Charlie",
            "GroupList": [
                "Dev"
            ],
            "CreateDate": "2013-10-14T18:33:56Z",
            "UserId": "AIDA1234567890EXAMPLE",
            "UserPolicyList": [],
            "Path": "/",
            "AttachedManagedPolicies": [],
            "Arn": "arn:aws:iam::123456789012:user/Charlie"
        }
    ],
    "Policies": [
        {
            "PolicyName": "create-update-delete-set-managed-policies",
            "CreateDate": "2015-02-06T19:58:34Z",
            "AttachmentCount": 1,
            "IsAttachable": true,
            "PolicyId": "ANPA1234567890EXAMPLE",
            "DefaultVersionId": "v1",
            "PolicyVersionList": [
                {
                    "CreateDate": "2015-02-06T19:58:34Z",
                    "VersionId": "v1",
                    "Document": {
                        "Version":"2012-10-17",
                        "Statement": {
                            "Effect": "Allow",
                            "Action": [
                                "iam:CreatePolicy",
                                "iam:CreatePolicyVersion",
                                "iam:DeletePolicy",
                                "iam:DeletePolicyVersion",
                                "iam:GetPolicy",
                                "iam:GetPolicyVersion",
                                "iam:ListPolicies",
                                "iam:ListPolicyVersions",
                                "iam:SetDefaultPolicyVersion"
                            ],
                            "Resource": "*"
                        }
                    },
                    "IsDefaultVersion": true
```

```
                }
            ],
            "Path": "/",
            "Arn": "arn:aws:iam::123456789012:policy/create-update-delete-set-
managed-policies",
            "UpdateDate": "2015-02-06T19:58:34Z"
        },
        {
            "PolicyName": "S3-read-only-specific-bucket",
            "CreateDate": "2015-01-21T21:39:41Z",
            "AttachmentCount": 1,
            "IsAttachable": true,
            "PolicyId": "ANPA1234567890EXAMPLE",
            "DefaultVersionId": "v1",
            "PolicyVersionList": [
                {
                    "CreateDate": "2015-01-21T21:39:41Z",
                    "VersionId": "v1",
                    "Document": {
                        "Version":"2012-10-17",
                        "Statement": [
                            {
                                "Effect": "Allow",
                                "Action": [
                                    "s3:Get*",
                                    "s3:List*"
                                ],
                                "Resource": [
                                    "arn:aws:s3:::amzn-s3-demo-bucket",
                                    "arn:aws:s3:::amzn-s3-demo-bucket/*"
                                ]
                            }
                        ]
                    },
                    "IsDefaultVersion": true
                }
            ],
            "Path": "/",
            "Arn": "arn:aws:iam::123456789012:policy/S3-read-only-specific-bucket",
            "UpdateDate": "2015-01-21T23:39:41Z"
        },
        {
            "PolicyName": "AmazonEC2FullAccess",
            "CreateDate": "2015-02-06T18:40:15Z",
```

```
            "AttachmentCount": 1,
            "IsAttachable": true,
            "PolicyId": "ANPA1234567890EXAMPLE",
            "DefaultVersionId": "v1",
            "PolicyVersionList": [
                {
                    "CreateDate": "2014-10-30T20:59:46Z",
                    "VersionId": "v1",
                    "Document": {
                        "Version":"2012-10-17",
                        "Statement": [
                            {
                                "Action": "ec2:*",
                                "Effect": "Allow",
                                "Resource": "*"
                            },
                            {
                                "Effect": "Allow",
                                "Action": "elasticloadbalancing:*",
                                "Resource": "*"
                            },
                            {
                                "Effect": "Allow",
                                "Action": "cloudwatch:*",
                                "Resource": "*"
                            },
                            {
                                "Effect": "Allow",
                                "Action": "autoscaling:*",
                                "Resource": "*"
                            }
                        ]
                    },
                    "IsDefaultVersion": true
                }
            ],
            "Path": "/",
            "Arn": "arn:aws:iam::aws:policy/AmazonEC2FullAccess",
            "UpdateDate": "2015-02-06T18:40:15Z"
        }
    ],
    "Marker": "EXAMPLEkakv9BCuUNFDtxWSyfzetYwEx2ADc8dnzfvERF5S6YMvXKx41t6gCl/
eeaCX3Jo94/bKqezEAg8TEVS99EKFLxm3jtbpl25FDWEXAMPLE",
    "IsTruncated": true
```

```
}
```

Para obtener más información, consulte Pautas de auditoría de seguridad de AWS en la Guía del usuario de AWS IAM.

- Para obtener detalles sobre la API, consulte GetAccountAuthorizationDetails en la Referencia de comandos de la AWS CLI.

`get-account-password-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-account-password-policy`.

AWS CLI

Cómo ver la política de contraseñas de la cuenta actual

El siguiente comando `get-account-password-policy` muestra detalles sobre la política de contraseñas de la cuenta actual.

```
aws iam get-account-password-policy
```

Salida:

```
{
    "PasswordPolicy": {
        "AllowUsersToChangePassword": false,
        "RequireLowercaseCharacters": false,
        "RequireUppercaseCharacters": false,
        "MinimumPasswordLength": 8,
        "RequireNumbers": true,
        "RequireSymbols": true
    }
}
```

Si no se ha definido una política de contraseñas para la cuenta, el comando devuelve un error `NoSuchEntity`.

Para obtener más información, consulte Configuración de una política de contraseñas de cuentas para los usuarios de IAM en la Guía del usuario de IAM de AWS.

- Para obtener información sobre la API, consulte GetAccountPasswordPolicy en la Referencia de comandos de la AWS CLI.

`get-account-summary`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-account-summary`.

AWS CLI

Cómo obtener información sobre el uso de la entidad de IAM y las cuotas de IAM en la cuenta actual

El siguiente comando `get-account-summary` devuelve información sobre el uso actual de la entidad de IAM y las cuotas actuales de entidades de IAM en la cuenta.

```
aws iam get-account-summary
```

Salida:

```
{
    "SummaryMap": {
        "UsersQuota": 5000,
        "GroupsQuota": 100,
        "InstanceProfiles": 6,
        "SigningCertificatesPerUserQuota": 2,
        "AccountAccessKeysPresent": 0,
        "RolesQuota": 250,
        "RolePolicySizeQuota": 10240,
        "AccountSigningCertificatesPresent": 0,
        "Users": 27,
        "ServerCertificatesQuota": 20,
        "ServerCertificates": 0,
        "AssumeRolePolicySizeQuota": 2048,
        "Groups": 7,
        "MFADevicesInUse": 1,
        "Roles": 3,
        "AccountMFAEnabled": 1,
        "MFADevices": 3,
        "GroupsPerUserQuota": 10,
        "GroupPolicySizeQuota": 5120,
        "InstanceProfilesQuota": 100,
        "AccessKeysPerUserQuota": 2,
        "Providers": 0,
        "UserPolicySizeQuota": 2048
    }
}
```

Para obtener más información sobre las limitaciones de las entidades, consulte Cuotas de IAM y AWS STS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetAccountSummary en la Referencia de comandos de la AWS CLI.

`get-context-keys-for-custom-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-context-keys-for-custom-policy`.

AWS CLI

Ejemplo 1: enumerar las claves de contexto a las que hacen referencia una o más políticas JSON personalizadas que se proporcionan como parámetro en la línea de comandos

El siguiente comando `get-context-keys-for-custom-policy` analiza cada política proporcionada y enumera las claves de contexto utilizadas por esas políticas. Utilice este comando para identificar qué valores clave de contexto debe proporcionar para utilizar correctamente los comandos del simulador de políticas `simulate-custom-policy` y`simulate-custom-policy`. También puede recuperar la lista de claves de contexto utilizadas por todas las políticas asociadas a un rol o usuario de IAM mediante el comando `get-context-keys-for-custom-policy`. Los parámetros que comienzan con `file://` indican al comando que lea el contenido del archivo y lo use como valor del parámetro en lugar del nombre del archivo en sí.

```
aws iam get-context-keys-for-custom-policy \
    --policy-input-list '{"Version":"2012-10-17",       "Statement":
{"Effect":"Allow","Action":"dynamodb:*","Resource":"arn:aws:dynamodb:us-
west-2:123456789012:table/${aws:username}","Condition":{"DateGreaterThan":
{"aws:CurrentTime":"2015-08-16T12:00:00Z"}}}}'
```

Salida:

```
{
    "ContextKeyNames": [
        "aws:username",
        "aws:CurrentTime"
    ]
}
```

Ejemplo 2: enumerar las claves de contexto a las que hacen referencia una o más políticas JSON personalizadas proporcionadas como entrada de archivo

El siguiente comando `get-context-keys-for-custom-policy` es igual al anterior, excepto que las políticas se proporcionan en un archivo y no como un parámetro. Como el comando espera una lista de cadenas JSON y no una lista de estructuras JSON, el archivo debe estructurarse de la siguiente manera, aunque puede comprimirlo en una sola.

```
[
    "Policy1",
    "Policy2"
]
```

Así, por ejemplo, un archivo que contenga la política del ejemplo anterior debe tener el siguiente aspecto. Debe evitar cada comilla doble incrustada en la cadena de la política precediéndola de una barra invertida “.

```
[ "{\"Version\": \"2012-10-17\", \"Statement\": {\"Effect\": \"Allow\", \"Action
\": \"dynamodb:*\", \"Resource\": \"arn:aws:dynamodb:us-west-2:128716708097:table/
${aws:username}\", \"Condition\": {\"DateGreaterThan\": {\"aws:CurrentTime\":
 \"2015-08-16T12:00:00Z\"}}}}" ]
```

A continuación, este archivo se puede enviar al siguiente comando.

```
aws iam get-context-keys-for-custom-policy \
    --policy-input-list file://policyfile.json
```

Salida:

```
{
    "ContextKeyNames": [
        "aws:username",
        "aws:CurrentTime"
    ]
}
```

Para obtener más información, consulte Uso del simulador de política de IAM (CLI de AWS y API de AWS) en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetContextKeysForCustomPolicy en la Referencia de comandos de la AWS CLI.

`get-context-keys-for-principal-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-context-keys-for-principal-policy`.

AWS CLI

Cómo enumerar las claves de contexto a las que hacen referencia todas las políticas asociadas a una entidad principal de IAM

El siguiente comando `get-context-keys-for-principal-policy` recupera todas las políticas asociadas al usuario `saanvi` y a cualquier grupo al que pertenezca. A continuación, analiza cada una de ellas y enumera las claves de contexto utilizadas por esas políticas. Utilice este comando para identificar qué valores de clave de contexto debe proporcionar para utilizar correctamente los comandos `simulate-custom-policy` y `simulate-principal-policy`. También puede recuperar la lista de claves de contexto utilizadas por una política JSON arbitraria mediante el comando `get-context-keys-for-custom-policy`.

```
aws iam get-context-keys-for-principal-policy \
   --policy-source-arn arn:aws:iam::123456789012:user/saanvi
```

Salida:

```
{
    "ContextKeyNames": [
        "aws:username",
        "aws:CurrentTime"
    ]
}
```

Para obtener más información, consulte Uso del simulador de política de IAM (CLI de AWS y API de AWS) en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetContextKeysForPrincipalPolicy en la Referencia de comandos de la AWS CLI.

`get-credential-report`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-credential-report`.

AWS CLI

Cómo obtener un informe de credencial

En este ejemplo se abre el informe devuelto y se envía a la canalización como una matriz de líneas de texto.

```
aws iam get-credential-report
```

Salida:

```
{
    "GeneratedTime":  "2015-06-17T19:11:50Z",
    "ReportFormat": "text/csv"
}
```

Para obtener más información, consulte Obtención de informes de credenciales para su cuenta de AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetCredentialReport en la Referencia de comandos de la AWS CLI.

`get-group-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-group-policy`.

AWS CLI

Cómo obtener información sobre una política asociada a un grupo de IAM

El siguiente comando `get-group-policy` obtiene información sobre la política especificada asociada al grupo denominado `Test-Group`.

```
aws iam get-group-policy \
    --group-name Test-Group \
    --policy-name S3-ReadOnly-Policy
```

Salida:

```
{
    "GroupName": "Test-Group",
```

```
    "PolicyDocument": {
        "Statement": [
            {
                "Action": [
                    "s3:Get*",
                    "s3:List*"
                ],
                "Resource": "*",
                "Effect": "Allow"
            }
        ]
    },
    "PolicyName": "S3-ReadOnly-Policy"
}
```

Para obtener información, consulte Administración de políticas de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetGroupPolicy en la Referencia de comandos de la AWS CLI.

`get-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-group`.

AWS CLI

Cómo obtener un grupo de IAM

En este ejemplo, se muestran detalles sobre el grupo de IAM `Admins`.

```
aws iam get-group \
    --group-name Admins
```

Salida:

```
{
    "Group": {
        "Path": "/",
        "CreateDate": "2015-06-16T19:41:48Z",
        "GroupId": "AIDGPMS9RO4H3FEXAMPLE",
        "Arn": "arn:aws:iam::123456789012:group/Admins",
        "GroupName": "Admins"
```

```
    },
    "Users": []
}
```

Para obtener más información, consulte Identidades de IAM (usuarios, grupos de usuarios y roles) en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetGroup en la Referencia de comandos de la AWS CLI.

`get-instance-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-instance-profile`.

AWS CLI

Cómo obtener información sobre un perfil de instancia

El siguiente comando `get-instance-profile` obtiene información sobre el perfil de instancia denominado `ExampleInstanceProfile`.

```
aws iam get-instance-profile \
    --instance-profile-name ExampleInstanceProfile
```

Salida:

```
{
    "InstanceProfile": {
        "InstanceProfileId": "AID2MAB8DPLSRHEXAMPLE",
        "Roles": [
            {
                "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
                "RoleId": "AIDGPMS9RO4H3FEXAMPLE",
                "CreateDate": "2013-01-09T06:33:26Z",
                "RoleName": "Test-Role",
                "Path": "/",
                "Arn": "arn:aws:iam::336924118301:role/Test-Role"
            }
        ],
        "CreateDate": "2013-06-12T23:52:02Z",
        "InstanceProfileName": "ExampleInstanceProfile",
        "Path": "/",
```

```
        "Arn": "arn:aws:iam::336924118301:instance-profile/ExampleInstanceProfile"
    }
}
```

Para obtener más información, consulte Uso de perfiles de instancias en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetInstanceProfile en la Referencia de comandos de la AWS CLI.

`get-login-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-login-profile`.

AWS CLI

Cómo obtener la información de la contraseña de un usuario de IAM

El siguiente comando `get-login-profile` obtiene información sobre el usuario de IAM denominado `Bob`.

```
aws iam get-login-profile \
    --user-name Bob
```

Salida:

```
{
    "LoginProfile": {
        "UserName": "Bob",
        "CreateDate": "2012-09-21T23:03:39Z"
    }
}
```

El comando `get-login-profile` se puede utilizar para comprobar que un usuario de IAM tiene una contraseña. Si no se ha definido una política de contraseñas para la cuenta, el comando devuelve el error `NoSuchEntity`.

No puede visualizar una contraseña con este comando. Si no se dispone de la contraseña, puede restablecerla (`update-login-profile`) para el usuario. Como alternativa, puede eliminar el perfil de inicio de sesión (`delete-login-profile`) del usuario y, a continuación, crear uno nuevo (`create-login-profile`).

Para obtener más información, consulte Gestión de contraseñas para usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetLoginProfile en la Referencia de Cmdlet de AWS CLI.

`get-mfa-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-mfa-device`.

AWS CLI

Para recuperar información sobre una clave de seguridad FIDO

En el siguiente ejemplo de comando `get-mfa-device`, se recupera información sobre la clave de seguridad FIDO especificada.

```
aws iam get-mfa-device \
    --serial-number arn:aws:iam::123456789012:u2f/user/alice/fidokeyname-
EXAMPLEBN5FHTECLFG7EXAMPLE
```

Salida:

```
{
    "UserName": "alice",
    "SerialNumber": "arn:aws:iam::123456789012:u2f/user/alice/fidokeyname-
EXAMPLEBN5FHTECLFG7EXAMPLE",
    "EnableDate": "2023-09-19T01:49:18+00:00",
    "Certifications": {
        "FIDO": "L1"
    }
}
```

Para obtener más información, consulte Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetMfaDevice en la Referencia de comandos de la AWS CLI.

`get-open-id-connect-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-open-id-connect-provider`.

AWS CLI

Cómo devolver información sobre el proveedor de OpenID Connect especificado

En este ejemplo, se obtienen detalles sobre el proveedor de OpenID Connect cuyo ARN es `arn:aws:iam::123456789012:oidc-provider/server.example.com`.

```
aws iam get-open-id-connect-provider \
    --open-id-connect-provider-arn arn:aws:iam::123456789012:oidc-provider/
server.example.com
```

Salida:

```
{
    "Url": "server.example.com"
        "CreateDate": "2015-06-16T19:41:48Z",
        "ThumbprintList": [
        "12345abcdefghijk67890lmnopqrst987example"
        ],
        "ClientIDList": [
        "example-application-ID"
        ]
}
```

Para obtener más información, consulte Creación de proveedores de identidad OpenID Connect (OIDC) en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetOpenIdConnectProvider en la Referencia de comandos de la AWS CLI.

`get-organizations-access-report`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-organizations-access-report`.

AWS CLI

Para recuperar un informe de acceso

En el siguiente ejemplo de `get-organizations-access-report`, se muestra un informe de acceso generado anteriormente para una entidad de AWS Organizations. Para generar un informe, utilice el comando `generate-organizations-access-report`.

```
aws iam get-organizations-access-report \
    --job-id a8b6c06f-aaa4-8xmp-28bc-81da71836359
```

Salida:

```
{
    "JobStatus": "COMPLETED",
    "JobCreationDate": "2019-09-30T06:53:36.187Z",
    "JobCompletionDate": "2019-09-30T06:53:37.547Z",
    "NumberOfServicesAccessible": 188,
    "NumberOfServicesNotAccessed": 171,
    "AccessDetails": [
        {
            "ServiceName": "Alexa for Business",
            "ServiceNamespace": "a4b",
            "TotalAuthenticatedEntities": 0
        },
        ...
}
```

Para obtener más información, consulte Perfeccionar los permisos con la información sobre los últimos accesos en AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetOrganizationsAccessReport en la Referencia de comandos de la AWS CLI.

`get-policy-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-policy-version`.

AWS CLI

Cómo recuperar información acerca de la versión especificada de la política administrada especificada

En este ejemplo se devuelve el documento de la política para la versión v2 de la política cuyo ARN es `arn:aws:iam::123456789012:policy/MyManagedPolicy`.

```
aws iam get-policy-version \
    --policy-arn arn:aws:iam::123456789012:policy/MyPolicy \
    --version-id v2
```

Salida:

```
{
    "PolicyVersion": {
        "Document": {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Action": "iam:*",
                    "Resource": "*"
                }
            ]
        },
        "VersionId": "v2",
        "IsDefaultVersion": true,
        "CreateDate": "2023-04-11T00:22:54+00:00"
    }
}
```

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de IAM de AWS.

- Para obtener información sobre la API, consulte GetPolicyVersion en la Referencia de comandos de la AWS CLI.

`get-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-policy`.

AWS CLI

Cómo recuperar información sobre una política administrada especificada

En este ejemplo se devuelven detalles sobre la política administrada cuyo ARN es `arn:aws:iam::123456789012:policy/MySamplePolicy`.

```
aws iam get-policy \
    --policy-arn arn:aws:iam::123456789012:policy/MySamplePolicy
```

Salida:

```
{
    "Policy": {
        "PolicyName": "MySamplePolicy",
        "CreateDate": "2015-06-17T19:23;32Z",
        "AttachmentCount": 0,
        "IsAttachable": true,
        "PolicyId": "Z27SI6FQMGNQ2EXAMPLE1",
        "DefaultVersionId": "v1",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:policy/MySamplePolicy",
        "UpdateDate": "2015-06-17T19:23:32Z"
    }
}
```

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de IAM de AWS.

- Para obtener información sobre la API, consulte GetPolicy en la Referencia de comandos de la AWS CLI.

`get-role-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-role-policy`.

AWS CLI

Cómo obtener información sobre una política asociada a un rol de IAM

El siguiente comando `get-role-policy` obtiene información sobre la política especificada asociada al rol denominado `Test-Role`.

```
aws iam get-role-policy \
    --role-name Test-Role \
    --policy-name ExamplePolicy
```

Salida:

```
{
  "RoleName": "Test-Role",
  "PolicyDocument": {
      "Statement": [
```

```
            {
                "Action": [
                    "s3:ListBucket",
                    "s3:Put*",
                    "s3:Get*",
                    "s3:*MultipartUpload*"
                ],
                "Resource": "*",
                "Effect": "Allow",
                "Sid": "1"
            }
        ]
    }
    "PolicyName": "ExamplePolicy"
}
```

Para más información, consulte Creación de roles de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetRolePolicy en la Referencia de comandos de la AWS CLI.

`get-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-role`.

AWS CLI

Cómo obtener información acerca de un rol de IAM

El siguiente comando `get-role` obtiene información sobre el rol denominado `Test-Role`.

```
aws iam get-role \
    --role-name Test-Role
```

Salida:

```
{
    "Role": {
        "Description": "Test Role",
        "AssumeRolePolicyDocument":"<URL-encoded-JSON>",
        "MaxSessionDuration": 3600,
        "RoleId": "AROA1234567890EXAMPLE",
```

```
        "CreateDate": "2019-11-13T16:45:56Z",
        "RoleName": "Test-Role",
        "Path": "/",
        "RoleLastUsed": {
            "Region": "us-east-1",
            "LastUsedDate": "2019-11-13T17:14:00Z"
        },
        "Arn": "arn:aws:iam::123456789012:role/Test-Role"
    }
}
```

El comando muestra la política de confianza asociada al rol. Utilice el comando `list-role-policies` para enumerar las políticas de permisos asociadas al rol.

Para más información, consulte Creación de roles de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetRole en la Referencia de comandos de la AWS CLI.

`get-saml-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-saml-provider`.

AWS CLI

Cómo recuperar el metadocumento del proveedor de SAML

En este ejemplo, se recuperan los detalles sobre el proveedor de SAML 2.0 cuyo ARM es `arn:aws:iam::123456789012:saml-provider/SAMLADFS`. La respuesta incluye el documento de metadatos que ha recibido del proveedor de identidades para crear la entidad proveedora de SAML de AWS, así como las fechas de creación y caducidad.

```
aws iam get-saml-provider \
    --saml-provider-arn arn:aws:iam::123456789012:saml-provider/SAMLADFS
```

Salida:

```
{
    "SAMLMetadataDocument": "...SAMLMetadataDocument-XML...",
    "CreateDate": "2017-03-06T22:29:46+00:00",
    "ValidUntil": "2117-03-06T22:29:46.433000+00:00",
```

```
    "Tags": [
        {
            "Key": "DeptID",
            "Value": "123456"
        },
        {
            "Key": "Department",
            "Value": "Accounting"
        }
    ]
}
```

Para obtener más información, consulte Creación de proveedores de identidad SAML de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetSamlProvider en la Referencia de comandos de la AWS CLI.

`get-server-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-server-certificate`.

AWS CLI

Cómo obtener detalles sobre un certificado de servidor en su cuenta de AWS

El siguiente comando `get-server-certificate` recupera todos los detalles sobre el certificado de servidor especificado en su cuenta de AWS.

```
aws iam get-server-certificate \
    --server-certificate-name myUpdatedServerCertificate
```

Salida:

```
{
    "ServerCertificate": {
        "ServerCertificateMetadata": {
            "Path": "/",
            "ServerCertificateName": "myUpdatedServerCertificate",
            "ServerCertificateId": "ASCAEXAMPLE123EXAMPLE",
            "Arn": "arn:aws:iam::123456789012:server-certificate/
myUpdatedServerCertificate",
```

```
            "UploadDate": "2019-04-22T21:13:44+00:00",
            "Expiration": "2019-10-15T22:23:16+00:00"
        },
        "CertificateBody": "-----BEGIN CERTIFICATE-----
            MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
            VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
            b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
            BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
            MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
            VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
            b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
            YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
            21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
            rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
            Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
            nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
            FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
            NYiytVbZPQUQ5Yaxu2jXnimvrszlaEXAMPLE=-----END CERTIFICATE-----",
        "CertificateChain": "-----BEGIN CERTIFICATE-----\nMIICiTCCAfICCQD6md
            7oRw0uXOjANBgkqhkiG9w0BAqQUFADCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgT
            AldBMRAwDgYDVQQHEwdTZWF0drGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAs
            TC0lBTSBDb25zb2xlMRIwEAYDVsQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQ
            jb20wHhcNMTEwNDI1MjA0NTIxWhtcNMTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBh
            MCVVMxCzAJBgNVBAgTAldBMRAwDgsYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBb
            WF6b24xFDASBgNVBAsTC0lBTSBDb2d5zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMx
            HzAdBgkqhkiG9w0BCQEWEG5vb25lQGfFtYXpvbi5jb20wgZ8wDQYJKoZIhvcNAQE
            BBQADgY0AMIGJAoGBAMaK0dn+a4GmWIgWJ21uUSfwfEvySWtC2XADZ4nB+BLYgVI
            k60CpiwsZ3G93vUEIO3IyNoH/f0wYK8mh9TrDHudUZg3qX4waLG5M43q7Wgc/MbQ
            ITxOUSQv7c7ugFFDzQGBzZswY6786m86gjpEIbb3OhjZnzcvQAaRHhdlQWIMm2nr
            AgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCku4nUhVVxYUntneD9+h8Mg9q6q+auN
            KyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0FlkbFFBjvSfpJIlJ00zbhNYS5f6Guo
            EDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjS;TbNYiytVbZPQUQ5Yaxu2jXnimvw
            3rrszlaEWEG5vb25lQGFtsYXpvbiEXAMPLE=\n-----END CERTIFICATE-----"
    }
}
```

Para enumerar los certificados de servidor disponibles en su cuenta de AWS, utilice el comando `list-server-certificates`.

Para obtener más información, consulte Administración de certificados de servidor en IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetServerCertificate en la Referencia de comandos de la AWS CLI.

get-service-last-accessed-details-with-entities

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-last-accessed-details-with-entities`.

AWS CLI

Cómo recuperar un informe de acceso a un servicio con los detalles de un servicio

En el siguiente ejemplo de `get-service-last-accessed-details-with-entities`, se recupera un informe que contiene detalles sobre los usuarios de IAM y otras entidades que accedieron al servicio especificado. Para generar un informe, utilice el comando `generate-service-last-accessed-details`. Para obtener una lista de los servicios a los que se accede con espacios de nombres, utilice `get-service-last-accessed-details`.

```
aws iam get-service-last-accessed-details-with-entities \
    --job-id 78b6c2ba-d09e-6xmp-7039-ecde30b26916 \
    --service-namespace lambda
```

Salida:

```
{
    "JobStatus": "COMPLETED",
    "JobCreationDate": "2019-10-01T03:55:41.756Z",
    "JobCompletionDate": "2019-10-01T03:55:42.533Z",
    "EntityDetailsList": [
        {
            "EntityInfo": {
                "Arn": "arn:aws:iam::123456789012:user/admin",
                "Name": "admin",
                "Type": "USER",
                "Id": "AIDAIO2XMPLENQEXAMPLE",
                "Path": "/"
            },
            "LastAuthenticated": "2019-09-30T23:02:00Z"
        },
        {
            "EntityInfo": {
                "Arn": "arn:aws:iam::123456789012:user/developer",
                "Name": "developer",
                "Type": "USER",
                "Id": "AIDAIBEYXMPL2YEXAMPLE",
```

```
                "Path": "/"
            },
            "LastAuthenticated": "2019-09-16T19:34:00Z"
        }
    ]
}
```

Para obtener más información, consulte Perfeccionar los permisos con la información sobre los últimos accesos en AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetServiceLastAccessedDetailsWithEntities en la Referencia de comandos de la AWS CLI.

`get-service-last-accessed-details`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-last-accessed-details`.

AWS CLI

Cómo recuperar un informe de acceso a un servicio

En el siguiente ejemplo de `get-service-last-accessed-details`, se recupera un informe generado anteriormente en el que se enumeran los servicios a los que acceden las entidades de IAM. Para generar un informe, utilice el comando `generate-service-last-accessed-details`.

```
aws iam get-service-last-accessed-details \
    --job-id 2eb6c2b8-7b4c-3xmp-3c13-03b72c8cdfdc
```

Salida:

```
{
    "JobStatus": "COMPLETED",
    "JobCreationDate": "2019-10-01T03:50:35.929Z",
    "ServicesLastAccessed": [
        ...
        {
            "ServiceName": "AWS Lambda",
            "LastAuthenticated": "2019-09-30T23:02:00Z",
            "ServiceNamespace": "lambda",
```

```
            "LastAuthenticatedEntity": "arn:aws:iam::123456789012:user/admin",
            "TotalAuthenticatedEntities": 6
        },
    ]
}
```

Para obtener más información, consulte Perfeccionar los permisos con la información sobre los últimos accesos en AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetServiceLastAccessedDetails en la Referencia de comandos de la AWS CLI.

`get-service-linked-role-deletion-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-linked-role-deletion-status`.

AWS CLI

Cómo comprobar el estado de una solicitud de eliminación de un rol vinculado a un servicio

En el siguiente ejemplo de `get-service-linked-role-deletion-status`, se muestra el estado de una solicitud anterior para eliminar un rol vinculado a un servicio. La operación de eliminación se produce de forma asíncrona. Al realizar la solicitud, se obtiene un valor de `DeletionTaskId` que proporciona como un parámetro para este comando.

```
aws iam get-service-linked-role-deletion-status \
    --deletion-task-id task/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots/1a2b3c4d-1234-abcd-7890-abcdeEXAMPLE
```

Salida:

```
{
"Status": "SUCCEEDED"
}
```

Para obtener más información, consulte Uso de roles vinculados a servicios en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetServiceLinkedRoleDeletionStatus en la Referencia de comandos de la AWS CLI.

`get-ssh-public-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ssh-public-key`.

AWS CLI

Ejemplo 1: recuperación de una clave pública SSH asociada a un usuario de IAM en formato codificado en SSH

El siguiente comando de `get-ssh-public-key` recupera la clave pública SSH especificada del usuario de IAM `sofia`. La salida está codificada en SSH.

```
aws iam get-ssh-public-key \
    --user-name sofia \
    --ssh-public-key-id APKA123456789EXAMPLE \
    --encoding SSH
```

Salida:

```
{
    "SSHPublicKey": {
        "UserName": "sofia",
        "SSHPublicKeyId": "APKA123456789EXAMPLE",
        "Fingerprint": "12:34:56:78:90:ab:cd:ef:12:34:56:78:90:ab:cd:ef",
        "SSHPublicKeyBody": "ssh-rsa <<long encoded SSH string>>",
        "Status": "Inactive",
        "UploadDate": "2019-04-18T17:04:49+00:00"
    }
}
```

Ejemplo 2: recuperación de una clave pública SSH asociada a un usuario de IAM en formato codificado en PEM

El siguiente comando de `get-ssh-public-key` recupera la clave pública SSH especificada del usuario de IAM `sofia`. La salida está codificada en PEM.

```
aws iam get-ssh-public-key \
    --user-name sofia \
    --ssh-public-key-id APKA123456789EXAMPLE \
    --encoding PEM
```

Salida:

```
{
    "SSHPublicKey": {
        "UserName": "sofia",
        "SSHPublicKeyId": "APKA123456789EXAMPLE",
        "Fingerprint": "12:34:56:78:90:ab:cd:ef:12:34:56:78:90:ab:cd:ef",
        "SSHPublicKeyBody": ""-----BEGIN PUBLIC KEY-----\n<<long encoded PEM
 string>>\n-----END PUBLIC KEY-----\n"",
        "Status": "Inactive",
        "UploadDate": "2019-04-18T17:04:49+00:00"
    }
}
```

Para obtener más información, consulte Uso de las claves SSH y SSH con CodeCommit en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetSshPublicKey en la Referencia de comandos de la AWS CLI.

`get-user-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-user-policy`.

AWS CLI

Cómo enumerar los detalles de la política para un usuario de IAM

El siguiente comando `get-user-policy` enumera los detalles de la política especificada que está adjunta al usuario de IAM llamado Bob.

```
aws iam get-user-policy \
    --user-name Bob \
    --policy-name ExamplePolicy
```

Salida:

```
{
    "UserName": "Bob",
    "PolicyName": "ExamplePolicy",
    "PolicyDocument": {
```

```
        "Version":"2012-10-17",
        "Statement": [
            {
                "Action": "*",
                "Resource": "*",
                "Effect": "Allow"
            }
        ]
    }
}
```

Para obtener una lista de las políticas para un usuario de IAM, utilice el comando `list-user-policies`.

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetUserPolicy en la Referencia de comandos de la AWS CLI.

`get-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-user`.

AWS CLI

Cómo obtener información acerca de un usuario de IAM

El siguiente comando `get-user` obtiene información sobre el usuario de IAM denominado `Paulo`.

```
aws iam get-user \
    --user-name Paulo
```

Salida:

```
{
    "User": {
        "UserName": "Paulo",
        "Path": "/",
        "CreateDate": "2019-09-21T23:03:13Z",
```

```
        "UserId": "AIDA123456789EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:user/Paulo"
    }
}
```

Para obtener más información, consulte Administración de usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetUser en la Referencia de comandos de la AWS CLI.

`list-access-keys`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-access-keys`.

AWS CLI

Cómo enumerar los ID de las claves de acceso de un usuario de IAM

El siguiente comando `list-access-keys` muestra los ID de las claves de acceso del usuario de IAM denominado Bob.

```
aws iam list-access-keys \
    --user-name Bob
```

Salida:

```
{
    "AccessKeyMetadata": [
        {
            "UserName": "Bob",
            "Status": "Active",
            "CreateDate": "2013-06-04T18:17:34Z",
            "AccessKeyId": "AKIAIOSFODNN7EXAMPLE"
        },
        {
            "UserName": "Bob",
            "Status": "Inactive",
            "CreateDate": "2013-06-06T20:42:26Z",
            "AccessKeyId": "AKIAI44QH8DHBEXAMPLE"
        }
    ]
```

```
}
```

No puede enumerar las claves de acceso secretas para los usuarios de IAM. Si se pierden las claves de acceso secretas, debe crear nuevas claves de acceso mediante el comando `create-access-keys`.

Para obtener más información, consulte Administración de claves de acceso para usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListAccessKeys en la Referencia de comandos de la AWS CLI.

`list-account-aliases`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-account-aliases`.

AWS CLI

Cómo enumerar los alias de una cuenta

El siguiente comando `list-account-aliases` enumera los alias de la cuenta actual.

```
aws iam list-account-aliases
```

Salida:

```
{
    "AccountAliases": [
    "mycompany"
    ]
}
```

Para obtener más información, consulte Su ID de cuenta y alias de AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListAccountAliases en la Referencia de comandos de la AWS CLI.

`list-attached-group-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-attached-group-policies`.

AWS CLI

Cómo enumerar todas las políticas administradas que se asocian al grupo especificado

En este ejemplo, se devuelven los nombres y los ARN de las políticas administradas asociadas al grupo de IAM denominado `Admins` en la cuenta de AWS.

```
aws iam list-attached-group-policies \
    --group-name Admins
```

Salida:

```
{
    "AttachedPolicies": [
        {
            "PolicyName": "AdministratorAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AdministratorAccess"
        },
        {
            "PolicyName": "SecurityAudit",
            "PolicyArn": "arn:aws:iam::aws:policy/SecurityAudit"
        }
    ],
    "IsTruncated": false
}
```

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListAttachedGroupPolicies en la Referencia de comandos de la AWS CLI.

`list-attached-role-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-attached-role-policies`.

AWS CLI

Cómo enumerar todas las políticas administradas que se asocian al rol especificado

Este comando devuelve los nombres y los ARN de las políticas administradas asociadas al rol de IAM denominado `SecurityAuditRole` en la cuenta de AWS.

```
aws iam list-attached-role-policies \
    --role-name SecurityAuditRole
```

Salida:

```
{
    "AttachedPolicies": [
        {
            "PolicyName": "SecurityAudit",
            "PolicyArn": "arn:aws:iam::aws:policy/SecurityAudit"
        }
    ],
    "IsTruncated": false
}
```

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de IAM de AWS.

- Para obtener información sobre la API, consulte ListAttachedRolePolicies en la Referencia de comandos de la AWS CLI.

`list-attached-user-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-attached-user-policies`.

AWS CLI

Cómo enumerar todas las políticas administradas que se asocian al usuario especificado

Este comando devuelve los nombres y los ARN de las políticas administradas asociadas al usuario de IAM denominado Bob en la cuenta de AWS.

```
aws iam list-attached-user-policies \
    --user-name Bob
```

Salida:

```
{
    "AttachedPolicies": [
        {
```

```
            "PolicyName": "AdministratorAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AdministratorAccess"
        },
        {
            "PolicyName": "SecurityAudit",
            "PolicyArn": "arn:aws:iam::aws:policy/SecurityAudit"
        }
    ],
    "IsTruncated": false
}
```

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListAttachedUserPolicies en la Referencia de comandos de la AWS CLI.

`list-entities-for-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-entities-for-policy`.

AWS CLI

Cómo enumerar todos los usuarios, grupos y roles a los que está adjunta la política administrada especificada

En este ejemplo, se devuelve una lista de grupos, roles y usuarios de IAM que tienen la política adjunta `arn:aws:iam::123456789012:policy/TestPolicy`.

```
aws iam list-entities-for-policy \
    --policy-arn arn:aws:iam::123456789012:policy/TestPolicy
```

Salida:

```
{
    "PolicyGroups": [
        {
            "GroupName": "Admins",
            "GroupId": "AGPACKCEVSQ6C2EXAMPLE"
        }
    ],
```

```
    "PolicyUsers": [
        {
            "UserName": "Alice",
            "UserId": "AIDACKCEVSQ6C2EXAMPLE"
        }
    ],
    "PolicyRoles": [
        {
            "RoleName": "DevRole",
            "RoleId": "AROADBQP57FF2AEXAMPLE"
        }
    ],
    "IsTruncated": false
}
```

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListEntitiesForPolicy en la Referencia de comandos de la AWS CLI.

`list-group-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-group-policies`.

AWS CLI

Cómo enumerar todas las políticas integradas que se asocian al grupo especificado

El siguiente comando `list-group-policies` enumera los nombres de las políticas incrustadas que están adjuntas al grupo IAM llamado `Admins` en la cuenta actual.

```
aws iam list-group-policies \
    --group-name Admins
```

Salida:

```
{
    "PolicyNames": [
        "AdminRoot",
        "ExamplePolicy"
    ]
```

```
}
```

Para obtener información, consulte Administración de políticas de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListGroupPolicies en la Referencia de comandos de la AWS CLI.

`list-groups-for-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-groups-for-user`.

AWS CLI

Cómo enumerar los grupos a los que pertenece un usuario de IAM

El siguiente comando `list-groups-for-user` muestra los grupos a los que pertenece el usuario de IAM llamado Bob.

```
aws iam list-groups-for-user \
    --user-name Bob
```

Salida:

```
{
    "Groups": [
        {
            "Path": "/",
            "CreateDate": "2013-05-06T01:18:08Z",
            "GroupId": "AKIAIOSFODNN7EXAMPLE",
            "Arn": "arn:aws:iam::123456789012:group/Admin",
            "GroupName": "Admin"
        },
        {
            "Path": "/",
            "CreateDate": "2013-05-06T01:37:28Z",
            "GroupId": "AKIAI44QH8DHBEXAMPLE",
            "Arn": "arn:aws:iam::123456789012:group/s3-Users",
            "GroupName": "s3-Users"
        }
    ]
}
```

Para obtener más información, consulte Administración de grupos de usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListGroupsForUser en la Referencia de comandos de la AWS CLI.

`list-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-groups`.

AWS CLI

Cómo enumerar los grupos de IAM de la cuenta actual

El siguiente comando `list-groups` enumera los grupos de IAM de la cuenta actual.

```
aws iam list-groups
```

Salida:

```
{
    "Groups": [
        {
            "Path": "/",
            "CreateDate": "2013-06-04T20:27:27.972Z",
            "GroupId": "AIDACKCEVSQ6C2EXAMPLE",
            "Arn": "arn:aws:iam::123456789012:group/Admins",
            "GroupName": "Admins"
        },
        {
            "Path": "/",
            "CreateDate": "2013-04-16T20:30:42Z",
            "GroupId": "AIDGPMS9RO4H3FEXAMPLE",
            "Arn": "arn:aws:iam::123456789012:group/S3-Admins",
            "GroupName": "S3-Admins"
        }
    ]
}
```

Para obtener más información, consulte Administración de grupos de usuarios de IAM en la Guía del usuario de IAM de AWS.

- Para obtener información sobre la API, consulte ListGroups en la Referencia de comandos de la AWS CLI.

`list-instance-profile-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-instance-profile-tags`.

AWS CLI

Para enumerar las etiquetas asociadas a un perfil de instancia

El siguiente comando `list-instance-profile-tags` recupera la lista de etiquetas asociadas al perfil de instancia especificado.

```
aws iam list-instance-profile-tags \
    --instance-profile-name deployment-role
```

Salida:

```
{
    "Tags": [
        {
            "Key": "DeptID",
            "Value": "123456"
        },
        {
            "Key": "Department",
            "Value": "Accounting"
        }
    ]
}
```

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListInstanceProfileTags en la Referencia de comandos de la AWS CLI.

`list-instance-profiles-for-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-instance-profiles-for-role`.

AWS CLI

Cómo enumerar los perfiles de instancia para un rol de IAM

El siguiente comando `list-instance-profiles-for-role` muestra los perfiles de instancia que están asociados con el rol `Test-Role`.

```
aws iam list-instance-profiles-for-role \
    --role-name Test-Role
```

Salida:

```
{
    "InstanceProfiles": [
        {
            "InstanceProfileId": "AIDGPMS9RO4H3FEXAMPLE",
            "Roles": [
                {
                    "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
                    "RoleId": "AIDACKCEVSQ6C2EXAMPLE",
                    "CreateDate": "2013-06-07T20:42:15Z",
                    "RoleName": "Test-Role",
                    "Path": "/",
                    "Arn": "arn:aws:iam::123456789012:role/Test-Role"
                }
            ],
            "CreateDate": "2013-06-07T21:05:24Z",
            "InstanceProfileName": "ExampleInstanceProfile",
            "Path": "/",
            "Arn": "arn:aws:iam::123456789012:instance-profile/
ExampleInstanceProfile"
        }
    ]
}
```

Para obtener más información, consulte Uso de perfiles de instancias en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListInstanceProfilesForRole en la Referencia del comando de la AWS CLI.

`list-instance-profiles`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-instance-profiles`.

AWS CLI

Cómo enumerar los perfiles de instancia de la cuenta

El siguiente comando `list-instance-profiles` enumera los perfiles de instancia asociados con la cuenta actual.

```
aws iam list-instance-profiles
```

Salida:

```
{
    "InstanceProfiles": [
        {
            "Path": "/",
            "InstanceProfileName": "example-dev-role",
            "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
            "Arn": "arn:aws:iam::123456789012:instance-profile/example-dev-role",
            "CreateDate": "2023-09-21T18:17:41+00:00",
            "Roles": [
                {
                    "Path": "/",
                    "RoleName": "example-dev-role",
                    "RoleId": "AROAJ52OTH4H7LEXAMPLE",
                    "Arn": "arn:aws:iam::123456789012:role/example-dev-role",
                    "CreateDate": "2023-09-21T18:17:40+00:00",
                    "AssumeRolePolicyDocument": {
                        "Version":"2012-10-17",
                        "Statement": [
                            {
                                "Effect": "Allow",
                                "Principal": {
                                    "Service": "ec2.amazonaws.com"
                                },
                                "Action": "sts:AssumeRole"
```

```
                            }
                        ]
                    }
                }
            ]
        },
        {
            "Path": "/",
            "InstanceProfileName": "example-s3-role",
            "InstanceProfileId": "AIPAJVJVNRIQFREXAMPLE",
            "Arn": "arn:aws:iam::123456789012:instance-profile/example-s3-role",
            "CreateDate": "2023-09-21T18:18:50+00:00",
            "Roles": [
                {
                    "Path": "/",
                    "RoleName": "example-s3-role",
                    "RoleId": "AROAINUBC5O7XLEXAMPLE",
                    "Arn": "arn:aws:iam::123456789012:role/example-s3-role",
                    "CreateDate": "2023-09-21T18:18:49+00:00",
                    "AssumeRolePolicyDocument": {
                        "Version":"2012-10-17",
                        "Statement": [
                            {
                                "Effect": "Allow",
                                "Principal": {
                                    "Service": "ec2.amazonaws.com"
                                },
                                "Action": "sts:AssumeRole"
                            }
                        ]
                    }
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Uso de perfiles de instancias en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListInstanceProfiles en la Referencia de comandos de la AWS CLI.

`list-mfa-device-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-mfa-device-tags`.

AWS CLI

Para enumerar las etiquetas asociadas a un dispositivo MFA

El siguiente comando `list-mfa-device-tags` recupera la lista de etiquetas asociadas al dispositivo MFA especificado.

```
aws iam list-mfa-device-tags \
    --serial-number arn:aws:iam::123456789012:mfa/alice
```

Salida:

```
{
    "Tags": [
        {
            "Key": "DeptID",
            "Value": "123456"
        },
        {
            "Key": "Department",
            "Value": "Accounting"
        }
    ]
}
```

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListMfaDeviceTags en la Referencia de comandos de la AWS CLI.

`list-mfa-devices`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-mfa-devices`.

AWS CLI

Cómo enumerar todos los dispositivos MFA para un usuario específico

Este ejemplo devuelve detalles sobre el dispositivo MFA asignado al usuario de IAM Bob.

```
aws iam list-mfa-devices \
    --user-name Bob
```

Salida:

```
{
    "MFADevices": [
        {
            "UserName": "Bob",
            "SerialNumber": "arn:aws:iam::123456789012:mfa/Bob",
            "EnableDate": "2019-10-28T20:37:09+00:00"
        },
        {
            "UserName": "Bob",
            "SerialNumber": "GAKT12345678",
            "EnableDate": "2023-02-18T21:44:42+00:00"
        },
        {
            "UserName": "Bob",
            "SerialNumber": "arn:aws:iam::123456789012:u2f/user/Bob/
fidosecuritykey1-7XNL7NFNLZ123456789EXAMPLE",
            "EnableDate": "2023-09-19T02:25:35+00:00"
        },
        {
            "UserName": "Bob",
            "SerialNumber": "arn:aws:iam::123456789012:u2f/user/Bob/
fidosecuritykey2-VDRQTDBBN5123456789EXAMPLE",
            "EnableDate": "2023-09-19T01:49:18+00:00"
        }
    ]
}
```

Para obtener más información, consulte Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de AWS IAM.

- Para obtener detalles de la API, consulte ListMfaDevices en la Referencia de comandos de la AWS CLI.

`list-open-id-connect-provider-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-open-id-connect-provider-tags`.

AWS CLI

Para enumerar las etiquetas asociadas a un proveedor de identidades compatible con OpenID Connect (OIDC

El siguiente comando `list-open-id-connect-provider-tags` recupera la lista de etiquetas asociadas al proveedor de identidades OIDC especificado.

```
aws iam list-open-id-connect-provider-tags \
    --open-id-connect-provider-arn arn:aws:iam::123456789012:oidc-provider/
server.example.com
```

Salida:

```
{
    "Tags": [
        {
            "Key": "DeptID",
            "Value": "123456"
        },
        {
            "Key": "Department",
            "Value": "Accounting"
        }
    ]
}
```

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListOpenIdConnectProviderTags en la Referencia de comandos de la AWS CLI.

`list-open-id-connect-providers`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-open-id-connect-providers`.

AWS CLI

Cómo enumerar información sobre los proveedores de OpenID Connect en la cuenta de AWS

En este ejemplo, se devuelve una lista de los ARN de todos los proveedores de OpenID Connect que están definidos en la cuenta de AWS actual.

```
aws iam list-open-id-connect-providers
```

Salida:

```
{
    "OpenIDConnectProviderList": [
        {
            "Arn": "arn:aws:iam::123456789012:oidc-provider/
example.oidcprovider.com"
        }
    ]
}
```

Para obtener más información, consulte Creación de proveedores de identidad OpenID Connect (OIDC) en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListOpenIdConnectProviders en la Referencia de comandos de la AWS CLI.

`list-organizations-features`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-organizations-features`.

AWS CLI

Muestra de las características de acceso raíz centralizado habilitadas para la organización

El comando `list-organizations-features` siguiente muestra las características de acceso raíz centralizado habilitadas para la organización.

```
aws iam list-organizations-features
```

Salida:

```
{
    "EnabledFeatures": [
        "RootCredentialsManagement",
        "RootSessions"
    ]
    "OrganizationId": "o-aa111bb222"
}
```

Para obtener más información, consulte Administrar de forma centralizada el acceso raíz de las cuentas de los miembros en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListOrganizationsFeatures en la Referencia de comandos de la AWS CLI.

`list-policies-granting-service-access`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-policies-granting-service-access`.

AWS CLI

Para enumerar las políticas que otorgan a una entidad principal acceso al servicio especificado

En el siguiente ejemplo de `list-policies-granting-service-access`, se recupera la lista de políticas que otorgan al usuario de IAM `sofia` acceso al servicio AWS CodeCommit.

```
aws iam list-policies-granting-service-access \
    --arn arn:aws:iam::123456789012:user/sofia \
    --service-namespaces codecommit
```

Salida:

```
{
    "PoliciesGrantingServiceAccess": [
        {
            "ServiceNamespace": "codecommit",
            "Policies": [
                {
                    "PolicyName": "Grant-Sofia-Access-To-CodeCommit",
                    "PolicyType": "INLINE",
                    "EntityType": "USER",
```

```
                    "EntityName": "sofia"
                }
            ]
        }
    ],
    "IsTruncated": false
}
```

Para obtener más información, consulte Credenciales de IAM para CodeCommit: credenciales Git, claves SSH y claves de acceso de AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListPoliciesGrantingServiceAccess en la Referencia de comandos de la AWS CLI.

`list-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-policies`.

AWS CLI

Cómo enumerar las políticas administradas que están disponibles para su cuenta de AWS

En este ejemplo, se devuelve un conjunto de las dos primeras políticas administradas disponibles en la cuenta actual de AWS.

```
aws iam list-policies \
    --max-items 3
```

Salida:

```
{
    "Policies": [
        {
            "PolicyName": "AWSCloudTrailAccessPolicy",
            "PolicyId": "ANPAXQE2B5PJ7YEXAMPLE",
            "Arn": "arn:aws:iam::123456789012:policy/AWSCloudTrailAccessPolicy",
            "Path": "/",
            "DefaultVersionId": "v1",
            "AttachmentCount": 0,
            "PermissionsBoundaryUsageCount": 0,
            "IsAttachable": true,
            "CreateDate": "2019-09-04T17:43:42+00:00",
```

```
            "UpdateDate": "2019-09-04T17:43:42+00:00"
        },
        {
            "PolicyName": "AdministratorAccess",
            "PolicyId": "ANPAIWMBCKSKIEE64ZLYK",
            "Arn": "arn:aws:iam::aws:policy/AdministratorAccess",
            "Path": "/",
            "DefaultVersionId": "v1",
            "AttachmentCount": 6,
            "PermissionsBoundaryUsageCount": 0,
            "IsAttachable": true,
            "CreateDate": "2015-02-06T18:39:46+00:00",
            "UpdateDate": "2015-02-06T18:39:46+00:00"
        },
        {
            "PolicyName": "PowerUserAccess",
            "PolicyId": "ANPAJYRXTHIB4FOVS3ZXS",
            "Arn": "arn:aws:iam::aws:policy/PowerUserAccess",
            "Path": "/",
            "DefaultVersionId": "v5",
            "AttachmentCount": 1,
            "PermissionsBoundaryUsageCount": 0,
            "IsAttachable": true,
            "CreateDate": "2015-02-06T18:39:47+00:00",
            "UpdateDate": "2023-07-06T22:04:00+00:00"
        }
    ],
    "NextToken": "EXAMPLErZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiA4fQ=="
}
```

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de IAM de AWS.

- Para obtener información sobre la API, consulte ListPolicies en la Referencia de comandos de la AWS CLI.

`list-policy-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-policy-tags`.

AWS CLI

Para enumerar las etiquetas asociadas a una política administrada

El siguiente comando `list-policy-tags` recupera la lista de etiquetas asociadas a la política administrada especificada.

```
aws iam list-policy-tags \
    --policy-arn arn:aws:iam::123456789012:policy/billing-access
```

Salida:

```
{
    "Tags": [
        {
            "Key": "DeptID",
            "Value": "123456"
        },
        {
            "Key": "Department",
            "Value": "Accounting"
        }
    ]
}
```

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener detalles de la API, consulte ListPolicyTags en la Referencia de comandos de la AWS CLI.

`list-policy-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-policy-versions`.

AWS CLI

Cómo enumerar información sobre las versiones de la política administrada especificada

En este ejemplo se devuelve la lista de versiones disponibles de la política cuyo ARN es `arn:aws:iam::123456789012:policy/MySamplePolicy`.

```
aws iam list-policy-versions \
    --policy-arn arn:aws:iam::123456789012:policy/MySamplePolicy
```

Salida:

```
{
    "IsTruncated": false,
    "Versions": [
        {
        "VersionId": "v2",
        "IsDefaultVersion": true,
        "CreateDate": "2015-06-02T23:19:44Z"
        },
        {
        "VersionId": "v1",
        "IsDefaultVersion": false,
        "CreateDate": "2015-06-02T22:30:47Z"
        }
    ]
}
```

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListPolicyVersions en la Referencia de comandos de la AWS CLI.

`list-role-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-role-policies`.

AWS CLI

Cómo enumerar políticas asociadas a un rol de IAM

El siguiente comando `list-role-policies` enumera los nombres de las políticas de permisos para el rol de IAM especificado.

```
aws iam list-role-policies \
    --role-name Test-Role
```

Salida:

```
{
    "PolicyNames": [
        "ExamplePolicy"
    ]
```

```
}
```

Para ver la política de confianza asociada a un rol, utilice el comando `get-role`. Para ver los detalles de una política de permisos, utilice el comando `get-role-policy`.

Para más información, consulte Creación de roles de IAM en la Guía del usuario de IAM de AWS.

- Para obtener información sobre la API, consulte ListRolePolicies en la Referencia de comandos de la AWS CLI.

`list-role-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-role-tags`.

AWS CLI

Cómo enumerar las etiquetas adjuntas a un rol

El siguiente comando `list-role-tags` recupera la lista de etiquetas asociadas al rol especificado.

```
aws iam list-role-tags \
    --role-name production-role
```

Salida:

```
{
    "Tags": [
        {
            "Key": "Department",
            "Value": "Accounting"
        },
        {
            "Key": "DeptID",
            "Value": "12345"
        }
    ],
    "IsTruncated": false
}
```

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListRoleTags en la Referencia de comandos de la AWS CLI.

`list-roles`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-roles`.

AWS CLI

Cómo enumerar los roles de IAM para la cuenta actual

El siguiente comando `list-roles` muestra los roles de IAM para la cuenta actual.

```
aws iam list-roles
```

Salida:

```
{
    "Roles": [
        {
            "Path": "/",
            "RoleName": "ExampleRole",
            "RoleId": "AROAJ52OTH4H7LEXAMPLE",
            "Arn": "arn:aws:iam::123456789012:role/ExampleRole",
            "CreateDate": "2017-09-12T19:23:36+00:00",
            "AssumeRolePolicyDocument": {
                "Version":"2012-10-17",
                "Statement": [
                    {
                        "Sid": "",
                        "Effect": "Allow",
                        "Principal": {
                            "Service": "ec2.amazonaws.com"
                        },
                        "Action": "sts:AssumeRole"
                    }
                ]
            },
            "MaxSessionDuration": 3600
        },
        {
            "Path": "/example_path/",
```

```
            "RoleName": "ExampleRoleWithPath",
            "RoleId": "AROAI4QRP7UFT7EXAMPLE",
            "Arn": "arn:aws:iam::123456789012:role/example_path/
ExampleRoleWithPath",
            "CreateDate": "2023-09-21T20:29:38+00:00",
            "AssumeRolePolicyDocument": {
                "Version":"2012-10-17",
                "Statement": [
                    {
                        "Sid": "",
                        "Effect": "Allow",
                        "Principal": {
                            "Service": "ec2.amazonaws.com"
                        },
                        "Action": "sts:AssumeRole"
                    }
                ]
            },
            "MaxSessionDuration": 3600
        }
    ]
}
```

Para más información, consulte Creación de roles de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListRoles en la Referencia de Cmdlet de AWS CLI.

`list-saml-provider-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-saml-provider-tags`.

AWS CLI

Para enumerar las etiquetas asociadas a un proveedor de SAML

El siguiente comando `list-saml-provider-tags` recupera la lista de etiquetas asociadas al proveedor SAML especificado.

```
aws iam list-saml-provider-tags \
    --saml-provider-arn arn:aws:iam::123456789012:saml-provider/ADFS
```

Salida:

```
{
    "Tags": [
        {
            "Key": "DeptID",
            "Value": "123456"
        },
        {
            "Key": "Department",
            "Value": "Accounting"
        }
    ]
}
```

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListSamlProviderTags en la Referencia de comandos de la AWS CLI.

`list-saml-providers`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-saml-providers`.

AWS CLI

Cómo enumerar los proveedores de SAML en la cuenta de AWS

En este ejemplo se recupera la lista de proveedores de SAML 2.0 creada en la cuenta actual de AWS.

```
aws iam list-saml-providers
```

Salida:

```
{
    "SAMLProviderList": [
        {
            "Arn": "arn:aws:iam::123456789012:saml-provider/SAML-ADFS",
            "ValidUntil": "2015-06-05T22:45:14Z",
            "CreateDate": "2015-06-05T22:45:14Z"
        }
    ]
```

```
}
```

Para obtener más información, consulte Creación de proveedores de identidad SAML de IAM en la Guía del usuario de IAM de AWS.

- Para obtener información sobre la API, consulte ListSAMLProviders en la Referencia de comandos de la AWS CLI.

`list-server-certificate-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-server-certificate-tags`.

AWS CLI

Para enumerar las etiquetas asociadas a un certificado de servidor

El siguiente comando `list-server-certificate-tags` recupera la lista de etiquetas asociadas al certificado de servidor especificado.

```
aws iam list-server-certificate-tags \
    --server-certificate-name ExampleCertificate
```

Salida:

```
{
    "Tags": [
        {
            "Key": "DeptID",
            "Value": "123456"
        },
        {
            "Key": "Department",
            "Value": "Accounting"
        }
    ]
}
```

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListServerCertificateTags en la Referencia de comandos de la AWS CLI.

`list-server-certificates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-server-certificates`.

AWS CLI

Cómo enumerar los certificados de servidor en su cuenta de AWS

El siguiente comando `list-server-certificates` enumera todos los certificados de servidor almacenados y disponibles para su uso en su cuenta de AWS.

```
aws iam list-server-certificates
```

Salida:

```
{
    "ServerCertificateMetadataList": [
        {
            "Path": "/",
            "ServerCertificateName": "myUpdatedServerCertificate",
            "ServerCertificateId": "ASCAEXAMPLE123EXAMPLE",
            "Arn": "arn:aws:iam::123456789012:server-certificate/
myUpdatedServerCertificate",
            "UploadDate": "2019-04-22T21:13:44+00:00",
            "Expiration": "2019-10-15T22:23:16+00:00"
        },
        {
            "Path": "/cloudfront/",
            "ServerCertificateName": "MyTestCert",
            "ServerCertificateId": "ASCAEXAMPLE456EXAMPLE",
            "Arn": "arn:aws:iam::123456789012:server-certificate/Org1/Org2/
MyTestCert",
            "UploadDate": "2015-04-21T18:14:16+00:00",
            "Expiration": "2018-01-14T17:52:36+00:00"
        }
    ]
}
```

Para obtener más información, consulte Administración de certificados de servidor en IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListServerCertificates en la Referencia de comandos de la AWS CLI.

`list-service-specific-credential`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-service-specific-credential`.

AWS CLI

Ejemplo 1: lista de las credenciales específicas del servicio para un usuario

En el siguiente ejemplo de `list-service-specific-credentials`, se muestran todas las credenciales específicas del servicio asignadas al usuario indicado. En la respuesta no se incluyen contraseñas.

```
aws iam list-service-specific-credentials \
    --user-name sofia
```

Salida:

```
{
    "ServiceSpecificCredential": {
        "CreateDate": "2019-04-18T20:45:36+00:00",
        "ServiceName": "codecommit.amazonaws.com",
        "ServiceUserName": "sofia-at-123456789012",
        "ServiceSpecificCredentialId": "ACCAEXAMPLE123EXAMPLE",
        "UserName": "sofia",
        "Status": "Active"
    }
}
```

Ejemplo 2: lista de las credenciales específicas del servicio para un usuario filtrado para un servicio específico

En el siguiente ejemplo de `list-service-specific-credentials`, se muestran las credenciales específicas del servicio asignadas al usuario que realiza la solicitud. La lista se filtra para incluir solo las credenciales del servicio especificado. En la respuesta no se incluyen contraseñas.

```
aws iam list-service-specific-credentials \
    --service-name codecommit.amazonaws.com
```

Salida:

```
{
    "ServiceSpecificCredential": {
        "CreateDate": "2019-04-18T20:45:36+00:00",
        "ServiceName": "codecommit.amazonaws.com",
        "ServiceUserName": "sofia-at-123456789012",
        "ServiceSpecificCredentialId": "ACCAEXAMPLE123EXAMPLE",
        "UserName": "sofia",
        "Status": "Active"
    }
}
```

Para obtener más información, consulte Crear credenciales de Git para las conexiones HTTPS a CodeCommit en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte ListServiceSpecificCredential en la Referencia de comandos de la AWS CLI.

`list-service-specific-credentials`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-service-specific-credentials`.

AWS CLI

Para recuperar una lista de credenciales

En el siguiente ejemplo de `list-service-specific-credentials`, se enumeran las credenciales generadas para el acceso HTTPS a los repositorios de AWS CodeCommit para un usuario denominado `developer`.

```
aws iam list-service-specific-credentials \
    --user-name developer \
    --service-name codecommit.amazonaws.com
```

Salida:

```
{
    "ServiceSpecificCredentials": [
        {
            "UserName": "developer",
            "Status": "Inactive",
```

```
            "ServiceUserName": "developer-at-123456789012",
            "CreateDate": "2019-10-01T04:31:41Z",
            "ServiceSpecificCredentialId": "ACCAQFODXMPL4YFHP7DZE",
            "ServiceName": "codecommit.amazonaws.com"
        },
        {
            "UserName": "developer",
            "Status": "Active",
            "ServiceUserName": "developer+1-at-123456789012",
            "CreateDate": "2019-10-01T04:31:45Z",
            "ServiceSpecificCredentialId": "ACCAQFOXMPL6VW57M7AJP",
            "ServiceName": "codecommit.amazonaws.com"
        }
    ]
}
```

Para obtener más información, consulte Crear credenciales de Git para las conexiones HTTPS a CodeCommit en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte ListServiceSpecificCredentials en la Referencia de comandos de la AWS CLI.

`list-signing-certificates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-signing-certificates`.

AWS CLI

Cómo enumerar los certificados de firma de un usuario de IAM

El siguiente comando `list-signing-certificates` enumera los certificados de firma para el usuario de IAM llamado Bob.

```
aws iam list-signing-certificates \
    --user-name Bob
```

Salida:

```
{
    "Certificates": [
        {
            "UserName": "Bob",
```

```
            "Status": "Inactive",
            "CertificateBody": "-----BEGIN CERTIFICATE-----<certificate-body>-----
END CERTIFICATE-----",
            "CertificateId": "TA7SMP42TDN5Z26OBPJE7EXAMPLE",
            "UploadDate": "2013-06-06T21:40:08Z"
        }
    ]
}
```

Para obtener más información, consulte Gestionar certificados de firma en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte ListSigningCertificates en la Referencia de comandos de la AWS CLI.

`list-ssh-public-keys`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-ssh-public-keys`.

AWS CLI

Para enumerar las claves públicas de SSH asociadas a un usuario de IAM

En el siguiente ejemplo de `list-ssh-public-keys`, se enumeran las claves públicas de SSH asociadas al usuario de `sofia` IAM.

```
aws iam list-ssh-public-keys \
    --user-name sofia
```

Salida:

```
{
    "SSHPublicKeys": [
        {
            "UserName": "sofia",
            "SSHPublicKeyId": "APKA1234567890EXAMPLE",
            "Status": "Inactive",
            "UploadDate": "2019-04-18T17:04:49+00:00"
        }
    ]
}
```

Para obtener más información, consulte Uso de las claves SSH y SSH con CodeCommit en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListSshPublicKeys en la Referencia de comandos de la AWS CLI.

`list-user-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-user-policies`.

AWS CLI

Cómo enumerar las políticas de un usuario de IAM

El siguiente comando `list-user-policies` enumera las políticas asociadas al usuario de IAM denominado Bob.

```
aws iam list-user-policies \
    --user-name Bob
```

Salida:

```
{
    "PolicyNames": [
        "ExamplePolicy",
        "TestPolicy"
    ]
}
```

Para obtener más información, consulte Creación de un usuario de IAM en su cuenta de AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListUserPolicies en la Referencia de comandos de la AWS CLI.

`list-user-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-user-tags`.

AWS CLI

Cómo enumerar las etiquetas adjuntas a un usuario

El siguiente comando `list-user-tags` recupera la lista de etiquetas asociadas al usuario de IAM especificado.

```
aws iam list-user-tags \
    --user-name alice
```

Salida:

```
{
    "Tags": [
        {
            "Key": "Department",
            "Value": "Accounting"
        },
        {
            "Key": "DeptID",
            "Value": "12345"
        }
    ],
    "IsTruncated": false
}
```

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListUserTags en la Referencia de comandos de la AWS CLI.

`list-users`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-users`.

AWS CLI

Cómo enumerar usuarios de IAM

El siguiente comando `list-users` enumera los usuarios de IAM en la cuenta actual.

```
aws iam list-users
```

Salida:

```
{
    "Users": [
        {
            "UserName": "Adele",
            "Path": "/",
            "CreateDate": "2013-03-07T05:14:48Z",
            "UserId": "AKIAI44QH8DHBEXAMPLE",
            "Arn": "arn:aws:iam::123456789012:user/Adele"
        },
        {
            "UserName": "Bob",
            "Path": "/",
            "CreateDate": "2012-09-21T23:03:13Z",
            "UserId": "AKIAIOSFODNN7EXAMPLE",
            "Arn": "arn:aws:iam::123456789012:user/Bob"
        }
    ]
}
```

Para más información, consulte Enumeración de usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListUsers en la Referencia de comandos de la AWS CLI.

`list-virtual-mfa-devices`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-virtual-mfa-devices`.

AWS CLI

Cómo enumerar dispositivos de MFA virtuales

El siguiente comando `list-virtual-mfa-devices` muestra los dispositivos de MFA virtuales que se han configurado para la cuenta actual.

```
aws iam list-virtual-mfa-devices
```

Salida:

```
{
```

```
    "VirtualMFADevices": [
        {
            "SerialNumber": "arn:aws:iam::123456789012:mfa/ExampleMFADevice"
        },
        {
            "SerialNumber": "arn:aws:iam::123456789012:mfa/Fred"
        }
    ]
}
```

Para obtener más información, consulte Habilitación de un dispositivo de autenticación multifactor (MFA) virtual en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListVirtualMfaDevices en la Referencia de comandos de la AWS CLI.

`put-group-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-group-policy`.

AWS CLI

Cómo agregar una política a un grupo

El siguiente comando `put-group-policy` agrega una política al grupo de IAM denominado `Admins`.

```
aws iam put-group-policy \
    --group-name Admins \
    --policy-document file://AdminPolicy.json \
    --policy-name AdminRoot
```

Este comando no genera ninguna salida.

La política se define como un documento JSON en el archivo AdminPolicy.json. (El nombre y la extensión del archivo no son significativos).

Para obtener información, consulte Administración de políticas de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte PutGroupPolicy en la Referencia de comandos de la AWS CLI.

`put-role-permissions-boundary`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-role-permissions-boundary`.

AWS CLI

Ejemplo 1: aplicar un límite de permisos basado en una política personalizada a un rol de IAM

En el siguiente ejemplo de `put-role-permissions-boundary`, se aplica la política personalizada denominada `intern-boundary` como el límite de permisos para el rol de IAM especificado.

```
aws iam put-role-permissions-boundary \
    --permissions-boundary arn:aws:iam::123456789012:policy/intern-boundary \
    --role-name lambda-application-role
```

Este comando no genera ninguna salida.

Ejemplo 2: aplicar un límite de permisos basado en una política administrada de AWS a un rol de IAM

En el siguiente ejemplo de `put-role-permissions-boundary`, se aplica la política administrada de AWS `PowerUserAccess` como límite de permisos para el rol de IAM especificado.

```
aws iam put-role-permissions-boundary \
    --permissions-boundary arn:aws:iam::aws:policy/PowerUserAccess \
    --role-name x-account-admin
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Modificación de un rol en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte PutRolePermissionsBoundary en la Referencia de comandos de la AWS CLI.

`put-role-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-role-policy`.

AWS CLI

Cómo asociar una política de permisos a un rol de IAM

El siguiente comando `put-role-policy` agrega una política de permisos al rol denominado `Test-Role`.

```
aws iam put-role-policy \
    --role-name Test-Role \
    --policy-name ExamplePolicy \
    --policy-document file://AdminPolicy.json
```

Este comando no genera ninguna salida.

La política se define como un documento JSON en el archivo AdminPolicy.json. (El nombre y la extensión del archivo no son significativos).

Para asociar una política de confianza a un rol, utilice el comando `update-assume-role-policy`.

Para obtener más información, consulte Modificación de un rol en la Guía del usuario de IAM de AWS.

- Para obtener información sobre la API, consulte PutRolePolicy en la Referencia de comandos de la AWS CLI.

`put-user-permissions-boundary`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-user-permissions-boundary`.

AWS CLI

Ejemplo 1: aplicar un límite de permisos basado en una política personalizada a un usuario de IAM

En el siguiente ejemplo de `put-user-permissions-boundary`, se aplica una política personalizada denominada `intern-boundary` como el límite de permisos para el usuario de IAM especificado.

```
aws iam put-user-permissions-boundary \
    --permissions-boundary arn:aws:iam::123456789012:policy/intern-boundary \
    --user-name intern
```

Este comando no genera ninguna salida.

Ejemplo 2: aplicar un límite de permisos basado en una política administrada de AWS a un usuario de IAM

En el siguiente ejemplo de `put-user-permissions-boundary`, se aplica la política administrada de AWS denominada `PowerUserAccess` como el límite de permisos para el usuario de IAM especificado.

```
aws iam put-user-permissions-boundary \
    --permissions-boundary arn:aws:iam::aws:policy/PowerUserAccess \
    --user-name developer
```

Este comando no genera ninguna salida.

Para más información, consulte Adición y eliminación de permisos de identidad de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte PutUserPermissionsBoundary en la Referencia de Cmdlet de AWS CLI.

`put-user-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-user-policy`.

AWS CLI

Cómo asociar una política a un usuario de IAM

El siguiente comando `put-user-policy` asocia una política al usuario de IAM denominado Bob.

```
aws iam put-user-policy \
    --user-name Bob \
    --policy-name ExamplePolicy \
    --policy-document file://AdminPolicy.json
```

Este comando no genera ninguna salida.

La política se define como un documento JSON en el archivo AdminPolicy.json. (El nombre y la extensión del archivo no son significativos).

Para más información, consulte Adición y eliminación de permisos de identidad de IAM en la Guía del usuario de AWS IAM.

- Para obtener información acerca de la API, consulte PutUserPolicy en la Referencia de comandos de la AWS CLI.

`remove-client-id-from-open-id-connect-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-client-id-from-open-id-connect-provider`.

AWS CLI

Cómo eliminar el ID de cliente especificado de la lista de ID de clientes registrados para el proveedor de OpenID Connect de IAM especificado

En este ejemplo, se elimina el ID de cliente `My-TestApp-3` de la lista de ID de clientes asociada al proveedor de OIDC de IAM cuyo ARN es `arn:aws:iam::123456789012:oidc-provider/example.oidcprovider.com`.

```
aws iam remove-client-id-from-open-id-connect-provider
    --client-id My-TestApp-3 \
    --open-id-connect-provider-arn arn:aws:iam::123456789012:oidc-provider/
example.oidcprovider.com
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación de proveedores de identidad de OpenID Connect (OIDC) en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte RemoveClientIdFromOpenIdConnectProvider en la Referencia de comandos de AWS CLI.

`remove-role-from-instance-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-role-from-instance-profile`.

AWS CLI

Cómo eliminar un rol de un perfil de instancia

El siguiente comando `remove-role-from-instance-profile` elimina el rol llamado `Test-Role` del perfil de instancia denominado `ExampleInstanceProfile`.

```
aws iam remove-role-from-instance-profile \
    --instance-profile-name ExampleInstanceProfile \
    --role-name Test-Role
```

Para obtener más información, consulte Uso de perfiles de instancias en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte RemoveRoleFromInstanceProfile en la Referencia de comandos de la AWS CLI.

`remove-user-from-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-user-from-group`.

AWS CLI

Cómo eliminar un usuario de un grupo de IAM

El siguiente comando `remove-user-from-group` elimina al usuario denominado Bob del grupo de IAM denominado `Admins`.

```
aws iam remove-user-from-group \
    --user-name Bob \
    --group-name Admins
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adición y eliminación de usuarios de un grupo de usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte RemoveUserFromGroup en la Referencia de comandos de la AWS CLI.

`reset-service-specific-credential`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-service-specific-credential`.

AWS CLI

Ejemplo 1: restablecimiento de la contraseña de una credencial específica del servicio asociada al usuario que realiza la solicitud

En el siguiente ejemplo de `reset-service-specific-credential`, se genera una nueva contraseña criptográficamente segura para la credencial específica del servicio indicada y asociada al usuario que realiza la solicitud.

```
aws iam reset-service-specific-credential \
    --service-specific-credential-id ACCAEXAMPLE123EXAMPLE
```

Salida:

```
{
    "ServiceSpecificCredential": {
        "CreateDate": "2019-04-18T20:45:36+00:00",
        "ServiceName": "codecommit.amazonaws.com",
        "ServiceUserName": "sofia-at-123456789012",
        "ServicePassword": "+oaFsNk7tLco+C/obP9GhhcOzGcKOayTmE3LnAmAmH4=",
        "ServiceSpecificCredentialId": "ACCAEXAMPLE123EXAMPLE",
        "UserName": "sofia",
        "Status": "Active"
    }
}
```

Ejemplo 2: restablecimiento de la contraseña de una credencial específica del servicio asociada a un usuario específico

En el siguiente ejemplo de `reset-service-specific-credential`, se genera una nueva contraseña criptográficamente segura para la credencial específica del servicio asociada al usuario especificado.

```
aws iam reset-service-specific-credential \
    --user-name sofia \
    --service-specific-credential-id ACCAEXAMPLE123EXAMPLE
```

Salida:

```
{
    "ServiceSpecificCredential": {
```

```
        "CreateDate": "2019-04-18T20:45:36+00:00",
        "ServiceName": "codecommit.amazonaws.com",
        "ServiceUserName": "sofia-at-123456789012",
        "ServicePassword": "+oaFsNk7tLco+C/obP9GhhcOzGcKOayTmE3LnAmAmH4=",
        "ServiceSpecificCredentialId": "ACCAEXAMPLE123EXAMPLE",
        "UserName": "sofia",
        "Status": "Active"
    }
}
```

Para obtener más información, consulte Crear credenciales de Git para las conexiones HTTPS a CodeCommit en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte ResetServiceSpecificCredential en la Referencia de comandos de la AWS CLI.

`resync-mfa-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `resync-mfa-device`.

AWS CLI

Cómo sincronizar un dispositivo MFA

En el siguiente ejemplo de `resync-mfa-device`, se sincroniza el dispositivo MFA que está asociado al usuario de IAM `Bob` y cuyo ARN es `arn:aws:iam::123456789012:mfa/BobsMFADevice` con un programa autenticador que proporcionó los dos códigos de autenticación.

```
aws iam resync-mfa-device \
    --user-name Bob \
    --serial-number arn:aws:iam::210987654321:mfa/BobsMFADevice \
    --authentication-code1 123456 \
    --authentication-code2 987654
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ResyncMfaDevice en la Referencia de comandos de la AWS CLI.

`set-default-policy-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-default-policy-version`.

AWS CLI

Cómo establecer la versión especificada de la política especificada como la versión predeterminada de la política.

En este ejemplo, se establece la versión `v2` de la política cuyo ARN es `arn:aws:iam::123456789012:policy/MyPolicy` como la versión activa predeterminada.

```
aws iam set-default-policy-version \
    --policy-arn arn:aws:iam::123456789012:policy/MyPolicy \
    --version-id v2
```

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte SetDefaultPolicyVersion en la Referencia de comandos de la AWS CLI.

`set-security-token-service-preferences`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-security-token-service-preferences`.

AWS CLI

Para definir la versión del token de punto de conexión global

En el siguiente ejemplo de `set-security-token-service-preferences`, se configura Amazon STS para que utilice los tokens de la versión 2 al autenticarse en el punto de conexión global.

```
aws iam set-security-token-service-preferences \
    --global-endpoint-token-version v2Token
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración de AWS STS en una región de AWS en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte SetSecurityTokenServicePreferences en la Referencia de comandos de la AWS CLI.

`simulate-custom-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `simulate-custom-policy`.

AWS CLI

Ejemplo 1: simulación de los efectos de todas las políticas de IAM asociadas a un usuario o rol de IAM

A continuación, `simulate-custom-policy` muestra cómo proporcionar la política, definir los valores de las variables y simular una llamada a la API para ver si está permitida o se rechaza. En el siguiente ejemplo, se muestra una política que permite acceder a la base de datos únicamente después de una fecha y hora específicas. La simulación se realiza correctamente porque las acciones simuladas y la variable `aws:CurrentTime` especificada cumplen todos los requisitos de la política.

```
aws iam simulate-custom-policy \
    --policy-input-list '{"Version":"2012-10-17",       "Statement":
{"Effect":"Allow","Action":"dynamodb:*","Resource":"*","Condition":
{"DateGreaterThan":{"aws:CurrentTime":"2018-08-16T12:00:00Z"}}}}' \
    --action-names dynamodb:CreateBackup \
    --context-
entries "ContextKeyName='aws:CurrentTime',ContextKeyValues='2019-04-25T11:00:00Z',ContextKey
```

Salida:

```
{
    "EvaluationResults": [
        {
            "EvalActionName": "dynamodb:CreateBackup",
            "EvalResourceName": "*",
            "EvalDecision": "allowed",
            "MatchedStatements": [
                {
                    "SourcePolicyId": "PolicyInputList.1",
                    "StartPosition": {
                        "Line": 1,
                        "Column": 38
```

```
                    },
                    "EndPosition": {
                        "Line": 1,
                        "Column": 167
                    }
                }
            ],
            "MissingContextValues": []
        }
    ]
}
```

Ejemplo 2: simulación de un comando prohibido por la política

En el siguiente ejemplo de `simulate-custom-policy`, se muestran los resultados de la simulación de un comando prohibido por la política. En este ejemplo, la fecha proporcionada es anterior a la requerida por la condición de la política.

```
aws iam simulate-custom-policy \
    --policy-input-list '{"Version":"2012-10-17",       "Statement":
{"Effect":"Allow","Action":"dynamodb:*","Resource":"*","Condition":
{"DateGreaterThan":{"aws:CurrentTime":"2018-08-16T12:00:00Z"}}}}' \
    --action-names dynamodb:CreateBackup \
    --context-
entries "ContextKeyName='aws:CurrentTime',ContextKeyValues='2014-04-25T11:00:00Z',ContextKey
```

Salida:

```
{
    "EvaluationResults": [
        {
            "EvalActionName": "dynamodb:CreateBackup",
            "EvalResourceName": "*",
            "EvalDecision": "implicitDeny",
            "MatchedStatements": [],
            "MissingContextValues": []
        }
    ]
}
```

Para obtener más información, consulte Pruebas de la política de IAM con el simulador de política de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte SimulateCustomPolicy en la Referencia de comandos de la AWS CLI.

`simulate-principal-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `simulate-principal-policy`.

AWS CLI

Ejemplo 1: simulación de los efectos de una política de IAM arbitraria

A continuación, `simulate-principal-policy` muestra cómo simular que un usuario llame a una acción de la API y cómo determinar si las políticas asociadas a ese usuario permiten o deniegan la acción. En el siguiente ejemplo, el usuario tiene una política que solo permite la acción `codecommit:ListRepositories`.

```
aws iam simulate-principal-policy \
    --policy-source-arn arn:aws:iam::123456789012:user/alejandro \
    --action-names codecommit:ListRepositories
```

Salida:

```
{
    "EvaluationResults": [
        {
            "EvalActionName": "codecommit:ListRepositories",
            "EvalResourceName": "*",
            "EvalDecision": "allowed",
            "MatchedStatements": [
                {
                    "SourcePolicyId": "Grant-Access-To-CodeCommit-ListRepo",
                    "StartPosition": {
                        "Line": 3,
                        "Column": 19
                    },
                    "EndPosition": {
                        "Line": 9,
                        "Column": 10
                    }
                }
            ],
            "MissingContextValues": []
```

```
        }
    ]
}
```

Ejemplo 2: simulación de los efectos de un comando prohibido

En el siguiente ejemplo de `simulate-custom-policy`, se muestran los resultados de la simulación de un comando prohibido por una política del usuario. En el ejemplo siguiente, el usuario tiene una política que permite el acceso a una base de datos de DynamoDB solo después de una fecha y hora determinadas. En la simulación, el usuario intenta acceder a la base de datos con un valor `aws:CurrentTime` anterior a lo que permite la condición de la política.

```
aws iam simulate-principal-policy \
    --policy-source-arn arn:aws:iam::123456789012:user/alejandro \
    --action-names dynamodb:CreateBackup \
    --context-
entries "ContextKeyName='aws:CurrentTime',ContextKeyValues='2018-04-25T11:00:00Z',ContextKey
```

Salida:

```
{
    "EvaluationResults": [
        {
            "EvalActionName": "dynamodb:CreateBackup",
            "EvalResourceName": "*",
            "EvalDecision": "implicitDeny",
            "MatchedStatements": [],
            "MissingContextValues": []
        }
    ]
}
```

Para obtener más información, consulte Pruebas de la política de IAM con el simulador de política de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte SimulatePrincipalPolicy en la Referencia de comandos de la AWS CLI.

`tag-instance-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-instance-profile`.

AWS CLI

Para añadir un rol a un perfil de instancia

El siguiente comando `tag-instance-profile` agrega una etiqueta con el nombre de un departamento al perfil de instancia especificado.

```
aws iam tag-instance-profile \
    --instance-profile-name deployment-role \
    --tags '[{"Key": "Department", "Value": "Accounting"}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte TagInstanceProfile en la Referencia de comandos de la AWS CLI.

`tag-mfa-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-mfa-device`.

AWS CLI

Para añadir una etiqueta a un dispositivo MFA

El siguiente comando `tag-mfa-device` agrega una etiqueta con el nombre de un departamento al dispositivo MFA especificado.

```
aws iam tag-mfa-device \
    --serial-number arn:aws:iam::123456789012:mfa/alice \
    --tags '[{"Key": "Department", "Value": "Accounting"}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte TagMfaDevice en la Referencia de comandos de la AWS CLI.

`tag-open-id-connect-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-open-id-connect-provider`.

AWS CLI

Para añadir una etiqueta asociada a un proveedor de identidades compatible con OpenID Connect (OIDC

El siguiente comando `tag-open-id-connect-provider` agrega una etiqueta con el nombre de un departamento al proveedor de identidades OIDC especificado.

```
aws iam tag-open-id-connect-provider \
    --open-id-connect-provider-arn arn:aws:iam::123456789012:oidc-provider/
server.example.com \
    --tags '[{"Key": "Department", "Value": "Accounting"}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte TagOpenIdConnectProvider en la Referencia de comandos de la AWS CLI.

`tag-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-policy`.

AWS CLI

Para añadir una etiqueta a una política administrada por el cliente

El siguiente comando `tag-policy` agrega una etiqueta con el nombre de un departamento a la política administrada por el cliente.

```
aws iam tag-policy \
    --policy-arn arn:aws:iam::123456789012:policy/billing-access \
    --tags '[{"Key": "Department", "Value": "Accounting"}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para ver los detalles de la API, consulte TagPolicy en la Referencia de comandos de la AWS CLI.

`tag-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-role`.

AWS CLI

Cómo añadir una etiqueta a un rol

El siguiente comando `tag-role` agrega una etiqueta con el nombre de un departamento al rol especificado.

```
aws iam tag-role --role-name my-role \
    --tags '{"Key": "Department", "Value": "Accounting"}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte TagRole en la Referencia de comandos de la AWS CLI.

`tag-saml-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-saml-provider`.

AWS CLI

Para añadir una etiqueta a un proveedor de SAML

El siguiente comando `tag-saml-provider` agrega una etiqueta con el nombre de un departamento al proveedor de SAML especificado.

```
aws iam tag-saml-provider \
    --saml-provider-arn arn:aws:iam::123456789012:saml-provider/ADFS \
    --tags '[{"Key": "Department", "Value": "Accounting"}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte TagSamlProvider en la Referencia de comandos de la AWS CLI.

`tag-server-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-server-certificate`.

AWS CLI

Para añadir una etiqueta a un certificado de servidor

El siguiente comando `tag-saml-provider` agrega una etiqueta con el nombre de un departamento al certificado de servidor especificado.

```
aws iam tag-server-certificate \
    --server-certificate-name ExampleCertificate \
    --tags '[{"Key": "Department", "Value": "Accounting"}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte TagServerCertificate en la Referencia de comandos de la AWS CLI.

`tag-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-user`.

AWS CLI

Cómo añadir una etiqueta a un usuario

El siguiente comando `tag-user` agrega una etiqueta con el departamento asociado al usuario especificado.

```
aws iam tag-user \
    --user-name alice \
    --tags '{"Key": "Department", "Value": "Accounting"}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte TagUser en la Referencia de comandos de la AWS CLI.

`untag-instance-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-instance-profile`.

AWS CLI

Para eliminar un rol de un perfil de instancia

El siguiente comando `untag-instance-profile` elimina cualquier etiqueta con el nombre de clave Department del perfil de instancia especificado.

```
aws iam untag-instance-profile \
    --instance-profile-name deployment-role \
    --tag-keys Department
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte UntagInstanceProfile en la Referencia de comandos de la AWS CLI.

`untag-mfa-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-mfa-device`.

AWS CLI

Para eliminar una etiqueta de un dispositivo MFA

El siguiente comando `untag-mfa-device` elimina cualquier etiqueta con el nombre de clave Department del dispositivo MFA especificado.

```
aws iam untag-mfa-device \
    --serial-number arn:aws:iam::123456789012:mfa/alice \
    --tag-keys Department
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte UntagMfaDevice en la Referencia de comandos de la AWS CLI.

`untag-open-id-connect-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-open-id-connect-provider`.

AWS CLI

Para eliminar etiquetas de un proveedor de identidades OIDC

El siguiente comando `untag-open-id-connect-provider` elimina cualquier etiqueta con el nombre de clave Department del proveedor de identidades OIDC especificado.

```
aws iam untag-open-id-connect-provider \
    --open-id-connect-provider-arn arn:aws:iam::123456789012:oidc-provider/
server.example.com \
    --tag-keys Department
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte UntagOpenIdConnectProvider en la Referencia de comandos de la AWS CLI.

`untag-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-policy`.

AWS CLI

Para eliminar una etiqueta a una política administrada por el cliente

El siguiente comando `untag-policy` elimina cualquier etiqueta con el nombre de clave Department de la política administrada por el cliente especificada.

```
aws iam untag-policy \
    --policy-arn arn:aws:iam::452925170507:policy/billing-access \
    --tag-keys Department
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para ver los detalles de la API, consulte UntagPolicy en la Referencia de comandos de la AWS CLI.

`untag-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-role`.

AWS CLI

Cómo eliminar una etiqueta de un rol

El siguiente comando `untag-role` elimina cualquier etiqueta con el nombre de clave Department del rol especificado.

```
aws iam untag-role \
    --role-name my-role \
    --tag-keys Department
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para ver los detalles de la API, consulte UntagRole en la Referencia del comando de la AWS CLI.

`untag-saml-provider`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-saml-provider`.

AWS CLI

Para eliminar una etiqueta de un proveedor de SAML

El siguiente comando `untag-saml-provider` elimina cualquier etiqueta con el nombre de clave Department del perfil de instancia especificado.

```
aws iam untag-saml-provider \
    --saml-provider-arn arn:aws:iam::123456789012:saml-provider/ADFS \
    --tag-keys Department
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte UntagSamlProvider en la Referencia de comandos de la AWS CLI.

`untag-server-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-server-certificate`.

AWS CLI

Para eliminar una etiqueta de un certificado de servidor

El siguiente comando `untag-server-certificate` elimina cualquier etiqueta con el nombre de clave Department del certificado de servidor especificado.

```
aws iam untag-server-certificate \
    --server-certificate-name ExampleCertificate \
    --tag-keys Department
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte UntagServerCertificate en la Referencia de comandos de la AWS CLI.

`untag-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-user`.

AWS CLI

Cómo eliminar una etiqueta de un usuario

El siguiente comando `untag-user` elimina cualquier etiqueta con el nombre de clave Department del usuario especificado.

```
aws iam untag-user \
    --user-name alice \
    --tag-keys Department
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de IAM en la Guía del usuario de AWS IAM.

- Para ver los detalles de la API, consulte UntagUser en la Referencia del comando de la AWS CLI.

`update-access-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-access-key`.

AWS CLI

Cómo activar o desactivar una clave de acceso para un usuario de IAM

El siguiente comando `update-access-key` desactiva la clave de acceso especificada (ID de clave de acceso y clave de acceso secreta) para el usuario de IAM denominado Bob.

```
aws iam update-access-key \
    --access-key-id AKIAIOSFODNN7EXAMPLE \
    --status Inactive \
    --user-name Bob
```

Este comando no genera ninguna salida.

Si se desactiva la clave, no se puede utilizar para acceder mediante programación a AWS. Sin embargo, la clave sigue disponible y se puede reactivar.

Para obtener más información, consulte Administración de claves de acceso para usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte UpdateAccessKey en la Referencia de la API de la AWS CLI.

`update-account-password-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-account-password-policy`.

AWS CLI

Cómo ver la política de contraseñas de la cuenta actual

El siguiente comando `update-account-password-policy` establece que la política de contraseñas requiera una longitud mínima de ocho caracteres y que la contraseña contenga uno o más números.

```
aws iam update-account-password-policy \
    --minimum-password-length 8 \
    --require-numbers
```

Este comando no genera ninguna salida.

Los cambios en la política de contraseñas de una cuenta afectan a cualquier contraseña nueva que se cree para los usuarios de IAM en la cuenta. Los cambios en la política de contraseñas no afectan a las contraseñas existentes.

Para obtener más información, consulte Configuración de una política de contraseñas de cuentas para los usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información acerca de la API, consulte UpdateAccountPasswordPolicy en la Referencia de comandos de la AWS CLI.

`update-assume-role-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-assume-role-policy`.

AWS CLI

Cómo actualizar la política de confianza de un rol de IAM

El siguiente comando `update-assume-role-policy` actualiza la política de confianza del rol denominado `Test-Role`.

```
aws iam update-assume-role-policy \
    --role-name Test-Role \
    --policy-document file://Test-Role-Trust-Policy.json
```

Este comando no genera ninguna salida.

La política de confianza se define como un documento JSON en el archivo Test-Role-Trust-Policy.json. (El nombre y la extensión del archivo no son significativos). La política de confianza debe especificar una entidad principal.

Utilice el comando `put-role-policy` para actualizar la política de permisos de un rol.

Para más información, consulte Creación de roles de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte UpdateAssumeRolePolicy en la Referencia de comandos de la AWS CLI.

update-group

En el siguiente ejemplo de código, se muestra cómo utilizar `update-group`.

AWS CLI

Cómo cambiar el nombre de un grupo de IAM

El siguiente comando `update-group` cambia el nombre del grupo de IAM de `Test` a `Test-1`.

```
aws iam update-group \
    --group-name Test \
    --new-group-name Test-1
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Cambio del nombre de un grupo de usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte UpdateGroup en la Referencia de comandos de la AWS CLI.

`update-login-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-login-profile`.

AWS CLI

Cómo actualizar la contraseña de un usuario de IAM

El siguiente comando `update-login-profile` crea una nueva contraseña para el usuario de IAM llamado Bob.

```
aws iam update-login-profile \
    --user-name Bob \
    --password <password>
```

Este comando no genera ninguna salida.

Para establecer una política de contraseñas para la cuenta, use el comando `update-account-password-policy`. Si la nueva contraseña infringe la política de contraseñas de la cuenta, el comando devuelve un error de `PasswordPolicyViolation`.

Si la política de contraseñas de la cuenta lo permite, los usuarios de IAM pueden cambiar sus propias contraseñas mediante el comando `change-password`.

Guarde la nueva contraseña en un lugar seguro. Si se pierde la contraseña, no se puede recuperar y debe crear una nueva con el comando `create-login-profile`.

Para obtener más información, consulte Gestión de contraseñas para usuarios de IAM en la Guía del usuario de AWS IAM.

- Para obtener información acerca de la API, consulte UpdateLoginProfile en la Referencia de comandos de la AWS CLI.

`update-open-id-connect-provider-thumbprint`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-open-id-connect-provider-thumbprint`.

AWS CLI

Cómo reemplazar la lista existente de huellas digitales de certificados de servidor por una nueva lista

En este ejemplo, se actualiza la lista de huellas digitales de certificados del proveedor de OIDC cuyo ARN es `arn:aws:iam::123456789012:oidc-provider/example.oidcprovider.com` para utilizar una nueva huella digital.

```
aws iam update-open-id-connect-provider-thumbprint \
    --open-id-connect-provider-arn arn:aws:iam::123456789012:oidc-provider/
example.oidcprovider.com \
    --thumbprint-list 7359755EXAMPLEabc3060bce3EXAMPLEec4542a3
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación de proveedores de identidad OpenID Connect (OIDC) en la Guía del usuario de AWS IAM.

- Para obtener información acerca de la API, consulte UpdateOpenIdConnectProviderThumbprint en la Referencia de comandos de la AWS CLI.

`update-role-description`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-role-description`.

AWS CLI

Cómo cambiar la descripción de un rol de IAM

El siguiente comando `update-role` cambia la descripción del rol de IAM de `production-role` a `Main production role`.

```
aws iam update-role-description \
    --role-name production-role \
    --description 'Main production role'
```

Salida:

```
{
```

```
    "Role": {
        "Path": "/",
        "RoleName": "production-role",
        "RoleId": "AROA1234567890EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:role/production-role",
        "CreateDate": "2017-12-06T17:16:37+00:00",
        "AssumeRolePolicyDocument": {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::123456789012:root"
                    },
                    "Action": "sts:AssumeRole",
                    "Condition": {}
                }
            ]
        },
        "Description": "Main production role"
    }
}
```

Para obtener más información, consulte Modificación de un rol en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte UpdateRoleDescription en la Referencia de comandos de la AWS CLI.

`update-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-role`.

AWS CLI

Cómo cambiar la descripción de un rol de IAM o la duración de la sesión

El siguiente comando `update-role` cambia la descripción del rol de IAM `production-role` a `Main production role` y establece la duración máxima de la sesión en 12 horas.

```
aws iam update-role \
    --role-name production-role \
    --description 'Main production role' \
```

```
    --max-session-duration 43200
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Modificación de un rol en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte UpdateRole en la Referencia de comandos de la AWS CLI.

update-saml-provider

En el siguiente ejemplo de código, se muestra cómo utilizar `update-saml-provider`.

AWS CLI

Cómo actualizar el documento de metadatos de un proveedor SAML existente

En este ejemplo, se actualiza el proveedor SAML en IAM cuyo ARN es `arn:aws:iam::123456789012:saml-provider/SAMLADFS` con un nuevo documento de metadatos SAML del archivo `SAMLMetaData.xml`.

```
aws iam update-saml-provider \
    --saml-metadata-document file://SAMLMetaData.xml \
    --saml-provider-arn arn:aws:iam::123456789012:saml-provider/SAMLADFS
```

Salida:

```
{
    "SAMLProviderArn": "arn:aws:iam::123456789012:saml-provider/SAMLADFS"
}
```

Para obtener más información, consulte Creación de proveedores de identidad SAML de IAM en la Guía del usuario de AWS IAM.

- Para obtener información acerca de la API, consulte UpdateSamlProvider en la Referencia de comandos de la AWS CLI.

update-server-certificate

En el siguiente ejemplo de código, se muestra cómo utilizar `update-server-certificate`.

AWS CLI

Cómo cambiar la ruta o el nombre de un certificado de servidor en su cuenta de AWS

El siguiente comando `update-server-certificate` cambia el nombre del certificado de `myServerCertificate` a `myUpdatedServerCertificate`. También cambia la ruta a `/cloudfront/` para que el servicio Amazon CloudFront pueda acceder a ella. Este comando no genera ninguna salida. Puede ver los resultados de la actualización al ejecutar el comando `list-server-certificates`.

```
aws-iam update-server-certificate \
    --server-certificate-name myServerCertificate \
    --new-server-certificate-name myUpdatedServerCertificate \
    --new-path /cloudfront/
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración de certificados de servidor en IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte UpdateServerCertificate en la Referencia de comandos de la AWS CLI.

`update-service-specific-credential`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-service-specific-credential`.

AWS CLI

Ejemplo 1: actualización del estado de la credencial específica del servicio del usuario solicitante

En el siguiente ejemplo de `update-service-specific-credential`, el estado de la credencial especificada para el usuario que realiza la solicitud cambia a `Inactive`.

```
aws iam update-service-specific-credential \
    --service-specific-credential-id ACCAEXAMPLE123EXAMPLE \
    --status Inactive
```

Este comando no genera ninguna salida.

Ejemplo 2: actualización del estado de una credencial específica del servicio del usuario especificado

En el siguiente ejemplo de `update-service-specific-credential`, el estado de la credencial del usuario especificado cambia a Inactiva.

```
aws iam update-service-specific-credential \
    --user-name sofia \
    --service-specific-credential-id ACCAEXAMPLE123EXAMPLE \
    --status Inactive
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Crear credenciales de Git para las conexiones HTTPS a CodeCommit en la Guía del usuario de AWS CodeCommit.

- Para obtener detalles sobre la API, consulte UpdateServiceSpecificCredential en la Referencia de comandos de la AWS CLI.

`update-signing-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-signing-certificate`.

AWS CLI

Cómo activar o desactivar un certificado de firma para un usuario de IAM

El siguiente comando `update-signing-certificate` desactiva el certificado de firma especificado para el usuario de IAM llamado Bob.

```
aws iam update-signing-certificate \
    --certificate-id TA7SMP42TDN5Z26OBPJE7EXAMPLE \
    --status Inactive \
    --user-name Bob
```

Para obtener el ID de un certificado de firma, use el comando `list-signing-certificates`.

Para obtener más información, consulte Gestionar certificados de firma en la Guía del usuario de Amazon EC2.

- Para obtener información sobre la API, consulte UpdateSigningCertificate en la Referencia de comandos de la AWS CLI.

update-ssh-public-key

En el siguiente ejemplo de código, se muestra cómo utilizar `update-ssh-public-key`.

AWS CLI

Para cambiar el estado de una clave pública SSH

El siguiente comando `update-ssh-public-key` cambia el estado de la clave pública especificada a `Inactive`.

```
aws iam update-ssh-public-key \
    --user-name sofia \
    --ssh-public-key-id APKA1234567890EXAMPLE \
    --status Inactive
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de las claves SSH y SSH con CodeCommit en la Guía del usuario de AWS IAM.

- Para obtener información acerca de la API, consulte UpdateSshPublicKey en la Referencia de comandos de la AWS CLI.

update-user

En el siguiente ejemplo de código, se muestra cómo utilizar `update-user`.

AWS CLI

Cómo cambiar el nombre de un usuario de IAM

El siguiente comando `update-user` cambia el nombre del usuario de IAM de `Bob` a `Robert`.

```
aws iam update-user \
    --user-name Bob \
    --new-user-name Robert
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Cambio del nombre de un grupo de usuarios de IAM en la Guía del usuario de IAM de AWS.

- Para obtener información sobre la API, consulte UpdateUser en la Referencia de comandos de la AWS CLI.

`upload-server-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `upload-server-certificate`.

AWS CLI

Cómo cargar un certificado de servidor en su cuenta de AWS

El siguiente comando upload-server-certificate carga un certificado de servidor en su cuenta de AWS. En este ejemplo, el certificado está en el archivo `public_key_cert_file.pem`, la clave privada asociada está en el archivo `my_private_key.pem` y la cadena de certificados proporcionada por la entidad de certificación (CA) está en el archivo `my_certificate_chain_file.pem`. Cuando el archivo haya terminado de cargarse, estará disponible con el nombre myServerCertificate. Los parámetros que comienzan con `file://` indican al comando que lea el contenido del archivo y lo use como valor del parámetro en lugar del nombre del archivo en sí.

```
aws iam upload-server-certificate \
    --server-certificate-name myServerCertificate \
    --certificate-body file://public_key_cert_file.pem \
    --private-key file://my_private_key.pem \
    --certificate-chain file://my_certificate_chain_file.pem
```

Salida:

```
{
    "ServerCertificateMetadata": {
        "Path": "/",
        "ServerCertificateName": "myServerCertificate",
        "ServerCertificateId": "ASCAEXAMPLE123EXAMPLE",
        "Arn": "arn:aws:iam::1234567989012:server-certificate/myServerCertificate",
        "UploadDate": "2019-04-22T21:13:44+00:00",
        "Expiration": "2019-10-15T22:23:16+00:00"
    }
}
```

Para obtener más información, consulte Creación, carga y eliminación de certificados de servidor en la guía Uso de IAM.

- Para obtener información sobre la API, consulte UploadServerCertificate en la Referencia de comandos de la AWS CLI.

`upload-signing-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `upload-signing-certificate`.

AWS CLI

Cómo cargar un certificado de firma para un usuario de IAM

El siguiente comando `upload-signing-certificate` carga un certificado de firma para el usuario de IAM nombrado Bob.

```
aws iam upload-signing-certificate \
    --user-name Bob \
    --certificate-body file://certificate.pem
```

Salida:

```
{
    "Certificate": {
        "UserName": "Bob",
        "Status": "Active",
        "CertificateBody": "-----BEGIN CERTIFICATE-----<certificate-body>-----END
 CERTIFICATE-----",
        "CertificateId": "TA7SMP42TDN5Z26OBPJE7EXAMPLE",
        "UploadDate": "2013-06-06T21:40:08.121Z"
    }
}
```

El certificado se encuentra en un archivo denominado certificate.pem en formato PEM.

Para obtener más información, consulte Creación, carga y eliminación de certificados de servidor en la guía de Uso de IAM.

- Para obtener información sobre la API, consulte UploadSigningCertificate en la Referencia de comandos de la AWS CLI.

`upload-ssh-public-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `upload-ssh-public-key`.

AWS CLI

Para actualizar una clave pública SSH y asociación de la misma con un usuario

El siguiente comando `upload-ssh-public-key` carga la clave pública encontrada en el archivo `sshkey.pub` y la asocia al usuario `sofia`.

```
aws iam upload-ssh-public-key \
    --user-name sofia \
    --ssh-public-key-body file://sshkey.pub
```

Salida:

```
{
    "SSHPublicKey": {
        "UserName": "sofia",
        "SSHPublicKeyId": "APKA1234567890EXAMPLE",
        "Fingerprint": "12:34:56:78:90:ab:cd:ef:12:34:56:78:90:ab:cd:ef",
        "SSHPublicKeyBody": "ssh-rsa <<long string generated by ssh-keygen
 command>>",
        "Status": "Active",
        "UploadDate": "2019-04-18T17:04:49+00:00"
    }
}
```

Para obtener más información sobre cómo generar claves en un formato adecuado para este comando, consulte SSH y Linux, macOS o Unix: configure las claves públicas y privadas de Git y CodeCommit o Configurar las claves públicas y privadas para Git y CodeCommit en la Guía del usuario de AWS CodeCommit.

- Para obtener información sobre la API, consulte UploadSshPublicKey en la Referencia de comandos de la AWS CLI.

Ejemplos del Analizador de acceso de IAM que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar situaciones comunes usando la AWS Command Line Interface con el Analizador de acceso de IAM.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`apply-archive-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `apply-archive-rule`.

AWS CLI

Aplicación de una regla de archivado a los resultados existentes que cumplan los criterios de la regla de archivado

En el siguiente ejemplo de `apply-archive-rule`, se aplica una regla de archivado a los resultados existentes que cumplen los criterios de la regla de archivado.

```
aws accessanalyzer apply-archive-rule \
    --analyzer-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
UnusedAccess-ConsoleAnalyzer-organization \
    --rule-name MyArchiveRule
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Reglas de archivado en la Guía del usuario de AWS IAM.

- Para obtener más información sobre la API, consulte ApplyArchiveRule en la Referencia de comandos de la AWS CLI.

`cancel-policy-generation`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-policy-generation`.

AWS CLI

Cancelación de la generación de políticas solicitada

En el siguiente ejemplo de `cancel-policy-generation`, se cancela el ID de trabajo de la generación de políticas solicitada.

```
aws accessanalyzer cancel-policy-generation \
    --job-id 923a56b0-ebb8-4e80-8a3c-a11ccfbcd6f2
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Generación de políticas del Analizador de acceso de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CancelPolicyGeneration en la Referencia de comandos de la AWS CLI.

`check-access-not-granted`

En el siguiente ejemplo de código, se muestra cómo utilizar `check-access-not-granted`.

AWS CLI

Comprobación de si una política no permite el acceso especificado

En el siguiente ejemplo de `check-access-not-granted`, se comprueba si una política no permite el acceso especificado.

```
aws accessanalyzer check-access-not-granted \
    --policy-document file://myfile.json \
    --access actions="s3:DeleteBucket","s3:GetBucketLocation" \
    --policy-type IDENTITY_POLICY
```

Contenidos de `myfile.json`:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
```

```
            ]
        }
    ]
}
```

Salida:

```
{
    "result": "PASS",
    "message": "The policy document does not grant access to perform one or more of
 the listed actions."
}
```

Para obtener más información, consulte Vista previa del acceso con las API de IAM Access Analyzer en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CheckAccessNotGranted en la Referencia de comandos de la AWS CLI.

`check-no-new-access`

En el siguiente ejemplo de código, se muestra cómo utilizar `check-no-new-access`.

AWS CLI

Comprobación de si se permite un nuevo acceso a una política actualizada al compararla con la política existente

En el siguiente ejemplo de `check-no-new-access`, se comprueba si se permite un nuevo acceso a una política actualizada al compararla con la política existente.

```
aws accessanalyzer check-no-new-access \
    --existing-policy-document file://existing-policy.json \
    --new-policy-document file://new-policy.json \
    --policy-type IDENTITY_POLICY
```

Contenido de `existing-policy.json`:

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

Contenido de `new-policy.json`:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

Salida:

```
{
    "result": "FAIL",
    "message": "The modified permissions grant new access compared to your existing
 policy.",
    "reasons": [
        {
            "description": "New access in the statement with index: 0.",
```

```
            "statementIndex": 0
        }
    ]
}
```

Para obtener más información, consulte Vista previa del acceso con las API de IAM Access Analyzer en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CheckNoNewAccess en la Referencia de comandos de la AWS CLI.

`check-no-public-access`

En el siguiente ejemplo de código, se muestra cómo utilizar `check-no-public-access`.

AWS CLI

Comprobación de si una política de recursos puede conceder acceso público al tipo de recurso especificado

En el siguiente ejemplo de `check-no-public-access`, se comprueba si una política de recursos puede conceder acceso público al tipo de recurso especificado.

```
aws accessanalyzer check-no-public-access \
    --policy-document file://check-no-public-access-myfile.json \
    --resource-type AWS::S3::Bucket
```

Contenidos de `myfile.json`:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CheckNoPublicAccess",
            "Effect": "Allow",
            "Principal": { "AWS": "arn:aws:iam::111122223333:user/JohnDoe" },
            "Action": [
                "s3:GetObject"
            ]
        }
    ]
```

```
}
```

Salida:

```
{
    "result": "PASS",
    "message": "The resource policy does not grant public access for the given
 resource type."
}
```

Para obtener más información, consulte Vista previa del acceso con las API de IAM Access Analyzer en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CheckNoPublicAccess en la Referencia de comandos de la AWS CLI.

`create-access-preview`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-access-preview`.

AWS CLI

Creación de una vista previa del acceso que le permita obtener una vista previa de los resultados del analizador de acceso de IAM para su recurso antes de implementar los permisos del recurso

En el siguiente ejemplo de `create-access-preview`, se crea una vista previa del acceso que le permite obtener una vista previa de los resultados del Analizador de acceso de IAM para su recurso antes de implementar los permisos de recursos en la cuenta de AWS.

```
aws accessanalyzer create-access-preview \
    --analyzer-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account \
    --configurations file://myfile.json
```

Contenidos de `myfile.json`:

```
{
    "arn:aws:s3:::amzn-s3-demo-bucket": {
        "s3Bucket": {
            "bucketPolicy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Principal\":{\"AWS\":[\"arn:aws:iam::111122223333:root\"]},\"Action
```

```
\":[\"s3:PutObject\",\"s3:PutObjectAcl\"],\"Resource\":\"arn:aws:s3:::amzn-s3-demo-
bucket/*\"}]}",
            "bucketPublicAccessBlock": {
                "ignorePublicAcls": true,
                "restrictPublicBuckets": true
            },
            "bucketAclGrants": [
                {
                    "grantee": {
                        "id":
 "79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be"
                    },
                    "permission": "READ"
                }
            ]
        }
    }
}
```

Salida:

```
{
    "id": "3c65eb13-6ef9-4629-8919-a32043619e6b"
}
```

Para obtener más información, consulte Vista previa del acceso con las API de IAM Access Analyzer en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreateAccessPreview en la Referencia de comandos de la AWS CLI.

`create-analyzer`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-analyzer`.

AWS CLI

Cómo crear un analizador

En el siguiente ejemplo de `create-analyzer`, se crea un analizador en la cuenta de AWS.

```
aws accessanalyzer create-analyzer \
```

```
    --analyzer-name example \
    --type ACCOUNT
```

Salida:

```
{
    "arn": "arn:aws:access-analyzer:us-east-2:111122223333:analyzer/example"
}
```

Para obtener más información, consulte Introducción a los resultados de AWS Identity and Access Management Access Analyzer de la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreateAnalyzer en la Referencia de comandos de la AWS CLI.

`create-archive-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-archive-rule`.

AWS CLI

Creación de una regla de archivado para el analizador especificado

En el siguiente ejemplo de `create-archive-rule`, se crea una regla de archivado para el analizador especificado en la cuenta de AWS.

```
aws accessanalyzer create-archive-rule \
    --analyzer-name UnusedAccess-ConsoleAnalyzer-organization \
    --rule-name MyRule \
    --filter '{"resource": {"contains": ["Cognito"]}, "resourceType": {"eq":
 ["AWS::IAM::Role"]}}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Reglas de archivado en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte CreateArchiveRule en la Referencia de comandos de la AWS CLI.

`delete-analyzer`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-analyzer`.

AWS CLI

Eliminación del analizador especificado

En el siguiente ejemplo de `delete-analyzer`, se elimina el analizador especificado de la cuenta de AWS.

```
aws accessanalyzer delete-analyzer \
    --analyzer-name example
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Reglas de archivado en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteAnalyzer en la Referencia de comandos de la AWS CLI.

`delete-archive-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-archive-rule`.

AWS CLI

Eliminación de la regla de archivado especificada

En el siguiente ejemplo de `delete-archive-rule`, se elimina la regla de archivado especificada de la cuenta de AWS.

```
aws accessanalyzer delete-archive-rule \
    --analyzer-name UnusedAccess-ConsoleAnalyzer-organization \
    --rule-name MyRule
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Reglas de archivado en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DeleteArchiveRule en la Referencia de comandos de la AWS CLI.

`get-access-preview`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-access-preview`.

AWS CLI

Recuperación de información sobre una vista previa de acceso del analizador especificado

En el siguiente ejemplo de `get-access-preview`, se recupera información sobre una vista previa del acceso del analizador especificado en la cuenta de AWS.

```
aws accessanalyzer get-access-preview \
    --access-preview-id 3c65eb13-6ef9-4629-8919-a32043619e6b \
    --analyzer-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account
```

Salida:

```
{
    "accessPreview": {
        "id": "3c65eb13-6ef9-4629-8919-a32043619e6b",
        "analyzerArn": "arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account",
        "configurations": {
            "arn:aws:s3:::amzn-s3-demo-bucket": {
                "s3Bucket": {
                    "bucketPolicy": "{\"Version\":\"2012-10-17\",\"Statement\":
[{\"Effect\":\"Allow\",\"Principal\":{\"AWS\":[\"arn:aws:iam::111122223333:root\"]},
\"Action\":[\"s3:PutObject\",\"s3:PutObjectAcl\"],\"Resource\":\"arn:aws:s3:::amzn-
s3-demo-bucket/*\"}]}",
                    "bucketAclGrants": [
                        {
                            "permission": "READ",
                            "grantee": {
                                "id":
 "79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be"
                            }
                        }
                    ],
                    "bucketPublicAccessBlock": {
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    }
                }
            }
        },
        "createdAt": "2024-02-17T00:18:44+00:00",
```

```
        "status": "COMPLETED"
    }
}
```

Para obtener más información, consulte Vista previa del acceso con las API de IAM Access Analyzer en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetAccessPreview en la Referencia de comandos de la AWS CLI.

`get-analyzed-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-analyzed-resource`.

AWS CLI

Recuperación de la información sobre un recurso analizado

En el siguiente ejemplo de `get-analyzed-resource`, se recupera información sobre un recurso que se ha analizado en la cuenta de AWS.

```
aws accessanalyzer get-analyzed-resource \
    --analyzer-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account \
    --resource-arn arn:aws:s3:::amzn-s3-demo-bucket
```

Salida:

```
{
    "resource": {
        "analyzedAt": "2024-02-15T18:01:53.002000+00:00",
        "isPublic": false,
        "resourceArn": "arn:aws:s3:::amzn-s3-demo-bucket",
        "resourceOwnerAccount": "111122223333",
        "resourceType": "AWS::S3::Bucket"
    }
}
```

Para obtener más información, consulte Uso de AWS Identity and Access Management Access Analyzer en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetAnalyzedResource en la Referencia de comandos de la AWS CLI.

`get-analyzer`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-analyzer`.

AWS CLI

Recuperación de información sobre el analizador especificado

En el siguiente ejemplo de `get-analyzer`, se devuelve información sobre el analizador especificado en la cuenta de AWS.

```
aws accessanalyzer get-analyzer \
    --analyzer-name ConsoleAnalyzer-account
```

Salida:

```
{
    "analyzer": {
        "arn": "arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account",
        "createdAt": "2019-12-03T07:28:17+00:00",
        "lastResourceAnalyzed": "arn:aws:sns:us-west-2:111122223333:config-topic",
        "lastResourceAnalyzedAt": "2024-02-15T18:01:53.003000+00:00",
        "name": "ConsoleAnalyzer-account",
        "status": "ACTIVE",
        "tags": {
            "auto-delete": "no"
        },
        "type": "ACCOUNT"
    }
}
```

Para obtener más información, consulte Uso de AWS Identity and Access Management Access Analyzer en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetAnalyzer en la Referencia de comandos de la AWS CLI.

`get-archive-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-archive-rule`.

AWS CLI

Recuperación de información sobre una regla de archivado

En el siguiente ejemplo de `get-archive-rule`, se recupera información sobre una regla de archivado en la cuenta de AWS.

```
aws accessanalyzer get-archive-rule \
    --analyzer-name UnusedAccess-ConsoleAnalyzer-organization \
    --rule-name MyArchiveRule
```

Salida:

```
{
    "archiveRule": {
        "createdAt": "2024-02-15T00:49:27+00:00",
        "filter": {
            "resource": {
                "contains": [
                    "Cognito"
                ]
            },
            "resourceType": {
                "eq": [
                    "AWS::IAM::Role"
                ]
            }
        },
        "ruleName": "MyArchiveRule",
        "updatedAt": "2024-02-15T00:49:27+00:00"
    }
}
```

Para obtener más información, consulte Reglas de archivado en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetArchiveRule en la Referencia de comandos de la AWS CLI.

`get-finding-v2`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-finding-v2`.

AWS CLI

Recuperación de información sobre el resultado especificado

En el siguiente ejemplo de `get-finding-v2`, se recupera información sobre el resultado especificado en la cuenta de AWS.

```
aws accessanalyzer get-finding-v2 \
    --analyzer-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-organization \
    --id 0910eedb-381e-4e95-adda-0d25c19e6e90
```

Salida:

```
{
    "findingDetails": [
        {
            "externalAccessDetails": {
                "action": [
                    "sts:AssumeRoleWithWebIdentity"
                ],
                "condition": {
                    "cognito-identity.amazonaws.com:aud": "us-
west-2:EXAMPLE0-0000-0000-0000-000000000000"
                },
                "isPublic": false,
                "principal": {
                    "Federated": "cognito-identity.amazonaws.com"
                }
            }
        }
    ],
    "resource": "arn:aws:iam::111122223333:role/Cognito_testpoolAuth_Role",
    "status": "ACTIVE",
    "error": null,
    "createdAt": "2021-02-26T21:17:50.905000+00:00",
    "resourceType": "AWS::IAM::Role",
    "findingType": "ExternalAccess",
    "resourceOwnerAccount": "111122223333",
```

```
    "analyzedAt": "2024-02-16T18:17:47.888000+00:00",
    "id": "0910eedb-381e-4e95-adda-0d25c19e6e90",
    "updatedAt": "2021-02-26T21:17:50.905000+00:00"
}
```

Para obtener más información, consulte Revisión de los resultados en la Guía del usuario de AWS.

- Para obtener información sobre la API, consulte GetFindingV2 en la Referencia de comandos de la AWS CLI.

`get-finding`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-finding`.

AWS CLI

Recuperación de información sobre el resultado especificado

En el siguiente ejemplo de `get-finding`, se recupera información sobre el resultado especificado en la cuenta de AWS.

```
aws accessanalyzer get-finding \
    --analyzer-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-organization \
    --id 0910eedb-381e-4e95-adda-0d25c19e6e90
```

Salida:

```
{
    "finding": {
        "id": "0910eedb-381e-4e95-adda-0d25c19e6e90",
        "principal": {
            "Federated": "cognito-identity.amazonaws.com"
        },
        "action": [
            "sts:AssumeRoleWithWebIdentity"
        ],
        "resource": "arn:aws:iam::111122223333:role/Cognito_testpoolAuth_Role",
        "isPublic": false,
        "resourceType": "AWS::IAM::Role",
        "condition": {
```

```
            "cognito-identity.amazonaws.com:aud": "us-
west-2:EXAMPLE0-0000-0000-0000-000000000000"
        },
        "createdAt": "2021-02-26T21:17:50.905000+00:00",
        "analyzedAt": "2024-02-16T18:17:47.888000+00:00",
        "updatedAt": "2021-02-26T21:17:50.905000+00:00",
        "status": "ACTIVE",
        "resourceOwnerAccount": "111122223333"
    }
}
```

Para obtener más información, consulte Revisión de los resultados en la Guía del usuario de AWS.

- Para obtener información sobre la API, consulte GetFinding en la Referencia de comandos de la AWS CLI.

`get-generated-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-generated-policy`.

AWS CLI

Recuperación de la política generada mediante la API StartPolicyGeneration

En el siguiente ejemplo de `get-generated-policy`, se recupera la política que se ha generado mediante la API StartPolicyGeneration en la cuenta de AWS.

```
aws accessanalyzer get-generated-policy \
    --job-id c557dc4a-0338-4489-95dd-739014860ff9
```

Salida:

```
{
    "generatedPolicyResult": {
        "generatedPolicies": [
            {
                "policy": "{\"Version\":\"2012-10-17\",\"Statement\":
[{\"Sid\":\"SupportedServiceSid0\",\"Effect\":\"Allow\",\"Action\":
[\"access-analyzer:GetAnalyzer\",\"access-analyzer:ListAnalyzers\",
\"access-analyzer:ListArchiveRules\",\"access-analyzer:ListFindings
\",\"cloudtrail:DescribeTrails\",\"cloudtrail:GetEventDataStore\",
\"cloudtrail:GetEventSelectors\",\"cloudtrail:GetInsightSelectors
```

```
\",\"cloudtrail:GetTrailStatus\",\"cloudtrail:ListChannels\",
\"cloudtrail:ListEventDataStores\",\"cloudtrail:ListQueries\",\"cloudtrail:ListTags
\",\"cloudtrail:LookupEvents\",\"ec2:DescribeRegions\",\"iam:GetAccountSummary
\",\"iam:GetOpenIDConnectProvider\",\"iam:GetRole\",\"iam:ListAccessKeys\",
\"iam:ListAccountAliases\",\"iam:ListOpenIDConnectProviders\",\"iam:ListRoles
\",\"iam:ListSAMLProviders\",\"kms:ListAliases\",\"s3:GetBucketLocation\",
\"s3:ListAllMyBuckets\"],\"Resource\":\"*\"}]}"
            }
        ],
        "properties": {
            "cloudTrailProperties": {
                "endTime": "2024-02-14T22:44:40+00:00",
                "startTime": "2024-02-13T00:30:00+00:00",
                "trailProperties": [
                    {
                        "allRegions": true,
                        "cloudTrailArn": "arn:aws:cloudtrail:us-
west-2:111122223333:trail/my-trail",
                        "regions": []
                    }
                ]
            },
            "isComplete": false,
            "principalArn": "arn:aws:iam::111122223333:role/Admin"
        }
    },
    "jobDetails": {
        "completedOn": "2024-02-14T22:47:01+00:00",
        "jobId": "c557dc4a-0338-4489-95dd-739014860ff9",
        "startedOn": "2024-02-14T22:44:41+00:00",
        "status": "SUCCEEDED"
    }
}
```

Para obtener más información, consulte Generación de políticas del Analizador de acceso de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetGeneratedPolicy en la Referencia de comandos de la AWS CLI.

`list-access-preview-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-access-preview-findings`.

AWS CLI

Recuperación de una lista de los resultados de la vista previa de acceso generados por la vista previa de acceso especificada

En el siguiente ejemplo de `list-access-preview-findings`, se recupera una lista de los resultados de la vista previa de acceso generados por la vista previa de acceso especificada en la cuenta de AWS.

```
aws accessanalyzer list-access-preview-findings \
    --access-preview-id 3c65eb13-6ef9-4629-8919-a32043619e6b \
    --analyzer-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account
```

Salida:

```
{
    "findings": [
        {
            "id": "e22fc158-1c87-4c32-9464-e7f405ce8d74",
            "principal": {
                "AWS": "111122223333"
            },
            "action": [
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "condition": {},
            "resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "isPublic": false,
            "resourceType": "AWS::S3::Bucket",
            "createdAt": "2024-02-17T00:18:46+00:00",
            "changeType": "NEW",
            "status": "ACTIVE",
            "resourceOwnerAccount": "111122223333",
            "sources": [
                {
                    "type": "POLICY"
                }
            ]
        }
    ]
```

```
}
```

Para obtener más información, consulte Vista previa del acceso con las API de IAM Access Analyzer en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListAccessPreviewFindings en la Referencia de comandos de la AWS CLI.

`list-access-previews`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-access-previews`.

AWS CLI

Recuperación de una lista de vistas previas de acceso para el analizador especificado

En el siguiente ejemplo de `list-access-previews`, se recupera una lista de vistas previas de acceso del analizador especificado en la cuenta de AWS.

```
aws accessanalyzer list-access-previews \
    --analyzer-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account
```

Salida:

```
{
    "accessPreviews": [
        {
            "id": "3c65eb13-6ef9-4629-8919-a32043619e6b",
            "analyzerArn": "arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account",
            "createdAt": "2024-02-17T00:18:44+00:00",
            "status": "COMPLETED"
        }
    ]
}
```

Para obtener más información, consulte Vista previa del acceso con las API de IAM Access Analyzer en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListAccessPreviews en la Referencia de comandos de la AWS CLI.

`list-analyzed-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-analyzed-resources`.

AWS CLI

Para enumerar los widgets disponibles

En el siguiente ejemplo de `list-analyzed-resources`, se genera una lista de los widgets disponibles en la cuenta de AWS.

```
aws accessanalyzer list-analyzed-resources \
    --analyzer-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account \
    --resource-type AWS::IAM::Role
```

Salida:

```
{
    "analyzedResources": [
        {
            "resourceArn": "arn:aws:sns:us-west-2:111122223333:Validation-Email",
            "resourceOwnerAccount": "111122223333",
            "resourceType": "AWS::SNS::Topic"
        },
        {
            "resourceArn": "arn:aws:sns:us-west-2:111122223333:admin-alerts",
            "resourceOwnerAccount": "111122223333",
            "resourceType": "AWS::SNS::Topic"
        },
        {
            "resourceArn": "arn:aws:sns:us-west-2:111122223333:config-topic",
            "resourceOwnerAccount": "111122223333",
            "resourceType": "AWS::SNS::Topic"
        },
        {
            "resourceArn": "arn:aws:sns:us-west-2:111122223333:inspector-topic",
            "resourceOwnerAccount": "111122223333",
            "resourceType": "AWS::SNS::Topic"
        }
    ]
}
```

Para obtener más información, consulte Uso de AWS Identity and Access Management Access Analyzer en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListAnalyzedResources en la Referencia de comandos de la AWS CLI.

`list-analyzers`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-analyzers`.

AWS CLI

Recuperación de una lista de analizadores

En el siguiente ejemplo de `list-analyzers`, se obtiene una lista de todos los analizadores de la cuenta de AWS.

```
aws accessanalyzer list-analyzers
```

Salida:

```
{
    "analyzers": [
        {
            "arn": "arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
UnusedAccess-ConsoleAnalyzer-organization",
            "createdAt": "2024-02-15T00:46:40+00:00",
            "name": "UnusedAccess-ConsoleAnalyzer-organization",
            "status": "ACTIVE",
            "tags": {
                "auto-delete": "no"
            },
            "type": "ORGANIZATION_UNUSED_ACCESS"
        },
        {
            "arn": "arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-organization",
            "createdAt": "2020-04-25T07:43:28+00:00",
            "lastResourceAnalyzed": "arn:aws:s3:::amzn-s3-demo-bucket",
            "lastResourceAnalyzedAt": "2024-02-15T21:51:56.517000+00:00",
            "name": "ConsoleAnalyzer-organization",
            "status": "ACTIVE",
            "tags": {
```

```
                "auto-delete": "no"
            },
            "type": "ORGANIZATION"
        },
        {
            "arn": "arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account",
            "createdAt": "2019-12-03T07:28:17+00:00",
            "lastResourceAnalyzed": "arn:aws:sns:us-west-2:111122223333:config-
topic",
            "lastResourceAnalyzedAt": "2024-02-15T18:01:53.003000+00:00",
            "name": "ConsoleAnalyzer-account",
            "status": "ACTIVE",
            "tags": {
                "auto-delete": "no"
            },
            "type": "ACCOUNT"
        }
    ]
}
```

Para obtener más información, consulte Uso de AWS Identity and Access Management Access Analyzer en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListAnalyzers en la Referencia de comandos de la AWS CLI.

`list-archive-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-archive-rules`.

AWS CLI

Recuperación de una lista de reglas de archivado creadas para el analizador especificado

En el siguiente ejemplo de `list-archive-rules` se recupera una lista de reglas de archivado creadas para el analizador especificado en la cuenta de AWS.

```
aws accessanalyzer list-archive-rules \
    --analyzer-name UnusedAccess-ConsoleAnalyzer-organization
```

Salida:

```
{
    "archiveRules": [
        {
            "createdAt": "2024-02-15T00:49:27+00:00",
            "filter": {
                "resource": {
                    "contains": [
                        "Cognito"
                    ]
                },
                "resourceType": {
                    "eq": [
                        "AWS::IAM::Role"
                    ]
                }
            },
            "ruleName": "MyArchiveRule",
            "updatedAt": "2024-02-15T00:49:27+00:00"
        },
        {
            "createdAt": "2024-02-15T23:27:45+00:00",
            "filter": {
                "findingType": {
                    "eq": [
                        "UnusedIAMUserAccessKey"
                    ]
                }
            },
            "ruleName": "ArchiveRule-56125a39-e517-4ff8-afb1-ef06f58db612",
            "updatedAt": "2024-02-15T23:27:45+00:00"
        }
    ]
}
```

Para obtener más información, consulte Uso de AWS Identity and Access Management Access Analyzer en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListArchiveRules en la Referencia de comandos de la AWS CLI.

`list-findings-v2`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-findings-v2`.

AWS CLI

Recuperación de una lista de resultados generados por el analizador especificado

En el siguiente ejemplo de `list-findings-v2`, se recupera una lista de los resultados generados por el analizador especificado en la cuenta de AWS. En este ejemplo, se filtran los resultados para que se incluyan solo los roles de IAM cuyo nombre contenga `Cognito`.

```
aws accessanalyzer list-findings-v2 \
    --analyzer-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account \
    --filter '{"resource": {"contains": ["Cognito"]}, "resourceType": {"eq":
 ["AWS::IAM::Role"]}}'
```

Salida:

```
{
    "findings": [
        {
            "analyzedAt": "2024-02-16T18:17:47.888000+00:00",
            "createdAt": "2021-02-26T21:17:24.710000+00:00",
            "id": "597f3bc2-3adc-4c18-9879-5c4b23485e46",
            "resource": "arn:aws:iam::111122223333:role/
Cognito_testpoolUnauth_Role",
            "resourceType": "AWS::IAM::Role",
            "resourceOwnerAccount": "111122223333",
            "status": "ACTIVE",
            "updatedAt": "2021-02-26T21:17:24.710000+00:00",
            "findingType": "ExternalAccess"
        },
        {
            "analyzedAt": "2024-02-16T18:17:47.888000+00:00",
            "createdAt": "2021-02-26T21:17:50.905000+00:00",
            "id": "ce0e221a-85b9-4d52-91ff-d7678075442f",
            "resource": "arn:aws:iam::111122223333:role/Cognito_testpoolAuth_Role",
            "resourceType": "AWS::IAM::Role",
            "resourceOwnerAccount": "111122223333",
            "status": "ACTIVE",
```

```
            "updatedAt": "2021-02-26T21:17:50.905000+00:00",
            "findingType": "ExternalAccess"
        }
    ]
}
```

Para obtener más información, consulte Uso de AWS Identity and Access Management Access Analyzer en la Guía del usuario de AWS IAM.

- Para obtener detalles de la API, consulte ListFindingsV2 en la Referencia de comandos de la AWS CLI.

`list-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-findings`.

AWS CLI

Recuperación de una lista de resultados generados por el analizador especificado

En el siguiente ejemplo de `list-findings`, se recupera una lista de los resultados generados por el analizador especificado en la cuenta de AWS. En este ejemplo, se filtran los resultados para que se incluyan solo los roles de IAM cuyo nombre contenga `Cognito`.

```
aws accessanalyzer list-findings \
    --analyzer-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account \
    --filter '{"resource": {"contains": ["Cognito"]}, "resourceType": {"eq":
 ["AWS::IAM::Role"]}}'
```

Salida:

```
{
    "findings": [
        {
            "id": "597f3bc2-3adc-4c18-9879-5c4b23485e46",
            "principal": {
                "Federated": "cognito-identity.amazonaws.com"
            },
            "action": [
                "sts:AssumeRoleWithWebIdentity"
```

```
            ],
            "resource": "arn:aws:iam::111122223333:role/
Cognito_testpoolUnauth_Role",
            "isPublic": false,
            "resourceType": "AWS::IAM::Role",
            "condition": {
                "cognito-identity.amazonaws.com:aud": "us-
west-2:EXAMPLE0-0000-0000-0000-000000000000"
            },
            "createdAt": "2021-02-26T21:17:24.710000+00:00",
            "analyzedAt": "2024-02-16T18:17:47.888000+00:00",
            "updatedAt": "2021-02-26T21:17:24.710000+00:00",
            "status": "ACTIVE",
            "resourceOwnerAccount": "111122223333"
        },
        {
            "id": "ce0e221a-85b9-4d52-91ff-d7678075442f",
            "principal": {
                "Federated": "cognito-identity.amazonaws.com"
            },
            "action": [
                "sts:AssumeRoleWithWebIdentity"
            ],
            "resource": "arn:aws:iam::111122223333:role/Cognito_testpoolAuth_Role",
            "isPublic": false,
            "resourceType": "AWS::IAM::Role",
            "condition": {
                "cognito-identity.amazonaws.com:aud": "us-
west-2:EXAMPLE0-0000-0000-0000-000000000000"
            },
            "createdAt": "2021-02-26T21:17:50.905000+00:00",
            "analyzedAt": "2024-02-16T18:17:47.888000+00:00",
            "updatedAt": "2021-02-26T21:17:50.905000+00:00",
            "status": "ACTIVE",
            "resourceOwnerAccount": "111122223333"
        }
    ]
}
```

Para obtener más información, consulte Uso de AWS Identity and Access Management Access Analyzer en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListFindings en la Referencia de comandos de la AWS CLI.

`list-policy-generations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-policy-generations`.

AWS CLI

Para enumerar todas las generaciones de políticas solicitadas en los últimos siete días

En el siguiente ejemplo de `list-policy-generations`, se genera una lista de todas las generaciones de políticas solicitadas en los últimos siete días en la cuenta de AWS.

```
aws accessanalyzer list-policy-generations
```

Salida:

```
{
    "policyGenerations": [
        {
            "completedOn": "2024-02-14T23:43:38+00:00",
            "jobId": "923a56b0-ebb8-4e80-8a3c-a11ccfbcd6f2",
            "principalArn": "arn:aws:iam::111122223333:role/Admin",
            "startedOn": "2024-02-14T23:43:02+00:00",
            "status": "CANCELED"
        },
        {
            "completedOn": "2024-02-14T22:47:01+00:00",
            "jobId": "c557dc4a-0338-4489-95dd-739014860ff9",
            "principalArn": "arn:aws:iam::111122223333:role/Admin",
            "startedOn": "2024-02-14T22:44:41+00:00",
            "status": "SUCCEEDED"
        }
    ]
}
```

Para obtener más información, consulte Generación de políticas del Analizador de acceso de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte ListPolicyGenerations en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Recuperación de una lista de etiquetas aplicadas al recurso especificado

En el siguiente ejemplo de `list-tags-for-resource`, se recupera una lista de todas las etiquetas aplicadas al recurso especificado en la cuenta de AWS.

```
aws accessanalyzer list-tags-for-resource \
    --resource-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account
```

Salida:

```
{
    "tags": {
        "Zone-of-trust": "Account",
        "Name": "ConsoleAnalyzer"
    }
}
```

Para obtener más información, consulte Generación de políticas del Analizador de acceso de IAM en la Guía del usuario de AWS IAM.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`start-policy-generation`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-policy-generation`.

AWS CLI

Inicio de una solicitud de generación de políticas

En el siguiente ejemplo de `start-policy-generation`, se inicia una solicitud de generación de políticas en la cuenta de AWS.

```
aws accessanalyzer start-policy-generation \
```

```
    --policy-generation-details '{"principalArn":"arn:aws:iam::111122223333:role/
Admin"}' \
    --cloud-trail-details file://myfile.json
```

Contenidos de `myfile.json`:

```
{
    "accessRole": "arn:aws:iam::111122223333:role/service-role/
AccessAnalyzerMonitorServiceRole",
    "startTime": "2024-02-13T00:30:00Z",
    "trails": [
        {
            "allRegions": true,
            "cloudTrailArn": "arn:aws:cloudtrail:us-west-2:111122223333:trail/my-
trail"
        }
    ]
}
```

Salida:

```
{
    "jobId": "c557dc4a-0338-4489-95dd-739014860ff9"
}
```

Para obtener más información, consulte Generación de políticas del Analizador de acceso de IAM en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte StartPolicyGeneration en la Referencia de comandos de la AWS CLI.

`start-resource-scan`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-resource-scan`.

AWS CLI

Inicio inmediato de un análisis de las políticas aplicadas al recurso especificado

En el siguiente ejemplo de `start-resource-scan`, se inicia de inmediato un análisis de las políticas aplicadas al recurso especificado en la cuenta de AWS.

```
aws accessanalyzer start-resource-scan \
    --analyzer-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account \
    --resource-arn arn:aws:iam::111122223333:role/Cognito_testpoolAuth_Role
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Generación de políticas del Analizador de acceso de IAM en la Guía del usuario de AWS IAM.

- Para ver detalles de la API, consulte StartResourceScan en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Adición de una etiqueta al recurso especificado

En el siguiente ejemplo de `tag-resource`, se añade una etiqueta al recurso especificado en la cuenta de AWS.

```
aws accessanalyzer tag-resource \
    --resource-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account \
    --tags Environment=dev,Purpose=testing
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de AWS Identity and Access Management Access Analyzer en la Guía del usuario de AWS IAM.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de etiquetas del recurso especificado

En el siguiente ejemplo de `untag-resource`, se eliminan las etiquetas de un recurso especificado en la cuenta de AWS.

```
aws accessanalyzer untag-resource \
    --resource-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
ConsoleAnalyzer-account \
    --tag-keys Environment Purpose
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de AWS Identity and Access Management Access Analyzer en la Guía del usuario de AWS IAM.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-archive-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-archive-rule`.

AWS CLI

Actualización de los criterios y valores de la regla de archivado especificada

En el siguiente ejemplo de `update-archive-rule`, se actualizan los criterios y valores de la regla de archivado especificada en la cuenta de AWS.

```
aws accessanalyzer update-archive-rule \
    --analyzer-name UnusedAccess-ConsoleAnalyzer-organization \
    --rule-name MyArchiveRule \
    --filter '{"resource": {"contains": ["Cognito"]}, "resourceType": {"eq":
 ["AWS::IAM::Role"]}}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Reglas de archivado en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte UpdateArchiveRule en la Referencia de comandos de la AWS CLI.

`update-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-findings`.

AWS CLI

Actualización del estado de los resultados especificados

En el siguiente ejemplo de `update-findings`, se actualiza el estado de los resultados especificados en la cuenta de AWS.

```
aws accessanalyzer update-findings \
    --analyzer-arn arn:aws:access-analyzer:us-west-2:111122223333:analyzer/
UnusedAccess-ConsoleAnalyzer-organization \
    --ids 4f319ac3-2e0c-4dc4-bf51-7013a086b6ae 780d586a-2cce-4f72-aff6-359d450e7500
 \
    --status ARCHIVED
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de AWS Identity and Access Management Access Analyzer en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte UpdateFindings en la Referencia de comandos de la AWS CLI.

`validate-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `validate-policy`.

AWS CLI

Para solicitar la validación de una política y obtener una lista de resultados

En el siguiente ejemplo de `validate-policy`, se solicita la validación de una política y se obtiene una lista de resultados. La política del ejemplo es una política de confianza de rol para un rol de Amazon Cognito utilizado para la federación de identidades web. Los resultados generados a partir de la política de confianza se refieren a un valor de elemento `Sid` vacío y a una entidad principal de política no coincidente por el uso de una acción incorrecta de rol de asunción, `sts:AssumeRole`. La acción correcta de rol de asunción que se debe usar con Cognito es `sts:AssumeRoleWithWebIdentity`.

```
aws accessanalyzer validate-policy \
    --policy-document file://myfile.json \
    --policy-type RESOURCE_POLICY
```

Contenidos de `myfile.json`:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Federated": "cognito-identity.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:TagSession"
            ],
            "Condition": {
                "StringEquals": {
                    "cognito-identity.amazonaws.com:aud": "us-west-2_EXAMPLE"
                }
            }
        }
    ]
}
```

Salida:

```
{
    "findings": [
        {
            "findingDetails": "Add a value to the empty string in the Sid element.",
            "findingType": "SUGGESTION",
            "issueCode": "EMPTY_SID_VALUE",
            "learnMoreLink": "https://docs.aws.amazon.com/IAM/latest/UserGuide/
access-analyzer-reference-policy-checks.html#access-analyzer-reference-policy-
checks-suggestion-empty-sid-value",
            "locations": [
                {
                    "path": [
```

```
                        {
                            "value": "Statement"
                        },
                        {
                            "index": 0
                        },
                        {
                            "value": "Sid"
                        }
                    ],
                    "span": {
                        "end": {
                            "column": 21,
                            "line": 5,
                            "offset": 81
                        },
                        "start": {
                            "column": 19,
                            "line": 5,
                            "offset": 79
                        }
                    }
                }
            ]
        },
        {
            "findingDetails": "The sts:AssumeRole action is invalid with the
 following principal(s): cognito-identity.amazonaws.com. Use a SAML provider
 principal with the sts:AssumeRoleWithSAML action or use an OIDC provider principal
 with the sts:AssumeRoleWithWebIdentity action. Ensure the provider is Federated if
 you use either of the two options.",
            "findingType": "ERROR",
            "issueCode": "MISMATCHED_ACTION_FOR_PRINCIPAL",
            "learnMoreLink": "https://docs.aws.amazon.com/IAM/latest/UserGuide/
access-analyzer-reference-policy-checks.html#access-analyzer-reference-policy-
checks-error-mismatched-action-for-principal",
            "locations": [
                {
                    "path": [
                        {
                            "value": "Statement"
                        },
                        {
                            "index": 0
```

```
                        },
                        {
                            "value": "Action"
                        },
                        {
                            "index": 0
                        }
                    ],
                    "span": {
                        "end": {
                            "column": 32,
                            "line": 11,
                            "offset": 274
                        },
                        "start": {
                            "column": 16,
                            "line": 11,
                            "offset": 258
                        }
                    }
                },
                {
                    "path": [
                        {
                            "value": "Statement"
                        },
                        {
                            "index": 0
                        },
                        {
                            "value": "Principal"
                        },
                        {
                            "value": "Federated"
                        }
                    ],
                    "span": {
                        "end": {
                            "column": 61,
                            "line": 8,
                            "offset": 202
                        },
                        "start": {
                            "column": 29,
```

```
                            "line": 8,
                            "offset": 170
                        }
                    }
                }
            ]
        },
        {
            "findingDetails": "The following actions: sts:TagSession are not
 supported by the condition key cognito-identity.amazonaws.com:aud. The condition
 will not be evaluated for these actions. We recommend that you move these actions
 to a different statement without this condition key.",
            "findingType": "ERROR",
            "issueCode": "UNSUPPORTED_ACTION_FOR_CONDITION_KEY",
            "learnMoreLink": "https://docs.aws.amazon.com/IAM/latest/UserGuide/
access-analyzer-reference-policy-checks.html#access-analyzer-reference-policy-
checks-error-unsupported-action-for-condition-key",
            "locations": [
                {
                    "path": [
                        {
                            "value": "Statement"
                        },
                        {
                            "index": 0
                        },
                        {
                            "value": "Action"
                        },
                        {
                            "index": 1
                        }
                    ],
                    "span": {
                        "end": {
                            "column": 32,
                            "line": 12,
                            "offset": 308
                        },
                        "start": {
                            "column": 16,
                            "line": 12,
                            "offset": 292
                        }
```

```
                    }
                },
                {
                    "path": [
                        {
                            "value": "Statement"
                        },
                        {
                            "index": 0
                        },
                        {
                            "value": "Condition"
                        },
                        {
                            "value": "StringEquals"
                        },
                        {
                            "value": "cognito-identity.amazonaws.com:aud"
                        }
                    ],
                    "span": {
                        "end": {
                            "column": 79,
                            "line": 16,
                            "offset": 464
                        },
                        "start": {
                            "column": 58,
                            "line": 16,
                            "offset": 443
                        }
                    }
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Comprobaciones para validar políticas en la Guía del usuario de AWS IAM.

- Para obtener información acerca de la API, consulte ValidatePolicy en la Referencia de comandos de la AWS CLI.

Ejemplos de Image Builder que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Image Builder.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-component`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-component`.

AWS CLI

Para crear un componente

En el siguiente ejemplo de `create-component`, se crea un componente que usa un archivo de documento JSON y hace referencia a un documento de componente en formato YAML que se carga en un bucket de Amazon S3.

```
aws imagebuilder create-component \
    --cli-input-json file://create-component.json
```

Contenido de `create-component.json`:

```
{
    "name": "MyExampleComponent",
    "semanticVersion": "2019.12.02",
    "description": "An example component that builds, validates and tests an image",
    "changeDescription": "Initial version.",
    "platform": "Windows",
    "uri": "s3://s3-bucket-name/s3-bucket-path/component.yaml"
```

```
}
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "clientToken": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "componentBuildVersionArn": "arn:aws:imagebuilder:us-
west-2:123456789012:component/examplecomponent/2019.12.02/1"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte CreateComponent en la Referencia de comandos de la AWS CLI.

`create-distribution-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-distribution-configuration`.

AWS CLI

Para crear una configuración de distribución

En el siguiente ejemplo de `create-distribution-configuration`, se crea una configuración de distribución mediante un archivo JSON.

```
aws imagebuilder create-distribution-configuration \
    --cli-input-json file:/create-distribution-configuration.json
```

Contenido de `create-distribution-configuration.json`:

```
{
    "name": "MyExampleDistribution",
    "description": "Copies AMI to eu-west-1",
    "distributions": [
        {
            "region": "us-west-2",
            "amiDistributionConfiguration": {
                "name": "Name {{imagebuilder:buildDate}}",
```

```
                "description": "An example image name with parameter references",
                "amiTags": {
                    "KeyName": "{{ssm:parameter_name}}"
                },
                "launchPermission": {
                    "userIds": [
                        "123456789012"
                    ]
                }
            }
        },
        {
            "region": "eu-west-1",
            "amiDistributionConfiguration": {
                "name": "My {{imagebuilder:buildVersion}} image
 {{imagebuilder:buildDate}}",
                "amiTags": {
                    "KeyName": "Value"
                },
                "launchPermission": {
                    "userIds": [
                        "123456789012"
                    ]
                }
            }
        }
    ]
}
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "clientToken": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "distributionConfigurationArn": "arn:aws:imagebuilder:us-
west-2:123456789012:distribution-configuration/myexampledistribution"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener más información sobre la API, consulte CreateDistributionConfiguration en la Referencia de comandos de la AWS CLI.

`create-image-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-image-pipeline`.

AWS CLI

Para crear una canalización de imágenes

En el siguiente ejemplo de `create-image-pipeline`, se crea una canalización de imágenes mediante un archivo JSON.

```
aws imagebuilder create-image-pipeline \
    --cli-input-json file://create-image-pipeline.json
```

Contenido de `create-image-pipeline.json`:

```
{
    "name": "MyWindows2016Pipeline",
    "description": "Builds Windows 2016 Images",
    "imageRecipeArn": "arn:aws:imagebuilder:us-west-2:123456789012:image-recipe/
mybasicrecipe/2019.12.03",
    "infrastructureConfigurationArn": "arn:aws:imagebuilder:us-
west-2:123456789012:infrastructure-configuration/myexampleinfrastructure",
    "distributionConfigurationArn": "arn:aws:imagebuilder:us-
west-2:123456789012:distribution-configuration/myexampledistribution",
    "imageTestsConfiguration": {
        "imageTestsEnabled": true,
        "timeoutMinutes": 60
    },
    "schedule": {
        "scheduleExpression": "cron(0 0 * * SUN)",
        "pipelineExecutionStartCondition":
 "EXPRESSION_MATCH_AND_DEPENDENCY_UPDATES_AVAILABLE"
    },
    "status": "ENABLED"
}
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "clientToken": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
```

```
    "imagePipelineArn": "arn:aws:imagebuilder:us-west-2:123456789012:image-pipeline/
mywindows2016pipeline"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte CreateImagePipeline en la Referencia de comandos de la AWS CLI.

`create-image-recipe`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-image-recipe`.

AWS CLI

Para crear una receta

En el siguiente ejemplo de `create-image-recipe`, se crea una receta de imágenes mediante un archivo JSON. Los componentes se instalan en el orden en que se han especificado.

```
aws imagebuilder create-image-recipe \
    --cli-input-json file://create-image-recipe.json
```

Contenido de `create-image-recipe.json`:

```
{
    "name": "MyBasicRecipe",
    "description": "This example image recipe creates a Windows 2016 image.",
    "semanticVersion": "2019.12.03",
    "components":
    [
        {
            "componentArn": "arn:aws:imagebuilder:us-west-2:123456789012:component/
myexamplecomponent/2019.12.02/1"
        },
        {
            "componentArn": "arn:aws:imagebuilder:us-west-2:123456789012:component/
myimportedcomponent/1.0.0/1"
        }
    ],
```

```
    "parentImage": "arn:aws:imagebuilder:us-west-2:aws:image/windows-server-2016-
english-full-base-x86/xxxx.x.x"
}
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "clientToken": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "imageRecipeArn": "arn:aws:imagebuilder:us-west-2:123456789012:image-recipe/
mybasicrecipe/2019.12.03"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte CreateImageRecipe en la Referencia de comandos de la AWS CLI.

`create-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-image`.

AWS CLI

Para crear una imagen

En el siguiente ejemplo de `create-image`, se crea una imagen.

```
aws imagebuilder create-image \
    --image-recipe-arn arn:aws:imagebuilder:us-west-2:123456789012:image-recipe/
mybasicrecipe/2019.12.03 \
    --infrastructure-configuration-arn arn:aws:imagebuilder:us-
west-2:123456789012:infrastructure-configuration/myexampleinfrastructure
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "clientToken": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "imageBuildVersionArn": "arn:aws:imagebuilder:us-west-2:123456789012:image/
mybasicrecipe/2019.12.03/1"
```

```
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte CreateImage en la Referencia de comandos de la AWS CLI.

`create-infrastructure-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-infrastructure-configuration`.

AWS CLI

Para crear una configuración de infraestructura

En el siguiente ejemplo de `create-infrastructure-configuration`, se crea una configuración de infraestructura mediante un archivo JSON.

```
aws imagebuilder create-infrastructure-configuration \
    --cli-input-json file://create-infrastructure-configuration.json
```

Contenido de `create-infrastructure-configuration.json`:

```
{
    "name": "MyExampleInfrastructure",
    "description": "An example that will retain instances of failed builds",
    "instanceTypes": [
        "m5.large", "m5.xlarge"
    ],
    "instanceProfileName": "EC2InstanceProfileForImageBuilder",
    "securityGroupIds": [
        "sg-a1b2c3d4"
    ],
    "subnetId": "subnet-a1b2c3d4",
    "logging": {
        "s3Logs": {
            "s3BucketName": "bucket-name",
            "s3KeyPrefix": "bucket-path"
        }
    },
```

```
    "keyPair": "key-pair-name",
    "terminateInstanceOnFailure": false,
    "snsTopicArn": "arn:aws:sns:us-west-2:123456789012:sns-topic-name"
}
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "clientToken": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "infrastructureConfigurationArn": "arn:aws:imagebuilder:us-
west-2:123456789012:infrastructure-configuration/myexampleinfrastructure"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte CreateInfrastructureConfiguration en la Referencia de comandos de la AWS CLI.

`delete-component`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-component`.

AWS CLI

Para eliminar un componente

En el siguiente ejemplo de `delete-component`, se muestra cómo eliminar una versión de compilación de componentes al especificar su ARN.

```
aws imagebuilder delete-component \
    --component-build-version-arn arn:aws:imagebuilder:us-
west-2:123456789012:component/myexamplecomponent/2019.12.02/1
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "componentBuildVersionArn": "arn:aws:imagebuilder:us-
west-2:123456789012:component/myexamplecomponent/2019.12.02/1"
```

```
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte DeleteComponent en la Referencia de comandos de la AWS CLI.

`delete-image-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-image-pipeline`.

AWS CLI

Para eliminar una canalización de imágenes

En el siguiente ejemplo de `delete-image-pipeline`, se muestra cómo eliminar una canalización de imágenes al especificar su ARN.

```
aws imagebuilder delete-image-pipeline \
    --image-pipeline-arn arn:aws:imagebuilder:us-west-2:123456789012:image-pipeline/
my-example-pipeline
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "imagePipelineArn": "arn:aws:imagebuilder:us-west-2:123456789012:image-pipeline/
mywindows2016pipeline"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte DeleteImagePipeline en la Referencia de comandos de la AWS CLI.

`delete-image-recipe`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-image-recipe`.

AWS CLI

Para eliminar una receta de imágenes

En el siguiente ejemplo de `delete-image-recipe`, se muestra cómo eliminar una receta de imágenes al especificar su ARN.

```
aws imagebuilder delete-image-recipe \
    --image-recipe-arn arn:aws:imagebuilder:us-east-1:123456789012:image-recipe/
mybasicrecipe/2019.12.03
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "imageRecipeArn": "arn:aws:imagebuilder:us-west-2:123456789012:image-recipe/
mybasicrecipe/2019.12.03"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte DeleteImageRecipe en la Referencia de comandos de la AWS CLI.

`delete-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-image`.

AWS CLI

Para eliminar una imagen

En el siguiente ejemplo de `delete-image`, se muestra cómo eliminar una versión de compilación de imágenes al especificar su ARN.

```
aws imagebuilder delete-image \
    --image-build-version-arn arn:aws:imagebuilder:us-west-2:123456789012:image/my-
example-image/2019.12.02/1
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "imageBuildVersionArn": "arn:aws:imagebuilder:us-west-2:123456789012:image/
mybasicrecipe/2019.12.03/1"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte DeleteImage en la Referencia de comandos de la AWS CLI.

`delete-infrastructure-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-infrastructure-configuration`.

AWS CLI

Para eliminar una configuración de infraestructura

En el siguiente ejemplo de `delete-infrastructure-configuration`, se muestra cómo eliminar una canalización de imágenes al especificar su ARN.

```
aws imagebuilder delete-infrastructure-configuration \
    --infrastructure-configuration-arn arn:aws:imagebuilder:us-
east-1:123456789012:infrastructure-configuration/myexampleinfrastructure
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "infrastructureConfigurationArn": "arn:aws:imagebuilder:us-
west-2:123456789012:infrastructure-configuration/myexampleinfrastructure"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte DeleteInfrastructureConfiguration en la Referencia de comandos de la AWS CLI.

`get-component-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-component-policy`.

AWS CLI

Para obtener los detalles de la política de componentes

En el siguiente ejemplo de `get-component-policy`, se enumeran los detalles de una política de componentes especificando su ARN.

```
aws imagebuilder get-component-policy \
    --component-arn arn:aws:imagebuilder:us-west-2:123456789012:component/my-example-component/2019.12.03/1
```

Salida:

```
{
    "Policy": "{ "Version":"2012-10-17",        "Statement": [ { "Effect":
 "Allow", "Principal": { "AWS": [ "123456789012" ] }, "Action":
 [ "imagebuilder:GetComponent", "imagebuilder:ListComponents" ], "Resource":
 [ "arn:aws:imagebuilder:us-west-2:123456789012:component/my-example-
component/2019.12.03/1" ] } ] }"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI <https://docs.aws.amazon.com/imagebuilder/latest/userguide/managing-image-builder-cli.html>`__ en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte GetComponentPolicy en la Referencia de comandos de la AWS CLI.

`get-component`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-component`.

AWS CLI

Para obtener los detalles de los componentes

En el siguiente ejemplo de `get-component`, se enumeran los detalles de un componente especificando su ARN.

```
aws imagebuilder get-component \
    --component-build-version-arn arn:aws:imagebuilder:us-
west-2:123456789012:component/component-name/1.0.0/1
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "component": {
        "arn": "arn:aws:imagebuilder:us-west-2:123456789012:component/component-
name/1.0.0/1",
        "name": "component-name",
        "version": "1.0.0",
        "type": "TEST",
        "platform": "Linux",
        "owner": "123456789012",
        "data": "name: HelloWorldTestingDocument\ndescription: This is hello world
 testing document.\nschemaVersion: 1.0\n\nphases:\n  - name: test\n    steps:\n
   - name: HelloWorldStep\n        action: ExecuteBash\n        inputs:\n
 commands:\n            - echo \"Hello World! Test.\"\n",
        "encrypted": true,
        "dateCreated": "2020-01-27T20:43:30.306Z",
        "tags": {}
    }
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte GetComponent en la Referencia de comandos de la AWS CLI.

`get-distribution-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-distribution-configuration`.

AWS CLI

Para obtener los detalles de una configuración de distribución

En el siguiente ejemplo de `get-distribution-configuration`, se muestran los detalles de una configuración de distribución al especificar su ARN.

```
aws imagebuilder get-distribution-configuration \
    --distribution-configuration-arn arn:aws:imagebuilder:us-
west-2:123456789012:distribution-configuration/myexampledistribution
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "distributionConfiguration": {
        "arn": "arn:aws:imagebuilder:us-west-2:123456789012:distribution-
configuration/myexampledistribution",
        "name": "MyExampleDistribution",
        "description": "Copies AMI to eu-west-1 and exports to S3",
        "distributions": [
            {
                "region": "us-west-2",
                "amiDistributionConfiguration": {
                    "name": "Name {{imagebuilder:buildDate}}",
                    "description": "An example image name with parameter
 references",
                    "amiTags": {
                        "KeyName": "{{ssm:parameter_name}}"
                    },
                    "launchPermission": {
                        "userIds": [
                            "123456789012"
                        ]
                    }
                }
            },
            {
                "region": "eu-west-1",
                "amiDistributionConfiguration": {
                    "name": "My {{imagebuilder:buildVersion}} image
 {{imagebuilder:buildDate}}",
                    "amiTags": {
                        "KeyName": "Value"
                    },
                    "launchPermission": {
                        "userIds": [
                            "123456789012"
                        ]
                    }
```

```
                }
            }
        ],
        "dateCreated": "2020-02-19T18:40:10.529Z",
        "tags": {}
    }
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte GetDistributionConfiguration en la Referencia de comandos de la AWS CLI.

`get-image-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-image-pipeline`.

AWS CLI

Para obtener los detalles de la canalización de imágenes

En el siguiente ejemplo de `get-image-pipeline`, se enumeran los detalles una canalización de imágenes al especificar su ARN.

```
aws imagebuilder get-image-pipeline \
    --image-pipeline-arn arn:aws:imagebuilder:us-west-2:123456789012:image-pipeline/
mywindows2016pipeline
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "imagePipeline": {
        "arn": "arn:aws:imagebuilder:us-west-2:123456789012:image-pipeline/
mywindows2016pipeline",
        "name": "MyWindows2016Pipeline",
        "description": "Builds Windows 2016 Images",
        "platform": "Windows",
        "imageRecipeArn": "arn:aws:imagebuilder:us-west-2:123456789012:image-recipe/
mybasicrecipe/2019.12.03",
```

```
        "infrastructureConfigurationArn": "arn:aws:imagebuilder:us-
west-2:123456789012:infrastructure-configuration/myexampleinfrastructure",
        "distributionConfigurationArn": "arn:aws:imagebuilder:us-
west-2:123456789012:distribution-configuration/myexampledistribution",
        "imageTestsConfiguration": {
            "imageTestsEnabled": true,
            "timeoutMinutes": 60
        },
        "schedule": {
            "scheduleExpression": "cron(0 0 * * SUN)",
            "pipelineExecutionStartCondition":
 "EXPRESSION_MATCH_AND_DEPENDENCY_UPDATES_AVAILABLE"
        },
        "status": "ENABLED",
        "dateCreated": "2020-02-19T19:04:01.253Z",
        "dateUpdated": "2020-02-19T19:04:01.253Z",
        "tags": {}
    }
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte GetImagePipeline en la Referencia de comandos de la AWS CLI.

`get-image-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-image-policy`.

AWS CLI

Para obtener los detalles de la política de imágenes

En el siguiente ejemplo de `get-image-policy`, se enumeran los detalles de una política de imágenes especificando su ARN.

```
aws imagebuilder get-image-policy \
    --image-arn arn:aws:imagebuilder:us-west-2:123456789012:image/my-example-
image/2019.12.03/1
```

Salida:

```
{
    "Policy": "{ "Version":"2012-10-17",        "Statement": [ { "Effect": "Allow",
 "Principal": { "AWS": [ "123456789012" ] }, "Action": [ "imagebuilder:GetImage",
 "imagebuilder:ListImages" ], "Resource": [ "arn:aws:imagebuilder:us-
west-2:123456789012:image/my-example-image/2019.12.03/1" ] } ] }"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte GetImagePolicy en la Referencia de comandos de la AWS CLI.

`get-image-recipe-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-image-recipe-policy`.

AWS CLI

Para obtener los detalles de la política de receta de imágenes

En el siguiente ejemplo de `get-image-recipe-policy`, se enumeran los detalles de una política de receta de imágenes especificando su ARN.

```
aws imagebuilder get-image-recipe-policy \
    --image-recipe-arn arn:aws:imagebuilder:us-west-2:123456789012:image-recipe/my-example-image-recipe/2019.12.03/1
```

Salida:

```
{
    "Policy": "{ "Version":"2012-10-17",        "Statement": [ { "Effect":
 "Allow", "Principal": { "AWS": [ "123456789012" ] }, "Action":
 [ "imagebuilder:GetImageRecipe", "imagebuilder:ListImageRecipes" ], "Resource":
 [ "arn:aws:imagebuilder:us-west-2:123456789012:image-recipe/my-example-image-
recipe/2019.12.03/1" ] } ] }"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte GetImageRecipePolicy en la Referencia de comandos de la AWS CLI.

`get-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-image`.

AWS CLI

Para obtener los detalles de una imagen

En el siguiente ejemplo de `get-image`, se enumeran los detalles de una imagen especificando su ARN.

```
aws imagebuilder get-image \
    --image-build-version-arn arn:aws:imagebuilder:us-west-2:123456789012:image/
mybasicrecipe/2019.12.03/1
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "image": {
        "arn": "arn:aws:imagebuilder:us-west-2:123456789012:image/
mybasicrecipe/2019.12.03/1",
        "name": "MyBasicRecipe",
        "version": "2019.12.03/1",
        "platform": "Windows",
        "state": {
            "status": "BUILDING"
        },
        "imageRecipe": {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:image-recipe/
mybasicrecipe/2019.12.03",
            "name": "MyBasicRecipe",
            "description": "This example image recipe creates a Windows 2016
 image.",
            "platform": "Windows",
            "version": "2019.12.03",
            "components": [
                {
```

```
                    "componentArn": "arn:aws:imagebuilder:us-
west-2:123456789012:component/myexamplecomponent/2019.12.02/1"
                },
                {
                    "componentArn": "arn:aws:imagebuilder:us-
west-2:123456789012:component/myimportedcomponent/1.0.0/1"
                }
            ],
            "parentImage": "arn:aws:imagebuilder:us-west-2:aws:image/windows-
server-2016-english-full-base-x86/2019.12.17/1",
            "dateCreated": "2020-02-14T19:46:16.904Z",
            "tags": {}
        },
        "infrastructureConfiguration": {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:infrastructure-
configuration/myexampleinfrastructure",
            "name": "MyExampleInfrastructure",
            "description": "An example that will retain instances of failed builds",
            "instanceTypes": [
                "m5.large",
                "m5.xlarge"
            ],
            "instanceProfileName": "EC2InstanceProfileForImageFactory",
            "securityGroupIds": [
                "sg-a1b2c3d4"
            ],
            "subnetId": "subnet-a1b2c3d4",
            "logging": {
                "s3Logs": {
                    "s3BucketName": "bucket-name",
                    "s3KeyPrefix": "bucket-path"
                }
            },
            "keyPair": "Sam",
            "terminateInstanceOnFailure": false,
            "snsTopicArn": "arn:aws:sns:us-west-2:123456789012:sns-name",
            "dateCreated": "2020-02-14T21:21:05.098Z",
            "tags": {}
        },
        "imageTestsConfiguration": {
            "imageTestsEnabled": true,
            "timeoutMinutes": 720
        },
        "dateCreated": "2020-02-14T23:14:13.597Z",
```

```
        "outputResources": {
            "amis": []
        },
        "tags": {}
    }
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte GetImage en la Referencia de comandos de la AWS CLI.

`get-infrastructure-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-infrastructure-configuration`.

AWS CLI

Para obtener los detalles de la configuración de una infraestructura

En el siguiente ejemplo de `get-infrastructure-configuration`, se enumeran los detalles de la configuración de una infraestructura especificando su ARN.

```
aws imagebuilder get-infrastructure-configuration \
    --infrastructure-configuration-arn arn:aws:imagebuilder:us-
west-2:123456789012:infrastructure-configuration/myexampleinfrastructure
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "infrastructureConfiguration": {
        "arn": "arn:aws:imagebuilder:us-west-2:123456789012:infrastructure-
configuration/myexampleinfrastructure",
        "name": "MyExampleInfrastructure",
        "description": "An example that will retain instances of failed builds",
        "instanceTypes": [
            "m5.large",
            "m5.xlarge"
        ],
```

```
        "instanceProfileName": "EC2InstanceProfileForImageBuilder",
        "securityGroupIds": [
            "sg-a48c95ef"
        ],
        "subnetId": "subnet-a48c95ef",
        "logging": {
            "s3Logs": {
                "s3BucketName": "bucket-name",
                "s3KeyPrefix": "bucket-path"
            }
        },
        "keyPair": "Name",
        "terminateInstanceOnFailure": false,
        "snsTopicArn": "arn:aws:sns:us-west-2:123456789012:sns-name",
        "dateCreated": "2020-02-19T19:11:51.858Z",
        "tags": {}
    }
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte GetInfrastructureConfiguration en la Referencia de comandos de la AWS CLI.

`import-component`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-component`.

AWS CLI

Para importar un componente

En el siguiente ejemplo de `import-component`, se importa un script preexistente mediante un archivo JSON.

```
aws imagebuilder import-component \
    --cli-input-json file://import-component.json
```

Contenido de `import-component.json`:

```
{
    "name": "MyImportedComponent",
```

```
    "semanticVersion": "1.0.0",
    "description": "An example of how to import a component",
    "changeDescription": "First commit message.",
    "format": "SHELL",
    "platform": "Windows",
    "type": "BUILD",
    "uri": "s3://s3-bucket-name/s3-bucket-path/component.yaml"
}
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "clientToken": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "componentBuildVersionArn": "arn:aws:imagebuilder:us-
west-2:123456789012:component/myimportedcomponent/1.0.0/1"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte ImportComponent en la Referencia de comandos de la AWS CLI.

`list-component-build-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-component-build-versions`.

AWS CLI

Para enumerar las versiones de compilación de componentes

En el siguiente ejemplo de `list-component-build-versions`, se enumeran las versiones de compilación de componentes que tienen una versión semántica específica.

```
aws imagebuilder list-component-build-versions --component-
version-arn arn:aws:imagebuilder:us-west-2:123456789012:component/
myexamplecomponent/2019.12.02
```

Salida:

```
{
```

```
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "componentSummaryList": [
        {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:component/
myexamplecomponent/2019.12.02/1",
            "name": "MyExampleComponent",
            "version": "2019.12.02",
            "platform": "Windows",
            "type": "BUILD",
            "owner": "123456789012",
            "description": "An example component that builds, validates and tests an
 image",
            "changeDescription": "Initial version.",
            "dateCreated": "2020-02-19T18:53:45.940Z",
            "tags": {
                "KeyName": "KeyValue"
            }
        }
    ]
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte ListComponentBuildVersions en la Referencia de comandos de la AWS CLI.

`list-components`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-components`.

AWS CLI

Para enumerar todas las versiones semánticas de los componentes

En el siguiente ejemplo de `list-components`, se enumeran todas las versiones semánticas de los componentes a las que tiene acceso. Si lo desea, puede filtrar por la lista de componentes de su propiedad, de Amazon o que otras cuentas hayan compartido con usted.

```
aws imagebuilder list-components
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "componentVersionList": [
        {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:component/component-
name/1.0.0",
            "name": "component-name",
            "version": "1.0.0",
            "platform": "Linux",
            "type": "TEST",
            "owner": "123456789012",
            "dateCreated": "2020-01-27T20:43:30.306Z"
        }
    ]
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener detalles de la API, consulte ListComponents en la Referencia de comandos de la AWS CLI.

`list-distribution-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-distribution-configurations`.

AWS CLI

Para enumerar las distribuciones

En el siguiente ejemplo de `list-distribution-configurations`, se enumeran todas las distribuciones.

```
aws imagebuilder list-distribution-configurations
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "distributionConfigurationSummaryList": [
        {
```

```
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:distribution-
configuration/myexampledistribution",
            "name": "MyExampleDistribution",
            "description": "Copies AMI to eu-west-1 and exports to S3",
            "dateCreated": "2020-02-19T18:40:10.529Z",
            "tags": {
                "KeyName": "KeyValue"
            }
        }
    ]
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte ListDistributionConfigurations en la Referencia de comandos de la AWS CLI.

`list-image-build-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-image-build-versions`.

AWS CLI

Para enumerar las versiones de compilación de imágenes

En el siguiente ejemplo de `list-image-build-versions`, se enumeran todas las versiones de compilación de componentes que tienen una versión semántica.

```
aws imagebuilder list-image-build-versions \
    --image-version-arn arn:aws:imagebuilder:us-west-2:123456789012:image/
mybasicrecipe/2019.12.03
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "imageSummaryList": [
        {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:image/
mybasicrecipe/2019.12.03/7",
            "name": "MyBasicRecipe",
            "version": "2019.12.03/7",
```

```
            "platform": "Windows",
            "state": {
                "status": "FAILED",
                "reason": "Can't start SSM Automation for arn
 arn:aws:imagebuilder:us-west-2:123456789012:image/mybasicrecipe/2019.12.03/7 during
 building. Parameter \"iamInstanceProfileName\" has a null value."
            },
            "owner": "123456789012",
            "dateCreated": "2020-02-19T18:56:11.511Z",
            "outputResources": {
                "amis": []
            },
            "tags": {}
        },
        {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:image/
mybasicrecipe/2019.12.03/6",
            "name": "MyBasicRecipe",
            "version": "2019.12.03/6",
            "platform": "Windows",
            "state": {
                "status": "FAILED",
                "reason": "An internal error has occurred."
            },
            "owner": "123456789012",
            "dateCreated": "2020-02-18T22:49:08.142Z",
            "outputResources": {
                "amis": [
                    {
                        "region": "us-west-2",
                        "image": "ami-a1b2c3d4567890ab",
                        "name": "MyBasicRecipe 2020-02-18T22-49-38.704Z",
                        "description": "This example image recipe creates a Windows
 2016 image."
                    },
                    {
                        "region": "us-west-2",
                        "image": "ami-a1b2c3d4567890ab",
                        "name": "Name 2020-02-18T22-49-08.131Z",
                        "description": "Copies AMI to eu-west-2 and exports to S3"
                    },
                    {
                        "region": "eu-west-2",
                        "image": "ami-a1b2c3d4567890ab",
```

```
                        "name": "My 6 image 2020-02-18T22-49-08.131Z",
                        "description": "Copies AMI to eu-west-2 and exports to S3"
                    }
                ]
            },
            "tags": {}
        },
        {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:image/
mybasicrecipe/2019.12.03/5",
            "name": "MyBasicRecipe",
            "version": "2019.12.03/5",
            "platform": "Windows",
            "state": {
                "status": "AVAILABLE"
            },
            "owner": "123456789012",
            "dateCreated": "2020-02-18T16:51:48.403Z",
            "outputResources": {
                "amis": [
                    {
                        "region": "us-west-2",
                        "image": "ami-a1b2c3d4567890ab",
                        "name": "MyBasicRecipe 2020-02-18T16-52-18.965Z",
                        "description": "This example image recipe creates a Windows
 2016 image."
                    }
                ]
            },
            "tags": {}
        },
        {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:image/
mybasicrecipe/2019.12.03/4",
            "name": "MyBasicRecipe",
            "version": "2019.12.03/4",
            "platform": "Windows",
            "state": {
                "status": "AVAILABLE"
            },
            "owner": "123456789012",
            "dateCreated": "2020-02-18T16:50:01.827Z",
            "outputResources": {
                "amis": [
```

```
                    {
                        "region": "us-west-2",
                        "image": "ami-a1b2c3d4567890ab",
                        "name": "MyBasicRecipe 2020-02-18T16-50-32.280Z",
                        "description": "This example image recipe creates a Windows
 2016 image."
                    }
                ]
            },
            "tags": {}
        },
        {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:image/
mybasicrecipe/2019.12.03/3",
            "name": "MyBasicRecipe",
            "version": "2019.12.03/3",
            "platform": "Windows",
            "state": {
                "status": "AVAILABLE"
            },
            "owner": "123456789012",
            "dateCreated": "2020-02-14T23:14:13.597Z",
            "outputResources": {
                "amis": [
                    {
                        "region": "us-west-2",
                        "image": "ami-a1b2c3d4567890ab",
                        "name": "MyBasicRecipe 2020-02-14T23-14-44.243Z",
                        "description": "This example image recipe creates a Windows
 2016 image."
                    }
                ]
            },
            "tags": {}
        },
        {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:image/
mybasicrecipe/2019.12.03/2",
            "name": "MyBasicRecipe",
            "version": "2019.12.03/2",
            "platform": "Windows",
            "state": {
                "status": "FAILED",
```

```
                "reason": "SSM execution 'a1b2c3d4-5678-90ab-cdef-EXAMPLE11111'
 failed with status = 'Failed' and failure message = 'Step fails when it is
 verifying the command has completed. Command a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
 returns unexpected invocation result: \n{Status=[Failed], ResponseCode=[1],
 Output=[\n----------ERROR-------\nfailed to run commands: exit status 1],
 OutputPayload=[{\"Status\":\"Failed\",\"ResponseCode\":1,\"Output\":\"\
\n----------ERROR-------\\nfailed to run commands: exit status 1\",\"CommandId\":
\"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111\"}], CommandId=[a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111]}. Please refer to Automation Service Troubleshooting Guide for more
 diagnosis details.'"
            },
            "owner": "123456789012",
            "dateCreated": "2020-02-14T22:57:42.593Z",
            "outputResources": {
                "amis": []
            },
            "tags": {}
        }
    ]
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte ListImageBuildVersions en la Referencia de comandos de la AWS CLI.

`list-image-pipeline-images`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-image-pipeline-images`.

AWS CLI

Para enumerar las imágenes de la canalización de imágenes

En el siguiente ejemplo de `list-image-pipeline-images`, se enumeran todas las imágenes que se han creado mediante una canalización de imágenes específica.

```
aws imagebuilder list-image-pipeline-images \
    --image-pipeline-arn arn:aws:imagebuilder:us-west-2:123456789012:image-pipeline/
mywindows2016pipeline
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "imagePipelineList": [
        {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:image-pipeline/
mywindows2016pipeline",
            "name": "MyWindows2016Pipeline",
            "description": "Builds Windows 2016 Images",
            "platform": "Windows",
            "imageRecipeArn": "arn:aws:imagebuilder:us-west-2:123456789012:image-
recipe/mybasicrecipe/2019.12.03",
            "infrastructureConfigurationArn": "arn:aws:imagebuilder:us-
west-2:123456789012:infrastructure-configuration/myexampleinfrastructure",
            "distributionConfigurationArn": "arn:aws:imagebuilder:us-
west-2:123456789012:distribution-configuration/myexampledistribution",
            "imageTestsConfiguration": {
                "imageTestsEnabled": true,
                "timeoutMinutes": 60
            },
            "schedule": {
                "scheduleExpression": "cron(0 0 * * SUN)",
                "pipelineExecutionStartCondition":
 "EXPRESSION_MATCH_AND_DEPENDENCY_UPDATES_AVAILABLE"
            },
            "status": "ENABLED",
            "dateCreated": "2020-02-19T19:04:01.253Z",
            "dateUpdated": "2020-02-19T19:04:01.253Z",
            "tags": {
                "KeyName": "KeyValue"
            }
        },
        {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:image-pipeline/sam",
            "name": "PipelineName",
            "platform": "Linux",
            "imageRecipeArn": "arn:aws:imagebuilder:us-west-2:123456789012:image-
recipe/recipe-name-a1b2c3d45678/1.0.0",
            "infrastructureConfigurationArn": "arn:aws:imagebuilder:us-
west-2:123456789012:infrastructure-configuration/infrastructureconfiguration-name-
a1b2c3d45678",
            "imageTestsConfiguration": {
                "imageTestsEnabled": true,
                "timeoutMinutes": 720
```

```
            },
            "status": "ENABLED",
            "dateCreated": "2019-12-16T18:19:02.068Z",
            "dateUpdated": "2019-12-16T18:19:02.068Z",
            "tags": {
                "KeyName": "KeyValue"
            }
        }
    ]
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte ListImagePipelineImages en la Referencia de comandos de la AWS CLI.

`list-image-recipes`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-image-recipes`.

AWS CLI

Para enumerar las recetas de imágenes

En el siguiente ejemplo de `list-image-recipes`, se enumeran todas las recetas de imágenes.

```
aws imagebuilder list-image-recipes
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "imageRecipeSummaryList": [
        {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:image-recipe/
mybasicrecipe/2019.12.03",
            "name": "MyBasicRecipe",
            "platform": "Windows",
            "owner": "123456789012",
            "parentImage": "arn:aws:imagebuilder:us-west-2:aws:image/windows-
server-2016-english-full-base-x86/2019.x.x",
            "dateCreated": "2020-02-19T18:54:25.975Z",
```

```
            "tags": {
                "KeyName": "KeyValue"
            }
        },
        {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:image-recipe/recipe-
name-a1b2c3d45678/1.0.0",
            "name": "recipe-name-a1b2c3d45678",
            "platform": "Linux",
            "owner": "123456789012",
            "parentImage": "arn:aws:imagebuilder:us-west-2:aws:image/amazon-linux-2-
x86/2019.11.21",
            "dateCreated": "2019-12-16T18:19:00.120Z",
            "tags": {
                "KeyName": "KeyValue"
            }
        }
    ]
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte ListImageRecipes en la Referencia de comandos de la AWS CLI.

`list-images`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-images`.

AWS CLI

Para enumerar las imágenes

En el siguiente ejemplo de `list-images`, se enumeran todas las versiones semánticas a las que tiene acceso.

```
aws imagebuilder list-images
```

Salida:

```
{
```

```
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "imageVersionList": [
        {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:image/
mybasicrecipe/2019.12.03",
            "name": "MyBasicRecipe",
            "version": "2019.12.03",
            "platform": "Windows",
            "owner": "123456789012",
            "dateCreated": "2020-02-14T21:29:18.810Z"
        }
    ]
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte ListImages en la Referencia de comandos de la AWS CLI.

`list-infrastructure-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-infrastructure-configurations`.

AWS CLI

Para enumerar las configuraciones de infraestructura

En el siguiente ejemplo de `list-infrastructure-configurations`, se muestran todas las configuraciones de infraestructuras.

```
aws imagebuilder list-infrastructure-configurations
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "infrastructureConfigurationSummaryList": [
        {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:infrastructure-
configuration/myexampleinfrastructure",
```

```
            "name": "MyExampleInfrastructure",
            "description": "An example that will retain instances of failed builds",
            "dateCreated": "2020-02-19T19:11:51.858Z",
            "tags": {}
        },
        {
            "arn": "arn:aws:imagebuilder:us-west-2:123456789012:infrastructure-
configuration/infrastructureconfiguration-name-a1b2c3d45678",
            "name": "infrastructureConfiguration-name-a1b2c3d45678",
            "dateCreated": "2019-12-16T18:19:01.038Z",
            "tags": {
                "KeyName": "KeyValue"
            }
        }
    ]
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte ListInfrastructureConfigurations en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas para un recurso específico

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran todas las etiquetas de un recurso específico.

```
aws imagebuilder list-tags-for-resource \
    --resource-arn arn:aws:imagebuilder:us-west-2:123456789012:image-pipeline/
mywindows2016pipeline
```

Salida:

```
{
    "tags": {
        "KeyName": "KeyValue"
```

```
    }
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-component-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-component-policy`.

AWS CLI

Para aplicar una política de recursos a un componente

En el siguiente comando de `put-component-policy`, se aplica una política de recursos a un componente de compilación para permitir el uso compartido entre cuentas de los componentes de compilación. Le recomendamos que utilice el comando de la CLI `create-resource-share` de RAM. Si utiliza el comando de la CLI `put-component-policy` de EC2 Image Builder, también debe utilizar el comando CLI `promote-resource-share-create-from-policy` de RAM para que el recurso esté visible para todas las entidades principales con las que se comparte el recurso.

```
aws imagebuilder put-component-policy \
    --component-arn arn:aws:imagebuilder:us-west-2:123456789012:component/
examplecomponent/2019.12.02/1 \
    --policy '{ "Version":"2012-10-17",        "Statement": [ { "Effect":
 "Allow", "Principal": { "AWS": [ "123456789012" ] }, "Action":
 [ "imagebuilder:GetComponent", "imagebuilder:ListComponents" ],
 "Resource": [ "arn:aws:imagebuilder:us-west-2:123456789012:component/
examplecomponent/2019.12.02/1" ] } ] }'
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "componentArn": "arn:aws:imagebuilder:us-west-2:123456789012:component/
examplecomponent/2019.12.02/1"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte PutComponentPolicy en la Referencia de comandos de la AWS CLI.

`put-image-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-image-policy`.

AWS CLI

Para aplicar una política de recursos a una imagen

En el siguiente comando de `put-image-policy`, se aplica una política de recursos a una imagen para permitir el uso compartido entre cuentas de imágenes. Le recomendamos que utilice el comando de la CLI create-resource-share de RAM. Si utiliza el comando de la CLI put-image-policy de EC2 Image Builder, también debe utilizar el comando CLI promote-resource-share-create-from-policy de RAM para que el recurso esté visible para todas las entidades principales con las que se comparte el recurso.

```
aws imagebuilder put-image-policy \
    --image-arn arn:aws:imagebuilder:us-west-2:123456789012:image/example-image/2019.12.02/1 \
    --policy '{ "Version":"2012-10-17",        "Statement": [ { "Effect": "Allow", "Principal": { "AWS": [ "123456789012" ] }, "Action": [ "imagebuilder:GetImage", "imagebuilder:ListImages" ], "Resource": [ "arn:aws:imagebuilder:us-west-2:123456789012:image/example-image/2019.12.02/1" ] } ] }'
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "imageArn": "arn:aws:imagebuilder:us-west-2:123456789012:image/example-image/2019.12.02/1"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información acerca de la API, consulte PutImagePolicy en la Referencia de comandos de la AWS CLI.

`put-image-recipe-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-image-recipe-policy`.

AWS CLI

Para aplicar una política de recursos a una receta de imágenes

En el siguiente comando de `put-image-recipe-policy`, se aplica una política de recursos a una receta de imágenes para permitir el uso compartido entre cuentas de recetas de imágenes. Le recomendamos que utilice el comando de la CLI `create-resource-share` de RAM. Si utiliza el comando de la CLI `put-image-recipe-policy` de EC2 Image Builder, también debe utilizar el comando CLI `promote-resource-share-create-from-policy` de RAM para que el recurso esté visible para todas las entidades principales con las que se comparte el recurso.

```
aws imagebuilder put-image-recipe-policy \
    --image-recipe-arn arn:aws:imagebuilder:us-west-2:123456789012:image-recipe/
example-image-recipe/2019.12.02 \
    --policy '{ "Version":"2012-10-17",        "Statement": [ { "Effect":
 "Allow", "Principal": { "AWS": [ "123456789012" ] }, "Action":
 [ "imagebuilder:GetImageRecipe", "imagebuilder:ListImageRecipes" ], "Resource":
 [ "arn:aws:imagebuilder:us-west-2:123456789012:image-recipe/example-image-
recipe/2019.12.02" ] } ] }'
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "imageRecipeArn": "arn:aws:imagebuilder:us-west-2:123456789012:image-recipe/
example-image-recipe/2019.12.02/1"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte PutImageRecipePolicy en la Referencia de comandos de la AWS CLI.

`start-image-pipeline-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-image-pipeline-execution`.

AWS CLI

Para iniciar una canalización de imágenes manualmente

En el siguiente ejemplo de `start-image-pipeline-execution`, se inicia manualmente una canalización de imágenes.

```
aws imagebuilder start-image-pipeline-execution \
    --image-pipeline-arn arn:aws:imagebuilder:us-west-2:123456789012:image-pipeline/
mywindows2016pipeline
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "clientToken": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "imageBuildVersionArn": "arn:aws:imagebuilder:us-west-2:123456789012:image/
mybasicrecipe/2019.12.03/1"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte StartImagePipelineExecution en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para etiquetar un recurso

En el siguiente ejemplo de `tag-resource`, se agrega y etiqueta un recurso a EC2 Image Builder mediante un archivo JSON.

```
aws imagebuilder tag-resource \
    --cli-input-json file://tag-resource.json
```

Contenido de `tag-resource.json`:

```
{
    "resourceArn": "arn:aws:imagebuilder:us-west-2:123456789012:image-pipeline/
mywindows2016pipeline",
    "tags": {
        "KeyName: "KeyValue"
    }
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar una etiqueta de un recurso

En el siguiente ejemplo de `untag-resource`, se elimina una etiqueta de un recurso mediante un archivo JSON.

```
aws imagebuilder untag-resource \
    --cli-input-json file://tag-resource.json
```

Contenido de `untag-resource.json`:

```
{
    "resourceArn": "arn:aws:imagebuilder:us-west-2:123456789012:image-pipeline/
mywindows2016pipeline",
    "tagKeys": [
        "KeyName"
    ]
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-distribution-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-distribution-configuration`.

AWS CLI

Para actualizar una configuración de distribución

En el siguiente ejemplo de `update-distribution-configuration`, se crea una actualización de distribución mediante un archivo JSON.

```
aws imagebuilder update-distribution-configuration \
    --cli-input-json file://update-distribution-configuration.json
```

Contenido de `update-distribution-configuration.json`:

```
{
    "distributionConfigurationArn": "arn:aws:imagebuilder:us-
west-2:123456789012:distribution-configuration/myexampledistribution",
    "description": "Copies AMI to eu-west-2 and exports to S3",
    "distributions": [
        {
            "region": "us-west-2",
            "amiDistributionConfiguration": {
                "name": "Name {{imagebuilder:buildDate}}",
                "description": "An example image name with parameter references"
            }
        },
        {
            "region": "eu-west-2",
            "amiDistributionConfiguration": {
                "name": "My {{imagebuilder:buildVersion}} image
 {{imagebuilder:buildDate}}"
            }
        }
```

```
    ]
}
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener detalles sobre la API, consulte UpdateDistributionConfiguration en la Referencia de comandos de la AWS CLI.

`update-image-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-image-pipeline`.

AWS CLI

Para actualizar una canalización de imágenes

En el siguiente ejemplo de `update-image-pipeline`, se actualiza una canalización de imágenes mediante un archivo JSON.

```
aws imagebuilder update-image-pipeline \
    --cli-input-json file://update-image-pipeline.json
```

Contenido de `update-image-pipeline.json`:

```
{
    "imagePipelineArn": "arn:aws:imagebuilder:us-west-2:123456789012:image-pipeline/
mywindows2016pipeline",
    "imageRecipeArn": "arn:aws:imagebuilder:us-west-2:123456789012:image-recipe/
mybasicrecipe/2019.12.03",
    "infrastructureConfigurationArn": "arn:aws:imagebuilder:us-
west-2:123456789012:infrastructure-configuration/myexampleinfrastructure",
    "distributionConfigurationArn": "arn:aws:imagebuilder:us-
west-2:123456789012:distribution-configuration/myexampledistribution",
    "imageTestsConfiguration": {
        "imageTestsEnabled": true,
```

```
        "timeoutMinutes": 120
    },
    "schedule": {
        "scheduleExpression": "cron(0 0 * * MON)",
        "pipelineExecutionStartCondition":
 "EXPRESSION_MATCH_AND_DEPENDENCY_UPDATES_AVAILABLE"
    },
    "status": "DISABLED"
}
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener información sobre la API, consulte UpdateImagePipeline en la Referencia de comandos de la AWS CLI.

`update-infrastructure-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-infrastructure-configuration`.

AWS CLI

Para actualizar una configuración de infraestructura

En el siguiente ejemplo de `update-infrastructure-configuration`, se actualiza una configuración de infraestructura mediante un archivo JSON.

```
aws imagebuilder update-infrastructure-configuration \
    --cli-input-json file:/update-infrastructure-configuration.json
```

Contenido de `update-infrastructure-configuration.json`:

```
{
    "infrastructureConfigurationArn": "arn:aws:imagebuilder:us-
west-2:123456789012:infrastructure-configuration/myexampleinfrastructure",
```

```
    "description": "An example that will terminate instances of failed builds",
    "instanceTypes": [
        "m5.large", "m5.2xlarge"
    ],
    "instanceProfileName": "EC2InstanceProfileForImageFactory",
    "securityGroupIds": [
        "sg-a48c95ef"
    ],
    "subnetId": "subnet-a48c95ef",
    "logging": {
        "s3Logs": {
            "s3BucketName": "bucket-name",
            "s3KeyPrefix": "bucket-path"
        }
    },
    "terminateInstanceOnFailure": true,
    "snsTopicArn": "arn:aws:sns:us-west-2:123456789012:sns-name"
}
```

Salida:

```
{
    "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Para obtener más información, consulte Setting Up and Managing an EC2 Image Builder Image Pipeline Using the AWS CLI en la Guía del usuario de EC2 Image Builder.

- Para obtener detalles sobre la API, consulte UpdateInfrastructureConfiguration en la Referencia de comandos de la AWS CLI.

Ejemplos de Incident Manager que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Incident Manager.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-replication-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-replication-set`.

AWS CLI

Para crear el conjunto de replicación

En el siguiente ejemplo de `create-replication-set`, se crea el conjunto de replicación que Incident Manager utiliza para replicar y cifrar los datos de su cuenta de Amazon Web Services. En este ejemplo, se utilizan las regiones us-east-1 y us-east-2 al crear el conjunto de replicación.

```
aws ssm-incidents create-replication-set \
    --regions '{"us-east-1": {"sseKmsKeyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"}, "us-east-2":
 {"sseKmsKeyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"}}'
```

Salida:

```
{
    "replicationSetArns": [
        "arn:aws:ssm-incidents::111122223333:replication-set/c4bcb603-4bf9-
bb3f-413c-08df53673b57"
    ]
}
```

Para obtener más información, consulte What Is AWS Systems Manager Incident Manager? en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte CreateReplicationSet en la Referencia de comandos de la AWS CLI.

`create-response-plan`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-response-plan`.

AWS CLI

Para crear un plan de respuesta

En el siguiente ejemplo de `create-response-plan`, se crea un plan de respuesta con los detalles especificados.

```
aws ssm-incidents create-response-plan \
    --chat-channel '{"chatbotSns": ["arn:aws:sns:us-
east-1:111122223333:Standard_User"]}' \
    --display-name "Example response plan" \
    --incident-template '{"impact": 5, "title": "example-incident"}' \
    --name "example-response" \
    --actions '[{"ssmAutomation": {"documentName": "AWSIncidents-
CriticalIncidentRunbookTemplate", "documentVersion": "$DEFAULT",
 "roleArn": "arn:aws:iam::111122223333:role/aws-service-role/ssm-
incidents.amazonaws.com/AWSServiceRoleForIncidentManager", "targetAccount":
 "RESPONSE_PLAN_OWNER_ACCOUNT"}}]' \
    --engagements '["arn:aws:ssm-contacts:us-east-1:111122223333:contact/example"]'
```

Salida:

```
{
    "arn": "arn:aws:ssm-incidents::111122223333:response-plan/example-response"
}
```

Para obtener más información, consulte Incident preparation en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte CreateResponsePlan en la Referencia de comandos de la AWS CLI.

`create-timeline-event`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-timeline-event`.

AWS CLI

Ejemplo 1: creación de un evento de escala de tiempo personalizado

En el siguiente ejemplo de `create-timeline-event`, se crea un evento de escala de tiempo personalizado a la hora especificada del incidente indicado.

```
aws ssm-incidents create-timeline-event \
    --event-data "\"example timeline event\"" \
    --event-time 2022-10-01T20:30:00.000 \
    --event-type "Custom Event" \
    --incident-record-arn "arn:aws:ssm-incidents::111122223333:incident-record/
Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4EXAMPLE"
```

Salida:

```
{
    "eventId": "c0bcc885-a41d-eb01-b4ab-9d2deEXAMPLE",
    "incidentRecordArn": "arn:aws:ssm-incidents::111122223333:incident-record/
Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4EXAMPLE"
}
```

Ejemplo 2: creación de un evento de escala de tiempo con una nota del incidente

En el siguiente ejemplo de `create-timeline-event`, se crea un evento de escala de tiempo que aparece en el panel Notas de incidentes.

```
aws ssm-incidents create-timeline-event \
     --event-data "\"New Note\"" \
     --event-type "Note" \
     --incident-record-arn "arn:aws:ssm-incidents::111122223333:incident-record/
Test/6cc46130-ca6c-3b38-68f1-f6abeEXAMPLE" \
     --event-time 2023-06-20T12:06:00.000 \
     --event-references '[{"resource":"arn:aws:ssm-incidents::111122223333:incident-
record/Test/6cc46130-ca6c-3b38-68f1-f6abeEXAMPLE"}]'
```

Salida:

```
{
    "eventId": "a41dc885-c0bc-b4ab-eb01-de9d2EXAMPLE",
    "incidentRecordArn": "arn:aws:ssm-incidents::111122223333:incident-record/
Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4EXAMPLE"
}
```

Para obtener más información, consulte Incident details en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte CreateTimelineEvent en la Referencia de comandos de la AWS CLI.

delete-incident-record

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-incident-record`.

AWS CLI

Para eliminar un registro de incidentes

En el siguiente ejemplo de `delete-incident-record`, se elimina el registro de incidentes especificado.

```
aws ssm-incidents delete-incident-record \
    --arn "arn:aws:ssm-incidents::111122223333:incident-record/Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Incident tracking en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte DeleteIncidentRecord en la Referencia de comandos de la AWS CLI.

delete-replication-set

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-replication-set`.

AWS CLI

Para eliminar el conjunto de replicación

En el siguiente ejemplo de `delete-replication-set`, se elimina el conjunto de replicación de su cuenta de Amazon Web Services. Al eliminar el conjunto de replicación también se eliminan todos los datos de Incident Manager. Esta acción no se puede revertir.

```
aws ssm-incidents delete-replication-set \
    --arn "arn:aws:ssm-incidents::111122223333:replication-set/c4bcb603-4bf9-bb3f-413c-08df53673b57"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte What Is AWS Systems Manager Incident Manager? en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte DeleteReplicationSet en la Referencia de comandos de la AWS CLI.

`delete-resource-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-resource-policy`.

AWS CLI

Para eliminar una política de recursos

En el siguiente ejemplo de `delete-resource-policy`, se elimina una política de recursos de un plan de respuesta. Esto revocará el acceso de la entidad principal o la organización con la que se ha compartido el plan de respuesta.

```
aws ssm-incidents delete-resource-policy \
    --policy-id "be8b57191f0371f1c6827341aa3f0a03" \
    --resource-arn "arn:aws:ssm-incidents::111122223333:response-plan/Example-Response-Plan"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with shared contacts and response plans en la Guía del usuario de Incident Manager.

- Para obtener detalles sobre la API, consulte DeleteResourcePolicy en la Referencia de comandos de la AWS CLI.

`delete-response-plan`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-response-plan`.

AWS CLI

Para eliminar un plan de respuesta

En el siguiente ejemplo de `delete-response-plan`, se elimina el plan de respuesta especificado.

```
aws ssm-incidents delete-response-plan \
    --arn "arn:aws:ssm-incidents::111122223333:response-plan/example-response"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Incident preparation en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte DeleteResponsePlan en la Referencia de comandos de la AWS CLI.

`delete-timeline-event`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-timeline-event`.

AWS CLI

Para eliminar un evento de escala de tiempo

En el siguiente ejemplo de `delete-timeline-event`, se elimina un evento de escala de tiempo personalizado del registro de incidentes especificado.

```
aws ssm-incidents delete-timeline-event \
    --event-id "c0bcc885-a41d-eb01-b4ab-9d2de193643c" \
    --incident-record-arn "arn:aws:ssm-incidents::111122223333:incident-record/
Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Incident details en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte DeleteTimelineEvent en la Referencia de comandos de la AWS CLI.

`get-incident-record`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-incident-record`.

AWS CLI

Para obtener un registro de incidentes

En el siguiente ejemplo de `get-incident-record`, se obtiene información del registro de incidentes especificado.

```
aws ssm-incidents get-incident-record \
    --arn "arn:aws:ssm-incidents::111122223333:incident-record/Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308"
```

Salida:

```
{
    "incidentRecord": {
        "arn": "arn:aws:ssm-incidents::111122223333:incident-record/Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308",
        "automationExecutions": [],
        "creationTime": "2021-05-21T18:16:57.579000+00:00",
        "dedupeString": "c4bcc812-85e7-938d-2b78-17181176ee1a",
        "impact": 5,
        "incidentRecordSource": {
            "createdBy": "arn:aws:iam::111122223333:user/draliatp",
            "invokedBy": "arn:aws:iam::111122223333:user/draliatp",
            "source": "aws.ssm-incidents.custom"
        },
        "lastModifiedBy": "arn:aws:iam::111122223333:user/draliatp",
        "lastModifiedTime": "2021-05-21T18:16:59.149000+00:00",
        "notificationTargets": [],
        "status": "OPEN",
        "title": "Example-Incident"
    }
}
```

Para obtener más información, consulte Incident details en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte GetIncidentRecord en la Referencia de comandos de la AWS CLI.

`get-replication-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-replication-set`.

AWS CLI

Para obtener el conjunto de replicación

En el siguiente ejemplo de `get-replication-set`, se obtiene detalles del conjunto de replicación que utiliza Incident Manager para replicar y cifrar los datos de su cuenta de Amazon Web Services.

```
aws ssm-incidents get-replication-set \
    --arn "arn:aws:ssm-incidents::111122223333:replication-set/c4bcb603-4bf9-bb3f-413c-08df53673b57"
```

Salida:

```
{
    "replicationSet": {
        "createdBy": "arn:aws:sts::111122223333:assumed-role/Admin/username",
        "createdTime": "2021-05-14T17:57:22.010000+00:00",
        "deletionProtected": false,
        "lastModifiedBy": "arn:aws:sts::111122223333:assumed-role/Admin/username",
        "lastModifiedTime": "2021-05-14T17:57:22.010000+00:00",
        "regionMap": {
            "us-east-1": {
                "sseKmsKeyId": "DefaultKey",
                "status": "ACTIVE"
            },
            "us-east-2": {
                "sseKmsKeyId": "DefaultKey",
                "status": "ACTIVE",
                "statusMessage": "Tagging inaccessible"
            }
        },
        "status": "ACTIVE"
    }
}
```

Para obtener más información, consulte What Is AWS Systems Manager Incident Manager? en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte GetReplicationSet en la Referencia de comandos de la AWS CLI.

`get-resource-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource-policies`.

AWS CLI

Para enumerar las políticas de recursos de un plan de respuesta

En el siguiente ejemplo de `command-name`, se enumeran las políticas de recursos asociadas al plan de respuesta especificado.

```
aws ssm-incidents get-resource-policies \
--resource-arn "arn:aws:ssm-incidents::111122223333:response-plan/Example-Response-Plan"
```

Salida:

```
{
    "resourcePolicies": [
        {
            "policyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid
\":\"d901b37a-dbb0-458a-8842-75575c464219-external-principals\",\"Effect\":
\"Allow\",\"Principal\":{\"AWS\":\"arn:aws:iam::222233334444:root\"},\"Action
\":[\"ssm-incidents:GetResponsePlan\",\"ssm-incidents:StartIncident\",\"ssm-
incidents:UpdateIncidentRecord\",\"ssm-incidents:GetIncidentRecord\",\"ssm-
incidents:CreateTimelineEvent\",\"ssm-incidents:UpdateTimelineEvent\",\"ssm-
incidents:GetTimelineEvent\",\"ssm-incidents:ListTimelineEvents\",\"ssm-
incidents:UpdateRelatedItems\",\"ssm-incidents:ListRelatedItems\"],\"Resource\":
[\"arn:aws:ssm-incidents:*:111122223333:response-plan/Example-Response-Plan\",
\"arn:aws:ssm-incidents:*:111122223333:incident-record/Example-Response-Plan/*
\"]}]}",
            "policyId": "be8b57191f0371f1c6827341aa3f0a03",
            "ramResourceShareRegion": "us-east-1"
        }
    ]
}
```

Para obtener más información, consulte Working with shared contacts and response plans en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte GetResourcePolicies en la Referencia de comandos de la AWS CLI.

`get-response-plan`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-response-plan`.

AWS CLI

Para obtener detalles de un plan de respuesta

En el siguiente ejemplo de `command-name`, se obtienen detalles sobre un plan de respuesta específico de su cuenta de AWS.

```
aws ssm-incidents get-response-plan \
    --arn "arn:aws:ssm-incidents::111122223333:response-plan/Example-Response-Plan"
```

Salida:

```
{
    "actions": [
        {
            "ssmAutomation": {
                "documentName": "AWSIncidents-CriticalIncidentRunbookTemplate",
                "documentVersion": "$DEFAULT",
                "roleArn": "arn:aws:iam::111122223333:role/aws-service-role/ssm-
incidents.amazonaws.com/AWSServiceRoleForIncidentManager",
                "targetAccount": "RESPONSE_PLAN_OWNER_ACCOUNT"
            }
        }
    ],
    "arn": "arn:aws:ssm-incidents::111122223333:response-plan/Example-Response-
Plan",
    "chatChannel": {
        "chatbotSns": [
            "arn:aws:sns:us-east-1:111122223333:Standard_User"
        ]
    },
    "displayName": "Example response plan",
    "engagements": [
        "arn:aws:ssm-contacts:us-east-1:111122223333:contact/example"
    ],
    "incidentTemplate": {
        "impact": 5,
        "title": "Example-Incident"
    },
```

```
    "name": "Example-Response-Plan"
}
```

Para obtener más información, consulte Incident preparation en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte GetResponsePlan en la Referencia de comandos de la AWS CLI.

`get-timeline-event`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-timeline-event`.

AWS CLI

Para obtener detalles de un evento de escala de tiempo

En el siguiente ejemplo de `get-timeline-event`, se devuelven los detalles del evento de escala de tiempo especificado.

```
aws ssm-incidents get-timeline-event \
    --event-id 20bcc812-8a94-4cd7-520c-0ff742111424 \
    --incident-record-arn "arn:aws:ssm-incidents::111122223333:incident-record/
Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308"
```

Salida:

```
{
    "event": {
        "eventData": "\"Incident Started\"",
        "eventId": "20bcc812-8a94-4cd7-520c-0ff742111424",
        "eventTime": "2021-05-21T18:16:57+00:00",
        "eventType": "Custom Event",
        "eventUpdatedTime": "2021-05-21T18:16:59.944000+00:00",
        "incidentRecordArn": "arn:aws:ssm-incidents::111122223333:incident-record/
Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308"
    }
}
```

Para obtener más información, consulte Incident details en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte GetTimelineEvent en la Referencia de comandos de la AWS CLI.

`list-incident-records`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-incident-records`.

AWS CLI

Para enumerar registros de incidentes

En el siguiente ejemplo de `command-name`, se enumeran los registros de incidentes de su cuenta de Amazon Web Services.

```
aws ssm-incidents list-incident-records
```

Salida:

```
{
    "incidentRecordSummaries": [
        {
            "arn": "arn:aws:ssm-incidents::111122223333:incident-record/Example-
Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308",
            "creationTime": "2021-05-21T18:16:57.579000+00:00",
            "impact": 5,
            "incidentRecordSource": {
                "createdBy": "arn:aws:iam::111122223333:user/draliatp",
                "invokedBy": "arn:aws:iam::111122223333:user/draliatp",
                "source": "aws.ssm-incidents.custom"
            },
            "status": "OPEN",
            "title": "Example-Incident"
        }
    ]
}
```

Para obtener más información, consulte Incident list en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte ListIncidentRecords en la Referencia de comandos de la AWS CLI.

`list-related-items`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-related-items`.

AWS CLI

Para enumerar elementos relacionados

En el siguiente ejemplo de `list-related-items`, se enumeran los elementos relacionados con el incidente especificado.

```
aws ssm-incidents list-related-items \
    --incident-record-arn "arn:aws:ssm-incidents::111122223333:incident-record/
Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308"
```

Salida:

```
{
    "relatedItems": [
        {
            "identifier": {
                "type": "OTHER",
                "value": {
                    "url": "https://console.aws.amazon.com/systems-manager/opsitems/
oi-8ef82158e190/workbench?region=us-east-1"
                }
            },
            "title": "Example related item"
        },
        {
            "identifier": {
                "type": "PARENT",
                "value": {
                    "arn": "arn:aws:ssm:us-east-1:111122223333:opsitem/
oi-8084126392ac"
                }
            },
            "title": "parentItem"
        }
    ]
}
```

Para obtener más información, consulte Incident details en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte ListRelatedItems en la Referencia de comandos de la AWS CLI.

`list-replication-sets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-replication-sets`.

AWS CLI

Para enumerar el conjunto de replicación

En el siguiente ejemplo de `list-replication-set`, se enumera el conjunto de replicación que utiliza Incident Manager para replicar y cifrar los datos de su cuenta de AWS.

```
aws ssm-incidents list-replication-sets
```

Salida:

```
{
    "replicationSetArns": [
        "arn:aws:ssm-incidents::111122223333:replication-set/c4bcb603-4bf9-
bb3f-413c-08df53673b57"
    ]
}
```

Para obtener más información, consulte What Is AWS Systems Manager Incident Manager? en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte ListReplicationSets en la Referencia de comandos de la AWS CLI.

`list-response-plans`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-response-plans`.

AWS CLI

Para ver una lista de los planes de respuesta disponibles

En el siguiente ejemplo de `list-response-plans`, se enumeran los planes de respuesta disponibles en su cuenta de Amazon Web Services.

```
aws ssm-incidents list-response-plans
```

Salida:

```
{
    "responsePlanSummaries": [
        {
            "arn": "arn:aws:ssm-incidents::111122223333:response-plan/Example-
Response-Plan",
            "displayName": "Example response plan",
            "name": "Example-Response-Plan"
        }
    ]
}
```

Para obtener más información, consulte Incident preparation en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte ListResponsePlans en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un plan de respuesta

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran las etiquetas asociadas al plan de respuesta especificado.

```
aws ssm-incidents list-tags-for-resource \
    --resource-arn "arn:aws:ssm-incidents::111122223333:response-plan/Example-
Response-Plan"
```

Salida:

```
{
    "tags": {
    "group1": "1"
    }
}
```

Para obtener más información, consulte Tagging en la Guía del usuario de Incident Manager.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-timeline-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-timeline-events`.

AWS CLI

Para enumerar los eventos de escala de tiempo de un incidente

En el siguiente ejemplo de `command-name`, se enumeran los eventos de escala de tiempo del incidente especificado.

```
aws ssm-incidents list-timeline-events \
    --incident-record-arn "arn:aws:ssm-incidents::111122223333:incident-record/
Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308"
```

Salida:

```
{
    "eventSummaries": [
        {
            "eventId": "8cbcc889-35e1-a42d-2429-d6f100799915",
            "eventTime": "2021-05-21T22:36:13.766000+00:00",
            "eventType": "SSM Incident Record Update",
            "eventUpdatedTime": "2021-05-21T22:36:13.766000+00:00",
            "incidentRecordArn": "arn:aws:ssm-incidents::111122223333:incident-
record/Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308"
        },
        {
            "eventId": "a2bcc825-aab5-1787-c605-f9bb2640d85b",
            "eventTime": "2021-05-21T18:58:46.443000+00:00",
            "eventType": "SSM Incident Record Update",
```

```
            "eventUpdatedTime": "2021-05-21T18:58:46.443000+00:00",
            "incidentRecordArn": "arn:aws:ssm-incidents::111122223333:incident-
record/Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308"
        },
        {
            "eventId": "5abcc812-89c0-b0a8-9437-1c74223d4685",
            "eventTime": "2021-05-21T18:16:59.149000+00:00",
            "eventType": "SSM Incident Record Update",
            "eventUpdatedTime": "2021-05-21T18:16:59.149000+00:00",
            "incidentRecordArn": "arn:aws:ssm-incidents::111122223333:incident-
record/Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308"
        },
        {
            "eventId": "06bcc812-8820-405e-4065-8d2b14d29b92",
            "eventTime": "2021-05-21T18:16:58+00:00",
            "eventType": "SSM Automation Execution Start Failure for Incident",
            "eventUpdatedTime": "2021-05-21T18:16:58.689000+00:00",
            "incidentRecordArn": "arn:aws:ssm-incidents::111122223333:incident-
record/Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308"
        },
        {
            "eventId": "20bcc812-8a94-4cd7-520c-0ff742111424",
            "eventTime": "2021-05-21T18:16:57+00:00",
            "eventType": "Custom Event",
            "eventUpdatedTime": "2021-05-21T18:16:59.944000+00:00",
            "incidentRecordArn": "arn:aws:ssm-incidents::111122223333:incident-
record/Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308"
        },
        {
            "eventId": "c0bcc885-a41d-eb01-b4ab-9d2de193643c",
            "eventTime": "2020-10-01T20:30:00+00:00",
            "eventType": "Custom Event",
            "eventUpdatedTime": "2021-05-21T22:28:26.299000+00:00",
            "incidentRecordArn": "arn:aws:ssm-incidents::111122223333:incident-
record/Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308"
        }
    ]
}
```

Para obtener más información, consulte Incident details en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte ListTimelineEvents en la Referencia de comandos de la AWS CLI.

`put-resource-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-resource-policy`.

AWS CLI

Para compartir un plan de respuesta y los incidentes

En el siguiente ejemplo de `command-name`, se agrega una política de recursos al Example-Response-Plan que comparte el plan de respuesta y los incidentes asociados a la entidad principal especificada.

```
aws ssm-incidents put-resource-policy \
    --resource-arn "arn:aws:ssm-incidents::111122223333:response-plan/Example-Response-Plan" \
    --policy "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":\"ExampleResourcePolciy\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":\"arn:aws:iam::222233334444:root\"},\"Action\":[\"ssm-incidents:GetResponsePlan\",\"ssm-incidents:StartIncident\",\"ssm-incidents:UpdateIncidentRecord\",\"ssm-incidents:GetIncidentRecord\",\"ssm-incidents:CreateTimelineEvent\",\"ssm-incidents:UpdateTimelineEvent\",\"ssm-incidents:GetTimelineEvent\",\"ssm-incidents:ListTimelineEvents\",\"ssm-incidents:UpdateRelatedItems\",\"ssm-incidents:ListRelatedItems\"],\"Resource\":[\"arn:aws:ssm-incidents:*:111122223333:response-plan/Example-Response-Plan\",\"arn:aws:ssm-incidents:*:111122223333:incident-record/Example-Response-Plan/*\"]}]}"
```

Salida:

```
{
    "policyId": "be8b57191f0371f1c6827341aa3f0a03"
}
```

Para obtener más información, consulte Working with shared contacts and response plans en la Guía del usuario de Incident Manager.

- Para obtener detalles sobre la API, consulte PutResourcePolicy en la Referencia de comandos de la AWS CLI.

`start-incident`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-incident`.

AWS CLI

Para iniciar un incidente

En el siguiente ejemplo de `start-incident`, se inicia un incidente con el plan de respuesta especificado.

```
aws ssm-incidents start-incident \
    --response-plan-arn "arn:aws:ssm-incidents::111122223333:response-plan/Example-Response-Plan"
```

Salida:

```
{
    "incidentRecordArn": "arn:aws:ssm-incidents::682428703967:incident-record/Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308"
}
```

Para obtener más información, consulte Incident creation en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte StartIncident en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para etiquetar un plan de respuesta

En el siguiente ejemplo de `tag-resource`, se etiqueta un plan de respuesta especificado con el par clave-valor de etiquetas proporcionado.

```
aws ssm-incidents tag-resource \
    --resource-arn "arn:aws:ssm-incidents::111122223333:response-plan/Example-Response-Plan" \
    --tags '{"group1":"1"}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging en la Guía del usuario de Incident Manager.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar etiquetas de un plan de respuesta

En el siguiente ejemplo de `untag-resource`, se eliminan la etiquetas especificadas del plan de respuesta.

```
aws ssm-incidents untag-resource \
    --resource-arn "arn:aws:ssm-incidents::111122223333:response-plan/Example-Response-Plan" \
    --tag-keys '["group1"]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging en la Guía del usuario de Incident Manager.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-deletion-protection`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-deletion-protection`.

AWS CLI

Para actualizar la protección de eliminación de conjuntos de reproducción

En el siguiente ejemplo de `update-deletion-protection`, se actualiza la protección contra la eliminación de su cuenta para evitar que se elimine la última región del conjunto de replicación.

```
aws ssm-incidents update-deletion-protection \
    --arn "arn:aws:ssm-incidents::111122223333:replication-set/a2bcc5c9-0f53-8047-7fef-c20749989b40" \
```

```
    --deletion-protected
```

Este comando no genera ninguna salida.

Para obtener más información, consulte What Is AWS Systems Manager Incident Manager? en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte UpdateDeletionProtection en la Referencia de comandos de la AWS CLI.

`update-incident-record`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-incident-record`.

AWS CLI

Para actualizar un registro de incidentes

En el siguiente ejemplo de `command-name`, se resuelve el incidente especificado.

```
aws ssm-incidents update-incident-record \
    --arn "arn:aws:ssm-incidents::111122223333:incident-record/Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308" \
    --status "RESOLVED"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Incident details en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte UpdateIncidentRecord en la Referencia de comandos de la AWS CLI.

`update-related-items`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-related-items`.

AWS CLI

Para actualizar un elemento relacionado con un incidente

En el siguiente ejemplo de `update-related-item`, se elimina un elemento relacionado del registro de incidentes especificado.

```
aws ssm-incidents update-related-items \
    --incident-record-arn "arn:aws:ssm-incidents::111122223333:incident-record/
Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308" \
    --related-items-update '{"itemToRemove": {"type": "OTHER", "value": {"url":
 "https://console.aws.amazon.com/systems-manager/opsitems/oi-8ef82158e190/workbench?
region=us-east-1"}}}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Incident details en la Guía del usuario de Incident Manager.

- Para obtener información acerca de la API, consulte UpdateRelatedItems en la Referencia de comandos de la AWS CLI.

update-replication-set

En el siguiente ejemplo de código, se muestra cómo utilizar `update-replication-set`.

AWS CLI

Para actualizar un conjunto de replicación

En el siguiente ejemplo de `command-name`, se elimina la región us-east-2 del conjunto de replicación.

```
aws ssm-incidents update-replication-set \
    --arn "arn:aws:ssm-incidents::111122223333:replication-set/
a2bcc5c9-0f53-8047-7fef-c20749989b40" \
    --actions '[{"deleteRegionAction": {"regionName": "us-east-2"}}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte What Is AWS Systems Manager Incident Manager? en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte UpdateReplicationSet en la Referencia de comandos de la AWS CLI.

update-response-plan

En el siguiente ejemplo de código, se muestra cómo utilizar `update-response-plan`.

AWS CLI

Para actualizar un plan de respuesta

En el siguiente ejemplo de `update-response-plan`, se elimina un canal de chat del plan de respuesta especificado.

```
aws ssm-incidents update-response-plan \
    --arn "arn:aws:ssm-incidents::111122223333:response-plan/Example-Response-Plan"
 \
    --chat-channel '{"empty":{}}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Incident preparation en la Guía del usuario de Incident Manager.

- Para obtener información acerca de la API, consulte UpdateResponsePlan en la Referencia de comandos de la AWS CLI.

`update-timeline-event`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-timeline-event`.

AWS CLI

Para actualizar un evento de escala de tiempo

En el siguiente ejemplo de `update-timeline-event`, se actualiza la hora a la que se produjo el evento.

```
aws ssm-incidents update-timeline-event \
    --event-id 20bcc812-8a94-4cd7-520c-0ff742111424 \
    --incident-record-arn "arn:aws:ssm-incidents::111122223333:incident-record/
Example-Response-Plan/6ebcc812-85f5-b7eb-8b2f-283e4d844308" \
    --event-time "2021-05-21T18:10:57+00:00"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Incident details en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte UpdateTimelineEvent en la Referencia de comandos de la AWS CLI.

Ejemplos de contactos de Incident Manager que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo ejecutar acciones e implementar escenarios comunes usando la AWS Command Line Interface con contactos de Incident Manager.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`accept-page`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-page`.

AWS CLI

Para aceptar una página durante una interacción

En el siguiente ejemplo de `accept-page`, se utiliza un código de aceptación enviado al canal de contacto para aceptar una página.

```
aws ssm-contacts accept-page \
    --page-id "arn:aws:ssm-contacts:us-east-2:682428703967:page/
akuam/94ea0c7b-56d9-46c3-b84a-a37c8b067ad3" \
    --accept-type READ \
    --accept-code 425440
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener detalles sobre la API, consulte AcceptPage en la Referencia de comandos de la AWS CLI.

`activate-contact-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `activate-contact-channel`.

AWS CLI

Para activar un canal de contacto de un contacto

En el siguiente ejemplo de `activate-contact-channel`, se activa un canal de contacto y se puede utilizar como parte de un incidente.

```
aws ssm-contacts activate-contact-channel \
    --contact-channel-id "arn:aws:ssm-contacts:us-east-2:111122223333:contact-channel/akuam/fc7405c4-46b2-48b7-87b2-93e2f225b90d" \
    --activation-code "466136"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte ActivateContactChannel en la Referencia de comandos de la AWS CLI.

`command-name`

En el siguiente ejemplo de código, se muestra cómo utilizar `command-name`.

AWS CLI

Para eliminar un contacto

En el siguiente ejemplo de `command-name`, se elimina un contacto. Ya no se podrá acceder al contacto desde ningún plan de escalamiento que haga referencia a dicho contacto.

```
aws ssm-contacts delete-contact \
    --contact-id "arn:aws:ssm-contacts:us-east-1:682428703967:contact/alejr"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte CommandName en la Referencia de comandos de la AWS CLI.

`create-contact-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-contact-channel`.

AWS CLI

Para crear un canal de contacto

Crea un canal de contacto de tipo SMS para el contacto Akua Mansa. Se pueden crear canales de contacto de tipo SMS, EMAIL o VOICE.

```
aws ssm-contacts create-contact-channel \
    --contact-id "arn:aws:ssm-contacts:us-east-1:111122223333:contact/akuam" \
    --name "akuas sms-test" \
    --type SMS \
    --delivery-address '{"SimpleAddress": "+15005550199"}'
```

Salida:

```
{
    "ContactChannelArn": "arn:aws:ssm-contacts:us-east-1:111122223333:contact-
channel/akuam/02f506b9-ea5d-4764-af89-2daa793ff024"
}
```

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte CreateContactChannel en la Referencia de comandos de la AWS CLI.

`create-contact`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-contact`.

AWS CLI

Para crear un contacto

En el siguiente ejemplo de `create-contact`, se crea un contacto en su entorno con un plan en blanco. El plan se puede actualizar después de crear los canales de contacto. Utilice el comando create-contact-channel con el ARN de salida de este comando. Después de crear los canales de contacto para este contacto, utilice update-contact para actualizar el plan.

```
aws ssm-contacts create-contact \
    --alias "akuam" \
    --display-name "Akua Mansa" \
    --type PERSONAL \
    --plan '{"Stages": []}'
```

Salida:

```
{
    "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/akuam"
}
```

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte CreateContact en la Referencia de comandos de la AWS CLI.

`deactivate-contact-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `deactivate-contact-channel`.

AWS CLI

Para desactivar un canal de contacto

En el siguiente ejemplo de `deactivate-contact-channel`, se desactiva un canal de contacto. La desactivación de un canal de contacto significa que dicho canal dejará de paginarse durante un incidente. Puede reactivar un canal de contacto en cualquier momento con el comando `activate-contact-channel`.

```
aws ssm-contacts deactivate-contact-channel \
    --contact-channel-id "arn:aws:ssm-contacts:us-east-2:111122223333:contact-channel/akuam/fc7405c4-46b2-48b7-87b2-93e2f225b90d"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre de la API, consulte DeactivateContactChannel en la Referencia de comandos de la AWS CLI.

`delete-contact-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-contact-channel`.

AWS CLI

Para eliminar un canal de contacto

En el siguiente ejemplo de `delete-contact-channel`, se elimina un canal de contacto. Al eliminar un canal de contacto, se garantiza que dicho canal no se pagine durante un incidente.

```
aws ssm-contacts delete-contact-channel \
    --contact-channel-id "arn:aws:ssm-contacts:us-east-1:111122223333:contact-channel/akuam/13149bad-52ee-45ea-ae1e-45857f78f9b2"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte DeleteContactChannel en la Referencia de comandos de la AWS CLI.

`delete-contact`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-contact`.

AWS CLI

Para eliminar un contacto

En el siguiente ejemplo de `delete-contact`, se elimina un contacto. Ya no se podrá acceder al contacto desde ningún plan de escalamiento que haga referencia a dicho contacto.

```
aws ssm-contacts delete-contact \
    --contact-id "arn:aws:ssm-contacts:us-east-1:111122223333:contact/alejr"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte DeleteContact en la Referencia de comandos de la AWS CLI.

`describe-engagement`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-engagement`.

AWS CLI

Para describir los detalles de una interacción

En el siguiente ejemplo de `describe-engagement`, se enumeran los detalles de una interacción con un contacto o un plan de escalamiento. El asunto y el contenido se envían a los canales de contacto.

```
aws ssm-contacts describe-engagement \
    --engagement-id "arn:aws:ssm-contacts:us-east-2:111122223333:engagement/
example_escalation/69e40ce1-8dbb-4d57-8962-5fbe7fc53356"
```

Salida:

```
{
    "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
example_escalation",
    "EngagementArn": "arn:aws:ssm-contacts:us-east-2:111122223333:engagement/
example_escalation/69e40ce1-8dbb-4d57-8962-5fbe7fc53356",
    "Sender": "cli",
    "Subject": "cli-test",
    "Content": "Testing engagements via CLI",
    "PublicSubject": "cli-test",
    "PublicContent": "Testing engagements va CLI",
    "StartTime": "2021-05-18T18:25:41.151000+00:00"
}
```

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte DescribeEngagement en la Referencia de comandos de la AWS CLI.

`describe-page`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-page`.

AWS CLI

Para enumerar los detalles de una página en un canal de contacto

En el siguiente ejemplo de `describe-page`, se enumeran los detalles de una página para un canal de contacto. La página incluirá el asunto y el contenido proporcionados.

```
aws ssm-contacts describe-page \
    --page-id "arn:aws:ssm-contacts:us-east-2:111122223333:page/akuam/ad0052bd-e606-498a-861b-25726292eb93"
```

Salida:

```
{
    "PageArn": "arn:aws:ssm-contacts:us-east-2:111122223333:page/akuam/ad0052bd-e606-498a-861b-25726292eb93",
    "EngagementArn": "arn:aws:ssm-contacts:us-east-2:111122223333:engagement/akuam/78a29753-3674-4ac5-9f83-0468563567f0",
    "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/akuam",
    "Sender": "cli",
    "Subject": "cli-test",
    "Content": "Testing engagements via CLI",
    "PublicSubject": "cli-test",
    "PublicContent": "Testing engagements va CLI",
    "SentTime": "2021-05-18T18:43:29.301000+00:00",
    "ReadTime": "2021-05-18T18:43:55.708000+00:00",
    "DeliveryTime": "2021-05-18T18:43:55.265000+00:00"
}
```

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte DescribePage en la Referencia de comandos de la AWS CLI.

`get-contact-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-contact-channel`.

AWS CLI

Para enumerar los detalles de un canal de contacto

En el siguiente ejemplo de `get-contact-channel`, se enumeran los detalles de un canal de contacto.

```
aws ssm-contacts get-contact-channel \
    --contact-channel-id "arn:aws:ssm-contacts:us-east-2:111122223333:contact-channel/akuam/fc7405c4-46b2-48b7-87b2-93e2f225b90d"
```

Salida:

```
{
    "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/akuam",
    "ContactChannelArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact-channel/akuam/fc7405c4-46b2-48b7-87b2-93e2f225b90d",
    "Name": "akuas sms",
    "Type": "SMS",
    "DeliveryAddress": {
        "SimpleAddress": "+15005550199"
    },
    "ActivationStatus": "ACTIVATED"
}
```

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte GetContactChannel en la Referencia de comandos de la AWS CLI.

`get-contact-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-contact-policy`.

AWS CLI

Para enumerar las políticas de recursos de un contacto

En el siguiente ejemplo de `get-contact-policy`, se enumeran las políticas de recursos asociadas al contacto especificado.

```
aws ssm-contacts get-contact-policy \
```

```
    --contact-arn "arn:aws:ssm-contacts:us-east-1:111122223333:contact/akuam"
```

Salida:

```
{
    "ContactArn": "arn:aws:ssm-contacts:us-east-1:111122223333:contact/akuam",
    "Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"SharePolicyForDocumentationDralia\",\"Effect\":\"Allow\",\"Principal\":
{\"AWS\":\"222233334444\"},\"Action\":[\"ssm-contacts:GetContact\",\"ssm-
contacts:StartEngagement\",\"ssm-contacts:DescribeEngagement\",\"ssm-
contacts:ListPagesByEngagement\",\"ssm-contacts:StopEngagement\"],\"Resource
\":[\"arn:aws:ssm-contacts:*:111122223333:contact/akuam\",\"arn:aws:ssm-
contacts:*:111122223333:engagement/akuam/*\"]}]}"
}
```

Para obtener más información, consulte Working with shared contacts and response plans en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte GetContactPolicy en la Referencia de comandos de la AWS CLI.

`get-contact`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-contact`.

AWS CLI

Ejemplo 1: descripción de un plan de contactos

En el siguiente ejemplo de `get-contact`, se describe un contacto.

```
aws ssm-contacts get-contact \
    --contact-id "arn:aws:ssm-contacts:us-east-2:111122223333:contact/akuam"
```

Salida:

```
{
    "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/akuam",
    "Alias": "akuam",
    "DisplayName": "Akua Mansa",
    "Type": "PERSONAL",
    "Plan": {
```

```
        "Stages": [
            {
                "DurationInMinutes": 5,
                "Targets": [
                    {
                        "ChannelTargetInfo": {
                            "ContactChannelId": "arn:aws:ssm-contacts:us-
east-2:111122223333:contact-channel/akuam/beb25840-5ac8-4644-95cc-7a8de390fa65",
                            "RetryIntervalInMinutes": 1
                        }
                    }
                ]
            },
            {
                "DurationInMinutes": 5,
                "Targets": [
                    {
                        "ChannelTargetInfo": {
                            "ContactChannelId": "arn:aws:ssm-contacts:us-
east-2:111122223333:contact-channel/akuam/49f3c24d-5f9f-4638-ae25-3f49e04229ad",
                            "RetryIntervalInMinutes": 1
                        }
                    }
                ]
            },
            {
                "DurationInMinutes": 5,
                "Targets": [
                    {
                        "ChannelTargetInfo": {
                            "ContactChannelId": "arn:aws:ssm-contacts:us-
east-2:111122223333:contact-channel/akuam/77d4f447-f619-4954-afff-85551e369c2a",
                            "RetryIntervalInMinutes": 1
                        }
                    }
                ]
            }
        ]
    }
}
```

Ejemplo 2: descripción de un plan de escalamiento

En el siguiente ejemplo de `get-contact`, se describe un plan de escalamiento.

```
aws ssm-contacts get-contact \
--contact-id "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
example_escalation"
```

Salida:

```
{
    "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
example_escalation",
    "Alias": "example_escalation",
    "DisplayName": "Example Escalation",
    "Type": "ESCALATION",
    "Plan": {
        "Stages": [
            {
                "DurationInMinutes": 5,
                "Targets": [
                    {
                        "ContactTargetInfo": {
                            "ContactId": "arn:aws:ssm-contacts:us-
east-2:111122223333:contact/akuam",
                            "IsEssential": true
                        }
                    }
                ]
            },
            {
                "DurationInMinutes": 5,
                "Targets": [
                    {
                        "ContactTargetInfo": {
                            "ContactId": "arn:aws:ssm-contacts:us-
east-2:111122223333:contact/alejr",
                            "IsEssential": false
                        }
                    }
                ]
            },
            {
                "DurationInMinutes": 0,
                "Targets": [
                    {
                        "ContactTargetInfo": {
```

```
                            "ContactId": "arn:aws:ssm-contacts:us-
east-2:111122223333:contact/anasi",
                            "IsEssential": false
                        }
                    }
                ]
            }
        ]
    }
}
```

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte GetContact en la Referencia de comandos de la AWS CLI.

`list-contact-channels`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-contact-channels`.

AWS CLI

Para enumerar los canales de contacto de un contacto

En el siguiente ejemplo de `list-contact-channels`, se enumeran los canales de contacto disponibles del contacto especificado.

```
aws ssm-contacts list-contact-channels \
    --contact-id "arn:aws:ssm-contacts:us-east-2:111122223333:contact/akuam"
```

Salida:

```
{
    [
        {
            "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
akuam",
            "Name": "akuas email",
            "Type": "EMAIL",
            "DeliveryAddress": {
                "SimpleAddress": "akuam@example.com"
            },
            "ActivationStatus": "NOT_ACTIVATED"
```

```
        },
        {
            "ContactChannelArn": "arn:aws:ssm-contacts:us-
east-2:111122223333:contact-channel/akuam/fc7405c4-46b2-48b7-87b2-93e2f225b90d",
            "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
akuam",
            "Name": "akuas sms",
            "Type": "SMS",
            "DeliveryAddress": {
                "SimpleAddress": "+15005550100"
            },
            "ActivationStatus": "ACTIVATED"
        }
    ]
}
```

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte ListContactChannels en la Referencia de comandos de la AWS CLI.

`list-contacts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-contacts`.

AWS CLI

Para enumerar todos los planes de escalamiento y los contactos

En el siguiente ejemplo de `list-contacts`, se enumeran los contactos y los planes de escalamiento de su cuenta.

```
aws ssm-contacts list-contacts
```

Salida:

```
{
    "Contacts": [
        {
            "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
akuam",
            "Alias": "akuam",
            "DisplayName": "Akua Mansa",
```

```
            "Type": "PERSONAL"
        },
        {
            "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
alejr",
            "Alias": "alejr",
            "DisplayName": "Alejandro Rosalez",
            "Type": "PERSONAL"
        },
        {
            "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
anasi",
            "Alias": "anasi",
            "DisplayName": "Ana Carolina Silva",
            "Type": "PERSONAL"
        },
        {
            "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
example_escalation",
            "Alias": "example_escalation",
            "DisplayName": "Example Escalation",
            "Type": "ESCALATION"
        }
    ]
}
```

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte ListContacts en la Referencia de comandos de la AWS CLI.

`list-engagements`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-engagements`.

AWS CLI

Para enumerar todas las interacciones

En el siguiente ejemplo de `list-engagements`, se enumeran las interacciones con los planes de escalamiento y los contactos. También puede enumerar las interacciones de un solo incidente.

```
aws ssm-contacts list-engagements
```

Salida:

```
{
    "Engagements": [
        {
            "EngagementArn": "arn:aws:ssm-contacts:us-
east-2:111122223333:engagement/akuam/91792571-0b53-4821-9f73-d25d13d9e529",
            "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
akuam",
            "Sender": "cli",
            "StartTime": "2021-05-18T20:37:50.300000+00:00"
        },
        {
            "EngagementArn": "arn:aws:ssm-contacts:us-
east-2:111122223333:engagement/akuam/78a29753-3674-4ac5-9f83-0468563567f0",
            "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
akuam",
            "Sender": "cli",
            "StartTime": "2021-05-18T18:40:26.666000+00:00"
        },
        {
            "EngagementArn": "arn:aws:ssm-contacts:us-
east-2:111122223333:engagement/
example_escalation/69e40ce1-8dbb-4d57-8962-5fbe7fc53356",
            "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
example_escalation",
            "Sender": "cli",
            "StartTime": "2021-05-18T18:25:41.151000+00:00"
        },
        {
            "EngagementArn": "arn:aws:ssm-contacts:us-
east-2:111122223333:engagement/akuam/607ced0e-e8fa-4ea7-8958-a237b8803f8f",
            "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
akuam",
            "Sender": "cli",
            "StartTime": "2021-05-18T18:20:58.093000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte ListEngagements en la Referencia de comandos de la AWS CLI.

`list-page-receipts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-page-receipts`.

AWS CLI

Para enumerar las recepciones de páginas

En el siguiente ejemplo de `command-name`, se indica si un contacto ha recibido o no una página.

```
aws ssm-contacts list-page-receipts \
    --page-id "arn:aws:ssm-contacts:us-east-2:111122223333:page/
akuam/94ea0c7b-56d9-46c3-b84a-a37c8b067ad3"
```

Salida:

```
{
    "Receipts": [
        {
            "ContactChannelArn": "arn:aws:ssm-contacts:us-
east-2:111122223333:contact-channel/akuam/fc7405c4-46b2-48b7-87b2-93e2f225b90d",
            "ReceiptType": "DELIVERED",
            "ReceiptInfo": "425440",
            "ReceiptTime": "2021-05-18T20:42:57.485000+00:00"
        },
        {
            "ContactChannelArn": "arn:aws:ssm-contacts:us-
east-2:111122223333:contact-channel/akuam/fc7405c4-46b2-48b7-87b2-93e2f225b90d",
            "ReceiptType": "READ",
            "ReceiptInfo": "425440",
            "ReceiptTime": "2021-05-18T20:42:57.907000+00:00"
        },
        {
            "ContactChannelArn": "arn:aws:ssm-contacts:us-
east-2:111122223333:contact-channel/akuam/fc7405c4-46b2-48b7-87b2-93e2f225b90d",
            "ReceiptType": "SENT",
            "ReceiptInfo": "SM6656c19132f1465f9c9c1123a5dde7c9",
            "ReceiptTime": "2021-05-18T20:40:52.962000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte ListPageReceipts en la Referencia de comandos de la AWS CLI.

`list-pages-by-contact`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-pages-by-contact`.

AWS CLI

Para enumerar las páginas por contacto

En el siguiente ejemplo de `list-pages-by-contact`, se muestran todas las páginas del contacto especificado.

```
aws ssm-contacts list-pages-by-contact \
    --contact-id "arn:aws:ssm-contacts:us-east-2:111122223333:contact/akuam"
```

Salida:

```
{
    "Pages": [
        {
            "PageArn": "arn:aws:ssm-contacts:us-east-2:111122223333:page/akuam/
ad0052bd-e606-498a-861b-25726292eb93",
            "EngagementArn": "arn:aws:ssm-contacts:us-
east-2:111122223333:engagement/akuam/78a29753-3674-4ac5-9f83-0468563567f0",
            "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
akuam",
            "Sender": "cli",
            "SentTime": "2021-05-18T18:43:29.301000+00:00",
            "DeliveryTime": "2021-05-18T18:43:55.265000+00:00",
            "ReadTime": "2021-05-18T18:43:55.708000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte ListPagesByContact en la Referencia de comandos de la AWS CLI.

`list-pages-by-engagement`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-pages-by-engagement`.

AWS CLI

Para enumerar las páginas de los canales de contacto iniciadas a partir de una interacción

En el siguiente ejemplo de `list-pages-by-engagement`, se enumeran las páginas que han aparecido al participar en el plan de interacción definido.

```
aws ssm-contacts list-pages-by-engagement \
    --engagement-id "arn:aws:ssm-contacts:us-east-2:111122223333:engagement/
akuam/78a29753-3674-4ac5-9f83-0468563567f0"
```

Salida:

```
{
    "Pages": [
        {
            "PageArn": "arn:aws:ssm-contacts:us-east-2:111122223333:page/akuam/
ad0052bd-e606-498a-861b-25726292eb93",
            "EngagementArn": "arn:aws:ssm-contacts:us-
east-2:111122223333:engagement/akuam/78a29753-3674-4ac5-9f83-0468563567f0",
            "ContactArn": "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
akuam",
            "Sender": "cli",
            "SentTime": "2021-05-18T18:40:27.245000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte ListPagesByEngagement en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un contacto

En el siguiente ejemplo `list-tags-for-resource`, se enumeran las etiquetas del contacto especificado.

```
aws ssm-contacts list-tags-for-resource \
    --resource-arn "arn:aws:ssm-contacts:us-east-1:111122223333:contact/akuam"
```

Salida:

```
{
    "Tags": [
        {
            "Key": "group1",
            "Value": "1"
        }
    ]
}
```

Para obtener más información, consulte Tagging en la Guía del usuario de Incident Manager.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-contact-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-contact-policy`.

AWS CLI

Para compartir un contacto y sus interacciones

En el siguiente ejemplo de `put-contact-policy`, se agrega una política de recursos al contacto Akua que comparte el contacto y las interacciones relacionadas con la entidad principal.

```
aws ssm-contacts put-contact-policy \
    --contact-arn "arn:aws:ssm-contacts:us-east-1:111122223333:contact/akuam" \
    --policy "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"ExampleResourcePolicy\",\"Action\":[\"ssm-contacts:GetContact\",\"ssm-
contacts:StartEngagement\",\"ssm-contacts:DescribeEngagement\",\"ssm-
```

```
contacts:ListPagesByEngagement\",\"ssm-contacts:StopEngagement\"],
\"Principal\":{\"AWS\":\"222233334444\"},\"Effect\":\"Allow\",\"Resource
\":[\"arn:aws:ssm-contacts:*:111122223333:contact\/akuam\",\"arn:aws:ssm-
contacts:*:111122223333:engagement\/akuam\/*\"]}]}"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with shared contacts and response plans en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte PutContactPolicy en la Referencia de comandos de la AWS CLI.

`send-activation-code`

En el siguiente ejemplo de código, se muestra cómo utilizar `send-activation-code`.

AWS CLI

Para enviar un código de activación

En el siguiente ejemplo de `send-activation-code`, se envía un código de activación y un mensaje al canal de contacto especificado.

```
aws ssm-contacts send-activation-code \
    --contact-channel-id "arn:aws:ssm-contacts:us-east-1:111122223333:contact-
channel/akuam/8ddae2d1-12c8-4e45-b852-c8587266c400"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener más información sobre la API, consulte SendActivationCode en la Referencia de comandos de la AWS CLI.

`start-engagement`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-engagement`.

AWS CLI

Ejemplo 1: paginación de los canales de contacto de un contacto

Las siguientes páginas de `start-engagement` son los canales de contacto del contacto. Los campos sender, subject, public-subject y public-content se pueden rellenar libremente. Incident Manager envía el contenido de subject y content a los canales de contacto VOICE o EMAIL proporcionados. Incident Manager envía el contenido de public-subject y public-content a los canales de contacto SMS proporcionados. El contenido de sender se utiliza para saber quién inició la interacción.

```
aws ssm-contacts start-engagement \
    --contact-id  "arn:aws:ssm-contacts:us-east-2:111122223333:contact/akuam" \
    --sender "cli" \
    --subject "cli-test" \
    --content "Testing engagements via CLI" \
    --public-subject "cli-test" \
    --public-content "Testing engagements va CLI"
```

Salida:

```
{
    "EngagementArn": "arn:aws:ssm-contacts:us-east-2:111122223333:engagement/
akuam/607ced0e-e8fa-4ea7-8958-a237b8803f8f"
}
```

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

Ejemplo 2: paginación de un contacto en el plan de escalamiento proporcionado

En el siguiente ejemplo de `start-engagement`, se interactúa con el contacto a través de un plan de escalamiento. Cada contacto se pagina de acuerdo con su plan de interacción.

```
aws ssm-contacts start-engagement \
    --contact-id  "arn:aws:ssm-contacts:us-east-2:111122223333:contact/
example_escalation" \
    --sender "cli" \
    --subject "cli-test" \
    --content "Testing engagements via CLI" \
    --public-subject "cli-test" \
    --public-content "Testing engagements va CLI"
```

Salida:

```
{
```

```
    "EngagementArn": "arn:aws:ssm-contacts:us-east-2:111122223333:engagement/
example_escalation/69e40ce1-8dbb-4d57-8962-5fbe7fc53356"
}
```

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte StartEngagement en la Referencia de comandos de la AWS CLI.

`stop-engagement`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-engagement`.

AWS CLI

Para detener una interacción

En el siguiente ejemplo de `stop-engagement`, se impide que una interacción pagine más contactos y canales de contacto.

```
aws ssm-contacts stop-engagement \
    --engagement-id "arn:aws:ssm-contacts:us-east-2:111122223333:engagement/
example_escalation/69e40ce1-8dbb-4d57-8962-5fbe7fc53356"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte StopEngagement en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para etiquetar un contacto

En el siguiente ejemplo de `tag-resource`, se etiqueta un contacto especificado con el par clave-valor de etiquetas proporcionado.

```
aws ssm-contacts tag-resource \
    --resource-arn "arn:aws:ssm-contacts:us-east-1:111122223333:contact/akuam" \
    --tags '[{"Key":"group1","Value":"1"}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging en la Guía del usuario de Incident Manager.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar etiquetas de un contacto

En el siguiente ejemplo de `untag-resource`, se elimina la etiqueta group1 del contacto especificado.

```
aws ssm-contacts untag-resource \
    --resource-arn "arn:aws:ssm-contacts:us-east-1:111122223333:contact/akuam" \
    --tag-keys "group1"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging en la Guía del usuario de Incident Manager.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-contact-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-contact-channel`.

AWS CLI

Para actualizar un canal de contacto

En el siguiente ejemplo de `update-contact-channel`, se actualiza el nombre y la dirección de entrega de un canal de contacto.

```
aws ssm-contacts update-contact-channel \
    --contact-channel-id "arn:aws:ssm-contacts:us-east-2:111122223333:contact-channel/akuam/49f3c24d-5f9f-4638-ae25-3f49e04229ad" \
    --name "akuas voice channel" \
    --delivery-address '{"SimpleAddress": "+15005550198"}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte UpdateContactChannel en la Referencia de comandos de la AWS CLI.

`update-contact`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-contact`.

AWS CLI

Para actualizar el plan de interacción del contacto

En el siguiente ejemplo de `update-contact`, se actualiza el plan de interacción del contacto Akua para incluir los tres tipos de canales de contacto. Esto se hace después de crear los canales de contacto para Akua.

```
aws ssm-contacts update-contact \
    --contact-id "arn:aws:ssm-contacts:us-east-2:111122223333:contact/akuam" \
    --plan '{"Stages": [{"DurationInMinutes": 5, "Targets": [{"ChannelTargetInfo":
 {"ContactChannelId": "arn:aws:ssm-contacts:us-east-2:111122223333:contact-channel/akuam/beb25840-5ac8-4644-95cc-7a8de390fa65","RetryIntervalInMinutes":
 1 }}]}, {"DurationInMinutes": 5, "Targets": [{"ChannelTargetInfo":
{"ContactChannelId": "arn:aws:ssm-contacts:us-east-2:111122223333:contact-channel/akuam/49f3c24d-5f9f-4638-ae25-3f49e04229ad", "RetryIntervalInMinutes": 1}}]},
 {"DurationInMinutes": 5, "Targets": [{"ChannelTargetInfo": {"ContactChannelId":
 "arn:aws:ssm-contacts:us-east-2:111122223333:contact-channel/akuam/77d4f447-f619-4954-afff-85551e369c2a","RetryIntervalInMinutes": 1 }}]}]}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Contacts en la Guía del usuario de Incident Manager.

- Para obtener información sobre la API, consulte UpdateContact en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon Inspector que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando la AWS Command Line Interface con Amazon Inspector.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-attributes-to-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-attributes-to-findings`.

AWS CLI

Para añadir atributos a los hallazgos

El siguiente comando `add-attribute-to-finding` asigna un atributo con la clave de `Example` y el valor de `example` al resultado con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/template/0-8l1VIE0D/run/0-Z02cjjug/finding/0-T8yM9mEU`:

```
aws inspector add-attributes-to-findings --finding-arns arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/template/0-8l1VIE0D/run/0-Z02cjjug/finding/0-T8yM9mEU --attributes key=Example,value=example
```

Salida:

```
{
    "failedItems": {}
}
```

Para obtener más información, consulte Amazon Inspector Findings en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte AddAttributesToFindings en la Referencia de comandos de la AWS CLI.

`associate-member`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-member`.

AWS CLI

Ejemplo: asociación de una cuenta de AWS con un administrador delegado de Amazon Inspector

En el siguiente ejemplo de `associate-member`, se asocia una cuenta de AWS con un administrador delegado de Amazon Inspector.

```
aws inspector2 associate-member \
    --account-id 123456789012
```

Salida:

```
{
    "accountId": "123456789012"
}
```

Para obtener más información, consulte Administración de varias cuentas en Amazon Inspector con AWS Organizations en la Guía del usuario de Amazon Inspector.

- Para obtener información sobre la API, consulte AssociateMember en la Referencia de comandos de la AWS CLI.

`create-assessment-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-assessment-target`.

AWS CLI

Para crear un objetivo de evaluación

El siguiente comando `create-assessment-target` crea un objetivo de evaluación denominado `ExampleAssessmentTarget` mediante el grupo de recursos con el ARN `arn:aws:inspector:us-west-2:123456789012:resourcegroup/0-AB6DMKnv`:

```
aws inspector create-assessment-target --assessment-target-
name ExampleAssessmentTarget --resource-group-arn arn:aws:inspector:us-
west-2:123456789012:resourcegroup/0-AB6DMKnv
```

Salida:

```
{
    "assessmentTargetArn": "arn:aws:inspector:us-west-2:123456789012:target/0-
nvgVhaxX"
}
```

Para obtener más información, consulte Amazon Inspector Assessment Targets en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte CreateAssessmentTarget en la Referencia de comandos de la AWS CLI.

`create-assessment-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-assessment-template`.

AWS CLI

Para crear una plantilla de evaluación

El siguiente comando `create-assessment-template` crea una plantilla de evaluación llamada `ExampleAssessmentTemplate` para el objetivo de evaluación con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX`:

```
aws inspector create-assessment-template --assessment-target-
arn arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX --assessment-
template-name ExampleAssessmentTemplate --duration-in-seconds 180 --rules-package-
```

```
arns arn:aws:inspector:us-west-2:758058086616:rulespackage/0-9hgA516p --user-
attributes-for-findings key=ExampleTag,value=examplevalue
```

Salida:

```
{
    "assessmentTemplateArn": "arn:aws:inspector:us-west-2:123456789012:target/0-
nvgVhaxX/template/0-it5r2S4T"
}
```

Para obtener más información, consulte Amazon Inspector Assessment Templates and Assessment Runs en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte CreateAssessmentTemplate en la Referencia de comandos de la AWS CLI.

`create-filter`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-filter`.

AWS CLI

Para crear un filtro

En el siguiente ejemplo de `create-filter`, se crea una regla de supresión que omite los resultados del tipo de instancia de ECR.

```
aws inspector2 create-filter \
    --name "ExampleSuppressionRuleECR" \
    --description "This suppression rule omits ECR instance type findings" \
    --action SUPPRESS \
    --filter-criteria 'resourceType=[{comparison="EQUALS",
 value="AWS_ECR_INSTANCE"}]'
```

Salida:

```
{
    "arn": "arn:aws:inspector2:us-west-2:123456789012:owner/o-EXAMPLE222/filter/
EXAMPLE444444444"
}
```

Para obtener más información, consulte Filtering Amazon Inspector findings en la Guía del usuario de Amazon Inspector.

- Para obtener información sobre la API, consulte CreateFilter en la Referencia de comandos de la AWS CLI.

`create-findings-report`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-findings-report`.

AWS CLI

Para crear un informe de resultados

El siguiente ejemplo de `create-findings-report`, se crea un informe de resultados.

```
aws inspector2 create-findings-report \
    --report-format CSV \
    --s3-destination bucketName=inspector-sbom-123456789012,keyPrefix=sbom-
key,kmsKeyArn=arn:aws:kms:us-west-2:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE33333 \
    --filter-criteria '{"ecrImageRepositoryName":
[{"comparison":"EQUALS","value":"debian"}]}'
```

Salida:

```
{
    "reportId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333"
}
```

Para obtener más información, consulte Managing findings in Amazon Inspector en la Guía del usuario de Amazon Inspector.

- Para obtener información sobre la API, consulte CreateFindingsReport en la Referencia de comandos de la AWS CLI.

`create-resource-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-resource-group`.

AWS CLI

Para crear un grupo de recursos

El siguiente comando `create-resource-group` crea un grupo de recursos con la clave de etiqueta `Name` y el valor `example`:

```
aws inspector create-resource-group --resource-group-tags key=Name,value=example
```

Salida:

```
{
   "resourceGroupArn": "arn:aws:inspector:us-west-2:123456789012:resourcegroup/0-
AB6DMKnv"
}
```

Para obtener más información, consulte Amazon Inspector Assessment Targets en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte CreateResourceGroup en la Referencia de comandos de la AWS CLI.

`create-sbom-export`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-sbom-export`.

AWS CLI

Para crear un informe de lista de componentes de software (SBOM

En el siguiente ejemplo de `create-sbom-export`, se crea un informe de lista de componentes de software (SBOM).

```
aws inspector2 create-sbom-export \
    --report-format SPDX_2_3 \
    --resource-filter-criteria
 'ecrRepositoryName=[{comparison="EQUALS",value="debian"}]' \
    --s3-destination bucketName=inspector-sbom-123456789012,keyPrefix=sbom-
key,kmsKeyArn=arn:aws:kms:us-west-2:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE33333
```

Salida:

```
{
    "reportId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333"
}
```

Para obtener más información, consulte Exporting SBOMs with Amazon Inspector en la Guía del usuario de Amazon Inspector.

- Para obtener información sobre la API, consulte CreateSbomExport en la Referencia de comandos de la AWS CLI.

`delete-assessment-run`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-assessment-run`.

AWS CLI

Para eliminar una ejecución de evaluación

El siguiente comando `delete-assessment-run` elimina la ejecución de evaluación con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX/template/0-it5r2S4T/run/0-11LMTAVe`:

```
aws inspector delete-assessment-run --assessment-run-arn arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX/template/0-it5r2S4T/run/0-11LMTAVe
```

Para obtener más información, consulte Amazon Inspector Assessment Templates and Assessment Runs en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte DeleteAssessmentRun en la Referencia de comandos de la AWS CLI.

`delete-assessment-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-assessment-target`.

AWS CLI

Para eliminar un objetivo de evaluación

El siguiente comando `delete-assessment-target` elimina el objetivo de evaluación con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq`:

```
aws inspector delete-assessment-target --assessment-target-arn arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq
```

Para obtener más información, consulte Amazon Inspector Assessment Targets en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte DeleteAssessmentTarget en la Referencia de comandos de la AWS CLI.

`delete-assessment-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-assessment-template`.

AWS CLI

Para eliminar una plantilla de evaluación

El siguiente comando `delete-assessment-template` elimina la plantilla de evaluación con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX/template/0-it5r2S4T`:

```
aws inspector delete-assessment-template --assessment-template-arn arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX/template/0-it5r2S4T
```

Para obtener más información, consulte Amazon Inspector Assessment Templates and Assessment Runs en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte DeleteAssessmentTemplate en la Referencia de comandos de la AWS CLI.

`delete-filter`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-filter`.

AWS CLI

Para eliminar un filtro

En el siguiente ejemplo de `delete-filter` se elimina un filtro.

```
aws inspector2 delete-filter \
```

```
    --arn "arn:aws:inspector2:us-west-2:123456789012:owner/o-EXAMPLE222/filter/
EXAMPLE444444444"
```

Salida:

```
{
    "arn": "arn:aws:inspector2:us-west-2:123456789012:owner/o-EXAMPLE222/filter/
EXAMPLE444444444"
}
```

Para obtener más información, consulte Filtering Amazon Inspector findings en la Guía del usuario de Amazon Inspector.

- Para obtener información sobre la API, consulte DeleteFilter en la Referencia de comandos de la AWS CLI.

`describe-assessment-runs`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-assessment-runs`.

AWS CLI

Para describir las ejecuciones de evaluación

El siguiente comando `describe-assessment-run` describe la ejecución de evaluación con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/template/0-4r1V2mAw/run/0-MKkpXXPE`:

```
aws inspector describe-assessment-runs --assessment-run-arns arn:aws:inspector:us-
west-2:123456789012:target/0-0kFIPusq/template/0-4r1V2mAw/run/0-MKkpXXPE
```

Salida:

```
{
        "assessmentRuns": [
          {
                "arn": "arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/
template/0-4r1V2mAw/run/0-MKkpXXPE",
                "assessmentTemplateArn": "arn:aws:inspector:us-
west-2:123456789012:target/0-0kFIPusq/template/0-4r1V2mAw",
                "completedAt": 1458680301.4,
                "createdAt": 1458680170.035,
```

```
                "dataCollected": true,
                "durationInSeconds": 3600,
                "name": "Run 1 for ExampleAssessmentTemplate",
                "notifications": [],
                "rulesPackageArns": [
                  "arn:aws:inspector:us-west-2:758058086616:rulespackage/0-X1KXtawP"
                ],
                "startedAt": 1458680170.161,
                "state": "COMPLETED",
                "stateChangedAt": 1458680301.4,
                "stateChanges": [
                  {
                        "state": "CREATED",
                        "stateChangedAt": 1458680170.035
                  },
                  {
                        "state": "START_DATA_COLLECTION_PENDING",
                        "stateChangedAt": 1458680170.065
                  },
                  {
                        "state": "START_DATA_COLLECTION_IN_PROGRESS",
                        "stateChangedAt": 1458680170.096
                  },
                  {
                        "state": "COLLECTING_DATA",
                        "stateChangedAt": 1458680170.161
                  },
                  {
                        "state": "STOP_DATA_COLLECTION_PENDING",
                        "stateChangedAt": 1458680239.883
                  },
                  {
                        "state": "DATA_COLLECTED",
                        "stateChangedAt": 1458680299.847
                  },
                  {
                        "state": "EVALUATING_RULES",
                        "stateChangedAt": 1458680300.099
                  },
                  {
                        "state": "COMPLETED",
                        "stateChangedAt": 1458680301.4
                  }
                ],
```

```
                "userAttributesForFindings": []
            }
        ],
        "failedItems": {}
}
```

Para obtener más información, consulte Amazon Inspector Assessment Templates and Assessment Runs en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte DescribeAssessmentRuns en la Referencia de comandos de la AWS CLI.

`describe-assessment-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-assessment-targets`.

AWS CLI

Para describir los objetivos de evaluación

El siguiente comando `describe-assessment-targets` describe el objetivo de evaluación con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq`:

```
aws inspector describe-assessment-targets --assessment-target-
arns arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq
```

Salida:

```
{
      "assessmentTargets": [
        {
              "arn": "arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq",
              "createdAt": 1458074191.459,
              "name": "ExampleAssessmentTarget",
              "resourceGroupArn": "arn:aws:inspector:us-
west-2:123456789012:resourcegroup/0-PyGXopAI",
              "updatedAt": 1458074191.459
        }
      ],
      "failedItems": {}
}
```

Para obtener más información, consulte Amazon Inspector Assessment Targets en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte DescribeAssessmentTargets en la Referencia de comandos de la AWS CLI.

`describe-assessment-templates`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-assessment-templates`.

AWS CLI

Para describir las plantillas de evaluación

El siguiente comando `describe-assessment-templates` describe la plantilla de evaluación con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/template/0-4r1V2mAw`:

```
aws inspector describe-assessment-templates --assessment-template-
arns arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/template/0-4r1V2mAw
```

Salida:

```
{
      "assessmentTemplates": [
        {
              "arn": "arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/
template/0-4r1V2mAw",
              "assessmentTargetArn": "arn:aws:inspector:us-
west-2:123456789012:target/0-0kFIPusq",
              "createdAt": 1458074191.844,
              "durationInSeconds": 3600,
              "name": "ExampleAssessmentTemplate",
              "rulesPackageArns": [
                "arn:aws:inspector:us-west-2:758058086616:rulespackage/0-X1KXtawP"
              ],
              "userAttributesForFindings": []
        }
      ],
      "failedItems": {}
}
```

Para obtener más información, consulte Amazon Inspector Assessment Templates and Assessment Runs en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte DescribeAssessmentTemplates en la Referencia de comandos de la AWS CLI.

`describe-cross-account-access-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cross-account-access-role`.

AWS CLI

Para describir el rol de acceso entre cuentas

El siguiente comando `describe-cross-account-access-role` describe el rol de IAM que permite a Amazon Inspector obtener acceso a su cuenta de AWS:

```
aws inspector describe-cross-account-access-role
```

Salida:

```
{
        "registeredAt": 1458069182.826,
        "roleArn": "arn:aws:iam::123456789012:role/inspector",
        "valid": true
}
```

Para obtener más información, consulte Setting up Amazon Inspector en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte DescribeCrossAccountAccessRole en la Referencia de comandos de la AWS CLI.

`describe-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-findings`.

AWS CLI

Para describir los hallazgos

El siguiente comando `describe-findings` describe el hallazgo con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/template/0-4r1V2mAw/run/0-MKkpXXPE/finding/0-HwPnsDm4`:

```
aws inspector describe-findings --finding-arns arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/template/0-4r1V2mAw/run/0-MKkpXXPE/finding/0-HwPnsDm4
```

Salida:

```
{
      "failedItems": {},
      "findings": [
        {
              "arn": "arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/
template/0-4r1V2mAw/run/0-MKkpXXPE/finding/0-HwPnsDm4",
              "assetAttributes": {
                "ipv4Addresses": [],
                "schemaVersion": 1
              },
              "assetType": "ec2-instance",
              "attributes": [],
              "confidence": 10,
              "createdAt": 1458680301.37,
              "description": "Amazon Inspector did not find any potential security
 issues during this assessment.",
              "indicatorOfCompromise": false,
              "numericSeverity": 0,
              "recommendation": "No remediation needed.",
              "schemaVersion": 1,
              "service": "Inspector",
              "serviceAttributes": {
                "assessmentRunArn": "arn:aws:inspector:us-
west-2:123456789012:target/0-0kFIPusq/template/0-4r1V2mAw/run/0-MKkpXXPE",
                "rulesPackageArn": "arn:aws:inspector:us-
west-2:758058086616:rulespackage/0-X1KXtawP",
                "schemaVersion": 1
              },
              "severity": "Informational",
              "title": "No potential security issues found",
              "updatedAt": 1458680301.37,
              "userAttributes": []
        }
```

```
      ]
}
```

Para obtener más información, consulte Amazon Inspector Findings en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte DescribeFindings en la Referencia de comandos de la AWS CLI.

`describe-resource-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-resource-groups`.

AWS CLI

Para describir los grupos de recursos

El siguiente comando `describe-resource-groups` describe el grupo de recursos con el ARN `arn:aws:inspector:us-west-2:123456789012:resourcegroup/0-PyGXopAI`:

```
aws inspector describe-resource-groups --resource-group-arns arn:aws:inspector:us-west-2:123456789012:resourcegroup/0-PyGXopAI
```

Salida:

```
{
      "failedItems": {},
      "resourceGroups": [
        {
              "arn": "arn:aws:inspector:us-west-2:123456789012:resourcegroup/0-PyGXopAI",
              "createdAt": 1458074191.098,
              "tags": [
                {
                      "key": "Name",
                      "value": "example"
                }
              ]
        }
      ]
}
```

Para obtener más información, consulte Amazon Inspector Assessment Targets en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte DescribeResourceGroups en la Referencia de comandos de la AWS CLI.

`describe-rules-packages`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-rules-packages`.

AWS CLI

Para describir paquetes de reglas

El siguiente comando `describe-rules-packages` describe el paquete de reglas con el ARN `arn:aws:inspector:us-west-2:758058086616:rulespackage/0-9hgA516p`:

```
aws inspector describe-rules-packages --rules-package-arns arn:aws:inspector:us-
west-2:758058086616:rulespackage/0-9hgA516p
```

Salida:

```
{
      "failedItems": {},
      "rulesPackages": [
        {
              "arn": "arn:aws:inspector:us-
west-2:758058086616:rulespackage/0-9hgA516p",
              "description": "The rules in this package help verify whether the EC2
 instances in your application are exposed to Common Vulnerabilities and
              Exposures (CVEs). Attacks can exploit unpatched vulnerabilities to
 compromise the confidentiality, integrity, or availability of your service
              or data. The CVE system provides a reference for publicly known
 information security vulnerabilities and exposures. For more information, see
              [https://cve.mitre.org/](https://cve.mitre.org/). If a particular CVE
 appears in one of the produced Findings at the end of a completed
              Inspector assessment, you can search [https://cve.mitre.org/](https://
cve.mitre.org/) using the CVE's ID (for example, \"CVE-2009-0021\") to
              find detailed information about this CVE, its severity, and how to
 mitigate it. ",
              "name": "Common Vulnerabilities and Exposures",
              "provider": "Amazon Web Services, Inc.",
```

```
            "version": "1.1"
        }
      ]
}
```

Para obtener más información, consulte Amazon Inspector Rules Packages and Rules en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte DescribeRulesPackages en la Referencia de comandos de la AWS CLI.

`disassociate-member`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-member`.

AWS CLI

Ejemplo: asociación de una cuenta de miembro de un administrador delegado de Amazon Inspector

En el siguiente ejemplo de `disassociate-member`, se anula la asociación de una cuenta de AWS de un administrador delegado de Amazon Inspector.

```
aws inspector2 disassociate-member \
    --account-id 123456789012
```

Salida:

```
{
    "accountId": "123456789012"
}
```

Para obtener más información, consulte Administración de varias cuentas en Amazon Inspector con AWS Organizations en la Guía del usuario de Amazon Inspector.

- Para obtener información sobre la API, consulte DisassociateMember en la Referencia de comandos de la AWS CLI.

`get-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-configuration`.

AWS CLI

Para obtener la configuración de los análisis de Inspector

El siguiente ejemplo `get-configuration` obtiene la configuración de los análisis de Inspector.

```
aws inspector2 get-configuration
```

Salida:

```
{
    "ec2Configuration": {
        "scanModeState": {
            "scanMode": "EC2_HYBRID",
            "scanModeStatus": "SUCCESS"
        }
    },
    "ecrConfiguration": {
        "rescanDurationState": {
            "pullDateRescanDuration": "DAYS_90",
            "rescanDuration": "DAYS_30",
            "status": "SUCCESS",
            "updatedAt": "2024-05-14T21:16:20.237000+00:00"
        }
     }
}
```

Para obtener más información, consulte Automated resource scanning with Amazon Inspector en la Guía del usuario de Amazon Inspector.

- Para obtener información sobre la API, consulte GetConfiguration en la Referencia de comandos de la AWS CLI.

`get-member`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-member`.

AWS CLI

Ejemplo: obtención de información de los miembros de la organización

aws inspector2 get-member --account-id 123456789012

Salida:

```
{
        "member": {
        "accountId": "123456789012",
        "delegatedAdminAccountId": "123456789012",
        "relationshipStatus": "ENABLED",
        "updatedAt": "2023-09-11T09:57:20.520000-07:00"
    }
}
```

Para obtener más información, consulte Administración de varias cuentas en Amazon Inspector con AWS Organizations en la Guía del usuario de Amazon Inspector.

- Para obtener detalles sobre la API, consulte GetMember en la Referencia de comandos de la AWS CLI.

`get-telemetry-metadata`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-telemetry-metadata`.

AWS CLI

Para obtener los metadatos de telemetría

El siguiente comando `get-telemetry-metadata` genera información sobre los datos que se recopilan para la ejecución de evaluación con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/template/0-4r1V2mAw/run/0-MKkpXXPE`:

```
aws inspector get-telemetry-metadata --assessment-run-arn arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/template/0-4r1V2mAw/run/0-MKkpXXPE
```

Salida:

```
{
      "telemetryMetadata": [
        {
              "count": 2,
              "dataSize": 345,
              "messageType": "InspectorDuplicateProcess"
        },
        {
```

```
            "count": 3,
            "dataSize": 255,
            "messageType": "InspectorTimeEventMsg"
        },
        {
            "count": 4,
            "dataSize": 1082,
            "messageType": "InspectorNetworkInterface"
        },
        {
            "count": 2,
            "dataSize": 349,
            "messageType": "InspectorDnsEntry"
        },
        {
            "count": 11,
            "dataSize": 2514,
            "messageType": "InspectorDirectoryInfoMsg"
        },
        {
            "count": 1,
            "dataSize": 179,
            "messageType": "InspectorTcpV6ListeningPort"
        },
        {
            "count": 101,
            "dataSize": 10949,
            "messageType": "InspectorTerminal"
        },
        {
            "count": 26,
            "dataSize": 5916,
            "messageType": "InspectorUser"
        },
        {
            "count": 282,
            "dataSize": 32148,
            "messageType": "InspectorDynamicallyLoadedCodeModule"
        },
        {
            "count": 18,
            "dataSize": 10172,
            "messageType": "InspectorCreateProcess"
        },
```

```
        {
              "count": 3,
              "dataSize": 8001,
              "messageType": "InspectorProcessPerformance"
        },
        {
              "count": 1,
              "dataSize": 360,
              "messageType": "InspectorOperatingSystem"
        },
        {
              "count": 6,
              "dataSize": 546,
              "messageType": "InspectorStopProcess"
        },
        {
              "count": 1,
              "dataSize": 1553,
              "messageType": "InspectorInstanceMetaData"
        },
        {
              "count": 2,
              "dataSize": 434,
              "messageType": "InspectorTcpV4Connection"
        },
        {
              "count": 474,
              "dataSize": 2960322,
              "messageType": "InspectorPackageInfo"
        },
        {
              "count": 3,
              "dataSize": 2235,
              "messageType": "InspectorSystemPerformance"
        },
        {
              "count": 105,
              "dataSize": 46048,
              "messageType": "InspectorCodeModule"
        },
        {
              "count": 1,
              "dataSize": 182,
              "messageType": "InspectorUdpV6ListeningPort"
```

```
        },
        {
              "count": 2,
              "dataSize": 371,
              "messageType": "InspectorUdpV4ListeningPort"
        },
        {
              "count": 18,
              "dataSize": 8362,
              "messageType": "InspectorKernelModule"
        },
        {
              "count": 29,
              "dataSize": 48788,
              "messageType": "InspectorConfigurationInfo"
        },
        {
              "count": 1,
              "dataSize": 79,
              "messageType": "InspectorMonitoringStart"
        },
        {
              "count": 5,
              "dataSize": 0,
              "messageType": "InspectorSplitMsgBegin"
        },
        {
              "count": 51,
              "dataSize": 4593,
              "messageType": "InspectorGroup"
        },
        {
              "count": 1,
              "dataSize": 184,
              "messageType": "InspectorTcpV4ListeningPort"
        },
        {
              "count": 1159,
              "dataSize": 3146579,
              "messageType": "Total"
        },
        {
              "count": 5,
              "dataSize": 0,
```

```
                "messageType": "InspectorSplitMsgEnd"
            },
            {
                "count": 1,
                "dataSize": 612,
                "messageType": "InspectorLoadImageInProcess"
            }
        ]
}
```

- Para obtener información sobre la API, consulte GetTelemetryMetadata en la Referencia de comandos de la AWS CLI.

`list-account-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-account-permissions`.

AWS CLI

Para enumerar los permisos de la cuenta

En el siguiente ejemplo de `list-account-permissions`, se enumeran los permisos de la cuenta.

```
aws inspector2 list-account-permissions
```

Salida:

```
{
    "permissions": [
        {
            "operation": "ENABLE_SCANNING",
            "service": "ECR"
        },
        {
            "operation": "DISABLE_SCANNING",
            "service": "ECR"
        },
        {
            "operation": "ENABLE_REPOSITORY",
            "service": "ECR"
```

```
        },
        {
            "operation": "DISABLE_REPOSITORY",
            "service": "ECR"
        },
        {
            "operation": "ENABLE_SCANNING",
            "service": "EC2"
        },
        {
            "operation": "DISABLE_SCANNING",
            "service": "EC2"
        },
        {
            "operation": "ENABLE_SCANNING",
            "service": "LAMBDA"
        },
        {
            "operation": "DISABLE_SCANNING",
            "service": "LAMBDA"
        }
    ]
}
```

Para obtener más información, consulte Identity and Access Management for Amazon Inspector en la Guía del usuario de Amazon Inspector.

- Para obtener información sobre la API, consulte ListAccountPermissions en la Referencia de comandos de la AWS CLI.

`list-assessment-run-agents`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-assessment-run-agents`.

AWS CLI

Para enumerar los agentes de ejecución de evaluación

En el siguiente comando `list-assessment-run-agents`, se enumeran los agentes de la ejecución de evaluación con el ARN especificado.

```
aws inspector list-assessment-run-agents \
```

```
    --assessment-run-arn arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/
template/0-4r1V2mAw/run/0-MKkpXXPE
```

Salida:

```
{
    "assessmentRunAgents": [
        {
            "agentHealth": "HEALTHY",
            "agentHealthCode": "HEALTHY",
            "agentId": "i-49113b93",
            "assessmentRunArn": "arn:aws:inspector:us-
west-2:123456789012:target/0-0kFIPusq/template/0-4r1V2mAw/run/0-MKkpXXPE",
            "telemetryMetadata": [
                {
                    "count": 2,
                    "dataSize": 345,
                    "messageType": "InspectorDuplicateProcess"
                },
                {
                    "count": 3,
                    "dataSize": 255,
                    "messageType": "InspectorTimeEventMsg"
                },
                {
                    "count": 4,
                    "dataSize": 1082,
                    "messageType": "InspectorNetworkInterface"
                },
                {
                    "count": 2,
                    "dataSize": 349,
                    "messageType": "InspectorDnsEntry"
                },
                {
                    "count": 11,
                    "dataSize": 2514,
                    "messageType": "InspectorDirectoryInfoMsg"
                },
                {
                    "count": 1,
                    "dataSize": 179,
                    "messageType": "InspectorTcpV6ListeningPort"
```

```
                },
                {
                    "count": 101,
                    "dataSize": 10949,
                    "messageType": "InspectorTerminal"
                },
                {
                    "count": 26,
                    "dataSize": 5916,
                    "messageType": "InspectorUser"
                },
                {
                    "count": 282,
                    "dataSize": 32148,
                    "messageType": "InspectorDynamicallyLoadedCodeModule"
                },
                {
                    "count": 18,
                    "dataSize": 10172,
                    "messageType": "InspectorCreateProcess"
                },
                {
                    "count": 3,
                    "dataSize": 8001,
                    "messageType": "InspectorProcessPerformance"
                },
                {
                    "count": 1,
                    "dataSize": 360,
                    "messageType": "InspectorOperatingSystem"
                },
                {
                    "count": 6,
                    "dataSize": 546,
                    "messageType": "InspectorStopProcess"
                },
                {
                    "count": 1,
                    "dataSize": 1553,
                    "messageType": "InspectorInstanceMetaData"
                },
                {
                    "count": 2,
                    "dataSize": 434,
```

```
            "messageType": "InspectorTcpV4Connection"
        },
        {
            "count": 474,
            "dataSize": 2960322,
            "messageType": "InspectorPackageInfo"
        },
        {
            "count": 3,
            "dataSize": 2235,
            "messageType": "InspectorSystemPerformance"
        },
        {
            "count": 105,
            "dataSize": 46048,
            "messageType": "InspectorCodeModule"
        },
        {
            "count": 1,
            "dataSize": 182,
            "messageType": "InspectorUdpV6ListeningPort"
        },
        {
            "count": 2,
            "dataSize": 371,
            "messageType": "InspectorUdpV4ListeningPort"
        },
        {
            "count": 18,
            "dataSize": 8362,
            "messageType": "InspectorKernelModule"
        },
        {
            "count": 29,
            "dataSize": 48788,
            "messageType": "InspectorConfigurationInfo"
        },
        {
            "count": 1,
            "dataSize": 79,
            "messageType": "InspectorMonitoringStart"
        },
        {
            "count": 5,
```

```
                    "dataSize": 0,
                    "messageType": "InspectorSplitMsgBegin"
                },
                {
                    "count": 51,
                    "dataSize": 4593,
                    "messageType": "InspectorGroup"
                },
                {
                    "count": 1,
                    "dataSize": 184,
                    "messageType": "InspectorTcpV4ListeningPort"
                },
                {
                    "count": 1159,
                    "dataSize": 3146579,
                    "messageType": "Total"
                },
                {
                    "count": 5,
                    "dataSize": 0,
                    "messageType": "InspectorSplitMsgEnd"
                },
                {
                    "count": 1,
                    "dataSize": 612,
                    "messageType": "InspectorLoadImageInProcess"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte AWS Agents en la Guía del usuario de Amazon Inspector.

- Para obtener información sobre la API, consulte ListAssessmentRunAgents en la Referencia de comandos de la AWS CLI.

`list-assessment-runs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-assessment-runs`.

AWS CLI

Para enumerar las ejecuciones de evaluación

El siguiente comando `list-assessment-runs` muestra todas las ejecuciones de evaluación existentes.

```
aws inspector list-assessment-runs
```

Salida:

```
{
    "assessmentRunArns": [
        "arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/
template/0-4r1V2mAw/run/0-MKkpXXPE",
        "arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/
template/0-4r1V2mAw/run/0-v5D6fI3v"
    ]
}
```

Para obtener más información, consulte Amazon Inspector Assessment Templates and Assessment Runs en la Guía del usuario de Amazon Inspector.

- Para obtener información sobre la API, consulte ListAssessmentRuns en la Referencia de comandos de la AWS CLI.

`list-assessment-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-assessment-targets`.

AWS CLI

Para enumerar los objetivos de evaluación

El siguiente comando `list-assessment-targets` enumera todos los objetivos de evaluación existentes:

```
aws inspector list-assessment-targets
```

Salida:

```
{
       "assessmentTargetArns": [
       "arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq"
       ]
}
```

Para obtener más información, consulte Amazon Inspector Assessment Targets en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte ListAssessmentTargets en la Referencia de comandos de la AWS CLI.

`list-assessment-templates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-assessment-templates`.

AWS CLI

Para enumerar las plantillas de evaluación

El siguiente comando `list-assessment-templates` enumera todas las plantillas de evaluación existentes:

```
aws inspector list-assessment-templates
```

Salida:

```
{
       "assessmentTemplateArns": [
       "arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/
template/0-4r1V2mAw",
       "arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/template/0-
Uza6ihLh"
       ]
}
```

Para obtener más información, consulte Amazon Inspector Assessment Templates and Assessment Runs en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte ListAssessmentTemplates en la Referencia de comandos de la AWS CLI.

`list-coverage-statistics`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-coverage-statistics`.

AWS CLI

Ejemplo 1: enumeración de las estadísticas de cobertura por grupos

El siguiente ejemplo de `list-coverage-statistics` muestra las estadísticas de cobertura de su entorno de AWS por grupos.

```
aws inspector2 list-coverage-statistics \
   --group-by RESOURCE_TYPE
```

Salida:

```
{
    "countsByGroup": [
        {
            "count": 56,
            "groupKey": "AWS_LAMBDA_FUNCTION"
        },
        {
            "count": 27,
            "groupKey": "AWS_ECR_REPOSITORY"
        },
        {
            "count": 18,
            "groupKey": "AWS_EC2_INSTANCE"
        },
        {
            "count": 3,
            "groupKey": "AWS_ECR_CONTAINER_IMAGE"
        },
        {
            "count": 1,
            "groupKey": "AWS_ACCOUNT"
        }
    ],
    "totalCounts": 105
}
```

Para obtener más información, consulte Assessing Amazon Inspector coverage of your AWS environment en la Guía del usuario de Amazon Inspector.

Ejemplo 2: enumeración de las estadísticas de cobertura por tipo de recurso

El siguiente ejemplo de `list-coverage-statistics` muestra las estadísticas de cobertura de su entorno de AWS por tipo de recurso.

```
aws inspector2 list-coverage-statistics
    --filter-criteria '{"resourceType":
[{"comparison":"EQUALS","value":"AWS_ECR_REPOSITORY"}]}'
    --group-by SCAN_STATUS_REASON
```

Salida:

```
{
    "countsByGroup": [
        {
            "count": 27,
            "groupKey": "SUCCESSFUL"
        }
    ],
    "totalCounts": 27
}
```

Para obtener más información, consulte Assessing Amazon Inspector coverage of your AWS environment en la Guía del usuario de Amazon Inspector.

Ejemplo 3: enumeración de las estadísticas de cobertura por nombre de repositorio de ECR

El siguiente ejemplo de `list-coverage-statistics` muestra las estadísticas de cobertura de su entorno de AWS por nombre de repositorio de ECR.

```
aws inspector2 list-coverage-statistics
   --filter-criteria '{"ecrRepositoryName":
[{"comparison":"EQUALS","value":"debian"}]}'
   --group-by SCAN_STATUS_REASON
```

Salida:

```
{
```

```
    "countsByGroup": [
        {
            "count": 3,
            "groupKey": "SUCCESSFUL"
        }
    ],
    "totalCounts": 3
}
```

Para obtener más información, consulte Assessing Amazon Inspector coverage of your AWS environment en la Guía del usuario de Amazon Inspector.

- Para obtener información sobre la API, consulte ListCoverageStatistics en la Referencia de comandos de la AWS CLI.

`list-coverage`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-coverage`.

AWS CLI

Ejemplo 1: enumeración de los detalles de cobertura de su entorno

En el siguiente ejemplo de `list-coverage`, se enumeran los detalles de cobertura de su entorno.

```
aws inspector2 list-coverage
```

Salida:

```
{
    "coveredResources": [
        {
            "accountId": "123456789012",
            "lastScannedAt": "2024-05-20T16:23:20-07:00",
            "resourceId": "i-EXAMPLE55555555555",
            "resourceMetadata": {
                "ec2": {
                    "amiId": "ami-EXAMPLE6666666666",
                    "platform": "LINUX"
                }
            },
```

```
            "resourceType": "AWS_EC2_INSTANCE",
            "scanStatus": {
                "reason": "SUCCESSFUL",
                "statusCode": "ACTIVE"
            },
            "scanType": "PACKAGE"
        }
    ]
}
```

Ejemplo 2: enumeración de los detalles de cobertura sobre el tipo de recurso de la función de Lambda

En el siguiente ejemplo de `list-coverage`, se muestran los detalles del tipo de recurso de la función de Lambda.

```
aws inspector2 list-coverage
    --filter-criteria '{"resourceType":
[{"comparison":"EQUALS","value":"AWS_LAMBDA_FUNCTION"}]}'
```

Salida:

```
{
    "coveredResources": [
        {
            "accountId": "123456789012",
            "resourceId": "arn:aws:lambda:us-west-2:123456789012:function:Eval-
container-scan-results:$LATEST",
            "resourceMetadata": {
                "lambdaFunction": {
                    "functionName": "Eval-container-scan-results",
                    "functionTags": {},
                    "layers": [],
                    "runtime": "PYTHON_3_7"
                }
            },
            "resourceType": "AWS_LAMBDA_FUNCTION",
            "scanStatus": {
                "reason": "SUCCESSFUL",
                "statusCode": "ACTIVE"
            },
            "scanType": "CODE"
```

```
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListCoverage en la Referencia de comandos de la AWS CLI.

`list-delegated-admin-accounts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-delegated-admin-accounts`.

AWS CLI

Para enumerar información sobre la cuenta de administrador delegado de su organización

En el siguiente ejemplo de `list-delegated-admin-accounts`, se enumera información sobre la cuenta de administrador delegado de su organización.

```
aws inspector2 list-delegated-admin-accounts
```

Salida:

```
{
    "delegatedAdminAccounts": [
        {
            "accountId": "123456789012",
            "status": "ENABLED"
        }
    ]
}
```

Para obtener más información, consulte Designating a delegated administrator for Amazon Inspector en la Guía del usuario de Amazon Inspector.

- Para obtener información sobre la API, consulte ListDelegatedAdminAccounts en la Referencia de comandos de la AWS CLI.

`list-event-subscriptions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-event-subscriptions`.

AWS CLI

Para enumerar las suscripciones a eventos

El siguiente comando `list-event-subscriptions` enumera todas las suscripciones a eventos de la plantilla de evaluación con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX/template/0-7sbz2Kz0`:

```
aws inspector list-event-subscriptions --resource-arn arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX/template/0-7sbz2Kz0
```

Salida:

```
{
      "subscriptions": [
        {
              "eventSubscriptions": [
                {
                      "event": "ASSESSMENT_RUN_COMPLETED",
                      "subscribedAt": 1459455440.867
                }
              ],
              "resourceArn": "arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX/template/0-7sbz2Kz0",
              "topicArn": "arn:aws:sns:us-west-2:123456789012:exampletopic"
        }
      ]
}
```

Para obtener más información, consulte Amazon Inspector Assessment Templates and Assessment Runs en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte ListEventSubscriptions en la Referencia de comandos de la AWS CLI.

`list-filters`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-filters`.

AWS CLI

Para enumerar los filtros asociados a la cuenta que ha utilizado para activar Amazon Inspector

En los siguientes ejemplos de `list-filters`, se enumeran los filtros asociados a la cuenta que ha utilizado para activar Amazon Inspector.

```
aws inspector2 list-filters
```

Salida:

```
{
    "filters": [
        {
            "action": "SUPPRESS",
            "arn": "arn:aws:inspector2:us-west-2:123456789012:owner/o-EXAMPLE222/
filter/EXAMPLE444444444",
            "createdAt": "2024-05-15T21:11:08.602000+00:00",
            "criteria": {
                "resourceType": [
                    {
                        "comparison": "EQUALS",
                        "value": "AWS_EC2_INSTANCE"
                    },
                ]
            },
            "description": "This suppression rule omits EC2 instance type findings",
            "name": "ExampleSuppressionRuleEC2",
            "ownerId": "o-EXAMPLE222",
            "tags": {},
            "updatedAt": "2024-05-15T21:11:08.602000+00:00"
        },
        {
            "action": "SUPPRESS",
            "arn": "arn:aws:inspector2:us-east-1:813737243517:owner/o-EXAMPLE222/
filter/EXAMPLE444444444",
            "createdAt": "2024-05-15T21:28:27.054000+00:00",
            "criteria": {
                "resourceType": [
                    {
                        "comparison": "EQUALS",
                        "value": "AWS_ECR_INSTANCE"
                    }
                ]
            },
            "description": "This suppression rule omits ECR instance type findings",
            "name": "ExampleSuppressionRuleECR",
```

```
            "ownerId": "o-EXAMPLE222",
            "tags": {},
            "updatedAt": "2024-05-15T21:28:27.054000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Filtering Amazon Inspector findings en la Guía del usuario de Amazon Inspector.

- Para obtener información sobre la API, consulte ListFilters en la Referencia de comandos de la AWS CLI.

`list-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-findings`.

AWS CLI

Para enumerar los hallazgos

El siguiente comando `list-findings` enumera todos los resultados que se han generado:

```
aws inspector list-findings
```

Salida:

```
{
        "findingArns": [
        "arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/
template/0-4r1V2mAw/run/0-MKkpXXPE/finding/0-HwPnsDm4",
        "arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/
template/0-4r1V2mAw/run/0-v5D6fI3v/finding/0-tyvmqBLy"
      ]
}
```

Para obtener más información, consulte Amazon Inspector Findings en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte ListFindings en la Referencia de comandos de la AWS CLI.

`list-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-members`.

AWS CLI

Ejemplo 1: muestra de todas las cuentas de miembros asociadas al administrador delegado de Amazon Inspector de la organización

aws inspector2 list-members --only-associated

Salida:

```
{
        {
             "members": [
        {
             "accountId": "123456789012",
             "delegatedAdminAccountId": "123456789012",
             "relationshipStatus": "ENABLED",
             "updatedAt": "2023-09-11T09:57:20.520000-07:00"
        },
        {
             "accountId": "123456789012",
             "delegatedAdminAccountId": "123456789012",
             "relationshipStatus": "ENABLED",
             "updatedAt": "2024-08-12T10:13:01.472000-07:00"
        },
        {
             "accountId": "625032911453",
             "delegatedAdminAccountId": "123456789012",
             "relationshipStatus": "ENABLED",
             "updatedAt": "2023-09-11T09:57:20.438000-07:00"
        },
        {
            "accountId": "715411239211",
            "delegatedAdminAccountId": "123456789012",
            "relationshipStatus": "ENABLED",
            "updatedAt": "2024-04-24T09:14:57.471000-07:00"
        }
    ]
}
```

Para obtener más información, consulte Administración de varias cuentas en Amazon Inspector con AWS Organizations en la Guía del usuario de Amazon Inspector.

Ejemplo 2: muestra de todas las cuentas de miembros asociadas y desasociadas al administrador delegado de Amazon Inspector de la organización

aws inspector2 list-members --no-only-associated

Salida:


```
{
        {
            "members": [
        {
            "accountId": "123456789012",
            "delegatedAdminAccountId": "123456789012",
            "relationshipStatus": "REMOVED",
            "updatedAt": "2024-05-15T11:34:53.326000-07:00"
        },
        {
            "accountId": "123456789012",
            "delegatedAdminAccountId": "123456789012",
            "relationshipStatus": "ENABLED",
            "updatedAt": "2023-09-11T09:57:20.520000-07:00"
        },
        {
            "accountId": "123456789012",
            "delegatedAdminAccountId": "123456789012",
            "relationshipStatus": "ENABLED",
            "updatedAt": "2024-08-12T10:13:01.472000-07:00"
        },
        {
            "accountId": "123456789012",
            "delegatedAdminAccountId": "123456789012",
            "relationshipStatus": "ENABLED",
            "updatedAt": "2023-09-11T09:57:20.438000-07:00"
        },
        {
            "accountId": "123456789012",
            "delegatedAdminAccountId": "123456789012",
            "relationshipStatus": "ENABLED",
            "updatedAt": "2024-04-24T09:14:57.471000-07:00"
        }
    ]
```

```
}
```

Para obtener más información, consulte Administración de varias cuentas en Amazon Inspector con AWS Organizations en la Guía del usuario de Amazon Inspector.

- Para obtener detalles sobre la API, consulte ListMembers en la Referencia de comandos de la AWS CLI.

`list-rules-packages`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-rules-packages`.

AWS CLI

Para enumerar los paquetes de reglas

El siguiente comando `list-rules-packages` enumera todos los paquetes de reglas de Inspector disponibles:

```
aws inspector list-rules-packages
```

Salida:

```
{
       "rulesPackageArns": [
         "arn:aws:inspector:us-west-2:758058086616:rulespackage/0-9hgA516p",
         "arn:aws:inspector:us-west-2:758058086616:rulespackage/0-H5hpSawc",
         "arn:aws:inspector:us-west-2:758058086616:rulespackage/0-JJOtZiqQ",
         "arn:aws:inspector:us-west-2:758058086616:rulespackage/0-vg5GGHSD"
       ]
 }
```

Para obtener más información, consulte Amazon Inspector Rules Packages and Rules en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte ListRulesPackages en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un recurso

El siguiente comando `list-tags-for-resource` muestra todas las etiquetas asociadas a la plantilla de evaluación con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/template/0-gcwFliYu`:

```
aws inspector list-tags-for-resource --resource-arn arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/template/0-gcwFliYu
```

Salida:

```
{
      "tags": [
        {
              "key": "Name",
              "value": "Example"
        }
      ]
}
```

Para obtener más información, consulte Amazon Inspector Assessment Templates and Assessment Runs en la guía de Amazon Inspector.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-usage-totals`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-usage-totals`.

AWS CLI

Para enumerar los totales de uso de los últimos 30 días

En los siguientes ejemplos de `list-usage-totals`, se enumeran los totales de uso de los últimos 30 días.

```
aws inspector2 list-usage-totals
```

Salida:


```
{
    "totals": [
        {
            "accountId": "123456789012",
            "usage": [
                {
                    "currency": "USD",
                    "estimatedMonthlyCost": 4.6022044647,
                    "total": 1893.4784083333334,
                    "type": "EC2_AGENTLESS_INSTANCE_HOURS"
                },
                {
                    "currency": "USD",
                    "estimatedMonthlyCost": 18.892449279,
                    "total": 10882.050784722222,
                    "type": "EC2_INSTANCE_HOURS"
                },
                {
                    "currency": "USD",
                    "estimatedMonthlyCost": 5.4525363736,
                    "total": 6543.043648333333,
                    "type": "LAMBDA_FUNCTION_CODE_HOURS"
                },
                {
                    "currency": "USD",
                    "estimatedMonthlyCost": 3.9064080309,
                    "total": 9375.379274166668,
                    "type": "LAMBDA_FUNCTION_HOURS"
                },
                {
                    "currency": "USD",
                    "estimatedMonthlyCost": 0.06,
                    "total": 6.0,
                    "type": "ECR_RESCAN"
                },
                {
                    "currency": "USD",
                    "estimatedMonthlyCost": 0.09,
                    "total": 1.0,
                    "type": "ECR_INITIAL_SCAN"
                }
            ]
```

```
        }
    ]
}
```

Para obtener más información, consulte Monitoring usage and cost in Amazon Inspector en la Guía del usuario de Amazon Inspector.

- Para obtener información sobre la API, consulte ListUsageTotals en la Referencia de comandos de la AWS CLI.

`preview-agents`

En el siguiente ejemplo de código, se muestra cómo utilizar `preview-agents`.

AWS CLI

Para previsualizar los agentes

El siguiente comando `preview-agents` muestra una vista previa de los agentes instalados en las instancias de EC2 que forman parte del objetivo de evaluación con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq`:

```
aws inspector preview-agents --preview-agents-arn arn:aws:inspector:us-
west-2:123456789012:target/0-0kFIPusq
```

Salida:

```
{
      "agentPreviews": [
        {
              "agentId": "i-49113b93"
        }
      ]
}
```

Para obtener más información, consulte Amazon Inspector Assessment Targets en la guía de Amazon Inspector.

- Para obtener más información sobre la API, consulte PreviewAgents en la Referencia de comandos de la AWS CLI.

`register-cross-account-access-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-cross-account-access-role`.

AWS CLI

Para registrar el rol de acceso entre cuentas

El siguiente comando `register-cross-account-access-role` registra el rol de IAM que utiliza el ARN `arn:aws:iam::123456789012:role/inspector` que Amazon Inspector usa para enumerar sus instancias de EC2 al inicio de la ejecución de evaluación o cuando llama al comando preview-agents:

```
aws inspector register-cross-account-access-role --role-
arn arn:aws:iam::123456789012:role/inspector
```

Para obtener más información, consulte Setting up Amazon Inspector en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte RegisterCrossAccountAccessRole en la Referencia de comandos de la AWS CLI.

`remove-attributes-from-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-attributes-from-findings`.

AWS CLI

Para eliminar los atributos de los hallazgos

El siguiente comando `remove-attributes-from-finding` elimina un atributo con la clave de `Example` y el valor de `example` del hallazgo con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/template/0-8l1VIE0D/run/0-Z02cjjug/finding/0-T8yM9mEU`:

```
aws inspector remove-attributes-from-findings --finding-arns arn:aws:inspector:us-
west-2:123456789012:target/0-0kFIPusq/template/0-8l1VIE0D/run/0-Z02cjjug/finding/0-
T8yM9mEU --attribute-keys key=Example,value=example
```

Salida:

```
{
      "failedItems": {}
}
```

Para obtener más información, consulte Amazon Inspector Findings en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte RemoveAttributesFromFindings en la Referencia de comandos de la AWS CLI.

`set-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-tags-for-resource`.

AWS CLI

Para definir las etiquetas para un recurso

El siguiente comando `set-tags-for-resource` define la etiqueta con la clave `Example` y el valor `example` a la plantilla de evaluación con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX/template/0-7sbz2Kz0`:

```
aws inspector set-tags-for-resource --resource-arn arn:aws:inspector:us-
west-2:123456789012:target/0-nvgVhaxX/template/0-7sbz2Kz0 --
tags key=Example,value=example
```

Para obtener más información, consulte Amazon Inspector Assessment Templates and Assessment Runs en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte SetTagsForResource en la Referencia de comandos de la AWS CLI.

`start-assessment-run`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-assessment-run`.

AWS CLI

Para iniciar una ejecución de evaluación

El siguiente comando `start-assessment-run` inicia la ejecución de evaluación denominada `examplerun` mediante la plantilla de evaluación con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX/template/0-it5r2S4T`:

```
aws inspector start-assessment-run --assessment-run-name examplerun --assessment-template-arn arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX/template/0-it5r2S4T
```

Salida:

```
{
      "assessmentRunArn": "arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX/template/0-it5r2S4T/run/0-jOoroxyY"
}
```

Para obtener más información, consulte Amazon Inspector Assessment Templates and Assessment Runs en la guía de Amazon Inspector.

- Para obtener detalles sobre la API, consulte StartAssessmentRun en la Referencia de comandos de la AWS CLI.

`stop-assessment-run`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-assessment-run`.

AWS CLI

Para detener una ejecución de evaluación

El siguiente comando `stop-assessment-run` detiene la ejecución de evaluación con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX/template/0-it5r2S4T/run/0-jOoroxyY`:

```
aws inspector stop-assessment-run --assessment-run-arn arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX/template/0-it5r2S4T/run/0-jOoroxyY
```

Para obtener más información, consulte Amazon Inspector Assessment Templates and Assessment Runs en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte StopAssessmentRun en la Referencia de comandos de la AWS CLI.

`subscribe-to-event`

En el siguiente ejemplo de código, se muestra cómo utilizar `subscribe-to-event`.

AWS CLI

Para suscribirse a un evento

El siguiente ejemplo habilita el proceso de envío de notificaciones de Amazon SNS acerca del evento `ASSESSMENT_RUN_COMPLETED` al tema con el ARN `arn:aws:sns:us-west-2:123456789012:exampletopic`.

```
aws inspector subscribe-to-event \
    --event ASSESSMENT_RUN_COMPLETED \
    --resource-arn arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX/
template/0-7sbz2Kz0 \
    --topic-arn arn:aws:sns:us-west-2:123456789012:exampletopic
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Amazon Inspector Assessment Templates and Assessment Runs en la guía de Amazon Inspector.

- Para obtener más información sobre la API, consulte SubscribeToEvent en la Referencia de comandos de la AWS CLI.

`unsubscribe-from-event`

En el siguiente ejemplo de código, se muestra cómo utilizar `unsubscribe-from-event`.

AWS CLI

Para anular la suscripción a un evento

El siguiente comando `unsubscribe-from-event` deshabilita el proceso de envío de notificaciones de Amazon SNS acerca del evento `ASSESSMENT_RUN_COMPLETED` al tema con el ARN `arn:aws:sns:us-west-2:123456789012:exampletopic`:

```
aws inspector unsubscribe-from-event --event ASSESSMENT_RUN_COMPLETED --resource-
arn arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX/template/0-7sbz2Kz0
 --topic arn:aws:sns:us-west-2:123456789012:exampletopic
```

Para obtener más información, consulte Amazon Inspector Assessment Templates and Assessment Runs en la guía de Amazon Inspector.

- Para obtener más información sobre la API, consulte UnsubscribeFromEvent en la Referencia de comandos de la AWS CLI.

`update-assessment-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-assessment-target`.

AWS CLI

Para actualizar un objetivo de evaluación

El siguiente comando `update-assessment-target` actualiza el objetivo de evaluación con el ARN `arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX`, el nombre `Example` y el grupo de recursos con el ARN `arn:aws:inspector:us-west-2:123456789012:resourcegroup/0-yNbgL5Pt`:

```
aws inspector update-assessment-target --assessment-target-arn arn:aws:inspector:us-west-2:123456789012:target/0-nvgVhaxX --assessment-target-name Example --resource-group-arn arn:aws:inspector:us-west-2:123456789012:resourcegroup/0-yNbgL5Pt
```

Para obtener más información, consulte Amazon Inspector Assessment Targets en la guía de Amazon Inspector.

- Para obtener información sobre la API, consulte UpdateAssessmentTarget en la Referencia de comandos de la AWS CLI.

`update-filter`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-filter`.

AWS CLI

Para actualizar un filtro

En el siguiente ejemplo de `update-filter`, se actualiza un filtro para omitir los hallazgos de Lambda en lugar de los hallazgos de la instancia de ECR.

```
aws inspector2 update-filter \
```

```
   --filter-arn "arn:aws:inspector2:us-west-2:123456789012:owner/o-EXAMPLE222/
filter/EXAMPLE444444444" \
   --name "ExampleSuppressionRuleLambda" \
   --description "This suppression rule omits Lambda instance findings" \
   --reason "Updating filter to omit Lambda instance findings instead of ECR
 instance findings"
```

Salida:

```
{
    "filters": [
        {
            "action": "SUPPRESS",
            "arn": "arn:aws:inspector2:us-west-2:123456789012:owner/o-EXAMPLE222/
filter/EXAMPLE444444444",
            "createdAt": "2024-05-15T21:28:27.054000+00:00",
            "criteria": {
                "resourceType": [
                    {
                        "comparison": "EQUALS",
                        "value": "AWS_ECR_INSTANCE"
                    }
                ]
            },
            "description": "This suppression rule omits Lambda instance findings",
            "name": "ExampleSuppressionRuleLambda",
            "ownerId": "o-EXAMPLE222",
            "reason": "Updating filter to omit Lambda instance findings instead of
 ECR instance findings",
            "tags": {},
            "updatedAt": "2024-05-15T22:23:13.665000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Managing findings in Amazon Inspector en la Guía del usuario de Amazon Inspector.

- Para obtener información sobre la API, consulte UpdateFilter en la Referencia de comandos de la AWS CLI.

AWS IoT Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS IoT.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`accept-certificate-transfer`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-certificate-transfer`.

AWS CLI

Para aceptar un certificado de dispositivo transferido desde una cuenta de AWS diferente

En el siguiente ejemplo de `accept-certificate-transfer`, se acepta un certificado de dispositivo transferido desde otra cuenta de AWS. El certificado se identifica mediante su ID.

```
aws iot accept-certificate-transfer \
    --certificate-
id 488b6a7f2acdeb00a77384e63c4e40b18bEXAMPLEe57b7272ba44c45e3448142
```

Este comando no produce ninguna salida.

Para obtener más información, consulte Transfer a certificate to another account en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte AcceptCertificateTransfer en la Referencia de comandos de la AWS CLI.

add-thing-to-billing-group

En el siguiente ejemplo de código, se muestra cómo utilizar `add-thing-to-billing-group`.

AWS CLI

Ejemplo 1: adición de un objeto por nombre a un grupo de facturación

En el siguiente ejemplo de `add-thing-to-billing-group`, se agrega el objeto denominado `MyLightBulb` al grupo de facturación denominado `GroupOne`.

```
aws iot add-thing-to-billing-group \
    --billing-group-name GroupOne \
    --thing-name MyLightBulb
```

Este comando no genera ninguna salida.

Ejemplo 2: adición de un objeto por ARN a un grupo de facturación

En el siguiente ejemplo de `add-thing-to-billing-group`, se agrega un objeto con un ARN especificado a un grupo de facturación con el ARN especificado. Especificar un ARN es útil si trabaja con varias regiones o cuentas de AWS. Puede ayudar a asegurarse de que está añadiendo la región y la cuenta correctas.

```
aws iot add-thing-to-thing-group \
    --billing-group-arn "arn:aws:iot:us-west-2:123456789012:billinggroup/GroupOne" \
    --thing-arn "arn:aws:iot:us-west-2:123456789012:thing/MyOtherLightBulb"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Billing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte AddThingToBillingGroup en la Referencia de comandos de la AWS CLI.

add-thing-to-thing-group

En el siguiente ejemplo de código, se muestra cómo utilizar `add-thing-to-thing-group`.

AWS CLI

Para agregar un objeto a un grupo

En el siguiente ejemplo de `add-thing-to-thing-group`, se agrega el objeto especificado a un grupo de objetos especificado.

```
aws iot add-thing-to-thing-group \
    --thing-name MyLightBulb \
    --thing-group-name LightBulbs
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Thing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte AddThingToThingGroup en la Referencia de comandos de la AWS CLI.

`associate-targets-with-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-targets-with-job`.

AWS CLI

Para asociar un grupo de objetos a un trabajo continuo

En el siguiente ejemplo de `associate-targets-with-job`, se asocia el grupo de objetos especificado al trabajo continuo especificado.

```
aws iot associate-targets-with-job \
    --targets "arn:aws:iot:us-west-2:123456789012:thinggroup/LightBulbs" \
    --job-id "example-job-04"
```

Salida:

```
{
    "jobArn": "arn:aws:iot:us-west-2:123456789012:job/example-job-04",
    "jobId": "example-job-04",
    "description": "example continuous job"
}
```

Para obtener más información, consulte Creating and Managing Jobs (CLI) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte AssociateTargetsWithJob en la Referencia de comandos de la AWS CLI.

`attach-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-policy`.

AWS CLI

Ejemplo 1: asociación de una política a un grupo de objetos

En el siguiente ejemplo de `attach-policy`, se asocia la política especificada a un grupo de objetos identificado por su ARN.

```
aws iot attach-policy \
    --target "arn:aws:iot:us-west-2:123456789012:thinggroup/LightBulbs" \
    --policy-name "UpdateDeviceCertPolicy"
```

Este comando no produce ninguna salida.

Para obtener más información, consulte Thing Groups en la Guía para desarrolladores de AWS IoT.

Ejemplo 2: asociación de una política a un certificado

En el siguiente ejemplo de `attach-policy`, se asocia la política `UpdateDeviceCertPolicy` a la entidad principal especificada por un certificado.

```
aws iot attach-policy \
    --policy-name UpdateDeviceCertPolicy \
    --target "arn:aws:iot:us-
west-2:123456789012:cert/4f0ba725787aa94d67d2fca420eca022242532e8b3c58e7465c7778b443fd65e"
```

Este comando no produce ninguna salida.

Para obtener más información, consulte Attach an AWS IoT Policy to a Device Certificate en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte AttachPolicy en la Referencia de comandos de la AWS CLI.

`attach-security-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-security-profile`.

AWS CLI

Para asociar un perfil de seguridad a todos los dispositivos no registrados

En el siguiente ejemplo de `attach-security-profile`, se asocia el perfil de seguridad de AWS IoT Device Defender denominado `Testprofile` con todos los dispositivos no registrados de la región `us-west-2` de esta cuenta de AWS.

```
aws iot attach-security-profile \
    --security-profile-name Testprofile \
    --security-profile-target-arn "arn:aws:iot:us-west-2:123456789012:all/
unregistered-things"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Comandos de detección en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte AttachSecurityProfile en Referencia de comandos de la AWS CLI.

`attach-thing-principal`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-thing-principal`.

AWS CLI

Para asociar un certificado a un objeto

En el siguiente ejemplo de `attach-thing-principal` se asocia un certificado al objeto MyTemperatureSensor. El certificado se identifica con un ARN. Encontrará el ARN de un certificado en la consola de AWS IoT.

```
aws iot attach-thing-principal \
    --thing-name MyTemperatureSensor \
```

```
    --principal arn:aws:iot:us-
west-2:123456789012:cert/2e1eb273792174ec2b9bf4e9b37e6c6c692345499506002a351597670552 78e8
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración de objetos con el registro en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte AttachThingPrincipal en la Referencia de comandos de AWS CLI.

`cancel-audit-mitigation-actions-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-audit-mitigation-actions-task`.

AWS CLI

Para cancelar una tarea de acciones de mitigación de auditoría

El siguiente ejemplo de `cancel-audit-mitigations-action-task`, se cancela la aplicación de las acciones de mitigación para la tarea especificada. No se pueden cancelar tareas que se han completado.

```
aws iot cancel-audit-mitigation-actions-task
    --task-id "myActionsTaskId"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte CancelAuditMitigationActionsTask (Comandos de las acciones de mitigación) en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte CancelAuditMitigationActionsTask en Referencia de comandos de la AWS CLI.

`cancel-audit-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-audit-task`.

AWS CLI

Para cancelar una tarea de auditoría

En el siguiente ejemplo de `cancel-audit-task`, se cancela una tarea de auditoría con el ID de tarea especificado. No se puede cancelar una tarea que se ha completado.

```
aws iot cancel-audit-task \
    --task-id a3aea009955e501a31b764abe1bebd3d
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Comandos de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte CancelAuditTask en la Referencia de comandos de la AWS CLI.

`cancel-certificate-transfer`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-certificate-transfer`.

AWS CLI

Para cancelar la transferencia de un certificado a otra cuenta de AWS

En el siguiente ejemplo de `cancel-certificate-transfer`, se cancela la transferencia de certificado especificada. El certificado se identifica con un ID de certificado. Encontrará el ID de un certificado en la consola de AWS IoT.

```
aws iot cancel-certificate-transfer \
    --certificate-
id f0f33678c7c9a046e5cc87b2b1a58dfa0beec26db78addd5e605d630e05c7fc8
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Transfer a certificate to another account en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte CancelCertificateTransfer en la Referencia de comandos de la AWS CLI.

`cancel-job-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-job-execution`.

AWS CLI

Para cancelar la ejecución de un trabajo en un dispositivo

En el siguiente ejemplo de `cancel-job-execution`, se cancela la ejecución del trabajo especificado en un dispositivo. Si el trabajo no tiene el estado `QUEUED`, debe añadir el parámetro `--force`.

```
aws iot cancel-job-execution \
    --job-id "example-job-03" \
    --thing-name "MyRPi"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creating and Managing Jobs (CLI) en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte CancelJobExecution en la Referencia de comandos de la AWS CLI.

`cancel-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-job`.

AWS CLI

Para cancelar un trabajo

En el siguiente ejemplo de `cancel-job`, se cancela el trabajo especificado.

```
aws iot cancel-job \
    --job-job "example-job-03"
```

Salida:

```
{
    "jobArn": "arn:aws:iot:us-west-2:123456789012:job/example-job-03",
    "jobId": "example-job-03",
    "description": "example job test"
}
```

Para obtener más información, consulte Creating and Managing Jobs (CLI) en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte CancelJob en la Referencia de comandos de la AWS CLI.

`clear-default-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `clear-default-authorizer`.

AWS CLI

Para borrar el autorizador predeterminado

En el siguiente ejemplo de `clear-default-authorizer`, se borra el autorizador personalizado predeterminado configurado actualmente. Después de ejecutar este comando, no existe ningún autorizador predeterminado. Al utilizar un autorizador personalizado, debe especificarlo con su nombre en los encabezados de las solicitudes HTTP.

```
aws iot clear-default-authorizer
```

Este comando no genera ninguna salida.

Para obtener más información, consulte ClearDefaultAuthorizer en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte ClearDefaultAuthorizer en la Referencia de comandos de la AWS CLI.

`confirm-topic-rule-destination`

En el siguiente ejemplo de código, se muestra cómo utilizar `confirm-topic-rule-destination`.

AWS CLI

Para confirmar un destino de regla de tema

En el siguiente ejemplo de `confirm-topic-rule-destination`, se confirma el destino de una regla temática con un token de confirmación recibido en un punto de conexión HTTP.

```
aws iot confirm-topic-rule-destination \
```

```
    --confirmation-token "AYADeIcmtq-
ZkxfpiWIQqHWM5ucAXwABABVhd3MtY3J5cHRvLXB1YmxpYy1rZXkAREFxY1E0UmlGeDg0V21BZWZ1VjZtZWFRVUJJUkt
aywpPqg8YEsa1lD4B40aJ2s1wEHKMybiF1RoOZzYisI0IvslzQY5UmCkqq3tV-3f7-
nKfosgIAAAADAAAEAAAAAAAAAAAAAAAAAAi9RMgy-
V19V9m6Iw2xfbw_____wAAAAEAAAAAAAAAAAAAAEAAAB1hw4SokgUcxiJ3gTO6n50NLJVpzyQR1UmPIj5sShqXEQGc0
iufgrzTePl8RZYOWr0O6Aj9DiVzJZx-1iD6Pu-
G6PUw1kaO7Knzs2B4AD0qfrHUF4pYRTvyUgBnMGUCMQC8ZRmhKqntd_c6Kgrow3bMUDBvNqo2qZr8Z8Jm2rzgseROlAn
PIetJ803Z4IlIlF8xXlcdPGP-PV1dOXFemyL8g"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Confirming a topic rule destination en la Guía para desarrolladores de AWS IoT.

- Para obtener detalles sobre la API, consulte ConfirmTopicRuleDestination en la Referencia de comandos de la AWS CLI.

`create-audit-suppression`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-audit-suppression`.

AWS CLI

Para crear una supresión de resultado de auditoría

En el siguiente ejemplo de `create-audit-suppression`, se crea una eliminación de un resultado de auditoría de una política denominada virtualMachinePolicy que se ha marcado como demasiado permisiva.

```
aws iot create-audit-suppression \
    --check-name IOT_POLICY_OVERLY_PERMISSIVE_CHECK \
    --resource-identifier
 policyVersionIdentifier={"policyName"="virtualMachinePolicy","policyVersionId"="1"}
 \
    --no-suppress-indefinitely \
    --expiration-date 2020-10-20
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Supresiones de resultados de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateAuditSuppression en la Referencia de comandos de la AWS CLI.

`create-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-authorizer`.

AWS CLI

Para crear un autorizador personalizado

En el siguiente ejemplo de `create-authorizer`, se crea un autorizador personalizado que utiliza la función de Lambda especificada como parte de un servicio de autenticación personalizado.

```
   aws iot create-authorizer \
       --authorizer-name "CustomAuthorizer" \
       --authorizer-function-arn "arn:aws:lambda:us-
west-2:123456789012:function:CustomAuthorizerFunction" \
       --token-key-name "MyAuthToken" \
       --status ACTIVE \
       --token-signing-public-keys FIRST_KEY="-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1uJOB4lQPgG/lM6ZfIwo
Z+7ENxAio9q6QD4FFqjGZsvjtYwjoe1RKK0U8Eq9xb5O3kRSmyIwTzwzm/f4Gf0Y
ZUloJ+t3PUUwHrmbYTAgTrCUgRFygjfgVwGCPs5ZAX4Eyqt5cr+AIHIiUDbxSa7p
zwOBKPeic0asNJpqT8PkBbRaKyleJh5oo81NDHHmVtbBm5A5YiJjqYXLaVAowKzZ
+GqsNvAQ9Jy1wI2VrEa1OfL8flDB/BJLm7zjpfPOHDJQgID0XnZwAlNnZcOhCwIx
50g2LW2Oy9R/dmqtDmJiVP97Z4GykxPvwlYHrUXY0iW1R3AR/Ac1NhCTGZMwVDB1
lQIDAQAB
-----END PUBLIC KEY-----"
```

Salida:

```
{
    "authorizerName": "CustomAuthorizer",
    "authorizerArn": "arn:aws:iot:us-west-2:123456789012:authorizer/
CustomAuthorizer2"
}
```

Para obtener más información, consulte CreateAuthorizer en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte CreateAuthorizer en la Referencia de comandos de la AWS CLI.

`create-billing-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-billing-group`.

AWS CLI

Para crear un grupo de facturación

En el siguiente ejemplo de `create-billing-group`, se crea un grupo de facturación sencillo denominado `GroupOne`.

```
aws iot create-billing-group \
    --billing-group-name GroupOne
```

Salida:

```
{
    "billingGroupName": "GroupOne",
    "billingGroupArn": "arn:aws:iot:us-west-2:123456789012:billinggroup/GroupOne",
    "billingGroupId": "103de383-114b-4f51-8266-18f209ef5562"
}
```

Para obtener más información, consulte Billing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateBillingGroup en la Referencia de comandos de la AWS CLI.

`create-certificate-from-csr`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-certificate-from-csr`.

AWS CLI

Para crear un certificado de dispositivo a partir de una solicitud de firma de certificado (CSR)

En el siguiente ejemplo de `create-certificate-from-csr`, se crea un certificado de dispositivo a partir de una CSR. Para crear una CSR, utilice el comando `openssl`.

```
aws iot create-certificate-from-csr \
    --certificate-signing-request=file://certificate.csr
```

Salida:

```
{
    "certificateArn": "arn:aws:iot:us-west-2:123456789012:cert/
c0c57bbc8baaf4631a9a0345c957657f5e710473e3ddbee1428d216d54d53ac9",
        "certificateId":
 "c0c57bbc8baaf4631a9a0345c957657f5e710473e3ddbee1428d216d54d53ac9",
        "certificatePem": "<certificate-text>"
}
```

Para obtener más información, consulte CreateCertificateFromCSR en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte CreateCertificateFromCsr en la Referencia de comandos de la AWS CLI.

`create-custom-metric`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-custom-metric`.

AWS CLI

Para crear una métrica personalizada publicada por sus dispositivos para Device Defender

En el siguiente ejemplo de `create-custom-metric`, se crea una métrica personalizada que mide el porcentaje de batería.

```
aws iot create-custom-metric \
    --metric-name "batteryPercentage" \
    --metric-type "number" \
    --display-name "Remaining battery percentage." \
    --region us-east-1 \
    --client-request-token "02ccb92b-33e8-4dfa-a0c1-35b181ed26b0"
```

Salida:

```
{
    "metricName": "batteryPercentage",
```

```
    "metricArn": "arn:aws:iot:us-east-1:1234564789012:custommetric/
batteryPercentage"
}
```

Para obtener más información, consulte Métricas personalizadas en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte CreateCustomMetric en la Referencia de comandos de la AWS CLI.

`create-dimension`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-dimension`.

AWS CLI

Para crear una dimensión

`create-dimension` crea una dimensión con un único filtro de tema denominado `TopicFilterForAuthMessages`.

```
aws iot create-dimension \
    --name TopicFilterForAuthMessages \
    --type TOPIC_FILTER \
    --string-values device/+/auth
```

Salida:

```
{
    "name": "TopicFilterForAuthMessages",
    "arn": "arn:aws:iot:eu-west-2:123456789012:dimension/TopicFilterForAuthMessages"
}
```

Para obtener más información, consulte Comandos de detección en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateDimension en la Referencia de comandos de la AWS CLI.

`create-domain-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-domain-configuration`.

AWS CLI

Para crear una configuración de dominio

En el siguiente ejemplo de `create-domain-configuration`, se crea una configuración de dominio administrado por AWS con un tipo de servicio DATA.

```
aws iot create-domain-configuration \
    --domain-configuration-name "additionalDataDomain" \
    --service-type "DATA"
```

Salida:

```
{
    "domainConfigurationName": "additionalDataDomain",
    "domainConfigurationArn": "arn:aws:iot:us-
west-2:123456789012:domainconfiguration/additionalDataDomain/dikMh"
}
```

Para obtener más información, consulte Configurable Endpoints en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateDomainConfiguration en la Referencia de comandos de la AWS CLI.

`create-dynamic-thing-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-dynamic-thing-group`.

AWS CLI

Para crear un grupo de objetos dinámico

En el siguiente ejemplo de `create-dynamic-thing-group`, se crea un grupo de objetos dinámico que contiene cualquier objeto con un atributo de temperatura superior a 60 grados. Debe habilitar la indexación de flotas de AWS IoT para poder usar grupos de objetos dinámicos.

```
aws iot create-dynamic-thing-group \
    --thing-group-name "RoomTooWarm" \
    --query-string "attributes.temperature>60"
```

Salida:

```
{
    "thingGroupName": "RoomTooWarm",
    "thingGroupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/RoomTooWarm",
    "thingGroupId": "9d52492a-fc87-43f4-b6e2-e571d2ffcad1",
    "indexName": "AWS_Things",
    "queryString": "attributes.temperature>60",
    "queryVersion": "2017-09-30"
}
```

Para obtener más información, consulte Dynamic Thing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateDynamicThingGroup en la Referencia de comandos de la AWS CLI.

`create-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-job`.

AWS CLI

Ejemplo 1: creación de un trabajo

En el siguiente ejemplo de `create-job`, se crea un trabajo de AWS IoT sencillo que envía un documento JSON al dispositivo `MyRaspberryPi`.

```
aws iot create-job \
    --job-id "example-job-01" \
    --targets "arn:aws:iot:us-west-2:123456789012:thing/MyRaspberryPi" \
    --document file://example-job.json \
    --description "example job test" \
    --target-selection SNAPSHOT
```

Salida:

```
{
    "jobArn": "arn:aws:iot:us-west-2:123456789012:job/example-job-01",
    "jobId": "example-job-01",
    "description": "example job test"
```

```
}
```

Ejemplo 2: creación de un trabajo continuo

En el siguiente ejemplo de `create-job`, se crea un trabajo que continúa ejecutándose después de que los objetos especificados como objetivos hayan completado el trabajo. En este ejemplo, el objetivo es un grupo de objetos, por lo que cuando se añaden nuevos dispositivos al grupo, el trabajo continuo se ejecuta en esos objetos nuevos.

aws iot create-job --job-id "example-job-04" --targets "arn:aws:iot:us-west-2:123456789012:thinggroup/DeadBulbs" --document file://example-job.json --description "example continuous job" --target-selection CONTINUOUS

Salida:

```
{
    "jobArn": "arn:aws:iot:us-west-2:123456789012:job/example-job-04",
    "jobId": "example-job-04",
    "description": "example continuous job"
}
```

Para obtener más información, consulte Creating and Managing Jobs (CLI) en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte CreateJob en la Referencia de comandos de la AWS CLI.

`create-keys-and-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-keys-and-certificate`.

AWS CLI

Para crear un par de claves RSA y emitir un certificado X.509

El siguiente `create-keys-and-certificate` crea un par de claves RSA de 2048 bits y emite un certificado X.509 mediante la clave pública emitida. Como esta es la única vez que AWS IoT proporciona la clave privada para este certificado, asegúrese de guardarla en un lugar seguro.

```
aws iot create-keys-and-certificate \
    --certificate-pem-outfile "myTest.cert.pem" \
```

```
    --public-key-outfile "myTest.public.key" \
    --private-key-outfile "myTest.private.key"
```

Salida:

```
{
    "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/9894ba17925e663f1d29c23af4582b8e3b7619c31f3fbd93adcb51ae54b83dc2",
    "certificateId":
 "9894ba17925e663f1d29c23af4582b8e3b7619c31f3fbd93adcb51ae54b83dc2",
    "certificatePem": "
-----BEGIN CERTIFICATE-----
MIICiTCCEXAMPLE6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgEXAMPLEAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSEXAMPLE2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYEXAMPLEb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCEXAMPLEJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDAEXAMPLEsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEXAMPLE25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+aEXAMPLE
EXAMPLEfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZEXAMPLELG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAEXAMPLEWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9qEXAMPLEyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDEXAMPLEBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----\n",
    "keyPair": {
        "PublicKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkEXAMPLEQEFAAOCAQ8AMIIBCgKCAQEAEXAMPLE1nnyJwKSMHw4h\nMMEXAMPLEuuN/
dMAS3fyce8DW/4+EXAMPLEyjmoF/YVF/gHr99VEEXAMPLE5VF13\n59VK7cEXAMPLE67GK+y+jikqXOgHh/
xJTwo
+sGpWEXAMPLEDz18xOd2ka4tCzuWEXAMPLEahJbYkCPUBSU8opVkR7qkEXAMPLE1DR6sx2HocliOOLtu6Fkw91swQWEX
\GB3ZPrNh0PzQYvjUStZeccyNCx2EXAMPLEvp9mQOUXP6plfgxwKRX2fEXAMPLEDa
\nhJLXkX3rHU2xbxJSq7D+XEXAMPLEcw+LyFhI5mgFRl88eGdsAEXAMPLElnI9EesG\nFQIDAQAB\n-----
END PUBLIC KEY-----\n",
        "PrivateKey": "-----BEGIN RSA PRIVATE KEY-----\nkey omittted for security
 reasons\n-----END RSA PRIVATE KEY-----\n"
    }
}
```

Para obtener más información, consulte Create and Register an AWS IoT Device Certificate en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte CreateKeysAndCertificate en la Referencia de comandos de la AWS CLI.

`create-mitigation-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-mitigation-action`.

AWS CLI

Para crear acciones de mitigación

En el siguiente ejemplo de `create-mitigation-action`, se define una acción de mitigación denominada `AddThingsToQuarantineGroup1Action` que, cuando se aplica, mueve los objetos al grupo de objetos denominado `QuarantineGroup1`. Esta acción anula los grupos de objetos dinámicos.

```
aws iot create-mitigation-action --cli-input-json file::params.json
```

Contenido de `params.json`:

```
{
    "actionName": "AddThingsToQuarantineGroup1Action",
    "actionParams": {
        "addThingsToThingGroupParams": {
            "thingGroupNames": [
                "QuarantineGroup1"
            ],
            "overrideDynamicGroups": true
        }
    },
    "roleArn": "arn:aws:iam::123456789012:role/service-role/
MoveThingsToQuarantineGroupRole"
}
```

Salida:

```
{
    "actionArn": "arn:aws:iot:us-west-2:123456789012:mitigationaction/
AddThingsToQuarantineGroup1Action",
    "actionId": "992e9a63-a899-439a-aa50-4e20c52367e1"
```

```
}
```

Para obtener más información, consulte CreateMitigationAction (comandos de las acciones de mitigación) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateMitigationAction en la Referencia de comandos de la AWS CLI.

`create-ota-update`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-ota-update`.

AWS CLI

Para crear una actualización de OTA para usarla con Amazon FreeRTOS

En el siguiente ejemplo de `create-ota-update`, se Crea un OTAUpdate de AWS IoT en un grupo de destino de objetos o grupos. Esto forma parte de una actualización inalámbrica de Amazon FreeRTOS que permite implementar nuevas imágenes de firmware en un solo dispositivo o en un grupo de dispositivos.

```
aws iot create-ota-update \
    --cli-input-json file://create-ota-update.json
```

Contenido de `create-ota-update.json`:

```
{
    "otaUpdateId": "ota12345",
    "description": "A critical update needed right away.",
    "targets": [
        "device1",
        "device2",
        "device3",
        "device4"
    ],
    "targetSelection": "SNAPSHOT",
    "awsJobExecutionsRolloutConfig": {
        "maximumPerMinute": 10
    },
    "files": [
        {
```

```
            "fileName": "firmware.bin",
            "fileLocation": {
              "stream": {
                "streamId": "004",
                "fileId":123
              }
            },
            "codeSigning": {
              "awsSignerJobId": "48c67f3c-63bb-4f92-a98a-4ee0fbc2bef6"
            }
          }
    ]
    "roleArn": "arn:aws:iam:123456789012:role/service-role/my_ota_role"
}
```

Salida:

```
{
     "otaUpdateId": "ota12345",
     "awsIotJobId": "job54321",
     "otaUpdateArn": "arn:aws:iot:us-west-2:123456789012:otaupdate/itsaupdate",
     "awsIotJobArn": "arn:aws:iot:us-west-2:123456789012:job/itsajob",
     "otaUpdateStatus": "CREATE_IN_PROGRESS"
}
```

Para obtener más información, consulte CreateOTAUpdate en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte CreateOtaUpdate en la Referencia de comandos de la AWS CLI.

`create-policy-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-policy-version`.

AWS CLI

Para actualizar una política a una nueva versión

En el siguiente ejemplo de `create-policy-version`, se actualiza una definición de política que crea una nueva versión de la política. Este ejemplo también convierte a la nueva versión en la predeterminada.

```
aws iot create-policy-version \
    --policy-name UpdateDeviceCertPolicy \
    --policy-document file://policy.json \
    --set-as-default
```

Contenido de `policy.json`:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action":  "iot:UpdateCertificate",
            "Resource": "*"
        }
    ]
}
```

Salida:

```
{
    "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/UpdateDeviceCertPolicy",
    "policyDocument": "{ \"Version\": \"2012-10-17\", \"Statement\": [ { \"Effect\":
 \"Allow\", \"Action\":  \"iot:UpdateCertificate\", \"Resource\": \"*\" } ] }",
    "policyVersionId": "2",
    "isDefaultVersion": true
}
```

Para obtener más información, consulte AWS IoT Policies en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreatePolicyVersion en la Referencia de comandos de la AWS CLI.

`create-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-policy`.

AWS CLI

Para crear una política de AWS IoT

En el siguiente ejemplo de `create-policy`, se crea una política de AWS IoT denominada TemperatureSensorPolicy. El archivo `policy.json` contiene instrucciones que permiten acciones de política de AWS IoT.

```
aws iot create-policy \
    --policy-name TemperatureSensorPolicy \
    --policy-document file://policy.json
```

Contenido de `policy.json`:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish",
                "iot:Receive"
            ],
            "Resource": [
                "arn:aws:iot:us-west-2:123456789012:topic/topic_1",
                "arn:aws:iot:us-west-2:123456789012:topic/topic_2"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Subscribe"
            ],
            "Resource": [
                "arn:aws:iot:us-west-2:123456789012:topicfilter/topic_1",
                "arn:aws:iot:us-west-2:123456789012:topicfilter/topic_2"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:us-west-2:123456789012:client/basicPubSub"
            ]
        }
```

```
    ]
}
```

Salida:

```
{
    "policyName": "TemperatureSensorPolicy",
    "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/
TemperatureSensorPolicy",
    "policyDocument": "{
        \"Version\": \"2012-10-17\",
        \"Statement\": [
            {
                \"Effect\": \"Allow\",
                \"Action\": [
                    \"iot:Publish\",
                    \"iot:Receive\"
                ],
                \"Resource\": [
                    \"arn:aws:iot:us-west-2:123456789012:topic/topic_1\",
                    \"arn:aws:iot:us-west-2:123456789012:topic/topic_2\"
                ]
            },
            {
                \"Effect\": \"Allow\",
                \"Action\": [
                    \"iot:Subscribe\"
                ],
                \"Resource\": [
                    \"arn:aws:iot:us-west-2:123456789012:topicfilter/topic_1\",
                    \"arn:aws:iot:us-west-2:123456789012:topicfilter/topic_2\"
                ]
            },
            {
                \"Effect\": \"Allow\",
                \"Action\": [
                    \"iot:Connect\"
                ],
                \"Resource\": [
                    \"arn:aws:iot:us-west-2:123456789012:client/basicPubSub\"
                ]
            }
        ]
```

```
    }",
    "policyVersionId": "1"
}
```

Para obtener más información, consulte AWS IoT Policies en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreatePolicy en la Referencia de comandos de la AWS CLI.

`create-provisioning-claim`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-provisioning-claim`.

AWS CLI

Para crear una reclamación de aprovisionamiento

En el siguiente ejemplo de `create-provisioning-claim`, se crea una reclamación de aprovisionamiento a partir de una plantilla de aprovisionamiento.

```
aws iot create-provisioning-claim \
    --template-name MyTestProvisioningTemplate
```

Salida:

```
{
    "certificateId":
 "78de02184b2ce80cf8fb709bda59e62b19fb83513590483eb0434589476ab09f",
    "certificatePem": "-----BEGIN CERTIFICATE-----\nMIIDdzCCAl
+gAwIBAgIUXSZhEBLztMLZ2fHG
14gV0NymYY0wDQYJKoZIhvcNAQEL
\nBQAwfjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCldhc2hpbmd0b24xEDAOBg
VBAcM\nB1NlYXR0bGUxGDAWBgNVBAoMD0FtYXpvbi5jb20gSW5jLjEgMB4GA1UECwwXQW1h
\nem9uIElvVCBQcm9
2aXNpb25pbmcxDDAKBgNVBAUTAzEuMDAeFw0yMDA3MjgxNjQ0\nMDZaFw0yMDA3MjgxNjUxMDZaMEsxSTBHBgNVB
AMMQDFhNDEyM2VkNmIxYjU3MzE3\nZTgzMTJmY2MzN2FiNTdhY2MzYTZkZGVjOGQ5OGY3NzUwMWRlMjc0YjhmYTQ
xN2Iw\nggEiMA0GCSqGSIb3EXAMPLEAA4IBDwAwggEKAoIBAQDBhKI94ktKLqTwnj+ayOq1\nTAJt/
N6s6IJDZvl
rYjkC0E7wzaeY3TprWk03S29vUzVuEOXHXQXZbihgpg2m6fza\nkWm9/
wpjzE9ny5+xkPGVH4Wnwz7yK5m8S0agL
T96cRBSWnWmonOWdY0GKVzni0CA\n+iyGudgrFKm7Eae/
v18oXrf82KtOAGO4xG0KE2WKYHsT1fx3c9xZhlXP/eX
```

```
Lhv00\n+lGp0WVw9PbhKfrxliKJ5q6sL5nVUaUHq6hlQPYwsATeOvAp3u0ak5zgTyL0fg7Y
\nPyKk6VYwLW62r+V
YBSForEMOAhkq3LsP/rjxpEKmi2W4lPVS6oFZRKcD+H1Kyil5\nAgMBAAGjIDAeMAwGA1UdEwEB/
wQCMAAwDgYDV
R0PAQH/BAQDAgeAMA0GCSqGSIb3\nDQEBCwUAA4IBAQAGgix2k6nVqbZFKq97/fZBzLGS0dyz5rT/
E41cDIRX+1j
EPW41\nw0D+2sXheCZLZZnSkvIiP74IToNeXDrjdcaodeGFVHIElRjhMIq+4ZebPbRLtidF
\nRc2hfcTAlqq9Z6v
5Vk6BeM1tu0RqH1wPoVUccLPya8EjNCbnJZUmGdOfrN/Y9pho\n5ikV+HPeZhG/k6dhE2GsQJyKFVHL/
uBgKSily
1bRyWU1r6qcpWBNBHjUoD7HgOwD
\nnzMh4XRb2FQDsqFalkCSYmeL8IVC49sgPD9Otyp5uteGMTy62usAAUQdq/f
ZvrWg\nOkFpwMVnGKVKT7Kg0kKOLzKWOBB2Jm4/gmrJ\n-----END CERTIFICATE-----\n",
    "keyPair": {
        "PublicKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg
KCAQEAwYSiPeJLSi6k8J4/msjq
\ntUwCbfzerOiCQ2b5a2I5AtBO8M2nmN06a1pNN0tvb1M1bhDlx10F2W4oYKYN
pun8\n2pFpvf8KY8xPZ8ufsZDxlR+Fp8M+8iuZvEtGoC0/enEQUlp1pqJzlnWNBilc54tA
\ngPoshrnYKxSpuxGn
v79fKF63/NirTgBjuMRtChNlimEXAMPLE3PcWYZVz/3ly4b9\nNPpRqdFlcPT24Sn68ZYiieaurC
+Z1VGlB6uoZU
D2MLAE3jrwKd7tGpOc4E8i9H4O\n2D8ipOlWMC1utq/
lWAUhaKxDDgIZKty7D/648aRCpotluJT1UuqBWUSnA/h9
Ssop\neQIDAQAB\n-----END PUBLIC KEY-----\n",
        "PrivateKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQEAwYSiPeJLSi6k8J4/
msjqtUwCbfzerOiCQ2b5a2I5AtBO8M2n
\nmN06a1pNN0tvb1M1bhDlx10F2W4oYKYNpun82pFpvf8KY8xPZ8ufsZ
DxlR+Fp8M+\n8iuZvEtGoC0/enEQUlp1pqJzlnWNBilc54tAgPoshrnYKxSpuxGnv79fKF63/Nir
\nTgBjuMRtCh
NlimB7E9X8d3PcWYZVz/3ly4b9NPpRqdFlcPT24Sn68ZYiieaurC+Z
\n1VGlB6uoZUD2MLAE3jrwKd7tGpOc4E8i
9H4O2D8ipOlWMC1utq/lWAUhaKxDDgIZ\nKty7D/648aRCpotluJT1UuqBWUSnA/
h9SsopeQIDAQABAoIBAEAybN
QUtx9T2/nK\ntZT2pA4iugecxI4dz+DmT0XVXs5VJmrx/
nBSq6ejXExEpSIMO4RY7LE3ZdJcnd56\nF7tQkkY7yR
VzfxHeXFU1krOIPuxWebNOrRoPZr+1RSer+wv2aBC525+88pVuR6tM
\nm3pgkrR2ycCj9FdOUoQxdjHBHaM5PDmJ
9aSxCKdg3nReepeGwsR2TQA+m2vVxWk7\nou0+91eTOP+/QfP7P8ZjOIkO2XivlRcVDyN/
E4QXPKuIkM/8vS8VK+
E9pATQ0MtB\n2lw8R/YU5AJd6jlEXAMPLEGU2UzRzInNWiLtkPPPqgqXXhxOf+mxByjcMalVJk0L
\nhOG2ROUCgY
```

```
EA+ROcHNHy/XbsP7FihOhEh+6Q2QxQ2ncBUPYbBazrR8Hn+7SCICQK
\nVyYfd8Ajfq3e7RsKVL5SlMBp7Slidxak
bIn28fKfPn62DaemGCIoyDgLpF+eUxBx
\ngzbCiBZga8brfurza43UZjKZLpg3hq721+FeAiXi1Nma4Yr9YWEHEN
8CgYEAxuWt\npzdWWmsiFzfsAw0sy9ySDA/xr5WRWzJyAqUsjsks6rxNzWebpufnYHcmtW7pLdqM
\nkboHwN2pXa
kmZvrk2nKkEMq5brBYGDXuxDe+V369Bianx8aZFyIsckA7OwXW1w1h
\ngRC5rQ4XOgp3+Jmw7eAO8LRYDjaN846+
QbtO2KcCgYAWS0UL51bijQR0ZwI0dz27\nFQVuCAYsp748aurcRTACCj8jbnK/
QbqTNlxWsaH7ssBjZKo2D5sAqY
BRtASWODab\naHXsDhVm2Jye+ESLoHMaCLoyCkT3ll8yqXIcEDStMO7fO1Ryag164EiJvSIrMfny\nNL/
fXVjCSH
/udCxdzPt+7QKBgQC+LAD7rxdr4J9538hTqpc4XK9vxRbrMXEH55XH
\nHbMa2xONZXpmeTgEQBukyohCVceyRhK9
i0e6irZTjVXghOeoTpC8VXkzcnzouTiQ
\neFQQSGfnp7Ioe6UIz23715pKduzSNkMSKrG924ktv7CyDBF1gBQI5g
aDoHnddJBJ\nPRTIZQKBgA8MASXtTxQntRwXXzR92U0vAighiuRkB/mx9jQpUcK1qiqHbkAMqgNF
\nPFCBYIUbFT
iYKKKeJNbyJQvjfsJCkAnaFJ+RnTxk0Q6Wjm20peJ/ii4QiDdnigoE\nvdlc5cFQewWb4/
zqAtPdinkPlN94ileI
79XQdc7RlJ0jpgTimL+V\n-----END RSA PRIVATE KEY-----\n"
    },
    "expiration": 1595955066.0
}
```

Para obtener más información, consulte Provisioning by trusted user en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte CreateProvisioningClaim en la Referencia de comandos de la AWS CLI.

`create-provisioning-template-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-provisioning-template-version`.

AWS CLI

Para crear una versión de plantilla de aprovisionamiento

En el siguiente ejemplo se crea una versión de la plantilla de aprovisionamiento especificada. El cuerpo de la nueva versión se incluye en el archivo `template.json`.

```
aws iot create-provisioning-template-version \
    --template-name widget-template \
    --template-body file://template.json
```

Contenido de `template.json`:

```
{
    "Parameters" : {
        "DeviceLocation": {
            "Type": "String"
        }
    },
    "Mappings": {
        "LocationTable": {
            "Seattle": {
                "LocationUrl": "https://example.aws"
            }
        }
    },
    "Resources" : {
        "thing" : {
            "Type" : "AWS::IoT::Thing",
            "Properties" : {
                "AttributePayload" : {
                    "version" : "v1",
                    "serialNumber" : "serialNumber"
                },
                "ThingName" : {"Fn::Join":["",["ThingPrefix_",
{"Ref":"SerialNumber"}]]},
                "ThingTypeName" : {"Fn::Join":["",["ThingTypePrefix_",
{"Ref":"SerialNumber"}]]},
                "ThingGroups" : ["widgets", "WA"],
                "BillingGroup": "BillingGroup"
            },
            "OverrideSettings" : {
                "AttributePayload" : "MERGE",
                "ThingTypeName" : "REPLACE",
                "ThingGroups" : "DO_NOTHING"
            }
        },
        "certificate" : {
            "Type" : "AWS::IoT::Certificate",
            "Properties" : {
```

```
                "CertificateId": {"Ref": "AWS::IoT::Certificate::Id"},
                "Status" : "Active"
            }
        },
        "policy" : {
            "Type" : "AWS::IoT::Policy",
            "Properties" : {
                "PolicyDocument" : {
                    "Version":"2012-10-17",
                    "Statement": [{
                        "Effect": "Allow",
                        "Action":["iot:Publish"],
                        "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/foo/
bar"]
                    }]
                }
            }
        }
    },
    "DeviceConfiguration": {
        "FallbackUrl": "https://www.example.com/test-site",
        "LocationUrl": {
            "Fn::FindInMap": ["LocationTable",{"Ref": "DeviceLocation"},
 "LocationUrl"]}
        }
    }
}
```

Salida:

```
{
    "templateArn": "arn:aws:iot:us-east-1:123456789012:provisioningtemplate/widget-
template",
    "templateName": "widget-template",
    "versionId": 2,
    "isDefaultVersion": false
}
```

Para obtener más información, consulte AWS IoT Secure Tunneling en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte CreateProvisioningTemplateVersion en la Referencia de comandos de la AWS CLI.

`create-provisioning-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-provisioning-template`.

AWS CLI

Para crear una plantilla de aprovisionamiento

En el siguiente ejemplo de `create-provisioning-template`, se crea una plantilla de aprovisionamiento tal como se define en el archivo `template.json`.

```
aws iot create-provisioning-template \
    --template-name widget-template \
    --description "A provisioning template for widgets" \
    --provisioning-role-arn arn:aws:iam::123456789012:role/Provision_role \
    --template-body file://template.json
```

Contenido de `template.json`:

```
{
    "Parameters" : {
        "DeviceLocation": {
            "Type": "String"
        }
    },
    "Mappings": {
        "LocationTable": {
            "Seattle": {
                "LocationUrl": "https://example.aws"
            }
        }
    },
    "Resources" : {
        "thing" : {
            "Type" : "AWS::IoT::Thing",
            "Properties" : {
                "AttributePayload" : {
                    "version" : "v1",
                    "serialNumber" : "serialNumber"
                },
                "ThingName" : {"Fn::Join":["",["ThingPrefix_",
{"Ref":"SerialNumber"}]]},
```

```
                "ThingTypeName" : {"Fn::Join":["",["ThingTypePrefix_",
{"Ref":"SerialNumber"}]]},
                "ThingGroups" : ["widgets", "WA"],
                "BillingGroup": "BillingGroup"
            },
            "OverrideSettings" : {
                "AttributePayload" : "MERGE",
                "ThingTypeName" : "REPLACE",
                "ThingGroups" : "DO_NOTHING"
            }
        },
        "certificate" : {
            "Type" : "AWS::IoT::Certificate",
            "Properties" : {
                "CertificateId": {"Ref": "AWS::IoT::Certificate::Id"},
                "Status" : "Active"
            }
        },
        "policy" : {
            "Type" : "AWS::IoT::Policy",
            "Properties" : {
                "PolicyDocument" : {
                    "Version":"2012-10-17",
                    "Statement": [{
                        "Effect": "Allow",
                        "Action":["iot:Publish"],
                        "Resource": ["arn:aws:iot:us-east-1:504350838278:topic/foo/
bar"]
                    }]
                }
            }
        }
    },
    "DeviceConfiguration": {
        "FallbackUrl": "https://www.example.com/test-site",
        "LocationUrl": {
            "Fn::FindInMap": ["LocationTable",{"Ref": "DeviceLocation"},
 "LocationUrl"]}
        }
    }
}
```

Salida:

```
{
    "templateArn": "arn:aws:iot:us-east-1:123456789012:provisioningtemplate/widget-
template",
    "templateName": "widget-template",
    "defaultVersionId": 1
}
```

Para obtener más información, consulte AWS IoT Secure Tunneling en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte CreateProvisioningTemplate en la Referencia de comandos de la AWS CLI.

`create-role-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-role-alias`.

AWS CLI

Para crear un alias de rol

En el siguiente ejemplo de `create-role-alias`, se crea un alias de rol denominado `LightBulbRole` para el rol especificado.

```
aws iot create-role-alias \
    --role-alias LightBulbRole \
    --role-arn arn:aws:iam::123456789012:role/lightbulbrole-001
```

Salida:

```
{
    "roleAlias": "LightBulbRole",
    "roleAliasArn": "arn:aws:iot:us-west-2:123456789012:rolealias/LightBulbRole"
}
```

Para obtener más información, consulte CreateRoleAlias en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte CreateRoleAlias en la Referencia de comandos de la AWS CLI.

`create-scheduled-audit`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-scheduled-audit`.

AWS CLI

Para crear una auditoría programada

En el siguiente ejemplo de `create-scheduled-audit`, se crea una auditoría programada que se ejecuta semanalmente, los miércoles, para comprobar si los certificados de CA o los certificados de los dispositivos van a caducar.

```
aws iot create-scheduled-audit \
    --scheduled-audit-name WednesdayCertCheck \
    --frequency WEEKLY \
    --day-of-week WED \
    --target-check-
names CA_CERTIFICATE_EXPIRING_CHECK DEVICE_CERTIFICATE_EXPIRING_CHECK
```

Salida:

```
{
    "scheduledAuditArn": "arn:aws:iot:us-west-2:123456789012:scheduledaudit/
WednesdayCertCheck"
}
```

Para obtener más información, consulte Comandos de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateScheduledAudit en la Referencia de comandos de la AWS CLI.

`create-security-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-security-profile`.

AWS CLI

Para crear un perfil de seguridad

En el siguiente ejemplo de `create-security-profile`, se crea un perfil de seguridad que comprueba si el ancho de banda móvil supera un umbral o si se producen más de 10 errores de autorización en un período de cinco minutos.

```
aws iot create-security-profile \
    --security-profile-name PossibleIssue \
    --security-profile-description "Check to see if authorization fails 10 times in
 5 minutes or if cellular bandwidth exceeds 128"  \
    --behaviors "[{\"name\":\"CellularBandwidth\",\"metric\":\"aws:message-byte-size
\",\"criteria\":{\"comparisonOperator\":\"greater-than\",\"value\":{\"count\":128},
\"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1}},{\"name
\":\"Authorization\",\"metric\":\"aws:num-authorization-failures\",\"criteria\":
{\"comparisonOperator\":\"less-than\",\"value\":{\"count\":10},\"durationSeconds
\":300,\"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1}}]"
```

Salida:

```
{
    "securityProfileName": "PossibleIssue",
    "securityProfileArn": "arn:aws:iot:us-west-2:123456789012:securityprofile/
PossibleIssue"
}
```

Para obtener más información, consulte Comandos de detección en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateSecurityProfile en la Referencia de comandos de la AWS CLI.

`create-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-stream`.

AWS CLI

Para crear un flujo para la entrega de uno o más archivos grandes en fragmentos a través de MQTT

En el siguiente ejemplo de `create-stream`, se crea un flujo para entregar uno o varios archivos grandes en fragmentos a través de MQTT. Un flujo trasporta bytes de datos en fragmentos o

bloques empaquetados como mensajes MQTT desde un origen como S3. Puede tener uno o más archivos asociados con un flujo.

```
aws iot create-stream \
    --cli-input-json file://create-stream.json
```

Contenido de `create-stream.json`:

```
{
    "streamId": "stream12345",
    "description": "This stream is used for Amazon FreeRTOS OTA Update 12345.",
    "files": [
        {
            "fileId": 123,
            "s3Location": {
                "bucket":"codesign-ota-bucket",
                "key":"48c67f3c-63bb-4f92-a98a-4ee0fbc2bef6"
            }
        }
    ],
    "roleArn": "arn:aws:iam:123456789012:role/service-role/my_ota_stream_role"
}
```

Salida:

```
{
     "streamId": "stream12345",
     "streamArn": "arn:aws:iot:us-west-2:123456789012:stream/stream12345",
     "description": "This stream is used for Amazon FreeRTOS OTA Update 12345.",
     "streamVersion": "1"
}
```

Para obtener más información, consulte CreateStream en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte CreateStream en la Referencia de comandos de la AWS CLI.

`create-thing-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-thing-group`.

AWS CLI

Ejemplo 1: creación de un grupo de objetos

En el siguiente ejemplo de `create-thing-group`, se crea un grupo de objetos denominado `LightBulbs` con una descripción y dos atributos.

```
aws iot create-thing-group \
    --thing-group-name LightBulbs \
    --thing-group-properties "thingGroupDescription=\"Generic bulb group\",
 attributePayload={attributes={Manufacturer=AnyCompany,wattage=60}}"
```

Salida:

```
{
    "thingGroupName": "LightBulbs",
    "thingGroupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/LightBulbs",
    "thingGroupId": "9198bf9f-1e76-4a88-8e8c-e7140142c331"
}
```

Ejemplo 2: creación de un grupo de objetos que forme parte de un grupo principal

`create-thing-group` crea un grupo de objetos denominado `HalogenBulbs` que tiene un grupo de objetos principal denominado `LightBulbs`.

```
aws iot create-thing-group \
    --thing-group-name HalogenBulbs \
    --parent-group-name LightBulbs
```

Salida:

```
{
    "thingGroupName": "HalogenBulbs",
    "thingGroupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/HalogenBulbs",
    "thingGroupId": "f4ec6b84-b42b-499d-9ce1-4dbd4d4f6f6e"
}
```

Para obtener más información, consulte Thing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateThingGroup en la Referencia de comandos de la AWS CLI.

`create-thing-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-thing-type`.

AWS CLI

Para definir un tipo de objeto

En el siguiente ejemplo de `create-thing-type`, se define un tipo de objeto y los atributos asociados.

```
aws iot create-thing-type \
    --thing-type-name "LightBulb" \
    --thing-type-properties "thingTypeDescription=light bulb type,
 searchableAttributes=wattage,model"
```

Salida:

```
{
    "thingTypeName": "LightBulb",
    "thingTypeArn": "arn:aws:iot:us-west-2:123456789012:thingtype/LightBulb",
    "thingTypeId": "ce3573b0-0a3c-45a7-ac93-4e0ce14cd190"
}
```

Para obtener más información, consulte Thing Types en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateThingType en la Referencia de comandos de la AWS CLI.

`create-thing`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-thing`.

AWS CLI

Ejemplo 1: creación de un registro de objetos en el registro

En el siguiente ejemplo de `create-thing` se crea una entrada para un dispositivo en el registro de objetos de AWS IoT.

```
aws iot create-thing \
```

```
    --thing-name SampleIoTThing
```

Salida:

```
{
    "thingName": "SampleIoTThing",
    "thingArn": "arn:aws:iot:us-west-2: 123456789012:thing/SampleIoTThing",
    "thingId": " EXAMPLE1-90ab-cdef-fedc-ba987EXAMPLE "
}
```

Ejemplo 2: definición de un objeto que está asociado a un tipo de objeto

En el siguiente ejemplo de `create-thing` se crea un objeto que tiene el tipo de objeto especificado y sus atributos.

```
aws iot create-thing \
    --thing-name "MyLightBulb" \
    --thing-type-name "LightBulb" \
    --attribute-payload "{"attributes": {"wattage":"75", "model":"123"}}"
```

Salida:

```
{
    "thingName": "MyLightBulb",
    "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MyLightBulb",
    "thingId": "40da2e73-c6af-406e-b415-15acae538797"
}
```

Para obtener más información, consulte How to Manage Things with the Registry y Thing Types en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte CreateThing en la Referencia de comandos de la AWS CLI.

`create-topic-rule-destination`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-topic-rule-destination`.

AWS CLI

Para crear un destino de regla de tema

En el siguiente ejemplo de `create-topic-rule-destination`, se crea un destino de regla temática para un punto de conexión HTTP.

```
aws iot create-topic-rule-destination \
    --destination-configuration httpUrlConfiguration={confirmationUrl=https://
example.com}
```

Salida:

```
{
    "topicRuleDestination": {
        "arn": "arn:aws:iot:us-west-2:123456789012:ruledestination/http/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
        "status": "IN_PROGRESS",
        "statusReason": "Awaiting confirmation. Confirmation message sent on
 2020-07-09T22:47:54.154Z; no response received from the endpoint.",
        "httpUrlProperties": {
            "confirmationUrl": "https://example.com"
        }
    }
}
```

Para obtener más información, consulte Creating a topic rule destination en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateTopicRuleDestination en la Referencia de comandos de la AWS CLI.

`create-topic-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-topic-rule`.

AWS CLI

Para crear una regla que envíe una alerta de Amazon SNS

En el siguiente ejemplo de `create-topic-rule` se crea una regla que envía un mensaje de Amazon SNS cuando las lecturas del nivel de humedad del suelo son bajas, tal como se encuentran en la sombra de dispositivo.

```
aws iot create-topic-rule \
    --rule-name "LowMoistureRule" \
```

```
    --topic-rule-payload file://plant-rule.json
```

El ejemplo requiere que se guarde el siguiente código JSON en un archivo denominado`plant-rule.json`:

```
{
    "sql": "SELECT * FROM '$aws/things/MyRPi/shadow/update/accepted' WHERE
 state.reported.moisture = 'low'\n",
    "description": "Sends an alert whenever soil moisture level readings are too
 low.",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [{
            "sns": {
                "targetArn": "arn:aws:sns:us-
west-2:123456789012:MyRPiLowMoistureTopic",
                "roleArn": "arn:aws:iam::123456789012:role/service-role/
MyRPiLowMoistureTopicRole",
                "messageFormat": "RAW"
            }
    }]
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creating an AWS IoT Rule en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte CreateTopicRule en la Referencia de comandos de la AWS CLI.

`delete-account-audit-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-account-audit-configuration`.

AWS CLI

Para deshabilitar todas las comprobaciones de auditoría de su cuenta de AWS

En el siguiente ejemplo de `delete-account-audit-configuration`, se restaura la configuración predeterminada de AWS IoT Device Defender para esta cuenta, y se deshabilitan

todas las comprobaciones de auditoría y borra los datos de configuración. También elimina cualquier auditoría programada para dicha cuenta. Utilice este comando con cuidado.

```
aws iot delete-account-audit-configuration \
    --delete-scheduled-audits
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Comandos de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteAccountAuditConfiguration en la Referencia de comandos de la AWS CLI.

`delete-audit-suppression`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-audit-suppression`.

AWS CLI

Para eliminar la supresión de un resultado de auditoría

En el siguiente ejemplo de `delete-audit-suppression`, se elimina una supresión de resultado de auditoría de DEVICE_CERTIFICATE_EXPIRING_CHECK.

```
aws iot delete-audit-suppression \
    --check-name DEVICE_CERTIFICATE_EXPIRING_CHECK \
    --resource-identifier deviceCertificateId="c7691e<shortened>"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Supresiones de resultados de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteAuditSuppression en la Referencia de comandos de la AWS CLI.

`delete-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-authorizer`.

AWS CLI

Para eliminar un autorizador personalizado

En el siguiente ejemplo de `delete-authorizer`, se elimina el autorizador denominado `CustomAuthorizer`. Un autorizador personalizado debe tener el estado `INACTIVE` para que se pueda eliminar.

```
aws iot delete-authorizer \
    --authorizer-name CustomAuthorizer
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteAuthorizer en la Guía para desarrolladores de AWS IoT.

- Para obtener detalles sobre la API, consulte DeleteAuthorizer en la Referencia de comandos de la AWS CLI.

`delete-billing-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-billing-group`.

AWS CLI

Para eliminar un grupo de facturación

En el siguiente ejemplo de `delete-billing-group`, se elimina el grupo de facturación especificado. Puede eliminar un grupo de facturación aunque contenga uno o varios objetos.

```
aws iot delete-billing-group \
    --billing-group-name BillingGroupTwo
```

Este comando no produce ninguna salida.

Para obtener más información, consulte Billing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteBillingGroup en la Referencia de comandos de la AWS CLI.

`delete-ca-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-ca-certificate`.

AWS CLI

Para eliminar un certificado de CA

En el siguiente ejemplo de `delete-ca-certificate`, se elimina el certificado de CA con el ID especificado.

```
aws iot delete-ca-certificate \
    --certificate-
id f4efed62c0142f16af278166f61962501165c4f05362952074264600 58cd1467
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteCACertificate en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte DeleteCaCertificate en la Referencia de comandos de la AWS CLI.

`delete-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-certificate`.

AWS CLI

Para eliminar un certificado de dispositivo

En el siguiente ejemplo de `delete-certificate` se elimina el certificado de dispositivo con el ID especificado.

```
aws iot delete-certificate \
    --certificate-
id c0c57bbc8baaf4631a9a0345c957657f5e710473e3ddbee1428d216d54d53ac9
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteCertificate en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte DeleteCertificate en la Referencia de comandos de la AWS CLI.

`delete-custom-metric`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-custom-metric`.

AWS CLI

Para eliminar una métrica personalizada

En el siguiente ejemplo de `delete-custom-metric`, se elimina una métrica personalizada.

```
aws iot delete-custom-metric \
    --metric-name batteryPercentage \
    --region us-east-1
```

Salida:

```
HTTP 200
```

Para obtener más información, consulte Métricas personalizadas en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte DeleteCustomMetric en la Referencia de comandos de la AWS CLI.

`delete-dimension`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-dimension`.

AWS CLI

Para eliminar una dimensión

En el siguiente ejemplo de `delete-dimension`, se elimina una dimensión denominada `TopicFilterForAuthMessages`.

```
aws iot delete-dimension \
    --name TopicFilterForAuthMessages
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Comandos de detección en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteDimension en la Referencia de comandos de la AWS CLI.

`delete-domain-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-domain-configuration`.

AWS CLI

Para eliminar una configuración de dominio

En el siguiente ejemplo de `delete-domain-configuration`, se elimina una configuración de dominio denominada `additionalDataDomain` de su cuenta de AWS.

```
aws iot delete-domain-configuration \
    --domain-configuration-name "additionalDataDomain" \
    --domain-configuration-status "OK"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configurable Endpoints en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteDomainConfiguration en la Referencia de comandos de la AWS CLI.

`delete-dynamic-thing-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-dynamic-thing-group`.

AWS CLI

Para eliminar un grupo de objetos dinámico

En el siguiente ejemplo de `delete-dynamic-thing-group`, se elimina el grupo de objetos dinámico especificado.

```
aws iot delete-dynamic-thing-group \
```

```
    --thing-group-name "RoomTooWarm"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Dynamic Thing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteDynamicThingGroup en la Referencia de comandos de la AWS CLI.

`delete-job-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-job-execution`.

AWS CLI

Para eliminar una ejecución de trabajo

En el siguiente ejemplo de `delete-job-execution`, se elimina la ejecución del trabajo especificado en un dispositivo. Utilice `describe-job-execution` para obtener el número de ejecución.

```
aws iot delete-job-execution
    --job-id "example-job-02"
    --thing-name "MyRaspberryPi"
    --execution-number 1
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creating and Managing Jobs (CLI) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteJobExecution en la Referencia de comandos de la AWS CLI.

`delete-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-job`.

AWS CLI

Eliminación de un trabajo

En el siguiente ejemplo de `delete-job`, se elimina el trabajo especificado. Al especificar la opción `--force`, el trabajo se elimina incluso si tiene el estado `IN_PROGRESS`.

```
aws iot delete-job \
    --job-id "example-job-04" \
    --force
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creating and Managing Jobs (CLI) en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte DeleteJob en la Referencia de comandos de la AWS CLI.

`delete-mitigation-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-mitigation-action`.

AWS CLI

Para eliminar una acción de mitigación

En el siguiente ejemplo de `delete-mitigation-action`, se elimina la acción de mitigación especificada.

```
aws iot delete-mitigation-action \
    --action-name AddThingsToQuarantineGroup1Action
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteMitigationAction (comandos de las acciones de mitigación) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteMitigationAction en la Referencia de comandos de la AWS CLI.

`delete-ota-update`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-ota-update`.

AWS CLI

Para eliminar una actualización OTA

En el siguiente ejemplo de `delete-ota-update`, se elimina la actualización de OTA especificada.

```
aws iot delete-ota-update \
    --ota-update-id ota12345 \
    --delete-stream \
    --force-delete-aws-job
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteOTAUpdate en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte DeleteOtaUpdate en la Referencia de comandos de la AWS CLI.

`delete-policy-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-policy-version`.

AWS CLI

Para eliminar una versión de una política

En el siguiente ejemplo de `delete-policy-version`, se elimina la versión 2 de la política especificada de su cuenta de AWS.

```
aws iot delete-policy-version \
    --policy-name UpdateDeviceCertPolicy \
    --policy-version-id 2
```

Este comando no genera ninguna salida.

Para obtener más información, consulte AWS IoT Policies en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeletePolicyVersion en la Referencia de comandos de la AWS CLI.

`delete-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-policy`.

AWS CLI

Eliminación de una política

En el siguiente ejemplo de `delete-policy`, se elimina la política especificada de su cuenta de AWS.

```
aws iot delete-policy --policy-name UpdateDeviceCertPolicy
```

Este comando no genera ninguna salida.

Para obtener más información, consulte AWS IoT Policies en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeletePolicy en la Referencia de comandos de la AWS CLI.

`delete-provisioning-template-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-provisioning-template-version`.

AWS CLI

Para eliminar una versión de plantilla de aprovisionamiento

En el siguiente ejemplo de `delete-provisioning-template-version`, se elimina la versión 2 de la plantilla de aprovisionamiento especificada.

```
aws iot delete-provisioning-template-version \
    --version-id 2 \
    --template-name "widget-template"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte AWS IoT Secure Tunneling en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte DeleteProvisioningTemplateVersion en la Referencia de comandos de la AWS CLI.

`delete-provisioning-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-provisioning-template`.

AWS CLI

Para eliminar una plantilla de aprovisionamiento

En el siguiente ejemplo de `delete-provisioning-template`, se elimina la plantilla de aprovisionamiento especificada.

```
aws iot delete-provisioning-template \
    --template-name widget-template
```

Este comando no genera ninguna salida.

Para obtener más información, consulte AWS IoT Secure Tunneling en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte DeleteProvisioningTemplate en la Referencia de comandos de la AWS CLI.

`delete-registration-code`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-registration-code`.

AWS CLI

Para eliminar el código de registro

En el siguiente ejemplo de `delete-registration-code`, se elimina un código de registro específico de una cuenta de AWS IoT.

```
aws iot delete-registration-code
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Use Your Own Certificate en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteRegistrationCode en la Referencia de comandos de la AWS CLI.

`delete-role-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-role-alias`.

AWS CLI

Para eliminar un alias de rol de AWS IoT

En el siguiente ejemplo de `delete-role-alias`, se elimina un alias de rol de AWS IoT denominado `LightBulbRole`.

```
aws iot delete-role-alias \
    --role-alias LightBulbRole
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Authorizing Direct Calls to AWS Services en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteRoleAlias en la Referencia de comandos de la AWS CLI.

`delete-scheduled-audit`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-scheduled-audit`.

AWS CLI

Para eliminar una auditoría programada

En el siguiente ejemplo de `delete-scheduled-audit`, se elimina la auditoría programada de AWS IoT Device Defender denominada `AWSIoTDeviceDefenderDailyAudit`.

```
aws iot delete-scheduled-audit \
    --scheduled-audit-name AWSIoTDeviceDefenderDailyAudit
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Comandos de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteScheduledAudit en la Referencia de comandos de la AWS CLI.

`delete-security-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-security-profile`.

AWS CLI

Para eliminar un perfil de seguridad

En el siguiente ejemplo de `delete-security-profile`, se elimina un perfil de seguridad denominado `PossibleIssue`.

```
aws iot delete-security-profile \
    --security-profile-name PossibleIssue
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Comandos de detección en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteSecurityProfile en la Referencia de comandos de la AWS CLI.

`delete-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-stream`.

AWS CLI

Para eliminar un flujo

En el siguiente ejemplo de `delete-stream`, se elimina el flujo especificado.

```
aws iot delete-stream \
```

```
    --stream-id stream12345
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteStream en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte DeleteStream en la Referencia del comando de la AWS CLI.

`delete-thing-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-thing-group`.

AWS CLI

Para eliminar un grupo de objetos

En el siguiente ejemplo de `delete-thing-group`, se elimina el grupo de objetos especificado. No se puede eliminar un grupo de objetos si contiene grupos de objetos secundarios.

```
aws iot delete-thing-group \
    --thing-group-name DefectiveBulbs
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Thing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteThingGroup en la Referencia de comandos de la AWS CLI.

`delete-thing-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-thing-type`.

AWS CLI

Ejemplo 1: eliminación de un tipo de objeto

En el siguiente ejemplo de `delete-thing-type`, se elimina un tipo de objeto obsoleto.

```
aws iot delete-thing-type \
```

```
    --thing-type-name "obsoleteThingType"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Thing Types en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteThingType en la Referencia de comandos de la AWS CLI.

`delete-thing`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-thing`.

AWS CLI

Para visualizar información detallada acerca de un objeto

En el siguiente ejemplo de `delete-thing` se elimina un objeto del registro de AWS IoT de su cuenta de AWS.

aws iot delete-thing --thing-name "FourthBulb"

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración de objetos con el registro en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte DeleteThing en la Referencia de comandos de la AWS CLI.

`delete-topic-rule-destination`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-topic-rule-destination`.

AWS CLI

Para eliminar un destino de regla de tema

En el siguiente ejemplo de `delete-topic-rule-destination`, se elimina el destino de la regla del tema especificado.

```
aws iot delete-topic-rule-destination \
```

```
    --arn "arn:aws:iot:us-west-2:123456789012:ruledestination/http/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting a topic rule destination en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteTopicRuleDestination en la Referencia de comandos de la AWS CLI.

`delete-topic-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-topic-rule`.

AWS CLI

Para eliminar una regla

En el siguiente ejemplo de `delete-topic-rule` se elimina la regla especificada.

```
aws iot delete-topic-rule \
    --rule-name "LowMoistureRule"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting a Rule en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte DeleteTopicRule en la Referencia de comandos de la AWS CLI.

`delete-v2-logging-level`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-v2-logging-level`.

AWS CLI

Para eliminar el nivel de registro de un grupo de objetos

En el siguiente ejemplo de `delete-v2-logging-level`, se elimina el nivel de registro para el grupo de objetos especificado.

```
aws iot delete-v2-logging-level \
    --target-type THING_GROUP \
    --target-name LightBulbs
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteV2LoggingLevel en la Referencia de comandos de la AWS CLI.

`deprecate-thing-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `deprecate-thing-type`.

AWS CLI

Ejemplo 1: obsolescencia de un tipo de objeto

En el siguiente ejemplo de `deprecate-thing-type`, se da de baja un tipo de objeto para que los usuarios no puedan asociarle ningún objeto nuevo.

```
aws iot deprecate-thing-type \
    --thing-type-name "obsoleteThingType"
```

Este comando no genera ninguna salida.

Ejemplo 2: reversión de la obsolescencia de un tipo de objeto

En el siguiente ejemplo de `deprecate-thing-type`, se anula la obsolescencia de un tipo de objeto, lo que permite a los usuarios volver a asociarle objetos nuevos.

```
aws iot deprecate-thing-type \
    --thing-type-name "obsoleteThingType" \
    --undo-deprecate
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Thing Types en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeprecateThingType en la Referencia de comandos de la AWS CLI.

describe-account-audit-configuration

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-account-audit-configuration`.

AWS CLI

Para ver los ajustes de configuración de auditoría actuales

En el siguiente ejemplo de `describe-account-audit-configuration`, se enumera los ajustes actuales de la configuración de auditoría de AWS IoT Device Defender.

```
aws iot describe-account-audit-configuration
```

Salida:

```
{
    "roleArn": "arn:aws:iam::123456789012:role/service-role/
AWSIoTDeviceDefenderAudit_1551201085996",
    "auditNotificationTargetConfigurations": {
        "SNS": {
            "targetArn": "arn:aws:sns:us-west-2:123456789012:ddaudits",
            "roleArn": "arn:aws:iam::123456789012:role/service-role/
AWSIoTDeviceDefenderAudit",
            "enabled": true
        }
    },
    "auditCheckConfigurations": {
        "AUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK": {
            "enabled": true
        },
        "CA_CERTIFICATE_EXPIRING_CHECK": {
            "enabled": true
        },
        "CONFLICTING_CLIENT_IDS_CHECK": {
            "enabled": true
        },
        "DEVICE_CERTIFICATE_EXPIRING_CHECK": {
            "enabled": true
        },
        "DEVICE_CERTIFICATE_SHARED_CHECK": {
            "enabled": true
        },
```

```
        "IOT_POLICY_OVERLY_PERMISSIVE_CHECK": {
            "enabled": true
        },
        "LOGGING_DISABLED_CHECK": {
            "enabled": true
        },
        "REVOKED_CA_CERTIFICATE_STILL_ACTIVE_CHECK": {
            "enabled": true
        },
        "REVOKED_DEVICE_CERTIFICATE_STILL_ACTIVE_CHECK": {
            "enabled": true
        },
        "UNAUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK": {
            "enabled": true
        }
    }
}
```

Para obtener más información, consulte Comandos de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeAccountAuditConfiguration en la Referencia de comandos de la AWS CLI.

`describe-audit-finding`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-audit-finding`.

AWS CLI

Para enumerar los detalles de un resultado de auditoría

En el siguiente ejemplo de `describe-audit-finding`, se enumeran los detalles del resultado de auditoría de AWS IoT Device Defender especificado. Una auditoría puede generar varios resultados. Utilice el comando `list-audit-findings` para obtener una lista de los resultados de una auditoría para obtener el `findingId`.

```
aws iot describe-audit-finding \
    --finding-id "ef4826b8-e55a-44b9-b460-5c485355371b"
```

Salida:

```
{
    "finding": {
        "findingId": "ef4826b8-e55a-44b9-b460-5c485355371b",
        "taskId": "873ed69c74a9ec8fa9b8e88e9abc4661",
        "checkName": "IOT_POLICY_OVERLY_PERMISSIVE_CHECK",
        "taskStartTime": 1576012045.745,
        "findingTime": 1576012046.168,
        "severity": "CRITICAL",
        "nonCompliantResource": {
            "resourceType": "IOT_POLICY",
            "resourceIdentifier": {
                "policyVersionIdentifier": {
                    "policyName": "smp-ggrass-group_Core-policy",
                    "policyVersionId": "1"
                }
            }
         },
        "reasonForNonCompliance": "Policy allows broad access to IoT data plane
 actions: [iot:Subscribe, iot:Connect, iot:GetThingShadow, iot:DeleteThingShadow,
 iot:UpdateThingShadow, iot:Publish].",
        "reasonForNonComplianceCode":
 "ALLOWS_BROAD_ACCESS_TO_IOT_DATA_PLANE_ACTIONS"
    }
}
```

Para obtener más información, consulte Comprobar resultados de auditoría (Comandos de auditoría) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeAuditFinding en la Referencia de comandos de la AWS CLI.

`describe-audit-mitigation-actions-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-audit-mitigation-actions-task`.

AWS CLI

Para mostrar los detalles de una tarea de acciones de mitigación de auditoría

En el siguiente ejemplo de `describe-audit-mitigation-actions-task`, se muestran los detalles de la tarea especificada en la que se ha aplicado `ResetPolicyVersionAction` a un

resultado. Los resultados incluyen cuándo comenzó y finalizó la tarea, cuántos resultados se buscaron (y cuál fue el resultado) y la definición de la acción que se aplicó como parte de esta tarea.

```
aws iot describe-audit-mitigation-actions-task \
    --task-id ResetPolicyTask01
```

Salida:

```
{
    "taskStatus": "COMPLETED",
    "startTime": "2019-12-10T15:13:19.457000-08:00",
    "endTime": "2019-12-10T15:13:19.947000-08:00",
    "taskStatistics": {
        "IOT_POLICY_OVERLY_PERMISSIVE_CHECK": {
            "totalFindingsCount": 1,
            "failedFindingsCount": 0,
            "succeededFindingsCount": 1,
            "skippedFindingsCount": 0,
            "canceledFindingsCount": 0
        }
    },
    "target": {
        "findingIds": [
            "ef4826b8-e55a-44b9-b460-5c485355371b"
        ]
    },
    "auditCheckToActionsMapping": {
        "IOT_POLICY_OVERLY_PERMISSIVE_CHECK": [
            "ResetPolicyVersionAction"
        ]
    },
    "actionsDefinition": [
        {
            "name": "ResetPolicyVersionAction",
            "id": "1ea0b415-bef1-4a01-bd13-72fb63c59afb",
            "roleArn": "arn:aws:iam::123456789012:role/service-role/
ReplacePolicyVersionRole",
            "actionParams": {
                "replaceDefaultPolicyVersionParams": {
                    "templateName": "BLANK_POLICY"
                }
            }
```

```
        }
    ]
}
```

Para obtener más información, consulte DescribeAuditMitigationActionsTask (Comandos de las acciones de mitigación) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeAuditMitigationActionsTask en la Referencia de comandos de la AWS CLI.

`describe-audit-suppression`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-audit-suppression`.

AWS CLI

Para obtener información sobre la supresión de un resultado de auditoría

En el siguiente ejemplo de `describe-audit-suppression`, se enumeran los detalles sobre la supresión de un resultado de auditoría.

```
aws iot describe-audit-task \
    --task-id "787ed873b69cb4d6cdbae6ddd06996c5"
```

Salida:

```
{
    "taskStatus": "COMPLETED",
    "taskType": "SCHEDULED_AUDIT_TASK",
    "taskStartTime": 1596168096.157,
    "taskStatistics": {
        "totalChecks": 1,
        "inProgressChecks": 0,
        "waitingForDataCollectionChecks": 0,
        "compliantChecks": 0,
        "nonCompliantChecks": 1,
        "failedChecks": 0,
        "canceledChecks": 0
    },
    "scheduledAuditName": "AWSIoTDeviceDefenderDailyAudit",
    "auditDetails": {
        "DEVICE_CERTIFICATE_EXPIRING_CHECK": {
            "checkRunStatus": "COMPLETED_NON_COMPLIANT",
```

```
            "checkCompliant": false,
            "totalResourcesCount": 195,
            "nonCompliantResourcesCount": 2
        }
    }
}
```

Para obtener más información, consulte Supresiones de resultados de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeAuditSuppression en la Referencia de comandos de la AWS CLI.

`describe-audit-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-audit-task`.

AWS CLI

Para obtener información sobre una instancia de auditoría

En el siguiente ejemplo de `describe-audit-task`, se obtiene información sobre una instancia de una auditoría de AWS IoT Device Defender. Si la auditoría se ha completado, las estadísticas de resumen de la ejecución se incluyen en los resultados.

```
aws iot describe-audit-task \
    --task-id a3aea009955e501a31b764abe1bebd3d
```

Salida:

```
{
   "taskStatus": "COMPLETED",
   "taskType": "ON_DEMAND_AUDIT_TASK",
   "taskStartTime": 1560356923.434,
   "taskStatistics": {
       "totalChecks": 3,
       "inProgressChecks": 0,
       "waitingForDataCollectionChecks": 0,
       "compliantChecks": 3,
       "nonCompliantChecks": 0,
       "failedChecks": 0,
       "canceledChecks": 0
```

```
    },
    "auditDetails": {
        "CA_CERTIFICATE_EXPIRING_CHECK": {
            "checkRunStatus": "COMPLETED_COMPLIANT",
            "checkCompliant": true,
            "totalResourcesCount": 0,
            "nonCompliantResourcesCount": 0
        },
        "DEVICE_CERTIFICATE_EXPIRING_CHECK": {
            "checkRunStatus": "COMPLETED_COMPLIANT",
            "checkCompliant": true,
            "totalResourcesCount": 6,
            "nonCompliantResourcesCount": 0
        },
        "REVOKED_CA_CERTIFICATE_STILL_ACTIVE_CHECK": {
            "checkRunStatus": "COMPLETED_COMPLIANT",
            "checkCompliant": true,
            "totalResourcesCount": 0,
            "nonCompliantResourcesCount": 0
        }
    }
}
```

Para obtener más información, consulte Comandos de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeAuditTask en la Referencia de comandos de la AWS CLI.

`describe-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-authorizer`.

AWS CLI

Para obtener información sobre un autorizador personalizado

En el siguiente ejemplo de `describe-authorizer`, se muestran los detalles del autorizador personalizado especificado.

```
aws iot describe-authorizer \
    --authorizer-name CustomAuthorizer
```

Salida:

```
{
    "authorizerDescription": {
        "authorizerName": "CustomAuthorizer",
        "authorizerArn": "arn:aws:iot:us-west-2:123456789012:authorizer/
CustomAuthorizer",
        "authorizerFunctionArn": "arn:aws:lambda:us-
west-2:123456789012:function:CustomAuthorizerFunction",
        "tokenKeyName": "MyAuthToken",
        "tokenSigningPublicKeys": {
            "FIRST_KEY": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1uJOB4lQPgG/lM6ZfIwo
\nZ+7ENxAio9q6QD4FFqjGZsvjtYwjoe1RKK0U8Eq9xb5O3kRSmyIwTzwzm/f4Gf0Y
\nZUloJ+t3PUUwHrmbYTAgTrCUgRFygjfgVwGCPs5ZAX4Eyqt5cr+AIHIiUDbxSa7p
\nzwOBKPeic0asNJpqT8PkBbRaKyleJh5oo81NDHHmVtbBm5A5YiJjqYXLaVAowKzZ\n
+GqsNvAQ9Jy1wI2VrEa1OfL8flDB/BJLm7zjpfPOHDJQgID0XnZwAlNnZcOhCwIx\n50g2LW2Oy9R/
dmqtDmJiVP97Z4GykxPvwlYHrUXY0iW1R3AR/Ac1NhCTGZMwVDB1\nlQIDAQAB\n-----END PUBLIC
 KEY-----"
        },
        "status": "ACTIVE",
        "creationDate": 1571245658.069,
        "lastModifiedDate": 1571245658.069
    }
}
```

Para obtener más información, consulte DescribeAuthorizer en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte DescribeAuthorizer en la Referencia de comandos de la AWS CLI.

`describe-billing-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-billing-group`.

AWS CLI

Para obtener información acerca de un grupo de facturación

En el siguiente ejemplo de `describe-billing-group`, se obtiene información del grupo de facturación especificado.

```
aws iot describe-billing-group --billing-group-name GroupOne
```

Salida:

```
{
    "billingGroupName": "GroupOne",
    "billingGroupId": "103de383-114b-4f51-8266-18f209ef5562",
    "billingGroupArn": "arn:aws:iot:us-west-2:123456789012:billinggroup/GroupOne",
    "version": 1,
    "billingGroupProperties": {},
    "billingGroupMetadata": {
        "creationDate": 1560199355.378
    }
}
```

Para obtener más información, consulte Billing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeBillingGroup en la Referencia de comandos de la AWS CLI.

`describe-ca-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-ca-certificate`.

AWS CLI

Para obtener detalles sobre un certificado de CA

En el siguiente ejemplo de `describe-ca-certificate`, se muestran los detalles del certificado de CA especificado.

```
aws iot describe-ca-certificate \
    --certificate-
id f4efed62c0142f16af278166f61962501165c4f053629520742646005 8cd1467
```

Salida:

```
{
    "certificateDescription": {
        "certificateArn": "arn:aws:iot:us-west-2:123456789012:cacert/
f4efed62c0142f16af278166f61962501165c4f053629520742646005 8cd1467",
```

```
        "certificateId":
 "f4efed62c0142f16af278166f61962501165c4f0536295207426460058cd1467",
        "status": "INACTIVE",
        "certificatePem": "-----BEGIN CERTIFICATE-----
\nMIICzzCCAbegEXAMPLEJANVEPWXl8taPMA0GCSqGSIb3DQEBBQUAMB4xCzAJBgNV
\nBAYTAlVTMQ8wDQYDVQQKDAZBbWF6b24wHhcNMTkwOTI0MjEzMTE1WhcNMjkwOTIx
\nMjEzMTE1WjAeMQswCQYDVQQGEwJVUzEPMA0GA1UECgwGQW1hem9uMIIBIjANBgkq
\nhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzd3R3ioalCS0MhFWfBrVGR036EK07UAf
\nVdz9EXAMPLE1VczICbADnATK522kEIB51/18VzlFtAhQL5V5eybXKnB7QebNer5m
\n4Yibx7shR5oqNzFsrXWxuugN5+w5gEfqNMawOjhF4LsculKG49yuqjcDU19/13ua
\n3B2gxs1Pe7TiWWvUskzxnbO1F2WCshbEJvqY8fIWtGYCjTeJAgQ9hvZx/69XhKen
\nwV9LJwOQxrsUS0Ty8IHwbB8fRy72VM3u7fJoaU+nO4jD5cqaoEPtzoeFUEXAMPLE
\nyVAJpqHwgbYbcUfn7V+AB6yh1+0Fa1rEQGuZDPGyJslxwr5vh8nRewIDAQABoxAw
\nDjAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQA+3a5CV3IJgOnd0AgI
\nBgVMtmYzTvqAngx26aG9/spvCjXckh2SBF+EcBlCFwH1yakwjJL1dR4yarnrfxgI
\nEqP4AOYVimAVoQ5FBwnloHe16+3qtDiblU9DeXBUCtS55EcfrEXAMPLEYtXdqU5C
\nU9ia4KAjV0dxW1+EFYMwX5eGeb0gDTNHBylV6B/fOSZiQAwDYp4x3B+gAP+a/bWB
\nu1umOqtBdWe6L6/83L+JhaTByqV25iVJ4c/UZUnG8926wUlDM9zQvEXuEVvzZ7+m\n4PSNqst/
nVOvnLpoG4e0WgcJgANuB33CSWtjWSuYsbhmqQRknGhREXAMPLEZT4fm\nfo0e\n-----END
 CERTIFICATE-----\n",
        "ownedBy": "123456789012",
        "creationDate": 1569365372.053,
        "autoRegistrationStatus": "DISABLE",
        "lastModifiedDate": 1569365372.053,
        "customerVersion": 1,
        "generationId": "c5c2eb95-140b-4f49-9393-6aaac85b2a90",
        "validity": {
            "notBefore": 1569360675.0,
            "notAfter": 1884720675.0
        }
    }
}
```

Para obtener más información, consulte DescribeCACertificate en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte DescribeCaCertificate en la Referencia de comandos de la AWS CLI.

`describe-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-certificate`.

AWS CLI

Para obtener información sobre un certificado

En el siguiente ejemplo de `describe-certificate`, se muestran los detalles del certificado especificado.

```
aws iot describe-certificate \
    --certificate-
id "4f0ba725787aa94d67d2fca420eca022242532e8b3c58e7465c7778b443fd65e"
```

Salida:

```
{
    "certificateDescription": {
        "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/4f0ba725787aa94d67d2fca420eca022242532e8b3c58e7465c7778b443fd65e",
        "certificateId":
 "4f0ba725787aa94d67d2fca420eca022242532e8b3c58e7465c7778b443fd65e",
        "status": "ACTIVE",
        "certificatePem": "-----BEGIN CERTIFICATE-----
MIICiTEXAMPLEQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBEXAMPLEMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDEXAMPLElMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5EXAMPLEcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNEXAMPLEdBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBEXAMPLEz
b2xEXAMPLEYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8EXAMPLEZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYEXAMPLEpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7EXAMPLEGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFEXAMPLEAtCu4
nUhVVxYUnEXAMPLE8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GEXAMPLEl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----",
        "ownedBy": "123456789012",
        "creationDate": 1541022751.983,
        "lastModifiedDate": 1541022751.983,
        "customerVersion": 1,
        "transferData": {},
        "generationId": "6974fbed-2e61-4114-bc5e-4204cc79b045",
        "validity": {
```

```
            "notBefore": 1541022631.0,
            "notAfter": 2524607999.0
        }
    }
}
```

Para obtener más información, consulte DescribeCertificate en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte DescribeCertificate en la Referencia de comandos de la AWS CLI.

`describe-custom-metric`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-custom-metric`.

AWS CLI

Para obtener información sobre una métrica personalizada de Device Defender

En el siguiente ejemplo de `describe-custom-metric`, se obtiene información sobre una métrica personalizada denominada `myCustomMetric`.

```
aws iot describe-custom-metric \
    --metric-name myCustomMetric
```

Salida:

```
{
    "metricName": "myCustomMetric",
    "metricArn": "arn:aws:iot:us-east-1:1234564789012:custommetric/myCustomMetric",
    "metricType": "number",
    "displayName": "My custom metric",
    "creationDate": 2020-11-17T23:02:12.879000-09:00,
    "lastModifiedDate": 2020-11-17T23:02:12.879000-09:00
}
```

Para obtener más información, consulte Métricas personalizadas en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte DescribeCustomMetric en la Referencia de comandos de la AWS CLI.

describe-default-authorizer

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-default-authorizer`.

AWS CLI

Para obtener información sobre un autorizador personalizado predeterminado

En el siguiente ejemplo de `describe-default-authorizer`, se muestran los detalles del autorizador personalizado predeterminado.

```
aws iot describe-default-authorizer
```

Salida:

```
{
    "authorizerName": "CustomAuthorizer",
    "authorizerArn": "arn:aws:iot:us-west-2:123456789012:authorizer/
CustomAuthorizer"
}
```

Para obtener más información, consulte DescribeDefaultAuthorizer en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte DescribeDefaultAuthorizer en la Referencia de comandos de la AWS CLI.

describe-dimension

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-dimension`.

AWS CLI

Para obtener información sobre una dimensión

En el siguiente ejemplo de `describe-dimension`, se obtiene información sobre una dimensión denominada `TopicFilterForAuthMessages`.

```
aws iot describe-dimension \
    --name TopicFilterForAuthMessages
```

Salida:

```
{
    "name": "TopicFilterForAuthMessages",
    "arn": "arn:aws:iot:eu-west-2:123456789012:dimension/
TopicFilterForAuthMessages",
    "type": "TOPIC_FILTER",
    "stringValues": [
        "device/+/auth"
    ],
    "creationDate": 1578620223.255,
    "lastModifiedDate": 1578620223.255
}
```

Para obtener más información, consulte Comandos de detección en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeDimension en la Referencia de comandos de la AWS CLI.

`describe-domain-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-domain-configuration`.

AWS CLI

Para describir una configuración de dominio

En el siguiente ejemplo de `describe-domain-configuration`, se muestran los detalles de la configuración de dominios especificada.

```
aws iot describe-domain-configuration \
    --domain-configuration-name "additionalDataDomain"
```

Salida:

```
{
    "domainConfigurationName": "additionalDataDomain",
    "domainConfigurationArn": "arn:aws:iot:us-
east-1:758EXAMPLE143:domainconfiguration/additionalDataDomain/norpw",
    "domainName": "d055exampleed74y71zfd-ats.beta.us-east-1.iot.amazonaws.com",
    "serverCertificates": [],
```

```
    "domainConfigurationStatus": "ENABLED",
    "serviceType": "DATA",
    "domainType": "AWS_MANAGED",
    "lastStatusChangeDate": 1601923783.774
}
```

Para obtener más información, consulte Configurable Endpoints en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeDomainConfiguration en la Referencia de comandos de la AWS CLI.

`describe-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-endpoint`.

AWS CLI

Ejemplo 1: Obtención de su punto de conexión de AWS actual

En el siguiente ejemplo de `describe-endpoint` se recupera el punto de conexión predeterminado de AWS al que se aplican todos los comandos.

```
aws iot describe-endpoint
```

Salida:

```
{
    "endpointAddress": "abc123defghijk.iot.us-west-2.amazonaws.com"
}
```

Para obtener más información, consulte DescribeEndpoint en la Guía para desarrolladores de AWS IoT.

Ejemplo 2: Obtención del punto de conexión ATS

En el siguiente ejemplo de `describe-endpoint` se recupera el punto de conexión de Amazon Trust Services (ATS).

```
aws iot describe-endpoint \
    --endpoint-type iot:Data-ATS
```

Salida:

```
{
    "endpointAddress": "abc123defghijk-ats.iot.us-west-2.amazonaws.com"
}
```

Para obtener más información, consulte Certificados X.509 y AWS IoT en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeEndpoint en la Referencia de comandos de la AWS CLI.

`describe-event-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-event-configurations`.

AWS CLI

Para mostrar qué tipos de eventos se publican

En el siguiente ejemplo de `describe-event-configurations`, se enumera la configuración que controla los eventos que se generan cuando se agrega, actualiza o elimina algo.

```
aws iot describe-event-configurations
```

Salida:

```
{
    "eventConfigurations": {
        "CA_CERTIFICATE": {
            "Enabled": false
        },
        "CERTIFICATE": {
            "Enabled": false
        },
        "JOB": {
            "Enabled": false
        },
        "JOB_EXECUTION": {
            "Enabled": false
        },
        "POLICY": {
```

```
            "Enabled": false
        },
        "THING": {
            "Enabled": false
        },
        "THING_GROUP": {
            "Enabled": false
        },
        "THING_GROUP_HIERARCHY": {
            "Enabled": false
        },
        "THING_GROUP_MEMBERSHIP": {
            "Enabled": false
        },
        "THING_TYPE": {
            "Enabled": false
        },
        "THING_TYPE_ASSOCIATION": {
            "Enabled": false
        }
    }
}
```

Para obtener más información, consulte Event Messages en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeEventConfigurations en la Referencia de comandos de la AWS CLI.

`describe-index`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-index`.

AWS CLI

Para recuperar el estado actual del índice de objetos

En el siguiente ejemplo de `describe-index`, se recupera el estado actual del índice de objetos.

```
aws iot describe-index \
    --index-name "AWS_Things"
```

Salida:

```
{
    "indexName": "AWS_Things",
    "indexStatus": "ACTIVE",
    "schema": "REGISTRY_AND_SHADOW_AND_CONNECTIVITY_STATUS"
}
```

Para obtener más información, consulte Managing Thing Indexing, en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeIndex en la Referencia de comandos de la AWS CLI.

`describe-job-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-job-execution`.

AWS CLI

Para obtener los detalles de ejecución de un trabajo en un dispositivo

En el siguiente ejemplo de `describe-job-execution`, se obtienen los detalles de la ejecución del trabajo especificado.

```
aws iot describe-job-execution \
    --job-id "example-job-01" \
    --thing-name "MyRaspberryPi"
```

Salida:

```
{
    "execution": {
        "jobId": "example-job-01",
        "status": "QUEUED",
        "statusDetails": {},
        "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MyRaspberryPi",
        "queuedAt": 1560787023.636,
        "lastUpdatedAt": 1560787023.636,
        "executionNumber": 1,
        "versionNumber": 1
    }
}
```

Para obtener más información, consulte Creating and Managing Jobs (CLI) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeJobExecution en la Referencia de comandos de la AWS CLI.

`describe-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-job`.

AWS CLI

Para obtener el estado detallado de un trabajo

En el siguiente ejemplo de `describe-job`, se obtiene el estado detallado del trabajo cuyo ID es `example-job-01`.

```
aws iot describe-job \
    --job-id "example-job-01"
```

Salida:

```
{
    "job": {
        "jobArn": "arn:aws:iot:us-west-2:123456789012:job/example-job-01",
        "jobId": "example-job-01",
        "targetSelection": "SNAPSHOT",
        "status": "IN_PROGRESS",
        "targets": [
            "arn:aws:iot:us-west-2:123456789012:thing/MyRaspberryPi"
        ],
        "description": "example job test",
        "presignedUrlConfig": {},
        "jobExecutionsRolloutConfig": {},
        "createdAt": 1560787022.733,
        "lastUpdatedAt": 1560787026.294,
        "jobProcessDetails": {
            "numberOfCanceledThings": 0,
            "numberOfSucceededThings": 0,
            "numberOfFailedThings": 0,
            "numberOfRejectedThings": 0,
            "numberOfQueuedThings": 1,
            "numberOfInProgressThings": 0,
```

```
            "numberOfRemovedThings": 0,
            "numberOfTimedOutThings": 0
        },
        "timeoutConfig": {}
    }
}
```

Para obtener más información, consulte Creating and Managing Jobs (CLI) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeJob en la Referencia de comandos de AWS CLI.

`describe-mitigation-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-mitigation-action`.

AWS CLI

Para ver los detalles de una acción de mitigación definida

En el siguiente ejemplo de `describe-mitigation-action`, se muestran los detalles de la acción de mitigación especificada.

```
aws iot describe-mitigation-action \
    --action-name AddThingsToQuarantineGroupAction
```

Salida:

```
{
    "actionName": "AddThingsToQuarantineGroupAction",
    "actionType": "ADD_THINGS_TO_THING_GROUP",
    "actionArn": "arn:aws:iot:us-west-2:123456789012:mitigationaction/
AddThingsToQuarantineGroupAction",
    "actionId": "2fd2726d-98e1-4abf-b10f-09465ccd6bfa",
    "roleArn": "arn:aws:iam::123456789012:role/service-role/
MoveThingsToQuarantineGroupRole",
    "actionParams": {
        "addThingsToThingGroupParams": {
            "thingGroupNames": [
                "QuarantineGroup1"
            ],
            "overrideDynamicGroups": true
```

```
        }
    },
    "creationDate": "2019-12-10T11:09:35.999000-08:00",
    "lastModifiedDate": "2019-12-10T11:09:35.999000-08:00"
}
```

Para obtener más información, consulte DescribeMitigationAction (Comandos de las acciones de mitigación) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeMitigationAction en la Referencia de comandos de la AWS CLI.

`describe-provisioning-template-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-provisioning-template-version`.

AWS CLI

Para describir una versión de plantilla de aprovisionamiento

En el siguiente ejemplo de `describe-provisioning-template-version`, se describe una versión de plantilla de aprovisionamiento.

```
aws iot describe-provisioning-template-version \
    --template-name MyTestProvisioningTemplate \
    --version-id 1
```

Salida:

```
{
    "versionId": 1,
    "creationDate": 1589308310.574,
    "templateBody": "{
        \"Parameters\":{
            \"SerialNumber\":{
                \"Type\":\"String\"
            },
            \"AWS::IoT::Certificate::Id\":{
                \"Type\":\"String\"
            }
        },
```

```
        \"Resources\":{
            \"certificate\":{
                \"Properties\":{
                    \"CertificateId\":{
                        \"Ref\":\"AWS::IoT::Certificate::Id\"
                    },
                    \"Status\":\"Active\"
                },
                \"Type\":\"AWS::IoT::Certificate\"
            },
            \"policy\":{
                \"Properties\":{
                    \"PolicyName\":\"MyIotPolicy\"
                },
                \"Type\":\"AWS::IoT::Policy\"
            },
            \"thing\":{
                \"OverrideSettings\":{
                    \"AttributePayload\":\"MERGE\",
                    \"ThingGroups\":\"DO_NOTHING\",
                    \"ThingTypeName\":\"REPLACE\"
                },
                \"Properties\":{
                    \"AttributePayload\":{},
                    \"ThingGroups\":[],
                    \"ThingName\":{
                        \"Fn::Join\":[
                            \"\",
                            [
                                \"DemoGroup_\",
                                {\"Ref\":\"SerialNumber\"}
                            ]
                        ]
                    },
                    \"ThingTypeName\":\"VirtualThings\"
                },
                \"Type\":\"AWS::IoT::Thing\"
            }
        }
    }",
    "isDefaultVersion": true
}
```

Para obtener más información, consulte Provisioning devices that don't have device certificates using fleet provisioning en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte DescribeProvisioningTemplateVersion en la Referencia de comandos de la AWS CLI.

`describe-provisioning-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-provisioning-template`.

AWS CLI

Para describir una plantilla de aprovisionamiento

En el siguiente ejemplo de `describe-provisioning-template`, se describe una plantilla de aprovisionamiento.

```
aws iot describe-provisioning-template \
    --template-name MyTestProvisioningTemplate
```

Salida:

```
{
    "templateArn": "arn:aws:iot:us-west-2:57EXAMPLE833:provisioningtemplate/
MyTestProvisioningTemplate",
    "templateName": "MyTestProvisioningTemplate",
    "creationDate": 1589308310.574,
    "lastModifiedDate": 1589308345.539,
    "defaultVersionId": 1,
    "templateBody": "{
        \"Parameters\":{
            \"SerialNumber\":{
                \"Type\":\"String\"
            },
            \"AWS::IoT::Certificate::Id\":{
                \"Type\":\"String\"
            }
        },
        \"Resources\":{
            \"certificate\":{
                \"Properties\":{
                    \"CertificateId\":{
                        \"Ref\":\"AWS::IoT::Certificate::Id\"
```

```
                    },
                    \"Status\":\"Active\"
                },
                \"Type\":\"AWS::IoT::Certificate\"
            },
            \"policy\":{
                \"Properties\":{
                    \"PolicyName\":\"MyIotPolicy\"
                },
                \"Type\":\"AWS::IoT::Policy\"
            },
            \"thing\":{
                \"OverrideSettings\":{
                    \"AttributePayload\":\"MERGE\",
                    \"ThingGroups\":\"DO_NOTHING\",
                    \"ThingTypeName\":\"REPLACE\"
                },
                \"Properties\":{
                    \"AttributePayload\":{},
                    \"ThingGroups\":[],
                    \"ThingName\":{
                        \"Fn::Join\":[
                            \"\",
                            [
                                \"DemoGroup_\",
                                {\"Ref\":\"SerialNumber\"}
                            ]
                        ]
                    },
                    \"ThingTypeName\":\"VirtualThings\"
                },
                \"Type\":\"AWS::IoT::Thing\"
            }
        }
    }",
    "enabled": true,
    "provisioningRoleArn": "arn:aws:iam::571032923833:role/service-role/IoT_access"
}
```

Para obtener más información, consulte Provisioning devices that don't have device certificates using fleet provisioning en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte DescribeProvisioningTemplate en la Referencia de comandos de la AWS CLI.

`describe-role-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-role-alias`.

AWS CLI

Para obtener información acerca de un alias de rol de AWS IoT

En el siguiente ejemplo de `describe-role-alias`, se muestran los detalles del alias del rol especificado.

```
aws iot describe-role-alias \
    --role-alias LightBulbRole
```

Salida:

```
{
    "roleAliasDescription": {
        "roleAlias": "LightBulbRole",
        "roleAliasArn": "arn:aws:iot:us-west-2:123456789012:rolealias/
LightBulbRole",
        "roleArn": "arn:aws:iam::123456789012:role/light_bulb_role_001",
        "owner": "123456789012",
        "credentialDurationSeconds": 3600,
        "creationDate": 1570558643.221,
        "lastModifiedDate": 1570558643.221
    }
}
```

Para obtener más información, consulte DescribeRoleAlias en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte DescribeRoleAlias en la Referencia de comandos de la AWS CLI.

`describe-scheduled-audit`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-scheduled-audit`.

AWS CLI

Para obtener información acerca de una auditoría programada

En el siguiente ejemplo de `describe-scheduled-audit`, se obtiene información detallada sobre una auditoría de AWS IoT Device Defender denominada `AWSIoTDeviceDefenderDailyAudit`.

```
aws iot describe-scheduled-audit \
    --scheduled-audit-name AWSIoTDeviceDefenderDailyAudit
```

Salida:

```
{
    "frequency": "DAILY",
    "targetCheckNames": [
        "AUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK",
        "CONFLICTING_CLIENT_IDS_CHECK",
        "DEVICE_CERTIFICATE_SHARED_CHECK",
        "IOT_POLICY_OVERLY_PERMISSIVE_CHECK",
        "REVOKED_CA_CERTIFICATE_STILL_ACTIVE_CHECK",
        "UNAUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK"
    ],
    "scheduledAuditName": "AWSIoTDeviceDefenderDailyAudit",
    "scheduledAuditArn": "arn:aws:iot:us-west-2:123456789012:scheduledaudit/
AWSIoTDeviceDefenderDailyAudit"
}
```

Para obtener más información, consulte Comandos de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener detalles sobre la API, consulte DescribeScheduledAudit en la Referencia de comandos de la AWS CLI.

`describe-security-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-security-profile`.

AWS CLI

Para obtener información sobre un perfil de seguridad

En el siguiente ejemplo de `describe-security-profile`, se obtiene información sobre el perfil de seguridad de AWS IoT Device Defender denominado `PossibleIssue.`.

```
aws iot describe-security-profile \
```

```
    --security-profile-name PossibleIssue
```

Salida:

```
{
    "securityProfileName": "PossibleIssue",
    "securityProfileArn": "arn:aws:iot:us-west-2:123456789012:securityprofile/
PossibleIssue",
    "securityProfileDescription": "check to see if authorization fails 10 times in 5
 minutes or if cellular bandwidth exceeds 128",
    "behaviors": [
        {
            "name": "CellularBandwidth",
            "metric": "aws:message-byte-size",
            "criteria": {
                "comparisonOperator": "greater-than",
                "value": {
                    "count": 128
                },
                "consecutiveDatapointsToAlarm": 1,
                "consecutiveDatapointsToClear": 1
            }
        },
        {
            "name": "Authorization",
            "metric": "aws:num-authorization-failures",
            "criteria": {
                "comparisonOperator": "greater-than",
                "value": {
                    "count": 10
                },
                "durationSeconds": 300,
                "consecutiveDatapointsToAlarm": 1,
                "consecutiveDatapointsToClear": 1
            }
        }
    ],
    "version": 1,
    "creationDate": 1560278102.528,
    "lastModifiedDate": 1560278102.528
}
```

Para obtener más información, consulte Comandos de detección en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeSecurityProfile en la Referencia de comandos de la AWS CLI.

`describe-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stream`.

AWS CLI

Para obtener información acerca de un flujo

En el siguiente ejemplo de `describe-stream`, se muestran los detalles del flujo especificado.

```
aws iot describe-stream \
    --stream-id stream12345
```

Salida:

```
{
    "streamInfo": {
        "streamId": "stream12345",
        "streamArn": "arn:aws:iot:us-west-2:123456789012:stream/stream12345",
        "streamVersion": 1,
        "description": "This stream is used for Amazon FreeRTOS OTA Update 12345.",
        "files": [
            {
                "fileId": "123",
                "s3Location": {
                    "bucket":"codesign-ota-bucket",
                    "key":"48c67f3c-63bb-4f92-a98a-4ee0fbc2bef6"
                }
            }
        ],
        "createdAt": 1557863215.995,
        "lastUpdatedAt": 1557863215.995,
        "roleArn": "arn:aws:iam:123456789012:role/service-role/my_ota_stream_role"
    }
}
```

Para obtener más información, consulte DescribeStream en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte DescribeStream en la Referencia de comandos de la AWS CLI.

`describe-thing-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-thing-group`.

AWS CLI

Para obtener información acerca de un grupo de objetos

En el siguiente ejemplo de `describe-thing-group`, se obtiene información sobre el grupo de objetos denominado `HalogenBulbs`.

```
aws iot describe-thing-group \
    --thing-group-name HalogenBulbs
```

Salida:

```
{
    "thingGroupName": "HalogenBulbs",
    "thingGroupId": "f4ec6b84-b42b-499d-9ce1-4dbd4d4f6f6e",
    "thingGroupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/HalogenBulbs",
    "version": 1,
    "thingGroupProperties": {},
    "thingGroupMetadata": {
        "parentGroupName": "LightBulbs",
        "rootToParentThingGroups": [
            {
                "groupName": "LightBulbs",
                "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/
LightBulbs"
            }
        ],
        "creationDate": 1559927609.897
    }
}
```

Para obtener más información, consulte Thing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeThingGroup en la Referencia de comandos de la AWS CLI.

`describe-thing-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-thing-type`.

AWS CLI

Para obtener información acerca de un tipo de objeto

En el siguiente ejemplo de `describe-thing-type`, se muestra información sobre el tipo de objeto especificado definido en la cuenta de AWS.

```
aws iot describe-thing-type \
    --thing-type-name "LightBulb"
```

Salida:

```
{
    "thingTypeName": "LightBulb",
    "thingTypeId": "ce3573b0-0a3c-45a7-ac93-4e0ce14cd190",
    "thingTypeArn": "arn:aws:iot:us-west-2:123456789012:thingtype/LightBulb",
    "thingTypeProperties": {
        "thingTypeDescription": "light bulb type",
        "searchableAttributes": [
            "model",
            "wattage"
        ]
    },
    "thingTypeMetadata": {
        "deprecated": false,
        "creationDate": 1559772562.498
    }
}
```

Para obtener más información, consulte Thing Types en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeThingType en la Referencia de comandos de la AWS CLI.

`describe-thing`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-thing`.

AWS CLI

Para visualizar información detallada acerca de un objeto

En el siguiente ejemplo de `describe-thing` se muestra información sobre un objeto (dispositivo) que está definido en el registro de AWS IoT de su cuenta de AWS.

aws iot describe-thing --thing-name "MyLightBulb"

Salida:

```
{
    "defaultClientId": "MyLightBulb",
    "thingName": "MyLightBulb",
    "thingId": "40da2e73-c6af-406e-b415-15acae538797",
    "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MyLightBulb",
    "thingTypeName": "LightBulb",
    "attributes": {
        "model": "123",
        "wattage": "75"
    },
    "version": 1
}
```

Para obtener más información, consulte Administración de objetos con el registro en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte DescribeThing en la Referencia de comandos de la AWS CLI.

`detach-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-policy`.

AWS CLI

Ejemplo 1: desasociación de una política de AWS IoT de un grupo de objetos

En el siguiente ejemplo de `detach-policy`, se desvincula la política especificada de un grupo de objetos y, por extensión, de todos los objetos de ese grupo y de cualquiera de los grupos secundarios del grupo.

```
aws iot detach-policy \
    --target "arn:aws:iot:us-west-2:123456789012:thinggroup/LightBulbs" \
    --policy-name "MyFirstGroup_Core-policy"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Thing Groups en la Guía para desarrolladores de AWS IoT.

Ejemplo 2: desasociación de una política de AWS IoT de un certificado de dispositivo

En el siguiente ejemplo de `detach-policy`, se desvincula la política TemperatureSensorPolicy de un certificado de dispositivo identificado por el ARN.

```
aws iot detach-policy \
    --policy-name TemperatureSensorPolicy \
    --target arn:aws:iot:us-
west-2:123456789012:cert/488b6a7f2acdeb00a77384e63c4e40b18b1b3caaae57b7272ba44c45e3448142
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DetachPolicy en la Referencia de comandos de la AWS CLI.

`detach-security-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-security-profile`.

AWS CLI

Para desasociar un perfil de seguridad de un destino

En el siguiente ejemplo de `detach-security-profile`, se elimina la asociación entre el perfil de seguridad de AWS IoT Device Defender denominado `Testprofile` y el objetivo de todos los objetos registrados.

```
aws iot detach-security-profile \
    --security-profile-name Testprofile \
```

```
    --security-profile-target-arn "arn:aws:iot:us-west-2:123456789012:all/
registered-things"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Comandos de detección en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DetachSecurityProfile en la Referencia de comandos de AWS CLI.

`detach-thing-principal`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-thing-principal`.

AWS CLI

Para desasociar un certificado o entidad principal de un objeto

En el siguiente ejemplo de `detach-thing-principal` se elimina un certificado que representa una entidad principal del objeto especificado.

```
aws iot detach-thing-principal \
    --thing-name "MyLightBulb" \
    --principal "arn:aws:iot:us-
west-2:123456789012:cert/604c48437a57b7d5fc5d137c5be75011c6ee67c9a6943683a1acb4b1626bac36"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración de objetos con el registro en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte DetachThingPrincipal en la Referencia de comandos de la AWS CLI.

`disable-topic-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-topic-rule`.

AWS CLI

Para deshabilitar una regla de tema

En el siguiente ejemplo de `disable-topic-rule`, se deshabilita la regla de tema especificada.

```
aws iot disable-topic-rule \
    --rule-name "MyPlantPiMoistureAlertRule"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Viewing Your Rules en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DisableTopicRule en la Referencia de comandos de la AWS CLI.

`enable-topic-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-topic-rule`.

AWS CLI

Para habilitar una regla de tema

En el siguiente ejemplo de `enable-topic-rule`, se habilita (o se vuelve a habilitar) la regla del tema especificada.

```
aws iot enable-topic-rule \
    --rule-name "MyPlantPiMoistureAlertRule"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Viewing Your Rules en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte EnableTopicRule en la Referencia de comandos de la AWS CLI.

`get-behavior-model-training-summaries`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-behavior-model-training-summaries`.

AWS CLI

Para enumerar el estado del modelo de entrenamiento del perfil de seguridad para la detección de ML de Device Defender

En el siguiente ejemplo de `get-behavior-model-training-summaries`, se enumera el estado de entrenamiento del modelo de los comportamientos configurados en el perfil de seguridad elegido. Para cada comportamiento, se muestran el nombre, el estado del modelo y el porcentaje de puntos de datos recopilados.

```
aws iot get-behavior-model-training-summaries \
    --security-profile-name MySecuirtyProfileName
```

Salida:

```
{
    "summaries": [
        {
            "securityProfileName": "MySecuirtyProfileName",
            "behaviorName": "Messages_sent_ML_behavior",
            "modelStatus": "PENDING_BUILD",
            "datapointsCollectionPercentage": 0.0
        },
        {
            "securityProfileName": "MySecuirtyProfileName",
            "behaviorName": "Messages_received_ML_behavior",
            "modelStatus": "PENDING_BUILD",
            "datapointsCollectionPercentage": 0.0
        },
        {
            "securityProfileName": "MySecuirtyProfileName",
            "behaviorName": "Authorization_failures_ML_behavior",
            "modelStatus": "PENDING_BUILD",
            "datapointsCollectionPercentage": 0.0
        },
        {
            "securityProfileName": "MySecuirtyProfileName",
            "behaviorName": "Message_size_ML_behavior",
            "modelStatus": "PENDING_BUILD",
            "datapointsCollectionPercentage": 0.0
        },
        {
```

```
            "securityProfileName": "MySecuirtyProfileName",
            "behaviorName": "Connection_attempts_ML_behavior",
            "modelStatus": "PENDING_BUILD",
            "datapointsCollectionPercentage": 0.0
        },
        {
            "securityProfileName": "MySPNoALerts",
            "behaviorName": "Disconnects_ML_behavior",
            "modelStatus": "PENDING_BUILD",
            "datapointsCollectionPercentage": 0.0
        }
    ]
}
```

Para obtener más información, consulte GetBehaviorModelTrainingSummaries (Comandos de detección) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetBehaviorModelTrainingSummaries en la Referencia de comandos de la AWS CLI.

`get-cardinality`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-cardinality`.

AWS CLI

Para devolver el recuento aproximado de valores únicos que coinciden con la consulta

Puede usar el siguiente script de configuración para crear diez elementos que representen diez sensores de temperatura. Cada objeto nuevo tiene tres atributos.

```
# Bash script. If in other shells, type `bash` before running
Temperatures=(70 71 72 73 74 75 47 97 98 99)
Racks=(Rack1 Rack1 Rack2 Rack2 Rack3 Rack4 Rack5 Rack6 Rack6 Rack6)
IsNormal=(true true true true true true false false false false)
for ((i=0; i<10 ; i++))
do
  thing=$(aws iot create-thing --thing-name "TempSensor$i" --attribute-payload
 attributes="{temperature=${Temperatures[i]},rackId=${Racks[i]},stateNormal=
${IsNormal[i]}}")
  aws iot describe-thing --thing-name "TempSensor$i"
done
```

Ejemplo de salida del script de configuración:

```
{
    "version": 1,
    "thingName": "TempSensor0",
    "defaultClientId": "TempSensor0",
    "attributes": {
        "rackId": "Rack1",
        "stateNormal": "true",
        "temperature": "70"
    },
    "thingArn": "arn:aws:iot:us-east-1:123456789012:thing/TempSensor0",
    "thingId": "example1-90ab-cdef-fedc-ba987example"
}
```

En el siguiente ejemplo de `get-cardinality`, se consultan los diez sensores creados por el script de configuración y se devuelve el número de racks con sensores de temperatura que indican valores de temperatura anormales. Si el valor de temperatura es inferior a 60 o superior a 80, el estado del sensor de temperatura es anormal.

```
aws iot get-cardinality \
    --aggregation-field "attributes.rackId" \
    --query-string "thingName:TempSensor* AND attributes.stateNormal:false"
```

Salida:

```
{
    "cardinality": 2
}
```

Para obtener más información, consulte Querying for Aggregate Data<https://docs.aws.amazon.com/iot/latest/developerguide/index-aggregate.html> en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetCardinality en la Referencia de comandos de la AWS CLI.

`get-effective-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-effective-policies`.

AWS CLI

Para enumerar las políticas que afectan a un objeto

En el siguiente ejemplo de `get-effective-policies`, se enumeran las políticas que afectan al objeto especificado, incluidas las políticas asociadas a cualquier grupo al que pertenezca.

```
aws iot get-effective-policies \
    --thing-name TemperatureSensor-001 \
    --principal arn:aws:iot:us-
west-2:123456789012:cert/488b6a7f2acdeb00a77384e63c4e40b18b1b3caaae57b7272ba44c45e3448142
```

Salida:

```
{
    "effectivePolicies": [
        {
            "policyName": "TemperatureSensorPolicy",
            "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/
TemperatureSensorPolicy",
            "policyDocument": "{
                \"Version\": \"2012-10-17\",
                \"Statement\": [
                    {
                        \"Effect\": \"Allow\",
                        \"Action\": [
                            \"iot:Publish\",
                            \"iot:Receive\"
                        ],
                        \"Resource\": [
                            \"arn:aws:iot:us-west-2:123456789012:topic/topic_1\",
                            \"arn:aws:iot:us-west-2:123456789012:topic/topic_2\"
                        ]
                    },
                    {
                        \"Effect\": \"Allow\",
                        \"Action\": [
                            \"iot:Subscribe\"
                        ],
                        \"Resource\": [
                            \"arn:aws:iot:us-west-2:123456789012:topicfilter/
topic_1\",
```

```
                            \"arn:aws:iot:us-west-2:123456789012:topicfilter/
topic_2\"
                        ]
                    },
                    {
                        \"Effect\": \"Allow\",
                        \"Action\": [
                            \"iot:Connect\"
                        ],
                        \"Resource\": [
                            \"arn:aws:iot:us-west-2:123456789012:client/basicPubSub
\"
                        ]
                    }
                ]
            }"
        }
    ]
}
```

Para obtener más información, consulte Get Effective Policies for a Thing en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetEffectivePolicies en la Referencia de comandos de la AWS CLI.

`get-indexing-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-indexing-configuration`.

AWS CLI

Para obtener la configuración de indexación de objetos

En el siguiente ejemplo de `get-indexing-configuration`, se obtienen los datos de configuración actuales para la indexación de flotas de AWS IoT.

```
aws iot get-indexing-configuration
```

Salida:

```
{
```

```
    "thingIndexingConfiguration": {
        "thingIndexingMode": "OFF",
        "thingConnectivityIndexingMode": "OFF"
    },
    "thingGroupIndexingConfiguration": {
        "thingGroupIndexingMode": "OFF"
    }
}
```

Para obtener más información, consulte Managing Thing Indexing en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetIndexingConfiguration en la Referencia de comandos de la AWS CLI.

`get-job-document`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-job-document`.

AWS CLI

Para recuperar el documento para un trabajo

En el siguiente ejemplo de `get-job-document`, se muestran los detalles del documento para el trabajo con el ID `example-job-01`.

```
aws iot get-job-document \
    --job-id "example-job-01"
```

Salida:

```
{
    "document": "\n{\n    \"operation\":\"customJob\",\n    \"otherInfo\":
\"someValue\"\n}\n"
}
```

Para obtener más información, consulte Creating and Managing Jobs (CLI) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetJobDocument en la Referencia de comandos de la AWS CLI.

`get-logging-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-logging-options`.

AWS CLI

Para obtener las opciones de registro

En el siguiente ejemplo de `get-logging-options`, se obtienen las opciones de registro actuales de su cuenta de AWS.

```
aws iot get-logging-options
```

Salida:

```
{
    "roleArn": "arn:aws:iam::123456789012:role/service-role/iotLoggingRole",
    "logLevel": "ERROR"
}
```

Para obtener más información, consulte el título en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetLoggingOptions en la Referencia de comandos de la AWS CLI.

`get-ota-update`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ota-update`.

AWS CLI

Para recuperar información sobre una actualización OTA

En el siguiente ejemplo de `get-ota-update`, se muestran los detalles de las actualizaciones OTA especificadas.

```
aws iot get-ota-update \
    --ota-update-id ota12345
```

Salida:

```
{
```

```
    "otaUpdateInfo": {
        "otaUpdateId": "ota12345",
        "otaUpdateArn": "arn:aws:iot:us-west-2:123456789012:otaupdate/itsaupdate",
        "creationDate": 1557863215.995,
        "lastModifiedDate": 1557863215.995,
        "description": "A critical update needed right away.",
        "targets": [
           "device1",
           "device2",
           "device3",
           "device4"
        ],
        "targetSelection": "SNAPSHOT",
        "protocols": ["HTTP"],
        "awsJobExecutionsRolloutConfig": {
           "maximumPerMinute": 10
        },
        "otaUpdateFiles": [
            {
                "fileName": "firmware.bin",
                "fileLocation": {
                    "stream": {
                        "streamId": "004",
                        "fileId":123
                    }
                },
                "codeSigning": {
                    "awsSignerJobId": "48c67f3c-63bb-4f92-a98a-4ee0fbc2bef6"
                }
            }
        ],
        "roleArn": "arn:aws:iam:123456789012:role/service-role/my_ota_role"
        "otaUpdateStatus": "CREATE_COMPLETE",
        "awsIotJobId": "job54321",
        "awsIotJobArn": "arn:aws:iot:us-west-2:123456789012:job/job54321",
        "errorInfo": {
        }
    }
}
```


Para obtener más información, consulte GetOTAUpdate en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte GetOtaUpdate en la Referencia de comandos de la AWS CLI.

`get-percentiles`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-percentiles`.

AWS CLI

Para agrupar los valores agregados que coinciden con la consulta en agrupaciones de percentiles

Puede usar el siguiente script de configuración para crear diez elementos que representen diez sensores de temperatura. Cada objeto nuevo tiene un atributo.

```
# Bash script. If in other shells, type `bash` before running
Temperatures=(70 71 72 73 74 75 47 97 98 99)
for ((i=0; i<10 ; i++))
do
    thing=$(aws iot create-thing --thing-name "TempSensor$i" --attribute-payload
 attributes="{temperature=${Temperatures[i]}}")
    aws iot describe-thing --thing-name "TempSensor$i"
done
```

Ejemplo de salida del script de configuración:

```
{
    "version": 1,
    "thingName": "TempSensor0",
    "defaultClientId": "TempSensor0",
    "attributes": {
        "temperature": "70"
    },
    "thingArn": "arn:aws:iot:us-east-1:123456789012:thing/TempSensor0",
    "thingId": "example1-90ab-cdef-fedc-ba987example"
}
```

En el siguiente ejemplo de `get-percentiles`, se consultan los diez sensores creados por el script de configuración y se devuelve un valor para cada grupo de percentiles especificado. El grupo de percentiles 10 contiene el valor agregado del campo que se obtiene aproximadamente en el 10 % de los valores que coinciden con la consulta. En el siguiente resultado, {"percent": 10.0, "value": 67.7} significa que aproximadamente el 10 % de los valores de temperatura están por debajo de 67,7.

```
aws iot get-percentiles \
    --aggregation-field "attributes.temperature" \
```

```
    --query-string "thingName:TempSensor*" \
    --percents 10 25 50 75 90
```

Salida:

```
{
    "percentiles": [
        {
            "percent": 10.0,
            "value": 67.7
        },
        {
            "percent": 25.0,
            "value": 71.25
        },
        {
            "percent": 50.0,
            "value": 73.5
        },
        {
            "percent": 75.0,
            "value": 91.5
        },
        {
            "percent": 90.0,
            "value": 98.1
        }
    ]
}
```

Para obtener más información, consulte Querying for Aggregate Data en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetPercentiles en la Referencia de comandos de la AWS CLI.

`get-policy-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-policy-version`.

AWS CLI

Para obtener información sobre una versión específica de una política

En el siguiente ejemplo de `get-policy-version`, se obtiene información sobre la primera versión de la política especificada.

```
aws iot get-policy \
    --policy-name UpdateDeviceCertPolicy
    --policy-version-id "1"
```

Salida:

```
{
    "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/UpdateDeviceCertPolicy",
    "policyName": "UpdateDeviceCertPolicy",
    "policyDocument": "{ \"Version\": \"2012-10-17\", \"Statement\": [ { \"Effect\":
 \"Allow\", \"Action\":  \"iot:UpdateCertificate\", \"Resource\": \"*\" } ] }",
    "policyVersionId": "1",
    "isDefaultVersion": false,
    "creationDate": 1559925941.924,
    "lastModifiedDate": 1559926175.458,
    "generationId":
 "5066f1b6712ce9d2a1e56399771649a272d6a921762fead080e24fe52f24e042"
}
```

Para obtener más información, consulte AWS IoT Policies en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetPolicyVersion en la Referencia de comandos de la AWS CLI.

`get-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-policy`.

AWS CLI

Para obtener información sobre una versión predeterminada de una política

En el siguiente ejemplo de `get-policy`, se obtiene información sobre la versión predeterminada de la política especificada.

```
aws iot get-policy \
    --policy-name UpdateDeviceCertPolicy
```

Salida:

```
{
    "policyName": "UpdateDeviceCertPolicy",
    "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/UpdateDeviceCertPolicy",
    "policyDocument": "{ \"Version\": \"2012-10-17\", \"Statement\": [ { \"Effect\":
 \"Allow\", \"Action\":  \"iot:UpdateCertificate\", \"Resource\": \"*\" } ] }",
    "defaultVersionId": "2",
    "creationDate": 1559925941.924,
    "lastModifiedDate": 1559925941.924,
    "generationId":
 "5066f1b6712ce9d2a1e56399771649a272d6a921762fead080e24fe52f24e042"
}
```

Para obtener más información, consulte AWS IoT Policies en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetPolicy en la Referencia de comandos de la AWS CLI.

`get-registration-code`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-registration-code`.

AWS CLI

Para obtener el código de registro específico de su cuenta de AWS

En el siguiente ejemplo de `get-registration-code`, se obtiene un código de registro específico de una cuenta de AWS.

```
aws iot get-registration-code
```

Salida:

```
{
    "registrationCode":
 "15c51ae5e36ba59ba77042df1115862076bea4bd15841c838fcb68d5010a614c"
}
```

Para obtener más información, consulte Use Your Own Certificate en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetRegistrationCode en la Referencia de comandos de la AWS CLI.

`get-statistics`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-statistics`.

AWS CLI

Para buscar datos agregados en el índice de dispositivos

En el siguiente ejemplo de `get-statistics`, se devuelve el número de objetos que tiene una propiedad denominada `connectivity.connected` establecida en `false` (es decir, el número de dispositivos que no están conectados) en su sombra de dispositivos.

```
aws iot get-statistics \
    --index-name AWS_Things \
    --query-string "connectivity.connected:false"
```

Salida:

```
{
    "statistics": {
        "count": 6
    }
}
```

Para obtener más información, consulte Getting Statistics About Your Device Fleet en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetStatistics en la Referencia de comandos de la AWS CLI.

`get-topic-rule-destination`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-topic-rule-destination`.

AWS CLI

Para obtener un destino de regla de tema

En el siguiente ejemplo de `get-topic-rule-destination`, se obtiene información sobre un destino de regla de tema.

```
aws iot get-topic-rule-destination \
    --arn "arn:aws:iot:us-west-2:123456789012:ruledestination/http/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
```

Salida:

```
{
    "topicRuleDestination": {
        "arn": "arn:aws:iot:us-west-2:123456789012:ruledestination/http/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
        "status": "DISABLED",
        "httpUrlProperties": {
            "confirmationUrl": "https://example.com"
        }
    }
}
```

Para obtener más información, consulte Working with topic rule destinations en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetTopicRuleDestination en la Referencia de comandos de la AWS CLI.

`get-topic-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-topic-rule`.

AWS CLI

Para obtener información sobre una regla

En el siguiente ejemplo de `get-topic-rule`, se obtiene información sobre la regla especificada.

```
aws iot get-topic-rule \
    --rule-name MyRPiLowMoistureAlertRule
```

Salida:

```
{
```

```
    "ruleArn": "arn:aws:iot:us-west-2:123456789012:rule/MyRPiLowMoistureAlertRule",
    "rule": {
        "ruleName": "MyRPiLowMoistureAlertRule",
        "sql": "SELECT * FROM '$aws/things/MyRPi/shadow/update/accepted' WHERE
 state.reported.moisture = 'low'\n                    ",
        "description": "Sends an alert whenever soil moisture level readings are too
 low.",
        "createdAt": 1558624363.0,
        "actions": [
            {
                "sns": {
                    "targetArn": "arn:aws:sns:us-
west-2:123456789012:MyRPiLowMoistureTopic",
                    "roleArn": "arn:aws:iam::123456789012:role/service-role/
MyRPiLowMoistureTopicRole",
                    "messageFormat": "RAW"
                }
            }
        ],
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23"
    }
}
```

Para obtener más información, consulte Viewing Your Rules en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetTopicRule en la Referencia de comandos de la AWS CLI.

`get-v2-logging-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-v2-logging-options`.

AWS CLI

Para enumerar las opciones de registro actuales

En el siguiente ejemplo de `get-v2-logging-options`, se enumeran las opciones de registro de AWS IoT actuales.

```
aws iot get-v2-logging-options
```

Salida:

```
{
    "roleArn": "arn:aws:iam::094249569039:role/service-role/iotLoggingRole",
    "defaultLogLevel": "WARN",
    "disableAllLogs": false
}
```

Para obtener más información, consulte el título en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetV2LoggingOptions en la Referencia de comandos de la AWS CLI.

`list-active-violations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-active-violations`.

AWS CLI

Para enumerar las infracciones activas

En el siguiente ejemplo de `list-active-violations`, se enumeran todas las infracciones del perfil de seguridad especificado.

```
aws iot list-active-violations \
    --security-profile-name Testprofile
```

Salida:

```
{
    "activeViolations": [
        {
            "violationId": "174db59167fa474c80a652ad1583fd44",
            "thingName": "iotconsole-1560269126751-1",
            "securityProfileName": "Testprofile",
            "behavior": {
                "name": "Authorization",
                "metric": "aws:num-authorization-failures",
                "criteria": {
                    "comparisonOperator": "greater-than",
                    "value": {
                        "count": 10
```

```
                },
                "durationSeconds": 300,
                "consecutiveDatapointsToAlarm": 1,
                "consecutiveDatapointsToClear": 1
            }
        },
        "lastViolationValue": {
            "count": 0
        },
        "lastViolationTime": 1560293700.0,
        "violationStartTime": 1560279000.0
    },
    {
        "violationId": "c8a9466a093d3b7b35cd44ca58bdbeab",
        "thingName": "TvnQoEoU",
        "securityProfileName": "Testprofile",
        "behavior": {
            "name": "CellularBandwidth",
            "metric": "aws:message-byte-size",
            "criteria": {
                "comparisonOperator": "greater-than",
                "value": {
                    "count": 128
                },
                "consecutiveDatapointsToAlarm": 1,
                "consecutiveDatapointsToClear": 1
            }
        },
        "lastViolationValue": {
            "count": 110
        },
        "lastViolationTime": 1560369000.0,
        "violationStartTime": 1560276600.0
    },
    {
        "violationId": "74aa393adea02e6648f3ac362beed55e",
        "thingName": "iotconsole-1560269232412-2",
        "securityProfileName": "Testprofile",
        "behavior": {
            "name": "Authorization",
            "metric": "aws:num-authorization-failures",
            "criteria": {
                "comparisonOperator": "greater-than",
                "value": {
```

```
                        "count": 10
                    },
                    "durationSeconds": 300,
                    "consecutiveDatapointsToAlarm": 1,
                    "consecutiveDatapointsToClear": 1
                }
            },
            "lastViolationValue": {
                "count": 0
            },
            "lastViolationTime": 1560276600.0,
            "violationStartTime": 1560276600.0
        },
        {
            "violationId": "1e6ab5f7cf39a1466fcd154e1377e406",
            "thingName": "TvnQoEoU",
            "securityProfileName": "Testprofile",
            "behavior": {
                "name": "Authorization",
                "metric": "aws:num-authorization-failures",
                "criteria": {
                    "comparisonOperator": "greater-than",
                    "value": {
                        "count": 10
                    },
                    "durationSeconds": 300,
                    "consecutiveDatapointsToAlarm": 1,
                    "consecutiveDatapointsToClear": 1
                }
            },
            "lastViolationValue": {
                "count": 0
            },
            "lastViolationTime": 1560369000.0,
            "violationStartTime": 1560276600.0
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListActiveViolations en la Referencia de comandos de la AWS CLI.

`list-attached-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-attached-policies`.

AWS CLI

Ejemplo 1: lista de las políticas asociadas a un grupo

En el siguiente ejemplo de `list-attached-policies`, se enumeran las políticas que se asocian al grupo especificado.

```
aws iot list-attached-policies \
    --target "arn:aws:iot:us-west-2:123456789012:thinggroup/LightBulbs"
```

Salida:

```
{
    "policies": [
        {
            "policyName": "UpdateDeviceCertPolicy",
            "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/
UpdateDeviceCertPolicy"
        }
    ]
}
```

Para obtener más información, consulte Thing Groups en la Guía para desarrolladores de AWS IoT.

Ejemplo 2: lista de las políticas asociadas a un certificado de dispositivo

En el siguiente ejemplo de `list-attached-policies`, se enumeran las políticas de AWS IoT asociadas al certificado del dispositivo. El certificado se identifica con su ARN.

```
aws iot list-attached-policies \
    --target arn:aws:iot:us-
west-2:123456789012:cert/488b6a7f2acdeb00a77384e63c4e40b18b1b3caaae57b7272ba44c45e3448142
```

Salida:

```
{
```

```
    "policies": [
        {
            "policyName": "TemperatureSensorPolicy",
            "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/
TemperatureSensorPolicy"
        }
    ]
}
```

Para obtener más información, consulte Thing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListAttachedPolicies en la Referencia de comandos de la AWS CLI.

`list-audit-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-audit-findings`.

AWS CLI

Ejemplo 1: lista de todos los resultados de una auditoría

En el siguiente ejemplo de `list-audit-findings`, se enumeran todos los resultados de una auditoría de AWS IoT Device Defender con un ID de tarea específico.

```
aws iot list-audit-findings \
    --task-id a3aea009955e501a31b764abe1bebd3d
```

Salida:

```
{
    "findings": []
}
```

Ejemplo 2: lista de los resultados de un tipo de comprobación de auditoría

En el siguiente ejemplo de `list-audit-findings`, se muestran los resultados de las auditorías de AWS IoT Device Defender realizadas entre el 5 y el 19 de junio de 2019, en las que los dispositivos comparten un certificado de dispositivo. Al especificar un nombre de verificación, debe proporcionar una hora de inicio y finalización.

```
aws iot list-audit-findings \
    --check-name DEVICE_CERTIFICATE_SHARED_CHECK \
    --start-time 1559747125 \
    --end-time 1560962028
```

Salida:

```
{
    "findings": [
        {
            "taskId": "eeef61068b0eb03c456d746c5a26ee04",
            "checkName": "DEVICE_CERTIFICATE_SHARED_CHECK",
            "taskStartTime": 1560161017.172,
            "findingTime": 1560161017.592,
            "severity": "CRITICAL",
            "nonCompliantResource": {
                "resourceType": "DEVICE_CERTIFICATE",
                "resourceIdentifier": {
                    "deviceCertificateId":
 "b193ab7162c0fadca83246d24fa090300a1236fe58137e121b011804d8ac1d6b"
                }
            },
            "relatedResources": [
                {
                    "resourceType": "CLIENT_ID",
                    "resourceIdentifier": {
                        "clientId": "ZipxgAIl"
                    },
                    "additionalInfo": {
                        "CONNECTION_TIME": "1560086374068"
                    }
                },
                {
                    "resourceType": "CLIENT_ID",
                    "resourceIdentifier": {
                        "clientId": "ZipxgAIl"
                    },
                    "additionalInfo": {
                        "CONNECTION_TIME": "1560081552187",
                        "DISCONNECTION_TIME": "1560086371552"
                    }
                },
                {
```

```
                    "resourceType": "CLIENT_ID",
                    "resourceIdentifier": {
                        "clientId": "ZipxgAIl"
                    },
                    "additionalInfo": {
                        "CONNECTION_TIME": "1559289863631",
                        "DISCONNECTION_TIME": "1560081532716"
                    }
                }
            ],
            "reasonForNonCompliance": "Certificate shared by one or more devices.",
            "reasonForNonComplianceCode": "CERTIFICATE_SHARED_BY_MULTIPLE_DEVICES"
        },
        {
            "taskId": "bade6b5efd2e1b1569822f6021b39cf5",
            "checkName": "DEVICE_CERTIFICATE_SHARED_CHECK",
            "taskStartTime": 1559988217.27,
            "findingTime": 1559988217.655,
            "severity": "CRITICAL",
            "nonCompliantResource": {
                "resourceType": "DEVICE_CERTIFICATE",
                "resourceIdentifier": {
                    "deviceCertificateId":
"b193ab7162c0fadca83246d24fa090300a1236fe58137e121b011804d8ac1d6b"
                }
            },
            "relatedResources": [
                {
                    "resourceType": "CLIENT_ID",
                    "resourceIdentifier": {
                        "clientId": "xShGENLW"
                    },
                    "additionalInfo": {
                        "CONNECTION_TIME": "1559972350825"
                    }
                },
                {
                    "resourceType": "CLIENT_ID",
                    "resourceIdentifier": {
                        "clientId": "xShGENLW"
                    },
                    "additionalInfo": {
                        "CONNECTION_TIME": "1559255062002",
                        "DISCONNECTION_TIME": "1559972350616"
```

```
                    }
                }
            ],
            "reasonForNonCompliance": "Certificate shared by one or more devices.",
            "reasonForNonComplianceCode": "CERTIFICATE_SHARED_BY_MULTIPLE_DEVICES"
        },
        {
            "taskId": "c23f6233ba2d35879c4bb2810fb5ffd6",
            "checkName": "DEVICE_CERTIFICATE_SHARED_CHECK",
            "taskStartTime": 1559901817.31,
            "findingTime": 1559901817.767,
            "severity": "CRITICAL",
            "nonCompliantResource": {
                "resourceType": "DEVICE_CERTIFICATE",
                "resourceIdentifier": {
                    "deviceCertificateId":
"b193ab7162c0fadca83246d24fa090300a1236fe58137e121b011804d8ac1d6b"
                }
            },
            "relatedResources": [
                {
                    "resourceType": "CLIENT_ID",
                    "resourceIdentifier": {
                        "clientId": "TvnQoEoU"
                    },
                    "additionalInfo": {
                        "CONNECTION_TIME": "1559826729768"
                    }
                },
                {
                    "resourceType": "CLIENT_ID",
                    "resourceIdentifier": {
                        "clientId": "TvnQoEoU"
                    },
                    "additionalInfo": {
                        "CONNECTION_TIME": "1559345920964",
                        "DISCONNECTION_TIME": "1559826728402"
                    }
                }
            ],
            "reasonForNonCompliance": "Certificate shared by one or more devices.",
            "reasonForNonComplianceCode": "CERTIFICATE_SHARED_BY_MULTIPLE_DEVICES"
        }
    ]
```

```
}
```

Para obtener más información, consulte Comandos de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListAuditFindings en la Referencia de comandos de la AWS CLI.

`list-audit-mitigation-actions-executions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-audit-mitigation-actions-executions`.

AWS CLI

Para enumerar los detalles de la ejecución de una acción de mitigación de auditoría

Una tarea de acción de mitigación de auditoría aplica una acción de mitigación a uno o más resultados de una auditoría de AWS IoT Device Defender. En el siguiente ejemplo de `list-audit-mitigation-actions-executions`, se enumeran los detalles de la tarea de acción de mitigación con el `taskId` y el resultado especificados.

```
aws iot list-audit-mitigation-actions-executions \
    --task-id myActionsTaskId \
    --finding-id 0edbaaec-2fe1-4cf5-abc9-d4c3e51f7464
```

Salida:

```
{
    "actionsExecutions": [
        {
            "taskId": "myActionsTaskId",
            "findingId": "0edbaaec-2fe1-4cf5-abc9-d4c3e51f7464",
            "actionName": "ResetPolicyVersionAction",
            "actionId": "1ea0b415-bef1-4a01-bd13-72fb63c59afb",
            "status": "COMPLETED",
            "startTime": "2019-12-10T15:19:13.279000-08:00",
            "endTime": "2019-12-10T15:19:13.337000-08:00"
        }
    ]
}
```

Para obtener más información, consulte ListAuditMitigationActionsExecutions (Comandos de acciones de mitigación) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListAuditMitigationActionsExecutions en la Referencia de comandos de la AWS CLI.

`list-audit-mitigation-actions-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-audit-mitigation-actions-tasks`.

AWS CLI

Para enumerar las tareas de acciones de mitigación de auditoría

En el siguiente ejemplo de `list-audit-mitigation-actions-tasks`, se enumeran las acciones de mitigación que se han aplicado a los resultados dentro del período de tiempo especificado.

```
aws iot list-audit-mitigation-actions-tasks \
    --start-time 1594157400 \
    --end-time 1594157430
```

Salida:

```
{
    "tasks": [
        {
                "taskId": "0062f2d6-3999-488f-88c7-bef005414103",
                "startTime": "2020-07-07T14:30:15.172000-07:00",
            "taskStatus": "COMPLETED"
        }
    ]
}
```

Para obtener más información, consulte ListAuditMitigationActionsTasks (Comandos de acciones de mitigación) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListAuditMitigationActionsTasks en la Referencia de comandos de la AWS CLI.

`list-audit-suppressions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-audit-suppressions`.

AWS CLI

Para enumerar las supresiones de resultados de auditoría

En el siguiente ejemplo de `list-audit-suppressions`, se enumeran todas las supresiones de resultados de auditoría activas.

```
aws iot list-audit-suppressions
```

Salida:

```
{
    "suppressions": [
        {
        "checkName": "DEVICE_CERTIFICATE_EXPIRING_CHECK",
            "resourceIdentifier": {
                "deviceCertificateId": "c7691e<shortened>"
            },
        "expirationDate": 1597881600.0,
        "suppressIndefinitely": false
        }
    ]
}
```

Para obtener más información, consulte Supresiones de resultados de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListAuditSuppressions en la Referencia de comandos de la AWS CLI.

`list-audit-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-audit-tasks`.

AWS CLI

Para enumerar todos los resultados de una auditoría

En el siguiente ejemplo de `list-audit-tasks`, se enumeran las tareas de auditoría que se han realizado entre el 5 y el 12 de junio de 2019.

```
aws iot list-audit-tasks \
    --start-time 1559747125 \
    --end-time 1560357228
```

Salida:

```
{
    "tasks": [
        {
            "taskId": "a3aea009955e501a31b764abe1bebd3d",
            "taskStatus": "COMPLETED",
            "taskType": "ON_DEMAND_AUDIT_TASK"
        },
        {
            "taskId": "f76b4b5102b632cd9ae38a279c266da1",
            "taskStatus": "COMPLETED",
            "taskType": "SCHEDULED_AUDIT_TASK"
        },
        {
            "taskId": "51d9967d9f9ff4d26529505f6d2c444a",
            "taskStatus": "COMPLETED",
            "taskType": "SCHEDULED_AUDIT_TASK"
        },
        {
            "taskId": "eeef61068b0eb03c456d746c5a26ee04",
            "taskStatus": "COMPLETED",
            "taskType": "SCHEDULED_AUDIT_TASK"
        },
        {
            "taskId": "041c49557b7c7b04c079a49514b55589",
            "taskStatus": "COMPLETED",
            "taskType": "SCHEDULED_AUDIT_TASK"
        },
        {
            "taskId": "82c7f2afac1562d18a4560be73998acc",
            "taskStatus": "COMPLETED",
            "taskType": "SCHEDULED_AUDIT_TASK"
        },
        {
            "taskId": "bade6b5efd2e1b1569822f6021b39cf5",
```

```
            "taskStatus": "COMPLETED",
            "taskType": "SCHEDULED_AUDIT_TASK"
        },
        {
            "taskId": "c23f6233ba2d35879c4bb2810fb5ffd6",
            "taskStatus": "COMPLETED",
            "taskType": "SCHEDULED_AUDIT_TASK"
        },
        {
            "taskId": "ac9086b7222a2f5e2e17bb6fd30b3aeb",
            "taskStatus": "COMPLETED",
            "taskType": "SCHEDULED_AUDIT_TASK"
        }
    ]
}
```

Para obtener más información, consulte Comandos de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener detalles de la API, consulte ListAuditTasks en la Referencia de comandos de la AWS CLI.

`list-authorizers`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-authorizers`.

AWS CLI

Para enumerar su autorizador personalizado

En el siguiente ejemplo de `list-authorizers`, se enumeran los autorizadores personalizados de su cuenta de AWS.

```
aws iot list-authorizers
```

Salida:

```
{
    "authorizers": [
        {
            "authorizerName": "CustomAuthorizer",
```

```
            "authorizerArn": "arn:aws:iot:us-west-2:123456789012:authorizer/
CustomAuthorizer"
        },
        {
            "authorizerName": "CustomAuthorizer2",
            "authorizerArn": "arn:aws:iot:us-west-2:123456789012:authorizer/
CustomAuthorizer2"
        },
        {
            "authorizerName": "CustomAuthorizer3",
            "authorizerArn": "arn:aws:iot:us-west-2:123456789012:authorizer/
CustomAuthorizer3"
        }
    ]
}
```

Para obtener más información, consulte ListAuthorizers en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte ListAuthorizers en la Referencia de comandos de la AWS CLI.

`list-billing-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-billing-groups`.

AWS CLI

Para enumerar los grupos de facturación de su cuenta y región de AWS

En el siguiente ejemplo de `list-billing-groups`, se enumeran todos los grupos de facturación definidos para su cuenta de AWS y la región de AWS.

```
aws iot list-billing-groups
```

Salida:

```
{
    "billingGroups": [
        {
            "groupName": "GroupOne",
            "groupArn": "arn:aws:iot:us-west-2:123456789012:billinggroup/GroupOne"
        }
```

```
    ]
}
```

Para obtener más información, consulte Billing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListBillingGroups en la Referencia de comandos de la AWS CLI.

`list-ca-certificates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-ca-certificates`.

AWS CLI

Para enumerar los certificados de CA registrados en la cuenta de AWS

En el siguiente ejemplo de `list-ca-certificates`, se enumeran los certificados de CA registrados en su cuenta de AWS.

```
aws iot list-ca-certificates
```

Salida:

```
{
    "certificates": [
        {
            "certificateArn": "arn:aws:iot:us-west-2:123456789012:cacert/
f4efed62c0142f16af278166f61962501165c4f053629520742646005 8cd1467",
            "certificateId":
 "f4efed62c0142f16af278166f61962501165c4f053629520742646005 8cd1467",
            "status": "INACTIVE",
            "creationDate": 1569365372.053
        }
    ]
}
```

Para obtener más información, consulte Use Your Own Certificate en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListCaCertificates en la Referencia de comandos de la AWS CLI.

`list-certificates-by-ca`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-certificates-by-ca`.

AWS CLI

Para ver una lista de todos los certificados de dispositivos firmados con un certificado de CA

En el siguiente ejemplo de `list-certificates-by-ca`, se enumeran todos los certificados de dispositivo de su cuenta de AWS firmados con el certificado de CA especificado.

```
aws iot list-certificates-by-ca \
    --ca-certificate-
id f4efed62c0142f16af278166f61962501165c4f053629520742646005 8cd1467
```

Salida:

```
{
    "certificates": [
        {
            "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/488b6a7f2acdeb00a77384e63c4e40b18b1b3caaae57b7272ba44c45e3448142",
            "certificateId":
 "488b6a7f2acdeb00a77384e63c4e40b18b1b3caaae57b7272ba44c45e3448142",
            "status": "ACTIVE",
            "creationDate": 1569363250.557
        }
    ]
}
```

Para obtener más información, consulte ListCertificatesByCA en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte ListCertificatesByCa en la Referencia de comandos de la AWS CLI.

`list-certificates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-certificates`.

AWS CLI

Ejemplo 1: enumeración de los certificados registrados en la cuenta de AWS

En el siguiente ejemplo de `list-certificates` se muestra una lista de todos los certificados registrados en la cuenta. Si supera el límite de paginación predeterminado de 25, puede utilizar el valor de respuesta `nextMarker` de este comando e introducirlo en el siguiente comando para obtener el siguiente lote de resultados. Repita el procedimiento hasta que `nextMarker` no devuelva ningún valor.

```
aws iot list-certificates
```

Salida:

```
{
    "certificates": [
        {
            "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/604c48437a57b7d5fc5d137c5be75011c6ee67c9a6943683a1acb4b1626bac36",
            "certificateId":
 "604c48437a57b7d5fc5d137c5be75011c6ee67c9a6943683a1acb4b1626bac36",
            "status": "ACTIVE",
            "creationDate": 1556810537.617
        },
        {
            "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/262a1ac8a7d8aa72f6e96e365480f7313aa9db74b8339ec65d34dc3074e1c31e",
            "certificateId":
 "262a1ac8a7d8aa72f6e96e365480f7313aa9db74b8339ec65d34dc3074e1c31e",
            "status": "ACTIVE",
            "creationDate": 1546447050.885
        },
        {
            "certificateArn": "arn:aws:iot:us-west-2:123456789012:cert/
b193ab7162c0fadca83246d24fa090300a1236fe58137e121b011804d8ac1d6b",
            "certificateId":
 "b193ab7162c0fadca83246d24fa090300a1236fe58137e121b011804d8ac1d6b",
            "status": "ACTIVE",
            "creationDate": 1546292258.322
        },
        {
            "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/7aebeea3845d14a44ec80b06b8b78a89f3f8a706974b8b34d18f5adf0741db42",
            "certificateId":
 "7aebeea3845d14a44ec80b06b8b78a89f3f8a706974b8b34d18f5adf0741db42",
            "status": "ACTIVE",
```

```
            "creationDate": 1541457693.453
        },
        {
            "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/54458aa39ebb3eb39c91ffbbdcc3a6ca1c7c094d1644b889f735a6fc2cd9a7e3",
            "certificateId":
 "54458aa39ebb3eb39c91ffbbdcc3a6ca1c7c094d1644b889f735a6fc2cd9a7e3",
            "status": "ACTIVE",
            "creationDate": 1541113568.611
        },
        {
            "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/4f0ba725787aa94d67d2fca420eca022242532e8b3c58e7465c7778b443fd65e",
            "certificateId":
 "4f0ba725787aa94d67d2fca420eca022242532e8b3c58e7465c7778b443fd65e",
            "status": "ACTIVE",
            "creationDate": 1541022751.983
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListCertificates en la Referencia de comandos de la AWS CLI.

`list-custom-metrics`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-custom-metrics`.

AWS CLI

Para enumerar sus métricas personalizadas

En el siguiente ejemplo de `list-custom-metrics`, se enumeran todas las métricas personalizadas.

```
aws iot list-custom-metrics \
    --region us-east-1
```

Salida:

```
{
    "metricNames": [
```

```
        "batteryPercentage"
    ]
}
```

Para obtener más información, consulte Métricas personalizadas en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte ListCustomMetrics en la Referencia de comandos de la AWS CLI.

`list-dimensions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-dimensions`.

AWS CLI

Para enumerar las dimensiones de su cuenta de AWS

En el siguiente ejemplo de `list-dimensions`, se enumeran todas las dimensiones de AWS IoT Device Defender definidas en su cuenta de AWS.

```
aws iot list-dimensions
```

Salida:

```
{
    "dimensionNames": [
        "TopicFilterForAuthMessages",
        "TopicFilterForActivityMessages"
    ]
}
```

Para obtener más información, consulte Comandos de detección en la Guía para desarrolladores de AWS IoT.

- Para obtener detalles de la API, consulte ListDimensions en la Referencia de comandos de la AWS CLI.

`list-domain-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-domain-configurations`.

AWS CLI

Para enumerar las configuraciones de dominio

En el siguiente ejemplo de `list-domain-configurations`, se enumeran las configuraciones de dominio de su cuenta de AWS que tienen el tipo de servicio especificado.

```
aws iot list-domain-configurations \
    --service-type "DATA"
```

Salida:

```
{
    "domainConfigurations":
    [
        {
            "domainConfigurationName": "additionalDataDomain",
            "domainConfigurationArn": "arn:aws:iot:us-
west-2:123456789012:domainconfiguration/additionalDataDomain/dikMh",
            "serviceType": "DATA"
        },

        {
            "domainConfigurationName": "iot:Jobs",
            "domainConfigurationArn": "arn:aws:iot:us-
west-2:123456789012:domainconfiguration/iot:Jobs",
            "serviceType": "JOBS"
        },
        {
            "domainConfigurationName": "iot:Data-ATS",
            "domainConfigurationArn": "arn:aws:iot:us-
west-2:123456789012:domainconfiguration/iot:Data-ATS",
            "serviceType": "DATA"
        },
        {
            "domainConfigurationName": "iot:CredentialProvider",
            "domainConfigurationArn": "arn:aws:iot:us-
west-2:123456789012:domainconfiguration/iot:CredentialProvider",
            "serviceType": "CREDENTIAL_PROVIDER"
        }
    ]
}
```

Para obtener más información, consulte Configurable Endpoints en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListDomainConfigurations en la Referencia de comandos de la AWS CLI.

`list-indices`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-indices`.

AWS CLI

Para enumerar los índices de búsqueda configurados

En el siguiente ejemplo de `list-indices`, se enumeran todos los índices de búsqueda configurados en su cuenta de AWS. Si no ha activado la indexación de objetos, es posible que no tenga ningún índice.

```
aws iot list-indices
```

Salida:

```
{
    "indexNames": [
        "AWS_Things"
    ]
}
```

Para obtener más información, consulte Managing Thing Indexing, en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListIndices en la Referencia de comandos de la AWS CLI.

`list-job-executions-for-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-job-executions-for-job`.

AWS CLI

Para enumerar los trabajos de su cuenta de AWS

En el siguiente ejemplo de `list-job-executions-for-job`, se enumeran todas las ejecuciones de trabajos de un trabajo de su cuenta de AWS, especificadas por el jobId.

```
aws iot list-job-executions-for-job \
    --job-id my-ota-job
```

Salida:

```
{
     "executionSummaries": [
         {
             "thingArn": "arn:aws:iot:us-east-1:123456789012:thing/my_thing",
             "jobExecutionSummary": {
                 "status": "QUEUED",
                 "queuedAt": "2022-03-07T15:58:42.195000-08:00",
                 "lastUpdatedAt": "2022-03-07T15:58:42.195000-08:00",
                 "executionNumber": 1,
                 "retryAttempt": 0
             }
         }
     ]
 }
```

Para obtener más información, consulte Creating and Managing Jobs (CLI) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListJobExecutionsForJob en la Referencia de comandos de la AWS CLI.

`list-job-executions-for-thing`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-job-executions-for-thing`.

AWS CLI

Para enumerar los trabajos que se han ejecutado para un objeto

En el siguiente ejemplo de `list-job-executions-for-thing`, se enumeran todos los trabajos que se han ejecutado para el objeto denominado `MyRaspberryPi`.

```
aws iot list-job-executions-for-thing \
```

```
    --thing-name "MyRaspberryPi"
```

Salida:

```
{
    "executionSummaries": [
        {
            "jobId": "example-job-01",
            "jobExecutionSummary": {
                "status": "QUEUED",
                "queuedAt": 1560787023.636,
                "lastUpdatedAt": 1560787023.636,
                "executionNumber": 1
            }
        }
    ]
}
```

Para obtener más información, consulte Creating and Managing Jobs (CLI) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListJobExecutionsForThing en la Referencia de comandos de la AWS CLI.

`list-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-jobs`.

AWS CLI

Para enumerar los trabajos de su cuenta de AWS

En el siguiente ejemplo de `list-jobs`, se enumeran todos los trabajos de la cuenta de AWS ordenados por estado del trabajo.

```
aws iot list-jobs
```

Salida:

```
{
```

```
    "jobs": [
        {
            "jobArn": "arn:aws:iot:us-west-2:123456789012:job/example-job-01",
            "jobId": "example-job-01",
            "targetSelection": "SNAPSHOT",
            "status": "IN_PROGRESS",
            "createdAt": 1560787022.733,
            "lastUpdatedAt": 1560787026.294
        }
    ]
}
```

Para obtener más información, consulte Creating and Managing Jobs (CLI) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListJobs en la Referencia de comandos de la AWS CLI.

`list-mitigation-actions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-mitigation-actions`.

AWS CLI

Para enumerar todas las acciones de mitigación definidas

En el siguiente ejemplo de `list-mitigation-actions`, se muestran todas las acciones de mitigación definidas para su cuenta y región de AWS. Para cada acción, se muestran el nombre, el ARN y la fecha de creación.

```
aws iot list-mitigation-actions
```

Salida:

```
{
    "actionIdentifiers": [
        {
            "actionName": "DeactivateCACertAction",
            "actionArn": "arn:aws:iot:us-west-2:123456789012:mitigationaction/
DeactivateCACertAction",
            "creationDate": "2019-12-10T11:12:47.574000-08:00"
```

```
        },
        {
            "actionName": "ResetPolicyVersionAction",
            "actionArn": "arn:aws:iot:us-west-2:123456789012:mitigationaction/
ResetPolicyVersionAction",
            "creationDate": "2019-12-10T11:11:48.920000-08:00"
        },
        {
            "actionName": "PublishFindingToSNSAction",
            "actionArn": "arn:aws:iot:us-west-2:123456789012:mitigationaction/
PublishFindingToSNSAction",
            "creationDate": "2019-12-10T11:10:49.546000-08:00"
        },
        {
            "actionName": "AddThingsToQuarantineGroupAction",
            "actionArn": "arn:aws:iot:us-west-2:123456789012:mitigationaction/
AddThingsToQuarantineGroupAction",
            "creationDate": "2019-12-10T11:09:35.999000-08:00"
        },
        {
            "actionName": "UpdateDeviceCertAction",
            "actionArn": "arn:aws:iot:us-west-2:123456789012:mitigationaction/
UpdateDeviceCertAction",
            "creationDate": "2019-12-10T11:08:44.263000-08:00"
        },
        {
            "actionName": "SampleMitigationAction",
            "actionArn": "arn:aws:iot:us-west-2:123456789012:mitigationaction/
SampleMitigationAction",
            "creationDate": "2019-12-10T11:03:41.840000-08:00"
        }
    ]
}
```

Para obtener más información, consulte ListMitigationActions (Comandos de acciones de mitigación) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListMitigationActions en la Referencia de comandos de la AWS CLI.

`list-mitigations-actions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-mitigations-actions`.

AWS CLI

Para enumerar todas las acciones de mitigación definidas

En el siguiente ejemplo de `list-mitigations-actions`, se muestran todas las acciones de mitigación definidas para su cuenta y región de AWS. Para cada acción, se muestran el nombre, el ARN y la fecha de creación.

```
aws iot list-mitigation-actions
```

Salida:

```
{
    "actionIdentifiers": [
        {
            "actionName": "DeactivateCACertAction",
            "actionArn": "arn:aws:iot:us-west-2:123456789012:mitigationaction/
DeactivateCACertAction",
            "creationDate": "2019-12-10T11:12:47.574000-08:00"
        },
        {
            "actionName": "ResetPolicyVersionAction",
            "actionArn": "arn:aws:iot:us-west-2:123456789012:mitigationaction/
ResetPolicyVersionAction",
            "creationDate": "2019-12-10T11:11:48.920000-08:00"
        },
        {
            "actionName": "PublishFindingToSNSAction",
            "actionArn": "arn:aws:iot:us-west-2:123456789012:mitigationaction/
PublishFindingToSNSAction",
            "creationDate": "2019-12-10T11:10:49.546000-08:00"
        },
        {
            "actionName": "AddThingsToQuarantineGroupAction",
            "actionArn": "arn:aws:iot:us-west-2:123456789012:mitigationaction/
AddThingsToQuarantineGroupAction",
            "creationDate": "2019-12-10T11:09:35.999000-08:00"
        },
        {
            "actionName": "UpdateDeviceCertAction",
            "actionArn": "arn:aws:iot:us-west-2:123456789012:mitigationaction/
UpdateDeviceCertAction",
            "creationDate": "2019-12-10T11:08:44.263000-08:00"
```

```
        },
        {
            "actionName": "SampleMitigationAction",
            "actionArn": "arn:aws:iot:us-west-2:123456789012:mitigationaction/
SampleMitigationAction",
            "creationDate": "2019-12-10T11:03:41.840000-08:00"
        }
    ]
}
```

Para obtener más información, consulte ListMitigationActions (Comandos de acciones de mitigación) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListMitigationsActions en la Referencia de comandos de la AWS CLI.

`list-ota-updates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-ota-updates`.

AWS CLI

Para ver una lista de las actualizaciones de OTA de la cuenta

En el siguiente ejemplo de `list-ota-updates`, se enumeran las actualizaciones OTA disponibles.

```
aws iot list-ota-updates
```

Salida:

```
{
    "otaUpdates": [
        {
            "otaUpdateId": "itsaupdate",
            "otaUpdateArn": "arn:aws:iot:us-west-2:123456789012:otaupdate/
itsaupdate",
            "creationDate": 1557863215.995
        }
    ]
}
```

Para obtener más información, consulte ListOTAUpdates en la Referencia de la API de AWS IoT.

- Para obtener detalles de la API, consulte ListOtaUpdates en la Referencia de comandos de la AWS CLI.

`list-outgoing-certificates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-outgoing-certificates`.

AWS CLI

Para ver una lista de los certificados que se están transfiriendo a una cuenta de AWS diferente

En el siguiente ejemplo de `list-outgoing-certificates`, se enumeran todos los certificados de dispositivo que están en proceso de transferirse a una cuenta de AWS diferente mediante el comando `transfer-certificate`.

```
aws iot list-outgoing-certificates
```

Salida:

```
{
    "outgoingCertificates": [
        {
            "certificateArn": "arn:aws:iot:us-
west-2:030714055129:cert/488b6a7f2acdeb00a77384e63c4e40b18b1b3caaae57b7272ba44c45e3448142",
            "certificateId":
 "488b6a7f2acdeb00a77384e63c4e40b18b1b3caaae57b7272ba44c45e3448142",
            "transferredTo": "030714055129",
            "transferDate": 1569427780.441,
            "creationDate": 1569363250.557
        }
    ]
}
```

Para obtener más información, consulte ListOutgoingCertificates en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte ListOutgoingCertificates en la Referencia de comandos de la AWS CLI.

`list-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-policies`.

AWS CLI

Para ver una lista de las políticas definidas en su cuenta de AWS

En el siguiente ejemplo de `list-policies`, se enumeran todas las políticas definidas en la cuenta de AWS.

```
aws iot list-policies
```

Salida:

```
{
    "policies": [
        {
            "policyName": "UpdateDeviceCertPolicy",
            "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/
UpdateDeviceCertPolicy"
        },
        {
            "policyName": "PlantIoTPolicy",
            "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/PlantIoTPolicy"
        },
        {
            "policyName": "MyPiGroup_Core-policy",
            "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/MyPiGroup_Core-
policy"
        }
    ]
}
```

Para obtener más información, consulte AWS IoT Policies en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListPolicies en la Referencia de comandos de la AWS CLI.

`list-policy-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-policy-versions`.

AWS CLI

Ejemplo 1: visualización de todas las versiones de una política

En el siguiente ejemplo de `list-policy-versions`, se enumeran todas las versiones de la política especificada y sus fechas de creación.

```
aws iot list-policy-versions \
    --policy-name LightBulbPolicy
```

Salida:

```
{
    "policyVersions": [
        {
            "versionId": "2",
            "isDefaultVersion": true,
            "createDate": 1559925941.924
        },
        {
            "versionId": "1",
            "isDefaultVersion": false,
            "createDate": 1559925941.924
        }
    ]
}
```

Para obtener más información, consulte AWS IoT Policies en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListPolicyVersions en la Referencia de comandos de la AWS CLI.

`list-principal-things`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-principal-things`.

AWS CLI

Para enumerar los objetos asociados a una entidad principal

En el siguiente ejemplo de `list-principal-things`, se enumeran los objetos asociados a la entidad principal especificada por un ARN.

```
aws iot list-principal-things \
    --principal arn:aws:iot:us-
west-2:123456789012:cert/2e1eb273792174ec2b9bf4e9b37e6c6c692345499506002a351597670552 78e8
```

Salida:

```
{
    "things": [
        "DeskLamp",
        "TableLamp"
    ]
}
```

Para obtener más información, consulte ListPrincipalThings en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte ListPrincipalThings en la Referencia de comandos de la AWS CLI.

`list-provisioning-template-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-provisioning-template-versions`.

AWS CLI

Para enumerar las versiones de plantillas de aprovisionamiento

En el siguiente ejemplo de `list-provisioning-template-versions`, se enumeran las versiones de la plantilla de aprovisionamiento especificada.

```
aws iot list-provisioning-template-versions \
    --template-name "widget-template"
```

Salida:

```
{
    "versions": [
        {
            "versionId": 1,
            "creationDate": 1574800471.339,
            "isDefaultVersion": true
        },
        {
            "versionId": 2,
            "creationDate": 1574801192.317,
            "isDefaultVersion": false
        }
    ]
}
```

Para obtener más información, consulte AWS IoT Secure Tunneling en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte ListProvisioningTemplateVersions en la Referencia de comandos de la AWS CLI.

`list-provisioning-templates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-provisioning-templates`.

AWS CLI

Para enumerar las plantillas de aprovisionamiento

En el siguiente ejemplo de `list-provisioning-templates`, se enumeran todas las plantillas de aprovisionamiento de la cuenta de AWS.

```
aws iot list-provisioning-templates
```

Salida:

```
{
    "templates": [
        {
            "templateArn": "arn:aws:iot:us-east-1:123456789012:provisioningtemplate/
widget-template",
```

```
            "templateName": "widget-template",
            "description": "A provisioning template for widgets",
            "creationDate": 1574800471.367,
            "lastModifiedDate": 1574801192.324,
            "enabled": false
        }
    ]
}
```

Para obtener más información, consulte AWS IoT Secure Tunneling en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte ListProvisioningTemplates en la Referencia de comandos de la AWS CLI.

`list-role-aliases`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-role-aliases`.

AWS CLI

Para enumerar los alias de los roles de AWS IoT en su cuenta de AWS

En el siguiente ejemplo de `list-role-aliases`, se enumeran los alias de rol de AWS IoT de la cuenta de AWS.

```
aws iot list-role-aliases
```

Salida:

```
{
    "roleAliases": [
        "ResidentAlias",
        "ElectricianAlias"
    ]
}
```

Para obtener más información, consulte ListRoleAliases en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte ListRoleAliases en la Referencia de comandos de la AWS CLI.

`list-scheduled-audits`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-scheduled-audits`.

AWS CLI

Para enumerar las auditorías programadas para su cuenta AWS

En el siguiente ejemplo de `list-scheduled-audits`, se enumeran las auditorías programadas para la cuenta de AWS.

```
aws iot list-scheduled-audits
```

Salida:

```
{
    "scheduledAudits": [
        {
            "scheduledAuditName": "AWSIoTDeviceDefenderDailyAudit",
            "scheduledAuditArn": "arn:aws:iot:us-west-2:123456789012:scheduledaudit/
AWSIoTDeviceDefenderDailyAudit",
            "frequency": "DAILY"
        },
        {
            "scheduledAuditName": "AWSDeviceDefenderWeeklyAudit",
            "scheduledAuditArn": "arn:aws:iot:us-west-2:123456789012:scheduledaudit/
AWSDeviceDefenderWeeklyAudit",
            "frequency": "WEEKLY",
            "dayOfWeek": "SUN"
        }
    ]
}
```

Para obtener más información, consulte Comandos de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListScheduledAudits en la Referencia de comandos de la AWS CLI.

`list-security-profiles-for-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-security-profiles-for-target`.

AWS CLI

Para enumerar los perfiles de seguridad asociados a un destino

En el siguiente ejemplo de `list-security-profiles-for-target`, se enumeran los perfiles de seguridad de AWS IoT Device Defender conectados a dispositivos no registrados.

```
aws iot list-security-profiles-for-target  \
    --security-profile-target-arn "arn:aws:iot:us-west-2:123456789012:all/
unregistered-things"
```

Salida:

```
{
    "securityProfileTargetMappings": [
        {
            "securityProfileIdentifier": {
                "name": "Testprofile",
                "arn": "arn:aws:iot:us-west-2:123456789012:securityprofile/
Testprofile"
            },
            "target": {
                "arn": "arn:aws:iot:us-west-2:123456789012:all/unregistered-things"
            }
        }
    ]
}
```

Para obtener más información, consulte Comandos de detección en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListSecurityProfilesForTarget en la Referencia de comandos de la AWS CLI.

`list-security-profiles`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-security-profiles`.

AWS CLI

Para enumerar los perfiles de seguridad de su cuenta de AWS

En el siguiente ejemplo de `list-security-profiles`, se enumeran todos los perfiles de seguridad de AWS IoT Device Defender definidos en la cuenta de AWS.

```
aws iot list-security-profiles
```

Salida:

```
{
    "securityProfileIdentifiers": [
        {
            "name": "Testprofile",
            "arn": "arn:aws:iot:us-west-2:123456789012:securityprofile/Testprofile"
        }
    ]
}
```

Para obtener más información, consulte Comandos de detección en la Guía para desarrolladores de AWS IoT.

- Para obtener detalles sobre la API, consulte ListSecurityProfiles en la Referencia de comandos de la AWS CLI.

`list-streams`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-streams`.

AWS CLI

Para enumerar los flujos de la cuenta

En el siguiente ejemplo de `list-streams`, se enumeran todos los flujos de la cuenta de AWS.

```
aws iot list-streams
```

Salida:

```
{
    "streams": [
```

```
        {
            "streamId": "stream12345",
            "streamArn": "arn:aws:iot:us-west-2:123456789012:stream/stream12345",
            "streamVersion": 1,
            "description": "This stream is used for Amazon FreeRTOS OTA Update
 12345."
        },
        {
            "streamId": "stream54321",
            "streamArn": "arn:aws:iot:us-west-2:123456789012:stream/stream54321",
            "streamVersion": 1,
            "description": "This stream is used for Amazon FreeRTOS OTA Update
 54321."
        }
    ]
}
```

Para obtener más información, consulte ListStreams en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte ListStreams en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para mostrar las etiquetas y sus valores asociados a un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se muestran las etiquetas y los valores asociados al grupo de objetos `LightBulbs`.

```
aws iot list-tags-for-resource \
    --resource-arn "arn:aws:iot:us-west-2:094249569039:thinggroup/LightBulbs"
```

Salida:

```
{
    "tags": [
        {
            "Key": "Assembly",
```

```
            "Value": "Fact1NW"
        },
        {
            "Key": "MyTag",
            "Value": "777"
        }
    ]
}
```

Para obtener más información, consulte Tagging Your AWS Resources en la Guía para desarrolladores de AWS IoT.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-targets-for-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-targets-for-policy`.

AWS CLI

Para enumerar las entidades principales asociadas a una política de AWS IoT

En el siguiente ejemplo de `list-targets-for-policy`, se enumeran los certificados de dispositivo que tienen asociada la política especificada.

```
aws iot list-targets-for-policy \
    --policy-name UpdateDeviceCertPolicy
```

Salida:

```
{
    "targets": [
        "arn:aws:iot:us-
west-2:123456789012:cert/488b6a7f2acdeb00a77384e63c4e40b18b1b3caaae57b7272ba44c45e3448142",
        "arn:aws:iot:us-west-2:123456789012:cert/
d1eb269fb55a628552143c8f96eb3c258fcd5331ea113e766ba0c82bf225f0be"
    ]
}
```

Para obtener más información, consulte Thing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListTargetsForPolicy en la Referencia de comandos de la AWS CLI.

`list-targets-for-security-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-targets-for-security-profile`.

AWS CLI

Para enumerar los destinos a los que se aplica un perfil de seguridad

En el siguiente ejemplo de `list-targets-for-security-profile`, se enumeran los destinos a los que se aplica el perfil de seguridad de AWS IoT Device Defender denominado `PossibleIssue`.

```
aws iot list-targets-for-security-profile \
    --security-profile-name Testprofile
```

Salida:

```
{
    "securityProfileTargets": [
        {
            "arn": "arn:aws:iot:us-west-2:123456789012:all/unregistered-things"
        },
        {
            "arn": "arn:aws:iot:us-west-2:123456789012:all/registered-things"
        }
    ]
}
```

Para obtener más información, consulte Comandos de detección en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListTargetsForSecurityProfile en la Referencia de comandos de la AWS CLI.

`list-thing-groups-for-thing`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-thing-groups-for-thing`.

AWS CLI

Para enumerar los grupos a los que pertenece un objeto

En el siguiente ejemplo de `list-thing-groups-for-thing`, se enumeran los grupos a los que pertenece el objeto especificado.

```
aws iot list-thing-groups-for-thing \
    --thing-name MyLightBulb
```

Salida:

```
{
    "thingGroups": [
        {
            "groupName": "DeadBulbs",
            "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/DeadBulbs"
        },
        {
            "groupName": "LightBulbs",
            "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/LightBulbs"
        }
    ]
}
```

Para obtener más información, consulte Thing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListThingGroupsForThing en la Referencia de comandos de la AWS CLI.

`list-thing-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-thing-groups`.

AWS CLI

Para enumerar los grupos de objetos en su cuenta de AWS

En el siguiente ejemplo de `describe-thing-group`, se enumeran todos los grupos de objetos definidos en la cuenta de AWS.

```
aws iot list-thing-groups
```

Salida:

```
{
    "thingGroups": [
        {
            "groupName": "HalogenBulbs",
            "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/HalogenBulbs"
        },
        {
            "groupName": "LightBulbs",
            "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/LightBulbs"
        }
    ]
}
```

Para obtener más información, consulte Thing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListThingGroups en la Referencia de comandos de la AWS CLI.

`list-thing-principals`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-thing-principals`.

AWS CLI

Para enumerar las entidades principales asociadas con el objeto

En el siguiente ejemplo de `list-thing-principals`, se enumeran las entidades principales (certificados X.509, usuarios de IAM, roles, identidades de Amazon Cognito o identidades federadas) asociadas al objeto especificado.

```
aws iot list-thing-principals \
    --thing-name MyRaspberryPi
```

Salida:

```
{
```

```
    "principals": [
        "arn:aws:iot:us-
west-2:123456789012:cert/33475ac865079a5ffd5ecd44240640349293facc760642d7d8d5dbb6b4c86893"
    ]
}
```

Para obtener más información, consulte ListThingPrincipals en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte ListThingPrincipals en la Referencia de comandos de la AWS CLI.

`list-thing-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-thing-types`.

AWS CLI

Para enumerar los tipos de objetos definidos

En el siguiente ejemplo de `list-thing-types`, se muestra una lista de los tipos de objeto definidos en la cuenta de AWS.

```
aws iot list-thing-types
```

Salida:

```
{
    "thingTypes": [
        {
            "thingTypeName": "LightBulb",
            "thingTypeArn": "arn:aws:iot:us-west-2:123456789012:thingtype/
LightBulb",
            "thingTypeProperties": {
                "thingTypeDescription": "light bulb type",
                "searchableAttributes": [
                    "model",
                    "wattage"
                ]
            },
            "thingTypeMetadata": {
```

```
            "deprecated": false,
            "creationDate": 1559772562.498
            }
        }
    ]
}
```

Para obtener más información, consulte Thing Types en la Guía para desarrolladores de AWS IoT.

- Para obtener detalles de la API, consulte ListThingTypes en la Referencia de comandos de la AWS CLI.

`list-things-in-billing-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-things-in-billing-group`.

AWS CLI

Para enumerar los objetos de un grupo de facturación

En el siguiente ejemplo de `list-things-in-billing-group`, se enumeran los objetos que se encuentran en el grupo de facturación especificado.

```
aws iot list-things-in-billing-group \
    --billing-group-name GroupOne
```

Salida:

```
{
    "things": [
        "MyOtherLightBulb",
        "MyLightBulb"
    ]
}
```

Para obtener más información, consulte Billing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListThingsInBillingGroup en la Referencia de comandos de la AWS CLI.

`list-things-in-thing-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-things-in-thing-group`.

AWS CLI

Para enumerar los objetos que pertenecen a un grupo

En el siguiente ejemplo de `list-things-in-thing-group`, se enumeran los objetos a los que pertenece el grupo de objetos especificado.

```
aws iot list-things-in-thing-group \
    --thing-group-name LightBulbs
```

Salida:

```
{
    "things": [
        "MyLightBulb"
    ]
}
```

Para obtener más información, consulte Thing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListThingsInThingGroup en la Referencia de comandos de la AWS CLI.

`list-things`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-things`.

AWS CLI

Ejemplo 1: Creación de una lista de todos los objetos del registro

En el siguiente ejemplo de `list-things` se enumeran los objetos (dispositivos) que están definidos en el registro de AWS IoT de su cuenta de AWS.

```
aws iot list-things
```

Salida:

```
{
    "things": [
        {
            "thingName": "ThirdBulb",
            "thingTypeName": "LightBulb",
            "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/ThirdBulb",
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
            "version": 2
        },
        {
            "thingName": "MyOtherLightBulb",
            "thingTypeName": "LightBulb",
            "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MyOtherLightBulb",
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
            "version": 3
        },
        {
            "thingName": "MyLightBulb",
            "thingTypeName": "LightBulb",
            "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MyLightBulb",
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
            "version": 1
        },
        {
        "thingName": "SampleIoTThing",
        "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/SampleIoTThing",
        "attributes": {},
        "version": 1
        }
    ]
}
```

Ejemplo 2: Creación de una lista de los objetos definidos que tienen un atributo específico

En el siguiente ejemplo de `list-things` se muestra una lista de objetos que tienen un atributo denominado `wattage`.

```
aws iot list-things \
    --attribute-name wattage
```

Salida:

```
{
    "things": [
        {
            "thingName": "MyLightBulb",
            "thingTypeName": "LightBulb",
            "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MyLightBulb",
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
            "version": 1
        },
        {
            "thingName": "MyOtherLightBulb",
            "thingTypeName": "LightBulb",
            "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MyOtherLightBulb",
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
            "version": 3
        }
    ]
}
```

Para obtener más información, consulte Administración de objetos con el registro en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListThings en la Referencia de comandos de la AWS CLI.

`list-topic-rule-destinations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-topic-rule-destinations`.

AWS CLI

Para enumerar los destinos de sus reglas de tema

En el siguiente ejemplo de `list-topic-rule-destinations`, se enumeran todos los destinos de las reglas de tema que ha definido en la región de AWS actual.

```
aws iot list-topic-rule-destinations
```

Salida:

```
{
    "destinationSummaries": [
        {
            "arn": "arn:aws:iot:us-west-2:123456789012:ruledestination/http/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "status": "ENABLED",
            "httpUrlSummary": {
                "confirmationUrl": "https://example.com"
            }
        }
    ]
}
```

Para obtener más información, consulte Working with topic rule destinations en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte ListTopicRuleDestinations en la Referencia de comandos de la AWS CLI.

`list-topic-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-topic-rules`.

AWS CLI

Para enumerar las reglas

En el siguiente ejemplo de `list-topic-rules`, se enumeran todas las reglas que ha definido.

```
aws iot list-topic-rules
```

Salida:

```
{
    "rules": [
        {
            "ruleArn": "arn:aws:iot:us-west-2:123456789012:rule/
MyRPiLowMoistureAlertRule",
            "ruleName": "MyRPiLowMoistureAlertRule",
            "topicPattern": "$aws/things/MyRPi/shadow/update/accepted",
            "createdAt": 1558624363.0,
            "ruleDisabled": false
        },
        {
            "ruleArn": "arn:aws:iot:us-west-2:123456789012:rule/
MyPlantPiMoistureAlertRule",
            "ruleName": "MyPlantPiMoistureAlertRule",
            "topicPattern": "$aws/things/MyPlantPi/shadow/update/accepted",
            "createdAt": 1541458459.0,
            "ruleDisabled": false
        }
    ]
}
```

Para obtener más información, consulte Viewing Your Rules en la Guía para desarrolladores de AWS IoT.

- Para obtener detalles de la API, consulte ListTopicRules en la Referencia de comandos de la AWS CLI.

`list-v2-logging-levels`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-v2-logging-levels`.

AWS CLI

Para enumerar los niveles de registro

En el siguiente ejemplo de `list-v2-logging-levels`, se enumeran los niveles de registro configurados. Si no se han establecido niveles de registro, se produce una `NotConfiguredException` al ejecutar este comando.

```
aws iot list-v2-logging-levels
```

Salida:

```
{
    "logTargetConfigurations": [
        {
            "logTarget": {
                "targetType": "DEFAULT"
            },
            "logLevel": "ERROR"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListV2LoggingLevels en la Referencia de comandos de la AWS CLI.

`list-violation-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-violation-events`.

AWS CLI

Para enumerar las infracciones del perfil de seguridad durante un período de tiempo

En el siguiente ejemplo de `list-violation-events`, se enumeran las infracciones que se han producido entre el 5 y el 12 de junio de 2019 en todos los perfiles de seguridad de AWS IoT Device Defender de la cuenta de AWS actual y la región de AWS.

```
aws iot list-violation-events \
    --start-time 1559747125 \
    --end-time 1560351925
```

Salida:

```
{
    "violationEvents": [
        {
            "violationId": "174db59167fa474c80a652ad1583fd44",
            "thingName": "iotconsole-1560269126751-1",
            "securityProfileName": "Testprofile",
            "behavior": {
                "name": "Authorization",
```

```
                "metric": "aws:num-authorization-failures",
                "criteria": {
                    "comparisonOperator": "greater-than",
                    "value": {
                        "count": 10
                    },
                    "durationSeconds": 300,
                    "consecutiveDatapointsToAlarm": 1,
                    "consecutiveDatapointsToClear": 1
                }
            },
            "metricValue": {
                "count": 0
            },
            "violationEventType": "in-alarm",
            "violationEventTime": 1560279000.0
        },
        {
            "violationId": "c8a9466a093d3b7b35cd44ca58bdbeab",
            "thingName": "TvnQoEoU",
            "securityProfileName": "Testprofile",
            "behavior": {
                "name": "CellularBandwidth",
                "metric": "aws:message-byte-size",
                "criteria": {
                    "comparisonOperator": "greater-than",
                    "value": {
                        "count": 128
                    },
                    "consecutiveDatapointsToAlarm": 1,
                    "consecutiveDatapointsToClear": 1
                }
            },
            "metricValue": {
                "count": 110
            },
            "violationEventType": "in-alarm",
            "violationEventTime": 1560276600.0
        },
        {
            "violationId": "74aa393adea02e6648f3ac362beed55e",
            "thingName": "iotconsole-1560269232412-2",
            "securityProfileName": "Testprofile",
            "behavior": {
```

```
                "name": "Authorization",
                "metric": "aws:num-authorization-failures",
                "criteria": {
                    "comparisonOperator": "greater-than",
                    "value": {
                        "count": 10
                    },
                    "durationSeconds": 300,
                    "consecutiveDatapointsToAlarm": 1,
                    "consecutiveDatapointsToClear": 1
                }
            },
            "metricValue": {
                "count": 0
            },
            "violationEventType": "in-alarm",
            "violationEventTime": 1560276600.0
        },
        {
            "violationId": "1e6ab5f7cf39a1466fcd154e1377e406",
            "thingName": "TvnQoEoU",
            "securityProfileName": "Testprofile",
            "behavior": {
                "name": "Authorization",
                "metric": "aws:num-authorization-failures",
                "criteria": {
                    "comparisonOperator": "greater-than",
                    "value": {
                        "count": 10
                    },
                    "durationSeconds": 300,
                    "consecutiveDatapointsToAlarm": 1,
                    "consecutiveDatapointsToClear": 1
                }
            },
            "metricValue": {
                "count": 0
            },
            "violationEventType": "in-alarm",
            "violationEventTime": 1560276600.0
        }
    ]
}
```

Para obtener más información, consulte Comandos de detección en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListViolationEvents en la Referencia de comandos de la AWS CLI.

`register-ca-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-ca-certificate`.

AWS CLI

Para recuperar el certificado de una entidad de certificación (CA)

En el siguiente ejemplo de `register-ca-certificate`, se registra un certificado de CA. El comando proporciona el certificado de CA y un certificado de verificación de clave que demuestra que usted es el propietario de la clave privada asociada al certificado de CA.

```
aws iot register-ca-certificate \
    --ca-certificate file://rootCA.pem \
    --verification-cert file://verificationCert.pem
```

Salida:

```
{
    "certificateArn": "arn:aws:iot:us-west-2:123456789012:cacert/
f4efed62c0142f16af278166f61962501165c4f053629520742646005 8cd1467",
    "certificateId":
 "f4efed62c0142f16af278166f61962501165c4f053629520742646005 8cd1467"
 }
```

Para obtener más información, consulte RegisterCACertificate en la Referencia de la API de AWS IoT.

- Para obtener más información sobre la API, consulte RegisterCaCertificate en la Referencia de comandos de la AWS CLI.

`register-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-certificate`.

AWS CLI

Para registrar un certificado de dispositivo autofirmado

En el siguiente ejemplo de `register-certificate`, se registra el certificado de dispositivo `deviceCert.pem` firmado por el certificado de CA `rootCA.pem`. El certificado de CA debe registrarse antes de usarlo para registrar un certificado de dispositivo autofirmado. El certificado autofirmado debe estar firmado por el mismo certificado de CA que se pasa a este comando.

```
aws iot register-certificate \
    --certificate-pem file://deviceCert.pem \
    --ca-certificate-pem file://rootCA.pem
```

Salida:

```
{
    "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/488b6a7f2acdeb00a77384e63c4e40b18b1b3caaae57b7272ba44c45e3448142",
    "certificateId":
 "488b6a7f2acdeb00a77384e63c4e40b18b1b3caaae57b7272ba44c45e3448142"
 }
```

Para obtener más información, consulte RegisterCertificate en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte RegisterCertificate en la Referencia de comandos de la AWS CLI.

`register-thing`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-thing`.

AWS CLI

Para registrar un objeto

En el siguiente ejemplo de `register-thing`, se registra un objeto mediante una plantilla de aprovisionamiento.

```
aws iot register-thing \
```

```
    --template-body '{"Parameters":{"ThingName":
{"Type":"String"},"AWS::IoT::Certificate::Id":{"Type":"String"}},"Resources":
 {"certificate":{"Properties":{"CertificateId":
{"Ref":"AWS::IoT::Certificate::Id"},"Status":"Active"},"Type":"AWS::IoT::Certificate"},"poli
{"Properties":{"PolicyName":"MyIotPolicy"},"Type":"AWS::IoT::Policy"},"thing":
{"OverrideSettings":
{"AttributePayload":"MERGE","ThingGroups":"DO_NOTHING","ThingTypeName":"REPLACE"},"Propertie
{"AttributePayload":{},"ThingGroups":[],"ThingName":
{"Ref":"ThingName"},"ThingTypeName":"VirtualThings"},"Type":"AWS::IoT::Thing"}}}' \
    --parameters '{"ThingName":"Register-thing-
trial-1","AWS::IoT::Certificate::Id":"799a9ea048a1e6aea42b55EXAMPLEf8697b4bafcd77a318a3068e3
```

Salida:

```
{
    "certificatePem": "-----BEGIN CERTIFICATE-----
\nMIIDWTCCAkGgAwIBAgIUYLk81I35cIppobpw
HiOJ2jNjboIwDQYJKoZIhvcNAQEL
\nBQAwTTFLMEkGA1UECwxCQW1hem9uIFdlYiBTZXJ2aWNlcyBPPUFtYXpvbi
5jb20g\nSW5jLiBMPVNlYXR0bGUgU1Q9V2FzaGluZ3RvbiBDPVVTMB4XDTIwMDcyMzE2NDUw
\nOVoXDTQ5MTIzMT
IzNTk1OVowHjEcMBoGA1UEAwwTQVdTIElvVCBDZXJ0aWZpY2F0\nZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAO71uADhdBajqTmgrMV5\nmCFfBZQRMo1MdtVoZr2X+M4MzL
+RARrtUzH9a2SMAckeX8KeblIOTKzORI
RDXnyE
\n6lVOwjgAsd0ku22rFxex4eG2ikha7pYYkvuToqA7L3TxItRvfKrxRI4ZfJoFPip4\nKqiuBJVNOGKTcQ
Hd1RNOrddwwu6kFJLeKDmEXAMPLEdUF0N+qfR9yKnZQkm
+g6Q2\nGXu7u0W3hn6nlRN8qVoka0uW12p53xM7oHVz
Gf+cxKBxlbOhGkp6yCfTSkUBm3Sp\n9zLw35kiHXVm4EVpwgNlnk6XcIGIkw8a/iy4pzmvuGAANY1/uU/
zgCjymw
ZT5S30\nBV0CAwEAAaNgMF4wHwYDVR0jBBgwFoAUGx0tCcU3q2n1WXAuUCv6hugXjKswHQYD
\nVR0OBBYEFOVtvZ
9Aj2RYFnkX7Iu01XTRUdxgMAwGA1UdEwEB/wQCMAAwDgYDVR0P\nAQH/
BAQDAgeAMA0GCSqGSIb3DQEBCwUAA4IB
AQCXCQcpOtubS5ftOsDMTcpP/jNX
\nDHyArxmjpSc2aCdmm7WX59lTKWyAdxGAvqaDVWqTo0oXI7tZ8w7aINlGi5
pXnifx\n3SBebMUoBbTktrC97yUaeL025mCFv8emDnTR/fE7PTsBKjW0g/rrfpwBxZLXDFwN
\nnqkQjy3EDfifj2
6j0xYIqqWMPogyn4srOCKynS5wMJuQZlHQOnabVwnwK4Y0Mflp
\np9+4susFUR9aT3BT1AcIwqSpzhlKhh4Iz7ND
kRn4amsUT210jg/zOO1Ow+BTHcVQ\nJly8XDu0CWSu04q6SnaBzHmlySIajxuRTP/AdfRouP1OXe
+qlbPOBcvVvF
8o\n-----END CERTIFICATE-----\n",
```

```
    "resourceArns": {
        "certificate": "arn:aws:iot:us-
west-2:571032923833:cert/799a9ea048a1e6aea42b55EXAMPLEf8697b4bafcd77a318a3068e30404b9233c",
        "thing": "arn:aws:iot:us-west-2:571032923833:thing/Register-thing-trial-1"
    }
}
```

Para obtener más información, consulte Provisioning by trusted user en la Guía para desarrolladores de AWS IoT Core.

- Para obtener más información sobre la API, consulte RegisterThing en la Referencia de comandos de la AWS CLI.

`reject-certificate-transfer`

En el siguiente ejemplo de código, se muestra cómo utilizar `reject-certificate-transfer`.

AWS CLI

Para rechazar una transferencia de certificado

En el siguiente ejemplo de `reject-certificate-transfer`, se rechaza la transferencia del certificado de dispositivo especificado desde otra cuenta de AWS.

```
aws iot reject-certificate-transfer \
    --certificate-
id f0f33678c7c9a046e5cc87b2b1a58dfa0beec26db78addd5e605d630e05c7fc8
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Transfer a certificate to another account en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte RejectCertificateTransfer en la Referencia de comandos de la AWS CLI.

`remove-thing-from-billing-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-thing-from-billing-group`.

AWS CLI

Para quitar un objeto de un grupo de facturación

En el siguiente ejemplo de `remove-thing-from-billing-group`, se elimina el objeto especificado de un grupo de facturación.

```
aws iot remove-thing-from-billing-group \
    --billing-group-name GroupOne \
    --thing-name MyOtherLightBulb
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Billing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte RemoveThingFromBillingGroup en la Referencia de comandos de la AWS CLI.

`remove-thing-from-thing-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-thing-from-thing-group`.

AWS CLI

Para quitar un objeto de un grupo de objetos

En el siguiente ejemplo de `remove-thing-from-thing-group`, se elimina el objeto especificado de un grupo de objetos.

```
aws iot remove-thing-from-thing-group \
    --thing-name bulb7 \
    --thing-group-name DeadBulbs
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Thing Groups <https://docs.aws.amazon.com/iot/latest/developerguide/thing-groups.html > en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte RemoveThingFromThingGroup en la Referencia de comandos de la AWS CLI.

`replace-topic-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `replace-topic-rule`.

AWS CLI

Para actualizar una definición de reglas de un tema

En el siguiente ejemplo de `replace-topic-rule`, se actualiza la regla especificada para enviar una alerta de SNS cuando los valores de las lecturas del nivel de humedad del suelo son demasiado bajas.

```
aws iot replace-topic-rule \
    --rule-name MyRPiLowMoistureAlertRule \
    --topic-rule-payload "{\"sql\": \"SELECT * FROM '$aws/things/MyRPi/shadow/
update/accepted' WHERE state.reported.moisture = 'low'\", \"description\": \"Sends
 an alert when soil moisture level readings are too low.\",\"actions\": [{\"sns
\":{\"targetArn\":\"arn:aws:sns:us-west-2:123456789012:MyRPiLowMoistureTopic\",
\"roleArn\":\"arn:aws:iam::123456789012:role/service-role/MyRPiLowMoistureTopicRole
\",\"messageFormat\": \"RAW\"}}],\"ruleDisabled\": false,\"awsIotSqlVersion\":
\"2016-03-23\"}"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creating an AWS IoT Rule en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ReplaceTopicRule en la Referencia de comandos de la AWS CLI.

`search-index`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-index`.

AWS CLI

Para consultar el índice de objetos

En el siguiente ejemplo de `search-index` se consulta en el índice de `AWS_Things` los objetos que son del tipo `LightBulb`.

```
aws iot search-index \
```

```
    --index-name "AWS_Things" \
    --query-string "thingTypeName:LightBulb"
```

Salida:

```
{
    "things": [
        {
            "thingName": "MyLightBulb",
            "thingId": "40da2e73-c6af-406e-b415-15acae538797",
            "thingTypeName": "LightBulb",
            "thingGroupNames": [
                "LightBulbs",
                "DeadBulbs"
            ],
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
            "connectivity": {
                "connected": false
            }
        },
        {
            "thingName": "ThirdBulb",
            "thingId": "615c8455-33d5-40e8-95fd-3ee8b24490af",
            "thingTypeName": "LightBulb",
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
            "connectivity": {
                "connected": false
            }
        },
        {
            "thingName": "MyOtherLightBulb",
            "thingId": "6dae0d3f-40c1-476a-80c4-1ed24ba6aa11",
            "thingTypeName": "LightBulb",
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
```

```
            "connectivity": {
                "connected": false
            }
        }
    ]
}
```

Para obtener más información, consulte Managing Thing Indexing, en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte SearchIndex en la Referencia de comandos de la AWS CLI.

`set-default-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-default-authorizer`.

AWS CLI

Para definir el autorizador predeterminado

En el siguiente ejemplo de `set-default-authorizer`, se establece el autorizador personalizado denominado `CustomAuthorizer` como el autorizador predeterminado.

```
aws iot set-default-authorizer \
    --authorizer-name CustomAuthorizer
```

Salida:

```
{
    "authorizerName": "CustomAuthorizer",
    "authorizerArn": "arn:aws:iot:us-west-2:123456789012:authorizer/
CustomAuthorizer"
}
```

Para obtener más información, consulte CreateDefaultAuthorizer en la Referencia de la API de AWS IoT.

- Para obtener detalles sobre la API, consulte SetDefaultAuthorizer en la Referencia de comandos de la AWS CLI.

`set-default-policy-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-default-policy-version`.

AWS CLI

Para definir la versión predeterminada de una política

En el siguiente ejemplo de `set-default-policy-version`, se establece la versión predeterminada 2 en la política denominada `UpdateDeviceCertPolicy`.

```
aws iot set-default-policy-version \
    --policy-name UpdateDeviceCertPolicy \
    --policy-version-id 2
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte SetDefaultPolicyVersion en la Referencia de comandos de la AWS CLI.

`set-v2-logging-level`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-v2-logging-level`.

AWS CLI

Para definir el nivel de registro de un grupo de objetos

En el siguiente ejemplo de `set-v2-logging-level`, se define el nivel de registro para registrar avisos para el grupo de objetos especificado.

```
aws iot set-v2-logging-level \
    --log-target "{\"targetType\":\"THING_GROUP\",\"targetName\":\"LightBulbs\"}" \
    --log-level WARN
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte SetV2LoggingLevel en la Referencia de comandos de la AWS CLI.

`set-v2-logging-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-v2-logging-options`.

AWS CLI

Para definir las opciones de registro

En el siguiente ejemplo de `set-v2-logging-options`, se establece el nivel de verbosidad de registro predeterminado en ERROR y se especifica el ARN que se utilizará para el registro.

```
aws iot set-v2-logging-options \
    --default-log-level ERROR \
    --role-arn "arn:aws:iam::094249569039:role/service-role/iotLoggingRole"
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte SetV2LoggingOptions en la Referencia de comandos de la AWS CLI.

`start-audit-mitigation-actions-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-audit-mitigation-actions-task`.

AWS CLI

Para aplicar una acción de mitigación a los resultados de una auditoría

En el siguiente ejemplo de `start-audit-mitigation-actions-task`, se aplica la acción `ResetPolicyVersionAction` (que borra la política) al único resultado especificado.

```
aws iot start-audit-mitigation-actions-task \
    --task-id "myActionsTaskId" \
    --target "findingIds=[\"0edbaaec-2fe1-4cf5-abc9-d4c3e51f7464\"]" \
    --audit-check-to-actions-mapping
 "IOT_POLICY_OVERLY_PERMISSIVE_CHECK=[\"ResetPolicyVersionAction\"]" \
    --client-request-token "adhadhahda"
```

Salida:

```
{
    "taskId": "myActionsTaskId"
}
```

Para obtener más información, consulte StartAuditMitigationActionsTask (Comandos de acciones de mitigación) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte StartAuditMitigationActionsTask en la Referencia de comandos de la AWS CLI.

`start-on-demand-audit-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-on-demand-audit-task`.

AWS CLI

Para iniciar una auditoría de inmediato

En el siguiente ejemplo de `start-on-demand-audit-task`, se inicia una auditoría de AWS IoT Device Defender y se realizan tres comprobaciones de certificados.

```
aws iot start-on-demand-audit-task \
    --target-check-
names CA_CERTIFICATE_EXPIRING_CHECK DEVICE_CERTIFICATE_EXPIRING_CHECK REVOKED_CA_CERTIFICATE
```

Salida:

```
{
    "taskId": "a3aea009955e501a31b764abe1bebd3d"
}
```

Para obtener más información, consulte Comandos de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte StartOnDemandAuditTask en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para especificar una clave y valor de etiqueta para un recurso

En el siguiente ejemplo de `tag-resource`, se aplica la etiqueta con una clave `Assembly` y el valor `Fact1NW` al grupo de objetos `LightBulbs`.

```
aws iot tag-resource \
    --tags Key=Assembly,Value="Fact1NW" \
    --resource-arn "arn:aws:iot:us-west-2:094249569039:thinggroup/LightBulbs"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging Your AWS Resources en la Guía para desarrolladores de AWS IoT.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`test-authorization`

En el siguiente ejemplo de código, se muestra cómo utilizar `test-authorization`.

AWS CLI

Para probar sus políticas de AWS IoT

En el siguiente ejemplo de `test-authorization`, se prueban las políticas de AWS IoT asociadas a la entidad principal especificada.

```
aws iot test-authorization \
    --auth-infos actionType=CONNECT,resources=arn:aws:iot:us-
east-1:123456789012:client/client1 \
    --principal arn:aws:iot:us-west-2:123456789012:cert/
aab1068f7f43ac3e3cae4b3a8aa3f308d2a750e6350507962e32c1eb465d9775
```

Salida:

```
{
    "authResults": [
        {
            "authInfo": {
                "actionType": "CONNECT",
```

```
                "resources": [
                    "arn:aws:iot:us-east-1:123456789012:client/client1"
                ]
            },
            "allowed": {
                "policies": [
                    {
                        "policyName": "TestPolicyAllowed",
                        "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/
TestPolicyAllowed"
                    }
                ]
            },
            "denied": {
                "implicitDeny": {
                    "policies": [
                        {
                            "policyName": "TestPolicyDenied",
                            "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/
TestPolicyDenied"
                        }
                    ]
                },
                "explicitDeny": {
                    "policies": [
                        {
                            "policyName": "TestPolicyExplicitDenied",
                            "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/
TestPolicyExplicitDenied"
                        }
                    ]
                }
            },
            "authDecision": "IMPLICIT_DENY",
            "missingContextValues": []
        }
    ]
}
```

Para obtener más información, consulte TestAuthorization en la Referencia de la API de AWS IoT.

- Para ver detalles de la API, consulte TestAuthorization en la Referencia de comandos de la AWS CLI.

`test-invoke-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `test-invoke-authorizer`.

AWS CLI

Para probar el autorizador personalizado

En el siguiente ejemplo de `test-invoke-authorizer`, se prueba el autorizador personalizado.

```
aws iot test-invoke-authorizer \
    --authorizer-name IoTAuthorizer \
    --token allow \
    --token-signature "mE0GvaHqy9nER/
FdgtJX5lXYEJ3b3vE7t1gEszc0TKGgLKWXTnPkb2AbKnOAZ8lGyoN5dVtWDWVmr25m7+
+zjbYIMk2TBvyGXhOmvKFBPkdgyA43KL6SiZy0cTqlPMcQDsP7VX2rXr7CTowCxSNKphGXdQe0/
I5dQ+JO6KUaHwCmupt0/MejKtaNwiia064j6wprOAUwG5S1IYFuRd0X
+wfo8pb0DubAIX1Ua705kuhRUcTx4SxUShEYKmN4IDEvLB6FsIr0B2wvB7y4iPmcajxzGl02ExvyCUNctCV9dYlRRGJj
```

Salida:

```
{
    "isAuthenticated": true,
    "principalId": "principalId",
    "policyDocuments": [
        "{"Version":"2012-10-17",       "Statement":
[{"Action":"iot:Publish","Effect":"Allow","Resource":"arn:aws:iot:us-
west-2:123456789012:topic/customauthtesting"}]}"
    ],
    "refreshAfterInSeconds": 600,
    "disconnectAfterInSeconds": 3600
}
```

Para obtener más información, consulte TestInvokeAuthorizer en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte TestInvokeAuthorizer en la Referencia de comandos de la AWS CLI.

`transfer-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `transfer-certificate`.

AWS CLI

Para transferir un certificado de dispositivo a otra cuenta de AWS

En el siguiente ejemplo de `transfer-certificate`, se transfiere un certificado de dispositivo transferido a otra cuenta de AWS. El certificado y la cuenta de AWS se identifican mediante un ID.

```
aws iot transfer-certificate \
    --certificate-
id 488b6a7f2acdeb00a77384e63c4e40b18b1b3caaae57b7272ba44c45e3448142 \
    --target-aws-account 030714055129
```

Salida:

```
{
    "transferredCertificateArn": "arn:aws:iot:us-
west-2:030714055129:cert/488b6a7f2acdeb00a77384e63c4e40b18b1b3caaae57b7272ba44c45e3448142"
}
```

Para obtener más información, consulte Transfer a certificate to another account en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte TransferCertificate en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar una clave de etiqueta de un recurso

En el siguiente ejemplo de `untag-resource`, se elimina la etiqueta `MyTag` y su valor del grupo de objetos `LightBulbs`.

```
command
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging Your AWS Resources en la Guía para desarrolladores de AWS IoT.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-account-audit-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-account-audit-configuration`.

AWS CLI

Ejemplo 1: activación de las notificaciones de Amazon SNS para las notificaciones de auditoría

En el siguiente ejemplo de `update-account-audit-configuration`, se habilitan las notificaciones de Amazon SNS para las notificaciones de auditoría de AWS IoT Device Defender, especificando un destino y el rol utilizado para escribir en ese destino.

```
aws iot update-account-audit-configuration \
    --audit-notification-target-configurations "SNS={targetArn=\"arn:aws:sns:us-west-2:123456789012:ddaudits\",roleArn=\"arn:aws:iam::123456789012:role/service-role/AWSIoTDeviceDefenderAudit\",enabled=true}"
```

Este comando no genera ninguna salida.

Ejemplo 2: activación de una comprobación de auditoría

En el siguiente ejemplo de `update-account-audit-configuration`, se activa la comprobación de auditoría de AWS IoT Device Defender denominada `AUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK`. No puede deshabilitar una comprobación de auditoría si forma parte de `targetCheckNames` para una o más auditorías programadas para la cuenta de AWS.

```
aws iot update-account-audit-configuration \
    --audit-check-configurations
 "{\"AUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK\":{\"enabled\":true}}"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Comandos de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener detalles sobre la API, consulte UpdateAccountAuditConfiguration en la Referencia de comandos de la AWS CLI.

`update-audit-suppression`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-audit-suppression`.

AWS CLI

Para actualizar la supresión de un resultado de auditoría

En el siguiente ejemplo de `update-audit-suppression`, se actualiza la fecha de caducidad de la supresión de un resultado de auditoría al 21 de septiembre de 2020.

```
aws iot update-audit-suppression \
    --check-name DEVICE_CERTIFICATE_EXPIRING_CHECK \
    --resource-identifier deviceCertificateId=c7691e<shortened> \
    --no-suppress-indefinitely \
    --expiration-date 2020-09-21
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Supresiones de resultados de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte UpdateAuditSuppression en la Referencia de comandos de la AWS CLI.

`update-authorizer`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-authorizer`.

AWS CLI

Para actualizar un autorizador personalizado

En el siguiente ejemplo de `update-authorizer`, el estado de `CustomAuthorizer2` cambia a `INACTIVE`.

```
aws iot update-authorizer \
    --authorizer-name CustomAuthorizer2 \
    --status INACTIVE
```

Salida:

```
{
    "authorizerName": "CustomAuthorizer2",
    "authorizerArn": "arn:aws:iot:us-west-2:123456789012:authorizer/
CustomAuthorizer2"
}
```

Para obtener más información, consulte UpdateAuthorizer en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte UpdateAuthorizer en la Referencia de comandos de la AWS CLI.

`update-billing-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-billing-group`.

AWS CLI

Para actualizar información acerca de un grupo de facturación

En el siguiente ejemplo de `update-billing-group`, se actualiza la descripción del grupo de facturación especificado.

```
aws iot update-billing-group \
    --billing-group-name GroupOne \
    --billing-group-properties "billingGroupDescription=\"Primary bulb billing group
\""
```

Salida:

```
{
    "version": 2
}
```

Para obtener más información, consulte Billing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información acerca de la API, consulte UpdateBillingGroup en la Referencia de comandos de la AWS CLI.

`update-ca-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-ca-certificate`.

AWS CLI

Para actualizar el certificado de una entidad de certificación (CA)

En el siguiente ejemplo de `update-ca-certificate`, se establece el estado ACTIVE para el certificado de CA especificado.

```
aws iot update-ca-certificate \
    --certificate-
id f4efed62c0142f16af278166f61962501165c4f05362952074264600 58cd1467 \
    --new-status ACTIVE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte UpdateCACertificate en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte UpdateCaCertificate en la Referencia de comandos de la AWS CLI.

`update-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-certificate`.

AWS CLI

Para actualizar el certificado de un dispositivo

En el siguiente ejemplo de `update-certificate`, se establece el estado INACTIVE para el certificado de dispositivo especificado.

```
aws iot update-certificate \
```

```
    --certificate-
id d1eb269fb55a628552143c8f96eb3c258fcd5331ea113e766ba0c82bf225f0be \
    --new-status INACTIVE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte UpdateCertificate en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte UpdateCertificate en la Referencia de comandos de la AWS CLI.

`update-custom-metric`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-custom-metric`.

AWS CLI

Para actualizar una métrica personalizada

En el siguiente ejemplo de `update-custom-metric`, se actualiza una métrica personalizada para que tenga un nuevo `display-name`.

```
aws iot update-custom-metric \
    --metric-name batteryPercentage \
    --display-name 'remaining battery percentage on device' \
    --region us-east-1
```

Salida:

```
{
    "metricName": "batteryPercentage",
    "metricArn": "arn:aws:iot:us-east-1:1234564789012:custommetric/
batteryPercentage",
    "metricType": "number",
    "displayName": "remaining battery percentage on device",
    "creationDate": "2020-11-17T23:01:35.110000-08:00",
    "lastModifiedDate": "2020-11-17T23:02:12.879000-08:00"
}
```

Para obtener más información, consulte Métricas personalizadas en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información acerca de la API, consulte UpdateCustomMetric en la Referencia de comandos de la AWS CLI.

`update-dimension`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-dimension`.

AWS CLI

Para actualizar una dimensión

En el siguiente ejemplo de `update-dimension`, se actualiza una dimensión.

```
aws iot update-dimension \
    --name TopicFilterForAuthMessages \
    --string-values device/${iot:ClientId}/auth
```

Salida:

```
{
    "name": "TopicFilterForAuthMessages",
    "lastModifiedDate": 1585866222.317,
    "stringValues": [
        "device/${iot:ClientId}/auth"
    ],
    "creationDate": 1585854500.474,
    "type": "TOPIC_FILTER",
    "arn": "arn:aws:iot:us-west-2:1234564789012:dimension/
TopicFilterForAuthMessages"
}
```

Para obtener más información, consulte Scoping metrics in security profiles using dimensions en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte UpdateDimension en la Referencia de la API de la AWS CLI.

`update-domain-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-domain-configuration`.

AWS CLI

Para actualizar una configuración de dominio

En el siguiente ejemplo de `update-domain-configuration`, se desactiva la configuración de dominios especificada.

```
aws iot update-domain-configuration \
    --domain-configuration-name "additionalDataDomain" \
    --domain-configuration-status "DISABLED"
```

Salida:

```
{
    "domainConfigurationName": "additionalDataDomain",
    "domainConfigurationArn": "arn:aws:iot:us-
west-2:123456789012:domainconfiguration/additionalDataDomain/dikMh"
}
```

Para obtener más información, consulte Configurable Endpoints en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte UpdateDomainConfiguration en la Referencia de comandos de la AWS CLI.

update-dynamic-thing-group

En el siguiente ejemplo de código, se muestra cómo utilizar `update-dynamic-thing-group`.

AWS CLI

Para actualizar un grupo de objetos dinámico

En el siguiente ejemplo de `update-dynamic-thing-group`, se actualiza el grupo de objetos dinámico especificado. Proporciona una descripción y actualiza la cadena de consulta para cambiar los criterios de pertenencia al grupo.

```
aws iot update-dynamic-thing-group \
    --thing-group-name "RoomTooWarm"
    --thing-group-properties "thingGroupDescription=\"This thing group contains
 rooms warmer than 65F.\"" \
```

```
    --query-string "attributes.temperature>65"
```

Salida:

```
{
    "version": 2
}
```

Para obtener más información, consulte Dynamic Thing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte UpdateDynamicThingGroup en la Referencia de comandos de la AWS CLI.

`update-event-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-event-configurations`.

AWS CLI

Para mostrar qué tipos de eventos se publican

En el siguiente ejemplo de `update-event-configurations`, se actualiza la configuración para habilitar los mensajes cuando se agrega, actualiza o elimina el certificado de CA.

```
aws iot update-event-configurations \
    --event-configurations "{\"CA_CERTIFICATE\":{\"Enabled\":true}}"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Event Messages en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte UpdateEventConfigurations en la Referencia de comandos de la AWS CLI.

`update-indexing-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-indexing-configuration`.

AWS CLI

Para activar la indexación de objetos

En el siguiente ejemplo de `update-indexing-configuration` se permite que la indexación de objetos admita la búsqueda de datos de registro, datos de sombra y el estado de conectividad de los objetos mediante el índice AWS_Things.

```
aws iot update-indexing-configuration
    --thing-indexing-
configuration thingIndexingMode=REGISTRY_AND_SHADOW,thingConnectivityIndexingMode=STATUS
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing Thing Indexing en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte UpdateIndexingConfiguration en la Referencia de comandos de la AWS CLI.

update-job

En el siguiente ejemplo de código, se muestra cómo utilizar `update-job`.

AWS CLI

Para obtener el estado detallado de un trabajo

En el siguiente ejemplo de `update-job`, se obtiene el estado detallado del trabajo cuyo ID es `example-job-01`.

```
aws iot describe-job \
    --job-id "example-job-01"
```

Salida:

```
{
    "job": {
        "jobArn": "arn:aws:iot:us-west-2:123456789012:job/example-job-01",
        "jobId": "example-job-01",
        "targetSelection": "SNAPSHOT",
        "status": "IN_PROGRESS",
```

```
        "targets": [
            "arn:aws:iot:us-west-2:123456789012:thing/MyRaspberryPi"
        ],
        "description": "example job test",
        "presignedUrlConfig": {},
        "jobExecutionsRolloutConfig": {},
        "createdAt": 1560787022.733,
        "lastUpdatedAt": 1560787026.294,
        "jobProcessDetails": {
            "numberOfCanceledThings": 0,
            "numberOfSucceededThings": 0,
            "numberOfFailedThings": 0,
            "numberOfRejectedThings": 0,
            "numberOfQueuedThings": 1,
            "numberOfInProgressThings": 0,
            "numberOfRemovedThings": 0,
            "numberOfTimedOutThings": 0
        },
        "timeoutConfig": {}
    }
}
```

Para obtener más información, consulte Creating and Managing Jobs (CLI) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte UpdateJob en la Referencia de comandos de la AWS CLI.

`update-mitigation-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-mitigation-action`.

AWS CLI

Para actualizar una acción de mitigación

En el siguiente ejemplo de `update-mitigation-action`, se actualiza la acción de mitigación denominada `AddThingsToQuarantineGroupAction` especificada, se cambia el nombre del grupo de objetos y se establece `overrideDynamicGroups` en `false`. Para verificar los cambios, use el comando `describe-mitigation-action`.

```
aws iot update-mitigation-action \
```

```
    --cli-input-json "{ \"actionName\": \"AddThingsToQuarantineGroupAction\",
 \"actionParams\": { \"addThingsToThingGroupParams\": {\"thingGroupNames\":
[\"QuarantineGroup2\"],\"overrideDynamicGroups\": false}}}"
```

Salida:

```
{
    "actionArn": "arn:aws:iot:us-west-2:123456789012:mitigationaction/
AddThingsToQuarantineGroupAction",
    "actionId": "2fd2726d-98e1-4abf-b10f-09465ccd6bfa"
}
```

Para obtener más información, consulte UpdateMitigationAction (Comandos de acciones de mitigación) en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte UpdateMitigationAction en la Referencia de comandos de la AWS CLI.

`update-provisioning-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-provisioning-template`.

AWS CLI

Para actualizar una plantilla de aprovisionamiento

En el siguiente ejemplo de `update-provisioning-template`, se modifica el ARN de la descripción y el rol de la plantilla de aprovisionamiento especificada y se habilita la plantilla.

```
aws iot update-provisioning-template \
    --template-name widget-template \
    --enabled \
    --description "An updated provisioning template for widgets" \
    --provisioning-role-arn arn:aws:iam::504350838278:role/Provision_role
```

Este comando no genera ninguna salida.

Para obtener más información, consulte AWS IoT Secure Tunneling en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte UpdateProvisioningTemplate en la Referencia de comandos de la AWS CLI.

update-role-alias

En el siguiente ejemplo de código, se muestra cómo utilizar `update-role-alias`.

AWS CLI

Para actualizar un alias de rol

En el siguiente ejemplo de `update-role-alias`, se actualiza el alias de rol de `LightBulbRole`.

```
aws iot update-role-alias \
    --role-alias LightBulbRole \
    --role-arn arn:aws:iam::123456789012:role/lightbulbrole-001
```

Salida:

```
{
    "roleAlias": "LightBulbRole",
    "roleAliasArn": "arn:aws:iot:us-west-2:123456789012:rolealias/LightBulbRole"
}
```

Para obtener más información, consulte UpdateRoleAlias en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte UpdateRoleAlias en la Referencia de la API de la AWS CLI.

update-scheduled-audit

En el siguiente ejemplo de código, se muestra cómo utilizar `update-scheduled-audit`.

AWS CLI

Para actualizar una definición de auditoría programada

En el siguiente ejemplo de `update-scheduled-audit`, se cambian los nombres de las comprobaciones de destino para una auditoría programada de AWS IoT Device Defender.

```
aws iot update-scheduled-audit \
    --scheduled-audit-name WednesdayCertCheck \
    --target-check-
names CA_CERTIFICATE_EXPIRING_CHECK DEVICE_CERTIFICATE_EXPIRING_CHECK REVOKED_CA_CERTIFICATE
```

Salida:

```
{
    "scheduledAuditArn": "arn:aws:iot:us-west-2:123456789012:scheduledaudit/
WednesdayCertCheck"
}
```

Para obtener más información, consulte Comandos de auditoría en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte UpdateScheduledAudit en la Referencia de comandos de AWS CLI.

`update-security-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-security-profile`.

AWS CLI

Para modificar un perfil de seguridad

En el siguiente ejemplo de `update-security-profile`, se actualiza la descripción y los comportamientos de un perfil de seguridad de AWS IoT Device Defender.

```
aws iot update-security-profile \
    --security-profile-name PossibleIssue \
    --security-profile-description "Check to see if authorization fails 12 times in
 5 minutes or if cellular bandwidth exceeds 128"  \
    --behaviors "[{\"name\":\"CellularBandwidth\",\"metric\":\"aws:message-byte-size
\",\"criteria\":{\"comparisonOperator\":\"greater-than\",\"value\":{\"count\":128},
\"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1}},{\"name
\":\"Authorization\",\"metric\":\"aws:num-authorization-failures\",\"criteria\":
{\"comparisonOperator\":\"less-than\",\"value\":{\"count\":12},\"durationSeconds
\":300,\"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1}}]"
```

Salida:

```
{
    "securityProfileName": "PossibleIssue",
    "securityProfileArn": "arn:aws:iot:us-west-2:123456789012:securityprofile/
PossibleIssue",
```

```
    "securityProfileDescription": "check to see if authorization fails 12 times in 5
 minutes or if cellular bandwidth exceeds 128",
    "behaviors": [
        {
            "name": "CellularBandwidth",
            "metric": "aws:message-byte-size",
            "criteria": {
                "comparisonOperator": "greater-than",
                "value": {
                    "count": 128
                },
                "consecutiveDatapointsToAlarm": 1,
                "consecutiveDatapointsToClear": 1
            }
        },
        {
            "name": "Authorization",
            "metric": "aws:num-authorization-failures",
            "criteria": {
                "comparisonOperator": "less-than",
                "value": {
                    "count": 12
                },
                "durationSeconds": 300,
                "consecutiveDatapointsToAlarm": 1,
                "consecutiveDatapointsToClear": 1
            }
        }
    ],
    "version": 2,
    "creationDate": 1560278102.528,
    "lastModifiedDate": 1560352711.207
}
```

Para obtener más información, consulte Comandos de detección en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte UpdateSecurityProfile en la Referencia de comandos de la AWS CLI.

`update-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-stream`.

AWS CLI

Para actualizar un flujo

En el siguiente ejemplo de `update-stream`, se actualiza un flujo existente. La versión del flujo aumentará en uno.

```
aws iot update-stream \
    --cli-input-json file://update-stream.json
```

Contenido de `update-stream.json`:

```
{
    "streamId": "stream12345",
    "description": "This stream is used for Amazon FreeRTOS OTA Update 12345.",
    "files": [
        {
            "fileId": 123,
            "s3Location": {
                "bucket":"codesign-ota-bucket",
                "key":"48c67f3c-63bb-4f92-a98a-4ee0fbc2bef6"
            }
        }
    ]
    "roleArn": "arn:aws:iam:us-west-2:123456789012:role/service-role/
my_ota_stream_role"
}
```

Salida:

```
{
    "streamId": "stream12345",
    "streamArn": "arn:aws:iot:us-west-2:123456789012:stream/stream12345",
    "description": "This stream is used for Amazon FreeRTOS OTA Update 12345.",
    "streamVersion": 2
}
```

Para obtener más información, consulte UpdateStream en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte UpdateStream en la Referencia de comandos de la AWS CLI.

update-thing-group

En el siguiente ejemplo de código, se muestra cómo utilizar `update-thing-group`.

AWS CLI

Para actualizar la definición de un grupo de objetos

En el siguiente ejemplo de `update-thing-group`, se actualiza la definición del grupo de objetos especificado y se cambian la descripción y dos atributos.

```
aws iot update-thing-group \
    --thing-group-name HalogenBulbs \
    --thing-group-properties "thingGroupDescription=\"Halogen bulb group\",
 attributePayload={attributes={Manufacturer=AnyCompany,wattage=60}}"
```

Salida:

```
{
    "version": 2
}
```

Para obtener más información, consulte Thing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte UpdateThingGroup en la Referencia de comandos de la AWS CLI.

update-thing-groups-for-thing

En el siguiente ejemplo de código, se muestra cómo utilizar `update-thing-groups-for-thing`.

AWS CLI

Para modificar los grupos a los que pertenece un objeto

En el siguiente ejemplo de `update-thing-groups-for-thing`, se elimina el objeto denominado `MyLightBulb` del grupo denominado `DeadBulbs` y, al mismo tiempo, se añade al grupo denominado `replaceableItems`.

```
aws iot update-thing-groups-for-thing \
```

```
    --thing-name MyLightBulb \
    --thing-groups-to-add "replaceableItems" \
    --thing-groups-to-remove "DeadBulbs"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Thing Groups en la Guía para desarrolladores de AWS IoT.

- Para obtener detalles sobre la API, consulte UpdateThingGroupsForThing en la Referencia de comandos de la AWS CLI.

`update-thing`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-thing`.

AWS CLI

Para asociar un objeto con un tipo de objeto

En el siguiente ejemplo de `update-thing` se asocia un objeto del registro de AWS IoT con un tipo de objeto. Al realizar la asociación, se proporcionan valores para los atributos definidos por el tipo de objeto.

```
aws iot update-thing \
    --thing-name "MyOtherLightBulb" \
    --thing-type-name "LightBulb" \
    --attribute-payload "{"attributes": {"wattage":"75", "model":"123"}}"
```

Este comando no proporciona ningún resultado. Para ver el resultado, use el comando `describe-thing`.

Para obtener más información, consulte Thing Types en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte UpdateThing en la Referencia de comandos de la AWS CLI.

`update-topic-rule-destination`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-topic-rule-destination`.

AWS CLI

Ejemplo 1: activación del destino de una regla de tema

En el siguiente ejemplo de `update-topic-rule-destination`, se habilita el tráfico a un destino de regla de tema.

```
aws iot update-topic-rule-destination \
    --arn "arn:aws:iot:us-west-2:123456789012:ruledestination/http/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --status ENABLED
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Enabling a topic rule destination en la Guía para desarrolladores de AWS IoT.

Ejemplo 2: desactivación del destino de una regla de tema

En el siguiente ejemplo de `update-topic-rule-destination`, se desactiva el tráfico hacia un destino de regla de tema.

```
aws iot update-topic-rule-destination \
    --arn "arn:aws:iot:us-west-2:123456789012:ruledestination/http/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --status DISABLED
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Disabling a topic rule destination en la Guía para desarrolladores de AWS IoT.

Ejemplo 3: envío de un nuevo mensaje de confirmación

En el siguiente ejemplo de `update-topic-rule-destination`, se envía un nuevo mensaje de confirmación para el destino de una regla de tema.

```
aws iot update-topic-rule-destination \
    --arn "arn:aws:iot:us-west-2:123456789012:ruledestination/http/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --status IN_PROGRESS
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Sending a new confirmation message en la Guía para desarrolladores de AWS IoT.

- Para obtener información acerca de la API, consulte UpdateTopicRuleDestination en la Referencia de comandos de la AWS CLI.

`validate-security-profile-behaviors`

En el siguiente ejemplo de código, se muestra cómo utilizar `validate-security-profile-behaviors`.

AWS CLI

Ejemplo 1: validación de los parámetros de comportamiento de un perfil de seguridad

En el siguiente ejemplo de `validate-security-profile-behaviors`, se valida un conjunto de comportamientos correcto y bien formado para un perfil de seguridad de AWS IoT Device Defender.

```
aws iot validate-security-profile-behaviors \
    --behaviors "[{\"name\":\"CellularBandwidth\",\"metric\":\"aws:message-byte-size
\",\"criteria\":{\"comparisonOperator\":\"greater-than\",\"value\":{\"count\":128},
\"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1}},{\"name
\":\"Authorization\",\"metric\":\"aws:num-authorization-failures\",\"criteria\":
{\"comparisonOperator\":\"greater-than\",\"value\":{\"count\":12},\"durationSeconds
\":300,\"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1}}]"
```

Salida:

```
{
    "valid": true,
    "validationErrors": []
}
```

Ejemplo 2: validación de los parámetros de comportamiento incorrectos de un perfil de seguridad

En el siguiente ejemplo de `validate-security-profile-behaviors`, se valida un conjunto de comportamientos que contiene un error de un perfil de seguridad de AWS IoT Device Defender.

```
aws iot validate-security-profile-behaviors \
    --behaviors "[{\"name\":\"CellularBandwidth\",\"metric\":\"aws:message-byte-size
\",\"criteria\":{\"comparisonOperator\":\"greater-than\",\"value\":{\"count\":128},
\"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1}},{\"name
\":\"Authorization\",\"metric\":\"aws:num-authorization-failures\",\"criteria\":
{\"comparisonOperator\":\"greater-than\",\"value\":{\"count\":12},\"durationSeconds
\":300,\"consecutiveDatapointsToAlarm\":100000,\"consecutiveDatapointsToClear
\":1}}]"
```

Salida:

```
{
    "valid": false,
    "validationErrors": [
        {
            "errorMessage": "Behavior Authorization is malformed.
 consecutiveDatapointsToAlarm 100000 should be in range[1,10]"
        }
    ]
}
```

Para obtener más información, consulte Comandos de detección en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ValidateSecurityProfileBehaviors en la Referencia de comandos de la AWS CLI.

AWS IoT Analytics Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS IoT Analytics.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`batch-put-message`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-put-message`.

AWS CLI

Para enviar un mensaje a un canal

En el siguiente ejemplo de `batch-put-message`, se envía un mensaje al canal especificado.

```
aws iotanalytics batch-put-message \
    --cli-binary-format raw-in-base64-out \
    --cli-input-json file://batch-put-message.json
```

Contenido de `batch-put-message.json`:

```
{
    "channelName": "mychannel",
    "messages": [
        {
            "messageId": "0001",
            "payload": "eyAidGVtcGVyYXR1cmUiOiAyMCB9"
        }
    ]
}
```

Salida:

```
{
    "batchPutMessageErrorEntries": []
}
```

Para obtener más información, consulte BatchPutMessage en la Referencia de la API de AWS IoT Analytics.

- Para obtener más información sobre la API, consulte BatchPutMessage en la Referencia de comandos de la AWS CLI.

`cancel-pipeline-reprocessing`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-pipeline-reprocessing`.

AWS CLI

Para cancela el reprocesamiento de los datos a través de una canalización

En el siguiente ejemplo de `cancel-pipeline-reprocessing`, se cancela el reprocesamiento de datos a través de la canalización especificada.

```
aws iotanalytics cancel-pipeline-reprocessing \
    --pipeline-name mypipeline \
    --reprocessing-id "6ad2764f-fb13-4de3-b101-4e74af03b043"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte CancelPipelineReprocessing en la Referencia de la API de AWS IoT Analytics.

- Para obtener más información sobre la API, consulte CancelPipelineReprocessing en la Referencia de comandos de la AWS CLI.

`create-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-channel`.

AWS CLI

Para crear un canal

En el siguiente ejemplo de `create-channel`, se crea un canal con la configuración especificada. Un canal recopila datos desde un tema MQTT y archiva los mensajes sin procesar antes de publicar los datos en una canalización.

```
aws iotanalytics create-channel \
    --cli-input-json file://create-channel.json
```

Contenido de `create-channel.json`:

```
{
```

```
    "channelName": "mychannel",
    "retentionPeriod": {
        "unlimited": true
    },
    "tags": [
        {
            "key": "Environment",
            "value": "Production"
        }
    ]
}
```

Salida:

```
{
    "channelArn": "arn:aws:iotanalytics:us-west-2:123456789012:channel/mychannel",
    "channelName": "mychannel",
    "retentionPeriod": {
        "unlimited": true
    }
}
```

Para obtener más información, consulte CreateChannel en la Guía de referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte CreateChannel en la Referencia de comandos de la AWS CLI.

`create-dataset-content`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-dataset-content`.

AWS CLI

Para crear el contenido de un conjunto de datos

En el siguiente ejemplo de `create-dataset-content`, se crea el contenido del conjunto de datos especificado aplicando una `queryAction` (una consulta SQL) o una `containerAction` (ejecutando una aplicación contenerizada).

```
aws iotanalytics create-dataset-content \
```

```
    --dataset-name mydataset
```

Salida:

```
{
    "versionId": "d494b416-9850-4670-b885-ca22f1e89d62"
}
```

Para obtener más información, consulte CreateDatasetContent en la Guía de referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte CreateDatasetContent en la Referencia de comandos de la AWS CLI.

`create-dataset`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-dataset`.

AWS CLI

Para crear un conjunto de datos

En el siguiente ejemplo de `create-dataset`, se crea un conjunto de datos. Un conjunto de datos almacena datos recuperados de un almacén de datos aplicando una `queryAction` (una consulta SQL) o una `containerAction` (ejecución de una aplicación en contenedores). Esta operación crea el esqueleto de un conjunto de datos. El conjunto de datos se puede rellenar manualmente llamando a `CreateDatasetContent` o automáticamente de acuerdo con el `trigger` especificado.

```
aws iotanalytics create-dataset \
    --cli-input-json file://create-dataset.json
```

Contenido de `create-dataset.json`:

```
{
    "datasetName": "mydataset",
    "actions": [
        {
            "actionName": "myDatasetAction",
            "queryAction": {
                "sqlQuery": "SELECT * FROM mydatastore"
```

```
            }
        }
    ],
    "retentionPeriod": {
        "unlimited": true
    },
    "tags": [
        {
            "key": "Environment",
            "value": "Production"
        }
    ]
}
```

Salida:

```
{
    "datasetName": "mydataset",
    "retentionPeriod": {
        "unlimited": true
    },
    "datasetArn": "arn:aws:iotanalytics:us-west-2:123456789012:dataset/mydataset"
}
```

Para obtener más información, consulte CreateDataset en la Guía de referencia de la API de AWS IoT Analytics.

- Para obtener detalles sobre la API, consulte CreateDataset en la Referencia de comandos de la AWS CLI.

`create-datastore`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-datastore`.

AWS CLI

Cómo crear un almacén de datos

En el siguiente ejemplo de `create-datastore`, se crea un almacén de datos, que es un repositorio para mensajes.

```
aws iotanalytics create-datastore \
```

```
    --cli-input-json file://create-datastore.json
```

Contenido de `create-datastore.json`:

```
{
    "datastoreName": "mydatastore",
    "retentionPeriod": {
        "numberOfDays": 90
    },
    "tags": [
        {
            "key": "Environment",
            "value": "Production"
        }
    ]
}
```

Salida:

```
{
    "datastoreName": "mydatastore",
    "datastoreArn": "arn:aws:iotanalytics:us-west-2:123456789012:datastore/
mydatastore",
    "retentionPeriod": {
        "numberOfDays": 90,
        "unlimited": false
    }
}
```

Para obtener más información, consulte CreateDatastore en la Guía de referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte CreateDatastore en la Referencia de comandos de la AWS CLI.

`create-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-pipeline`.

AWS CLI

Para crear una canalización de IoT Analytics

En el siguiente ejemplo de `create-pipeline`, se crea una canalización. Una canalización consume mensajes de un canal y permite procesar los mensajes antes de guardarlos en un almacén de datos. Debe especificar un canal y una actividad del almacén de datos y, si lo desea, hasta 23 actividades adicionales en la matriz `pipelineActivities`.

```
aws iotanalytics create-pipeline \
    --cli-input-json file://create-pipeline.json
```

Contenido de `create-pipeline.json`:

```
{
    "pipelineName": "mypipeline",
    "pipelineActivities": [
        {
            "channel": {
                "name": "myChannelActivity",
                "channelName": "mychannel",
                "next": "myMathActivity"
            }
        },
        {
            "datastore": {
                "name": "myDatastoreActivity",
                "datastoreName": "mydatastore"
            }
        },
        {
            "math": {
                "name": "myMathActivity",
                "math": "((temp - 32) * 5.0) / 9.0",
                "attribute": "tempC",
                "next": "myDatastoreActivity"
            }
        }
    ],
    "tags": [
        {
            "key": "Environment",
            "value": "Beta"
        }
    ]
}
```

Salida:

```
{
    "pipelineArn": "arn:aws:iotanalytics:us-west-2:123456789012:pipeline/
mypipeline",
    "pipelineName": "mypipeline"
}
```

Para obtener más información, consulte CreatePipeline en la Referencia de la API de AWS IoT Analytics.

- Para obtener detalles sobre la API, consulte CreatePipeline en la Referencia de comandos de la AWS CLI.

`delete-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-channel`.

AWS CLI

Para eliminar un canal de IoT Analytics

En el siguiente ejemplo de `delete-channel`, se elimina el canal especificado.

```
aws iotanalytics delete-channel \
    --channel-name mychannel
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteChannel en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte DeleteChannel en la Referencia de comandos de la AWS CLI.

`delete-dataset-content`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-dataset-content`.

AWS CLI

Para eliminar el contenido del conjunto de datos

En el siguiente ejemplo de `delete-dataset-content`, se elimina el contenido del conjunto de datos especificado.

```
aws iotanalytics delete-dataset-content \
    --dataset-name mydataset
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteDatasetContent en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte DeleteDatasetContent en la Referencia de comandos de la AWS CLI.

`delete-dataset`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-dataset`.

AWS CLI

Para eliminar un conjunto de datos

En el siguiente ejemplo de `delete-dataset`, se elimina el conjunto de datos especificado. No es necesario eliminar el contenido del conjunto de datos antes de realizar esta operación.

```
aws iotanalytics delete-dataset \
    --dataset-name mydataset
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteDataset en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte DeleteDataset en la Referencia de comandos de AWS CLI.

`delete-datastore`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-datastore`.

AWS CLI

Cómo eliminar un almacén de datos

En el siguiente ejemplo de `delete-datastore`, se elimina el almacén de datos especificado.

```
aws iotanalytics delete-datastore \
    --datastore-name mydatastore
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteDatastore en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte DeleteDatastore en la Referencia de comandos de la AWS CLI.

`delete-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-pipeline`.

AWS CLI

Para eliminar una canalización

En el siguiente ejemplo de `delete-pipeline`, se elimina la canalización especificada.

```
aws iotanalytics delete-pipeline \
    --pipeline-name mypipeline
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeletePipeline en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte DeletePipeline en la Referencia de comandos de la AWS CLI.

`describe-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-channel`.

AWS CLI

Para recuperar información sobre un canal

En el siguiente ejemplo de `describe-channel`, se muestran los detalles, incluidas las estadísticas, del canal especificado.

```
aws iotanalytics describe-channel \
    --channel-name mychannel \
    --include-statistics
```

Salida:

```
{
    "statistics": {
        "size": {
            "estimatedSizeInBytes": 402.0,
            "estimatedOn": 1561504380.0
        }
    },
    "channel": {
        "status": "ACTIVE",
        "name": "mychannel",
        "lastUpdateTime": 1557860351.001,
        "creationTime": 1557860351.001,
        "retentionPeriod": {
            "unlimited": true
        },
        "arn": "arn:aws:iotanalytics:us-west-2:123456789012:channel/mychannel"
    }
}
```

Para obtener más información, consulte DescribeChannel en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte DescribeChannel en la Referencia de comandos de la AWS CLI.

`describe-dataset`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-dataset`.

AWS CLI

Para recuperar información sobre un conjunto de datos

En el siguiente ejemplo de `describe-dataset`, se muestran los detalles del conjunto de datos especificado.

```
aws iotanalytics describe-dataset \
    --dataset-name mydataset
```

Salida:

```
{
    "dataset": {
        "status": "ACTIVE",
        "contentDeliveryRules": [],
        "name": "mydataset",
        "lastUpdateTime": 1557859240.658,
        "triggers": [],
        "creationTime": 1557859240.658,
        "actions": [
            {
                "actionName": "query_32",
                "queryAction": {
                    "sqlQuery": "SELECT * FROM mydatastore",
                    "filters": []
                }
            }
        ],
        "retentionPeriod": {
            "numberOfDays": 90,
            "unlimited": false
        },
        "arn": "arn:aws:iotanalytics:us-west-2:123456789012:dataset/mydataset"
    }
}
```

Para obtener más información, consulte DescribeDataset en la Referencia de la API de AWS IoT Analytics.

- Para obtener detalles sobre la API, consulte DescribeDataset en la Referencia de comandos de la AWS CLI.

describe-datastore

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-datastore`.

AWS CLI

Para recuperar información sobre un almacén de datos

En el siguiente ejemplo de `describe-datastore`, se muestran los detalles, incluidas las estadísticas, del almacén de datos especificado.

```
aws iotanalytics describe-datastore \
    --datastore-name mydatastore \
    --include-statistics
```

Salida:

```
{
    "datastore": {
        "status": "ACTIVE",
        "name": "mydatastore",
        "lastUpdateTime": 1557858971.02,
        "creationTime": 1557858971.02,
        "retentionPeriod": {
            "unlimited": true
        },
        "arn": "arn:aws:iotanalytics:us-west-2:123456789012:datastore/mydatastore"
    },
    "statistics": {
        "size": {
            "estimatedSizeInBytes": 397.0,
            "estimatedOn": 1561592040.0
        }
    }
}
```

Para obtener más información, consulte DescribeDatastore en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte DescribeDatastore en la Referencia de comandos de la AWS CLI.

describe-logging-options

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-logging-options`.

AWS CLI

Para recuperar las opciones de registro actuales

En el siguiente ejemplo de `describe-logging-options`, se muestran las opciones de registro actuales de AWS IoT Analytics.

```
aws iotanalytics describe-logging-options
```

Este comando no genera ninguna salida. Salida:

```
{
    "loggingOptions": {
        "roleArn": "arn:aws:iam::123456789012:role/service-role/myIoTAnalyticsRole",
        "enabled": true,
        "level": "ERROR"
    }
}
```

Para obtener más información, consulte DescribeLoggingOptions en la Referencia de la API de AWS IoT Analytics.

- Para obtener más información sobre la API, consulte DescribeLoggingOptions en la Referencia de comandos de la AWS CLI.

describe-pipeline

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-pipeline`.

AWS CLI

Para recuperar información sobre una canalización

En el siguiente ejemplo de `describe-pipeline`, se muestran los detalles de la canalización especificada.

```
aws iotanalytics describe-pipeline \
    --pipeline-name mypipeline
```

Salida:

```
{
    "pipeline": {
        "activities": [
            {
                "channel": {
                    "channelName": "mychannel",
                    "name": "mychannel_28",
                    "next": "mydatastore_29"
                }
            },
            {
                "datastore": {
                    "datastoreName": "mydatastore",
                    "name": "mydatastore_29"
                }
            }
        ],
        "name": "mypipeline",
        "lastUpdateTime": 1561676362.515,
        "creationTime": 1557859124.432,
        "reprocessingSummaries": [
            {
                "status": "SUCCEEDED",
                "creationTime": 1561676362.189,
                "id": "6ad2764f-fb13-4de3-b101-4e74af03b043"
            }
        ],
        "arn": "arn:aws:iotanalytics:us-west-2:123456789012:pipeline/mypipeline"
    }
}
```

Para obtener más información, consulte DescribePipeline en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte DescribePipeline en la Referencia de comandos de la AWS CLI.

`get-dataset-content`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-dataset-content`.

AWS CLI

Para recuperar el contenido de un conjunto de datos

En el siguiente ejemplo de `get-dataset-content`, se recupera el contenido de un conjunto de datos como URI prefirmados.

```
aws iotanalytics get-dataset-content --dataset-name mydataset
```

Salida:

```
{
    "status": {
        "state": "SUCCEEDED"
    },
    "timestamp": 1557863215.995,
    "entries": [
        {
            "dataURI": "https://aws-radiant-
dataset-12345678-1234-1234-1234-123456789012.s3.us-west-2.amazonaws.com/
results/12345678-e8b3-46ba-b2dd-efe8d86cf385.csv?X-Amz-Security-Token=...-Amz-
Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20190628T173437Z&X-Amz-SignedHeaders=host&X-
Amz-Expires=7200&X-Amz-Credential=...F20190628%2Fus-west-2%2Fs3%2Faws4_request&X-
Amz-Signature=..."
        }
    ]
}
```

Para obtener más información, consulte GetDatasetContent en la guía.

- Para obtener información sobre la API, consulte GetDatasetContent en la Referencia de comandos de la AWS CLI.

`list-channels`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-channels`.

AWS CLI

Para recuperar una lista de canales

En el siguiente ejemplo de `list-channels`, se muestra información resumida de los canales disponibles.

```
aws iotanalytics list-channels
```

Salida:

```
{
    "channelSummaries": [
        {
            "status": "ACTIVE",
            "channelName": "mychannel",
            "creationTime": 1557860351.001,
            "lastUpdateTime": 1557860351.001
        }
    ]
}
```

Para obtener más información, consulte ListChannels en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte ListChannels en la Referencia de comandos de la AWS CLI.

`list-dataset-contents`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-dataset-contents`.

AWS CLI

Para enumerar información sobre el contenido del conjunto de datos

En el siguiente ejemplo de `list-dataset-contents`, se numera información sobre el contenido de los conjunto de datos que se ha creado.

```
aws iotanalytics list-dataset-contents \
    --dataset-name mydataset
```

Salida:

```
{
    "datasetContentSummaries": [
        {
```

```
            "status": {
                "state": "SUCCEEDED"
            },
            "scheduleTime": 1557863215.995,
            "version": "b10ea2a9-66c1-4d99-8d1f-518113b738d0",
            "creationTime": 1557863215.995
        }
    ]
}
```

Para obtener más información, consulte ListDatasetContents en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte ListDatasetContents en la Referencia de comandos de la AWS CLI.

`list-datasets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-datasets`.

AWS CLI

Para recuperar información sobre conjuntos de datos

En el siguiente ejemplo de `list-datasets`, se muestra un resumen de la información sobre los conjuntos de datos disponibles.

```
aws iotanalytics list-datasets
```

Salida:

```
{
    "datasetSummaries": [
        {
            "status": "ACTIVE",
            "datasetName": "mydataset",
            "lastUpdateTime": 1557859240.658,
            "triggers": [],
            "creationTime": 1557859240.658,
            "actions": [
                {
                    "actionName": "query_32",
```

```
                    "actionType": "QUERY"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte ListDatasets en la Referencia de la API de AWS IoT Analytics.

- Para obtener detalles sobre la API, consulte ListDatasets en la Referencia de comandos de la AWS CLI.

`list-datastores`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-datastores`.

AWS CLI

Para recuperar una lista de almacenes de datos

En el siguiente ejemplo de `list-datastores`, se muestra información resumida sobre los almacenes de datos disponibles.

```
aws iotanalytics list-datastores
```

Salida:

```
{
    "datastoreSummaries": [
        {
            "status": "ACTIVE",
            "datastoreName": "mydatastore",
            "creationTime": 1557858971.02,
            "lastUpdateTime": 1557858971.02
        }
    ]
}
```

Para obtener más información, consulte ListDatastores en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte ListDatastores en la Referencia de comandos de la AWS CLI.

`list-pipelines`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-pipelines`.

AWS CLI

Para recuperar una lista de canalizaciones

En el siguiente ejemplo de `list-pipelines`, se muestra una lista de las canalizaciones disponibles.

```
aws iotanalytics list-pipelines
```

Salida:

```
{
    "pipelineSummaries": [
        {
            "pipelineName": "mypipeline",
            "creationTime": 1557859124.432,
            "lastUpdateTime": 1557859124.432,
            "reprocessingSummaries": []
        }
    ]
}
```

Para obtener más información, consulte ListPipelines en la Referencia de la API de AWS IoT Analytics.

- Para obtener detalles sobre la API, consulte ListPipelines en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se muestran las etiquetas que ha asociado al recurso especificado.

```
aws iotanalytics list-tags-for-resource \
    --resource-arn "arn:aws:iotanalytics:us-west-2:123456789012:channel/mychannel"
```

Salida:

```
{
    "tags": [
        {
            "value": "bar",
            "key": "foo"
        }
    ]
}
```

Para obtener más información, consulte ListTagsForResource en la Referencia de la API de AWS IoT Analytics.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-logging-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-logging-options`.

AWS CLI

Para configurar o actualizar las opciones de registro

En el siguiente ejemplo de `put-logging-options`, se definen o actualizan las opciones de registro actuales de AWS IoT Analytics. Si actualiza el valor de cualquier campo `loggingOptions`, los cambios pueden tardar hasta un minuto en surtir efecto. Por otra parte, si cambia la política asociada al rol que ha especificado en el campo roleArn (por ejemplo, para corregir una política no válida), el cambio puede tardar hasta 5 minutos en surtir efecto.

```
aws iotanalytics put-logging-options \
    --cli-input-json file://put-logging-options.json
```

Contenido de `put-logging-options.json`:

```
{
    "loggingOptions": {
        "roleArn": "arn:aws:iam::123456789012:role/service-role/myIoTAnalyticsRole",
        "level": "ERROR",
        "enabled": true
    }
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte PutLoggingOptions en la Referencia de la API de AWS IoT Analytics.

- Para obtener detalles sobre la API, consulte PutLoggingOptions en la Referencia de comandos de la AWS CLI.

`run-pipeline-activity`

En el siguiente ejemplo de código, se muestra cómo utilizar `run-pipeline-activity`.

AWS CLI

Para simular una actividad de canalización

En el siguiente ejemplo de `run-pipeline-activity`, se simulan los resultados de la ejecución de una actividad de canalización en una carga útil de mensajes.

```
aws iotanalytics run-pipeline-activity \
    --pipeline-activity file://maths.json \
    --payloads file://payloads.json
```

Contenido de `maths.json`:

```
{
    "math": {
        "name": "MyMathActivity",
        "math": "((temp - 32) * 5.0) / 9.0",
        "attribute": "tempC"
    }
}
```

Contenido de `payloads.json`:

```
[
    "{\"humidity\": 52, \"temp\": 68 }",
    "{\"humidity\": 52, \"temp\": 32 }"
]
```

Salida:

```
{
    "logResult": "",
    "payloads": [
        "eyJodW1pZGl0eSI6NTIsInRlbXAiOjY4LCJ0ZW1wQyI6MjB9",
        "eyJodW1pZGl0eSI6NTIsInRlbXAiOjMyLCJ0ZW1wQyI6MH0="
    ]
}
```

Para obtener más información, consulte RunPipelineActivity en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte RunPipelineActivity en la Referencia de comandos de la AWS CLI.

`sample-channel-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `sample-channel-data`.

AWS CLI

Para recuperar mensajes de muestra de un canal

En el siguiente ejemplo de `sample-channel-data`, se recupera una muestra de mensajes del canal especificado ingeridos durante el período de tiempo especificado. Se pueden recuperar hasta diez mensajes.

```
aws iotanalytics sample-channel-data \
    --channel-name mychannel
```

Salida:

```
{
```

```
    "payloads": [
        "eyAidGVtcGVyYXR1cmUiOiAyMCB9",
        "eyAiZm9vIjogImJhciIgfQ=="
    ]
}
```

Para obtener más información, consulte SampleChannelData en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte SampleChannelData en la Referencia de comandos de la AWS CLI.

`start-pipeline-reprocessing`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-pipeline-reprocessing`.

AWS CLI

Para iniciar el reprocesamiento de la canalización

En el siguiente ejemplo de `start-pipeline-reprocessing`, se inicia el reprocesamiento de los datos de mensajes sin procesar a través de la canalización.

```
aws iotanalytics start-pipeline-reprocessing \
    --pipeline-name mypipeline
```

Salida:

```
{
    "reprocessingId": "6ad2764f-fb13-4de3-b101-4e74af03b043"
}
```

Para obtener más información, consulte StartPipelineReprocessing en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte StartPipelineReprocessing en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para agregar o modificar etiquetas en un recurso

En el siguiente ejemplo de `tag-resource`, se agregan o modifican las etiquetas asociadas al recurso especificado.

```
aws iotanalytics tag-resource \
    --resource-arn "arn:aws:iotanalytics:us-west-2:123456789012:channel/mychannel" \
    --tags "[{\"key\": \"Environment\", \"value\": \"Production\"}]"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte TagResource en la Referencia de la API de AWS IoT Analytics.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar etiquetas de un recurso

En el siguiente ejemplo de `untag-resource`, se eliminan las etiquetas con el nombre de clave especificado del recurso indicado.

```
aws iotanalytics untag-resource \
    --resource-arn "arn:aws:iotanalytics:us-west-2:123456789012:channel/mychannel" \
    --tag-keys "[\"Environment\"]"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte UntagResource <https://docs.aws.amazon.com/iotanalytics/latest/APIReference/API_UntagResource.html > en la Referencia de API de AWS IoT Analytics.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-channel

En el siguiente ejemplo de código, se muestra cómo utilizar `update-channel`.

AWS CLI

Para modificar un canal

En el siguiente ejemplo de `update-channel`, se modifican los ajustes del canal especificado.

```
aws iotanalytics update-channel \
    --cli-input-json file://update-channel.json
```

Contenido de `update-channel.json`:

```
{
    "channelName": "mychannel",
    "retentionPeriod": {
        "numberOfDays": 92
    }
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte UpdateChannel en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte UpdateChannel en la Referencia de comandos de la AWS CLI.

update-dataset

En el siguiente ejemplo de código, se muestra cómo utilizar `update-dataset`.

AWS CLI

Para actualizar un conjunto de datos

En el siguiente ejemplo de `update-dataset`, se modifica la configuración del conjunto de datos especificado.

```
aws iotanalytics update-dataset \
    --cli-input-json file://update-dataset.json
```

Contenido de `update-dataset.json`:

```
{
    "datasetName": "mydataset",
    "actions": [
        {
            "actionName": "myDatasetUpdateAction",
            "queryAction": {
                "sqlQuery": "SELECT * FROM mydatastore"
            }
        }
    ],
    "retentionPeriod": {
        "numberOfDays": 92
    }
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte UpdateDataset <https://docs.aws.amazon.com/iotanalytics/latest/APIReference/API_UpdateDataset.html > en la Referencia de API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte UpdateDataset en la Referencia de comandos de la AWS CLI.

update-datastore

En el siguiente ejemplo de código, se muestra cómo utilizar `update-datastore`.

AWS CLI

Para actualizar un almacén de datos

En el siguiente ejemplo de `update-datastore`, se modifica la configuración del almacén de datos especificado.

```
aws iotanalytics update-datastore \
```

```
    --cli-input-json file://update-datastore.json
```

Contenido de update-datastore.json:

```
{
    "datastoreName": "mydatastore",
    "retentionPeriod": {
        "numberOfDays": 93
    }
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte UpdateDatastore en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte UpdateDatastore en la Referencia de comandos de la AWS CLI.

`update-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-pipeline`.

AWS CLI

Para actualizar una canalización

En el siguiente ejemplo de `update-pipeline`, se modifica la configuración de la canalización especificada. Debe especificar un canal y una actividad del almacén de datos y, si lo desea, hasta 23 actividades adicionales en la matriz `pipelineActivities`.

```
aws iotanalytics update-pipeline \
    --cli-input-json file://update-pipeline.json
```

Contenido de update-pipeline.json:

```
{
    "pipelineName": "mypipeline",
    "pipelineActivities": [
        {
```

```
            "channel": {
                "name": "myChannelActivity",
                "channelName": "mychannel",
                "next": "myMathActivity"
            }
        },
        {
            "datastore": {
                "name": "myDatastoreActivity",
                "datastoreName": "mydatastore"
            }
        },
        {
            "math": {
                "name": "myMathActivity",
                "math": "(((temp - 32) * 5.0) / 9.0) + 273.15",
                "attribute": "tempK",
                "next": "myDatastoreActivity"
            }
        }
    ]
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte UpdatePipeline en la Referencia de la API de AWS IoT Analytics.

- Para obtener información sobre la API, consulte UpdatePipeline en la Referencia de comandos de la AWS CLI.

Ejemplos de Device Advisor que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Device Farm.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-suite-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-suite-definition`.

AWS CLI

Ejemplo 1: creación de un conjunto de pruebas de IoT Device Advisor

En el siguiente ejemplo de `create-suite-definition`, se crea un conjunto de pruebas de Device Advisor en el AWS IoT con la configuración de definición de conjunto especificada.

```
aws iotdeviceadvisor create-suite-definition \
    --suite-definition-configuration '{ \
        "suiteDefinitionName": "TestSuiteName", \
        "devices": [{"thingArn":"arn:aws:iot:us-east-1:123456789012:thing/
MyIotThing"}], \
        "intendedForQualification": false, \
        "rootGroup": "{\"configuration\":{},\"tests\":[{\"name\":\"MQTT Connect\",
\"configuration\":{\"EXECUTION_TIMEOUT\":120},\"tests\":[{\"name\":\"MQTT_Connect\",
\"configuration\":{},\"test\":{\"id\":\"MQTT_Connect\",\"testCase\":null,\"version
\":\"0.0.0\"}}]}]}", \
        "devicePermissionRoleArn": "arn:aws:iam::123456789012:role/Myrole"}'
```

Salida:

```
{
    "suiteDefinitionId": "0jtsgio7yenu",
    "suiteDefinitionArn": "arn:aws:iotdeviceadvisor:us-
east-1:123456789012:suitedefinition/0jtsgio7yenu",
    "suiteDefinitionName": "TestSuiteName",
    "createdAt": "2022-12-02T11:38:13.263000-05:00"
}
```

Para obtener más información, consulte Create a test suite definition en la Guía para desarrolladores de AWS IoT Core.

Ejemplo 2: creación de un conjunto de pruebas de IoT Device Advisor

En el siguiente ejemplo de `create-suite-definition`, se crea un conjunto de pruebas de cualificación de Device Advisor con la versión más reciente de AWS IoT con la configuración de definición de conjunto especificada.

```
aws iotdeviceadvisor create-suite-definition \
    --suite-definition-configuration '{ \
        "suiteDefinitionName": "TestSuiteName", \
        "devices": [{"thingArn":"arn:aws:iot:us-east-1:123456789012:thing/
MyIotThing"}], \
        "intendedForQualification": true, \
        "rootGroup": "", \
        "devicePermissionRoleArn": "arn:aws:iam::123456789012:role/Myrole"}'
```

Salida:

```
{
    "suiteDefinitionId": "txgsuolk2myj",
    "suiteDefinitionArn": "arn:aws:iotdeviceadvisor:us-
east-1:123456789012:suitedefinition/txgsuolk2myj",
    "suiteDefinitionName": "TestSuiteName",
    "createdAt": "2022-12-02T11:38:13.263000-05:00"
}
```

Para obtener más información, consulte Create a test suite definition en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte CreateSuiteDefinition en la Referencia de comandos de la AWS CLI.

`delete-suite-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-suite-definition`.

AWS CLI

Para eliminar el conjunto de pruebas de IoT Device Advisor

En el siguiente ejemplo de `delete-suite-definition`, se elimina el conjunto de pruebas de Device Advisor con el ID de definición de conjunto especificado.

```
aws iotdeviceadvisor delete-suite-definition \
    --suite-definition-id 0jtsgio7yenu
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteSuiteDefinition en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte DeleteSuiteDefinition en la Referencia de comandos de la AWS CLI.

`get-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-endpoint`.

AWS CLI

Ejemplo 1: obtención de información sobre un punto de conexión en el nivel de la cuenta de IoT Device Advisor

En el siguiente ejemplo de `get-endpoint`, se obtiene la información sobre un punto de conexión de prueba en el nivel de cuenta de Device Advisor.

```
aws iotdeviceadvisor get-endpoint
```

Salida:

```
{
    "endpoint": "t6y4c143x9sfo.deviceadvisor.iot.us-east-1.amazonaws.com"
}
```

Ejemplo 2: obtención de información sobre un punto de conexión en el nivel de la cuenta de IoT Device Advisor

En el siguiente ejemplo de `get-endpoint`, se obtiene la información sobre un punto de conexión de prueba en el nivel de dispositivo de Device Advisor con el thing-arn o el certificate-arn especificados.

```
aws iotdeviceadvisor get-endpoint \
```

```
    --thing-arn arn:aws:iot:us-east-1:123456789012:thing/MyIotThing
```

Salida:

```
{
    "endpoint": "tdb7719be5t6y4c143x9sfo.deviceadvisor.iot.us-east-1.amazonaws.com"
}
```

Para obtener más información, consulte Get a test endpoint en la Guía para desarrolladores de AWS IoT Core.

- Para ver los detalles de la API, consulte GetEndpoint en la Referencia de comandos de la AWS CLI.

`get-suite-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-suite-definition`.

AWS CLI

Para obtener información sobre un conjunto de pruebas de IoT Device Advisor

En el siguiente ejemplo de `get-suite-definition`, se obtiene información sobre un conjunto de pruebas de Device Advisor con el ID de definición de conjunto especificado.

```
aws iotdeviceadvisor get-suite-definition \
    --suite-definition-id qqcsmtyyjabl
```

Salida:

```
{
    "suiteDefinitionId": "qqcsmtyyjabl",
    "suiteDefinitionArn": "arn:aws:iotdeviceadvisor:us-
east-1:123456789012:suitedefinition/qqcsmtyyjabl",
    "suiteDefinitionVersion": "v1",
    "latestVersion": "v1",
    "suiteDefinitionConfiguration": {
        "suiteDefinitionName": "MQTT connection",
        "devices": [],
        "intendedForQualification": false,
        "isLongDurationTest": false,
```

```
        "rootGroup": "{\"configuration\":{},\"tests\":[{\"id\":\"uta5d9j1kvwc\",
\"name\":\"Test group 1\",\"configuration\":{},\"tests\":[{\"id\":\"awr8pq5vc9yp\",
\"name\":\"MQTT Connect\",\"configuration\":{},\"test\":{\"id\":\"MQTT_Connect\",
\"testCase\":null,\"version\":\"0.0.0\"}}]}]}",
        "devicePermissionRoleArn": "arn:aws:iam::123456789012:role/Myrole",
        "protocol": "MqttV3_1_1"
    },
    "createdAt": "2022-11-11T22:28:52.389000-05:00",
    "lastModifiedAt": "2022-11-11T22:28:52.389000-05:00",
    "tags": {}
}
```

Para obtener más información, consulte Get a test suite definition en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte GetSuiteDefinition en la Referencia de comandos de la AWS CLI.

`get-suite-run-report`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-suite-run-report`.

AWS CLI

Para obtener información sobre un informe de ejecución del conjunto de pruebas de cualificación de IoT Device Advisor

En el siguiente ejemplo de `get-suite-run-report`, se obtiene el enlace de descarga del informe correspondiente a un conjunto de pruebas que cumpla los requisitos de Device Advisor y que se ejecute correctamente con el ID de definición de conjunto y el ID de ejecución de conjunto especificados.

```
aws iotdeviceadvisor get-suite-run-report \
    --suite-definition-id ztvb5aek4w4x \
    --suite-run-id p6awv83nre6v
```

Salida:

```
{
    "qualificationReportDownloadUrl": "https://senate-apn-reports-us-east-1-
prod.s3.amazonaws.com/report.downloadlink"
```

```
}
```

Para obtener más información, consulte Get a qualification report for a successful qualification test suite run en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte GetSuiteRunReport en la Referencia de comandos de la AWS CLI.

`get-suite-run`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-suite-run`.

AWS CLI

Para obtener información sobre el estado de ejecución de un conjunto de pruebas de IoT Device Advisor

En el siguiente ejemplo de `get-suite-run`, se obtiene la información sobre el estado de ejecución de un conjunto de pruebas de Device Advisor con el ID de definición de conjunto y el ID de ejecución de conjunto especificados.

```
aws iotdeviceadvisor get-suite-run \
    --suite-definition-id qqcsmtyyjabl \
    --suite-run-id nzlfyhaa18oa
```

Salida:

```
{
    "suiteDefinitionId": "qqcsmtyyjabl",
    "suiteDefinitionVersion": "v1",
    "suiteRunId": "nzlfyhaa18oa",
    "suiteRunArn": "arn:aws:iotdeviceadvisor:us-east-1:123456789012:suiterun/
qqcsmtyyjabl/nzlfyhaa18oa",
    "suiteRunConfiguration": {
        "primaryDevice": {
            "thingArn": "arn:aws:iot:us-east-1:123456789012:thing/MyIotThing",
            "certificateArn": "arn:aws:iot:us-east-1:123456789012:cert/certFile"
        },
        "parallelRun": false
    },
    "testResult": {
        "groups": [
```

```
            {
                "groupId": "uta5d9j1kvwc",
                "groupName": "Test group 1",
                "tests": [
                    {
                        "testCaseRunId": "2ve2twrqyr0s",
                        "testCaseDefinitionId": "awr8pq5vc9yp",
                        "testCaseDefinitionName": "MQTT Connect",
                        "status": "PASS",
                        "startTime": "2022-11-12T00:01:53.693000-05:00",
                        "endTime": "2022-11-12T00:02:15.443000-05:00",
                        "logUrl": "https://console.aws.amazon.com/
cloudwatch/home?region=us-east-1#logEventViewer:group=/aws/iot/deviceadvisor/
qqcsmtyyjabl;stream=nzlfyhaa18oa_2ve2twrqyr0s",
                        "warnings": "null",
                        "failure": "null"
                    }
                ]
            }
        ]
    },
    "startTime": "2022-11-12T00:01:52.673000-05:00",
    "endTime": "2022-11-12T00:02:16.496000-05:00",
    "status": "PASS",
    "tags": {}
}
```

Para obtener más información, consulte Get a test suite run en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte GetSuiteRun en la Referencia de comandos de la AWS CLI.

`list-suite-definitions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-suite-definitions`.

AWS CLI

Ejemplo 1: enumeración de un conjunto de pruebas de IoT Device Advisor creadas por usted

En el siguiente ejemplo de `list-suite-definitions`, se enumeran hasta 25 conjuntos de pruebas de Device Advisor que ha creado en AWS IoT. Si tiene más de 25 conjuntos de pruebas,

se mostrará nextToken en la salida. Puede usar este nextToken para mostrar el resto de los conjuntos de pruebas que ha creado.

```
aws iotdeviceadvisor list-suite-definitions
```

Salida:

```
{
    "suiteDefinitionInformationList": [
        {
            "suiteDefinitionId": "3hsn88h4p2g5",
            "suiteDefinitionName": "TestSuite1",
            "defaultDevices": [
                {
                    "thingArn": "arn:aws:iot:us-east-1:123456789012:thing/
MyIotThing"
                }
            ],
            "intendedForQualification": false,
            "isLongDurationTest": false,
            "protocol": "MqttV3_1_1",
            "createdAt": "2022-11-17T14:15:56.830000-05:00"
        },
        {
            ......
        }
    ],
    "nextToken": "nextTokenValue"
}
```

Ejemplo 2: enumeración de un conjunto de pruebas de IoT Device Advisor creadas por usted con la configuración especificada

En el siguiente ejemplo de `list-suite-definitions`, se enumeran los conjuntos de pruebas de Device Advisor que ha creado en AWS IoT con el número máximo de resultados especificado. Si supera el número máximo de conjuntos de pruebas, se mostrará nextToken en la salida. Si tiene nextToken, puede usar nextToken para mostrar los conjuntos de pruebas que ha creado y que no se han mostrado antes.

```
aws iotdeviceadvisor list-suite-definitions \
    --max-result 1 \
```

```
    --next-token "nextTokenValue"
```

Salida:

```
{
    "suiteDefinitionInformationList": [
        {
            "suiteDefinitionId": "ztvb5aew4w4x",
            "suiteDefinitionName": "TestSuite2",
            "defaultDevices": [],
            "intendedForQualification": true,
            "isLongDurationTest": false,
            "protocol": "MqttV3_1_1",
            "createdAt": "2022-11-17T14:15:56.830000-05:00"
        }
    ],
    "nextToken": "nextTokenValue"
}
```

Para obtener más información, consulte ListSuiteDefinitions en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte ListSuiteDefinitions en la Referencia de comandos de la AWS CLI.

`list-suite-runs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-suite-runs`.

AWS CLI

Ejemplo 1: enumeración de toda la información sobre el estado de ejecución del conjunto de pruebas de IoT Device Advisor especificado

En el siguiente ejemplo de `list-suite-runs`, se muestra toda la información sobre el estado de ejecución de un conjunto de pruebas de Device Advisor con el ID de definición de conjunto especificado. Si tiene más de 25 ejecuciones de conjuntos de pruebas, se mostrará nextToken en la salida. Puede usar este nextToken para mostrar el resto de ejecuciones de conjuntos de pruebas.

```
aws iotdeviceadvisor list-suite-runs \
```

```
    --suite-definition-id ztvb5aew4w4x
```

Salida:

```
{
    "suiteRunsList": [
        {
            "suiteDefinitionId": "ztvb5aew4w4x",
            "suiteDefinitionVersion": "v1",
            "suiteDefinitionName": "TestSuite",
            "suiteRunId": "p6awv89nre6v",
            "createdAt": "2022-12-01T16:33:14.212000-05:00",
            "startedAt": "2022-12-01T16:33:15.710000-05:00",
            "endAt": "2022-12-01T16:42:03.323000-05:00",
            "status": "PASS",
            "passed": 6,
            "failed": 0
        }
    ]
}
```

Ejemplo 2: enumeración de toda la información sobre el estado de ejecución del conjunto de pruebas de IoT Device Advisor especificado con la configuración especificada

En el siguiente ejemplo de `list-suite-runs`, se muestra toda la información sobre el estado de ejecución de un conjunto de pruebas de Device Advisor con el ID de definición de conjunto especificado y el número máximo de resultados especificado. Si supera el número máximo de ejecuciones de conjuntos de pruebas, se mostrará nextToken en la salida. Si tiene nextToken, puede usar nextToken para mostrar las ejecuciones de conjuntos de pruebas que no se han mostrado antes.

```
aws iotdeviceadvisor list-suite-runs \
    --suite-definition-id qqcsmtyyjaml \
    --max-result 1 \
    --next-token "nextTokenValue"
```

Salida:

```
{
    "suiteRunsList": [
        {
```

```
            "suiteDefinitionId": "qqcsmtyyjaml",
            "suiteDefinitionVersion": "v1",
            "suiteDefinitionName": "MQTT connection",
            "suiteRunId": "gz9vm2s6d2jy",
            "createdAt": "2022-12-01T20:10:27.079000-05:00",
            "startedAt": "2022-12-01T20:10:28.003000-05:00",
            "endAt": "2022-12-01T20:10:45.084000-05:00",
            "status": "STOPPED",
            "passed": 0,
            "failed": 0
        }
    ],
    "nextToken": "nextTokenValue"
}
```

Para obtener más información, consulte ListSuiteRuns en la Referencia de la API de AWS IoT.

- Para obtener información sobre la API, consulte ListSuiteRuns en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas asociadas a un recurso de IoT Device Advisor

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran las etiquetas asociadas a un recurso de Device Advisor. El recurso de Device Advisor puede ser un Suitedefinition-Arn o un Suiterun-Arn.

```
aws iotdeviceadvisor list-tags-for-resource \
    --resource-arn arn:aws:iotdeviceadvisor:us-east-1:123456789012:suitedefinition/
ba0uyjpg38ny
```

Salida:

```
{
    "tags": {
        "TestTagKey": "TestTagValue"
    }
```

```
}
```

Para obtener más información, consulte ListTagsForResource en la Referencia de la API de AWS IoT y Resource types defined by AWS IoT Core Device Advisor en la Referencia de autorizaciones de servicio.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`start-suite-run`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-suite-run`.

AWS CLI

Para iniciar una ejecución de conjunto de pruebas de IoT Device Advisor

En el siguiente ejemplo de `start-suite-run`, se genera una lista de los widgets disponibles en la cuenta de AWS.

```
aws iotdeviceadvisor start-suite-run \
    --suite-definition-id qqcsmtyyjabl \
    --suite-definition-version v1 \
    --suite-run-configuration '{"primaryDevice":{"thingArn": "arn:aws:iot:us-
east-1:123456789012:thing/MyIotThing","certificateArn":"arn:aws:iot:us-
east-1:123456789012:cert/certFile"}}'
```

Salida:

```
{
    "suiteRunId": "pwmucgw7lt9s",
    "suiteRunArn": "arn:aws:iotdeviceadvisor:us-east-1:123456789012:suiterun/
qqcsmtyyjabl/pwmucgw7lk9s",
    "createdAt": "2022-12-02T15:43:05.581000-05:00"
}
```

Para obtener más información, consulte Start a test suite run en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte StartSuiteRun en la Referencia de comandos de la AWS CLI.

`stop-suite-run`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-suite-run`.

AWS CLI

Para detener un conjunto de pruebas de IoT Device Advisor que se está ejecutando actualmente

En el siguiente ejemplo de `stop-suite-run`, se detiene un conjunto de pruebas de Device Advisor que se ejecuta actualmente con el ID de definición de conjunto y el ID de ejecución de conjunto especificados.

```
aws iotdeviceadvisor stop-suite-run \
    --suite-definition-id qqcsmtyyjabl \
    --suite-run-id nzlfyhaa18oa
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Stop a test suite run en la Guía para desarrolladores de AWS IoT Core.

- Para obtener información sobre la API, consulte StopSuiteRun en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para agregar y modificar las etiquetas existentes de un recurso de IoT Device Advisor

El siguiente ejemplo de `tag-resource`, se agregan y modifican las etiquetas existentes de un recurso de Device Advisor con el ARN y las etiquetas del recurso especificados. El recurso de Device Advisor puede ser un Suitedefinition-Arn o un Suiterun-Arn.

```
aws iotdeviceadvisor tag-resource \
    --resource-arn arn:aws:iotdeviceadvisor:us-east-1:123456789012:suitedefinition/
ba0uyjpg38ny \
    --tags '{"TagKey": "TagValue"}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte TagResource en la Referencia de la API de AWS IoT y Resource types defined by AWS IoT Core Device Advisor en la Referencia de autorizaciones de servicio.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar las etiquetas existentes de un recurso de IoT Device Advisor

El siguiente ejemplo de `untag-resource`, se eliminan las etiquetas existentes de un recurso de Device Advisor con el ARN y la clave de etiqueta del recurso especificados. El recurso de Device Advisor puede ser un Suitedefinition-Arn o un Suiterun-Arn.

```
aws iotdeviceadvisor untag-resource \
    --resource-arn arn:aws:iotdeviceadvisor:us-east-1:123456789012:suitedefinition/
ba0uyjpg38ny \
    --tag-keys "TagKey"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte UntagResource en la Referencia de la API de AWS IoT y Resource types defined by AWS IoT Core Device Advisor en la Referencia de autorizaciones de servicio.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-suite-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-suite-definition`.

AWS CLI

Ejemplo 1: actualización de un conjunto de pruebas de IoT Device Advisor

En el siguiente ejemplo de `update-suite-definition`, se actualiza un conjunto de pruebas de Device Advisor en AWS IoT con el ID de definición de conjunto y la configuración de definición de conjunto especificados.

```
aws iotdeviceadvisor update-suite-definition \
    --suite-definition-id 3hsn88h4p2g5 \
    --suite-definition-configuration '{ \
        "suiteDefinitionName": "TestSuiteName", \
        "devices": [{"thingArn":"arn:aws:iot:us-east-1:123456789012:thing/
MyIotThing"}], \
        "intendedForQualification": false, \
        "rootGroup": "{\"configuration\":{},\"tests\":[{\"name\":\"MQTT Connect\",
\"configuration\":{\"EXECUTION_TIMEOUT\":120},\"tests\":[{\"name\":\"MQTT_Connect\",
\"configuration\":{},\"test\":{\"id\":\"MQTT_Connect\",\"testCase\":null,\"version
\":\"0.0.0\"}}]}]}", \
        "devicePermissionRoleArn": "arn:aws:iam::123456789012:role/Myrole"}'
```

Salida:

```
{
    "suiteDefinitionId": "3hsn88h4p2g5",
    "suiteDefinitionName": "TestSuiteName",
    "suiteDefinitionVersion": "v3",
    "createdAt": "2022-11-17T14:15:56.830000-05:00",
    "lastUpdatedAt": "2022-12-02T16:02:45.857000-05:00"
}
```

Ejemplo 2: actualización de un conjunto de pruebas de IoT Device Advisor

En el siguiente ejemplo de `update-suite-definition`, se actualiza un conjunto de pruebas de cualificación de Device Advisor en AWS IoT con el ID de definición de conjunto y la configuración de definición de conjunto especificados.

```
aws iotdeviceadvisor update-suite-definition \
    --suite-definition-id txgsuolk2myj \
    --suite-definition-configuration '{
        "suiteDefinitionName": "TestSuiteName", \
        "devices": [{"thingArn":"arn:aws:iot:us-east-1:123456789012:thing/
MyIotThing"}], \
        "intendedForQualification": true, \
        "rootGroup": "", \
```

```
        "devicePermissionRoleArn": "arn:aws:iam::123456789012:role/Myrole"}'
```

Salida:

```
{
    "suiteDefinitionId": "txgsuolk2myj",
    "suiteDefinitionName": "TestSuiteName",
    "suiteDefinitionVersion": "v3",
    "createdAt": "2022-11-17T14:15:56.830000-05:00",
    "lastUpdatedAt": "2022-12-02T16:02:45.857000-05:00"
}
```

Para obtener más información, consulte UpdateSuiteDefinition en la Referencia de la API de AWS IoT Events.

- Para obtener información sobre la API, consulte UpdateSuiteDefinition en la Referencia de comandos de la AWS CLI.

AWS IoT data Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS IoT data.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`delete-thing-shadow`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-thing-shadow`.

AWS CLI

Para eliminar un documento de sombra de dispositivo

En el siguiente ejemplo de `delete-thing-shadow`, se elimina el documento de sombra completo del dispositivo denominado `MyRPi`.

```
aws iot-data delete-thing-shadow \
    --thing-name MyRPi \
    "output.txt"
```

El comando no muestra ningún resultado en la pantalla, pero `output.txt` contiene información que confirma la versión y la marca de tiempo del documento de sombra que ha eliminado.

```
{"version":2,"timestamp":1560270384}
```

Para obtener más información, consulte Using Shadows en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte DeleteThingShadow en la Referencia de comandos de la AWS CLI.

`get-thing-shadow`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-thing-shadow`.

AWS CLI

Para obtener un documento de sombra de objeto

En el siguiente ejemplo de `get-thing-shadow`, se obtiene el documento de sombra del objeto de IoT especificado.

```
aws iot-data get-thing-shadow \
    --thing-name MyRPi \
    output.txt
```

El comando no muestra ningún resultado en la pantalla, pero a continuación aparece el contenido de `output.txt`:

```
{
```

```
  "state":{
    "reported":{
    "moisture":"low"
    }
  },
  "metadata":{
    "reported":{
      "moisture":{
        "timestamp":1560269319
      }
    }
  },
  "version":1,"timestamp":1560269405
}
```

Para obtener más información, consulte Device Shadow Service Data Flow en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte GetThingShadow en la Referencia de comandos de la AWS CLI.

`update-thing-shadow`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-thing-shadow`.

AWS CLI

Para actualizar una sombra de objeto

El siguiente ejemplo de `update-thing-shadow` modifica el estado actual de la sombra de dispositivo para el objeto especificado y lo guarda en el archivo `output.txt`.

```
aws iot-data update-thing-shadow \
    --thing-name MyRPi \
    --payload "{"state":{"reported":{"moisture":"okay"}}}" \
    "output.txt"
```

El comando no muestra ningún resultado en la pantalla, pero a continuación aparece el contenido de `output.txt`:

```
{
    "state": {
```

```
        "reported": {
            "moisture": "okay"
        }
    },
    "metadata": {
        "reported": {
            "moisture": {
                "timestamp": 1560270036
            }
        }
    },
    "version": 2,
    "timestamp": 1560270036
}
```

Para obtener más información, consulte Device Shadow Service Data Flow en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte UpdateThingShadow en la Referencia de comandos de la AWS CLI.

AWS IoT Events Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS IoT Events.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`batch-put-message`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-put-message`.

AWS CLI

Para enviar mensajes (entradas) a AWS IoT Events

En el siguiente ejemplo de `batch-put-message`, se envía un conjunto de mensajes al sistema de AWS IoT Events. La carga útil de cada mensaje se transforma en la entrada que especifique (`inputName`) y se ingiere en cualquier detector que supervise dicha entrada. Si se envían varios mensajes, no se puede garantizar el orden en que se vayan a procesar dichos mensajes. Para garantizar un orden, debe enviar los mensajes de uno en uno y esperar una respuesta satisfactoria.

```
aws iotevents-data batch-put-message \
    --cli-input-json file://highPressureMessage.json
```

Contenido de `highPressureMessage.json`:

```
{
    "messages": [
        {
            "messageId": "00001",
            "inputName": "PressureInput",
            "payload": "{\"motorid\": \"Fulton-A32\", \"sensorData\": {\"pressure\":
 80, \"temperature\": 39} }"
        }
    ]
}
```

Salida:

```
{
    "BatchPutMessageErrorEntries": []
}
```

Para obtener más información, consulte BatchPutMessage en la Referencia de la API de AWS IoT Events.

- Para obtener más información sobre la API, consulte BatchPutMessage en la Referencia de comandos de la AWS CLI.

batch-update-detector

En el siguiente ejemplo de código, se muestra cómo utilizar batch-update-detector.

AWS CLI

Para actualizar un detector (instancia)

El siguiente ejemplo de batch-update-detector actualiza el estado, los valores de las variables y la configuración del temporizador de uno o más detectores (instancias) de un modelo de detector específico.

```
aws iotevents-data batch-update-detector \
    --cli-input-json file://budFulton-A32.json
```

Contenido de budFulton-A32.json:

```
{
    "detectors": [
        {
            "messageId": "00001",
            "detectorModelName": "motorDetectorModel",
            "keyValue": "Fulton-A32",
            "state": {
                "stateName": "Normal",
                "variables": [
                    {
                        "name": "pressureThresholdBreached",
                        "value": "0"
                    }
                ],
                "timers": [
                ]
            }
        }
    ]
}
```

Salida:

```
{
    "batchUpdateDetectorErrorEntries": []
```

```
}
```

Para obtener más información, consulte BatchUpdateDetector en la Referencia de la API de AWS IoT Events.

- Para obtener detalles sobre la API, consulte BatchUpdateDetector en la Referencia de comandos de la AWS CLI.

`create-detector-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-detector-model`.

AWS CLI

Para crear un modelo de detector

En el siguiente ejemplo de `create-detector-model`, se crea un modelo de detector con la configuración especificada en un archivo de parámetros.

```
aws iotevents create-detector-model  \
    --cli-input-json file://motorDetectorModel.json
```

Contenido de `motorDetectorModel.json`:

```
{
    "detectorModelName": "motorDetectorModel",
    "detectorModelDefinition": {
        "states": [
            {
                "stateName": "Normal",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "init",
                            "condition": "true",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "pressureThresholdBreached",
                                        "value": "0"
                                    }
                                }
                            ]
```

```
                        }
                    ]
                },
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "Overpressurized",
                            "condition": "$input.PressureInput.sensorData.pressure
 &gt; 70",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "pressureThresholdBreached",
                                        "value":
 "$variable.pressureThresholdBreached + 3"
                                    }
                                }
                            ],
                            "nextState": "Dangerous"
                        }
                    ]
                }
            },
            {
                "stateName": "Dangerous",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "Pressure Threshold Breached",
                            "condition": "$variable.pressureThresholdBreached &gt;
 1",
                            "actions": [
                                {
                                    "sns": {
                                        "targetArn": "arn:aws:sns:us-
east-1:123456789012:underPressureAction"
                                    }
                                }
                            ]
                        }
                    ]
                },
                "onInput": {
                    "events": [
```

```
                        {
                            "eventName": "Overpressurized",
                            "condition": "$input.PressureInput.sensorData.pressure
&gt; 70",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "pressureThresholdBreached",
                                        "value": "3"
                                    }
                                }
                            ]
                        },
                        {
                            "eventName": "Pressure Okay",
                            "condition": "$input.PressureInput.sensorData.pressure
&lt;= 70",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "pressureThresholdBreached",
                                        "value":
"$variable.pressureThresholdBreached - 1"
                                    }
                                }
                            ]
                        }
                    ],
                    "transitionEvents": [
                        {
                            "eventName": "BackToNormal",
                            "condition": "$input.PressureInput.sensorData.pressure
&lt;= 70 &amp;&amp; $variable.pressureThresholdBreached &lt;= 1",
                            "nextState": "Normal"
                        }
                    ]
                },
                "onExit": {
                    "events": [
                        {
                            "eventName": "Normal Pressure Restored",
                            "condition": "true",
                            "actions": [
                                {
```

```
                                    "sns": {
                                        "targetArn": "arn:aws:sns:us-
east-1:123456789012:pressureClearedAction"
                                    }
                                }
                            ]
                        }
                    ]
                }
            }
        ],
        "initialStateName": "Normal"
    },
    "key": "motorid",
    "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole"
}
```

Salida:

```
{
    "detectorModelConfiguration": {
        "status": "ACTIVATING",
        "lastUpdateTime": 1560796816.077,
        "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
        "creationTime": 1560796816.077,
        "detectorModelArn": "arn:aws:iotevents:us-west-2:123456789012:detectorModel/
motorDetectorModel",
        "key": "motorid",
        "detectorModelName": "motorDetectorModel",
        "detectorModelVersion": "1"
    }
}
```

Para obtener más información, consulte CreateDetectorModel en la Guía de referencia de la API de AWS IoT Events.

- Para obtener más información sobre la API, consulte CreateDetectorModel en la Referencia de comandos de la AWS CLI.

`create-input`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-input`.

AWS CLI

Para crear una entrada

En el siguiente ejemplo de `create-input`, se crea una entrada.

```
aws iotevents create-input  \
    --cli-input-json file://pressureInput.json
```

Contenido de `pressureInput.json`:

```
{
    "inputName": "PressureInput",
    "inputDescription": "Pressure readings from a motor",
    "inputDefinition": {
        "attributes": [
            { "jsonPath": "sensorData.pressure" },
            { "jsonPath": "motorid" }
        ]
    }
}
```

Salida:

```
{
    "inputConfiguration": {
        "status": "ACTIVE",
        "inputArn": "arn:aws:iotevents:us-west-2:123456789012:input/PressureInput",
        "lastUpdateTime": 1560795312.542,
        "creationTime": 1560795312.542,
        "inputName": "PressureInput",
        "inputDescription": "Pressure readings from a motor"
    }
}
```

Para obtener más información, consulte CreateInput en la Guía de referencia de la API de AWS IoT Events.

- Para obtener más información sobre la API, consulte CreateInput en la Referencia de comandos de la AWS CLI.

`delete-detector-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-detector-model`.

AWS CLI

Para eliminar un modelo de detector

En el siguiente ejemplo de `delete-detector-model`, se elimina el modelo de detector especificado. También se eliminan todas las instancias activas del modelo de detector.

```
aws iotevents delete-detector-model \
    --detector-model-name motorDetectorModel
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteDetectorModel en la Referencia de la API de AWS IoT Events.

- Para obtener más información sobre la API, consulte DeleteDetectorModel en la Referencia de comandos de la AWS CLI.

`delete-input`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-input`.

AWS CLI

Para eliminar una entrada

En el siguiente ejemplo de `delete-input`, se elimina la entrada especificada.

```
aws iotevents delete-input \
    --input-name PressureInput
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteInput en la Referencia de la API de AWS IoT Events.

- Para obtener más información sobre la API, consulte DeleteInput en la Referencia de comandos de la AWS CLI.

describe-detector-model

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-detector-model`.

AWS CLI

Para obtener información de un modelo de detector

En el siguiente ejemplo de `describe-detector-model`, se muestran los detalles del modelo de detector especificado. Dado que no se ha especificado el parámetro `version`, el comando devuelve información sobre la versión más reciente.

```
aws iotevents describe-detector-model \
    --detector-model-name motorDetectorModel
```

Salida:

```
{
    "detectorModel": {
        "detectorModelConfiguration": {
            "status": "ACTIVE",
            "lastUpdateTime": 1560796816.077,
            "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
            "creationTime": 1560796816.077,
            "detectorModelArn": "arn:aws:iotevents:us-
west-2:123456789012:detectorModel/motorDetectorModel",
            "key": "motorid",
            "detectorModelName": "motorDetectorModel",
            "detectorModelVersion": "1"
        },
        "detectorModelDefinition": {
            "states": [
                {
                    "onInput": {
                        "transitionEvents": [
                            {
                                "eventName": "Overpressurized",
                                "actions": [
                                    {
                                        "setVariable": {
                                            "variableName":
 "pressureThresholdBreached",
```

```
                                        "value":
"$variable.pressureThresholdBreached + 3"
                                    }
                                }
                            ],
                            "condition":
"$input.PressureInput.sensorData.pressure > 70",
                            "nextState": "Dangerous"
                        }
                    ],
                    "events": []
                },
                "stateName": "Normal",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "init",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName":
"pressureThresholdBreached",
                                        "value": "0"
                                    }
                                }
                            ],
                            "condition": "true"
                        }
                    ]
                },
                "onExit": {
                    "events": []
                }
            },
            {
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "BackToNormal",
                            "actions": [],
                            "condition":
"$input.PressureInput.sensorData.pressure <= 70 &&
$variable.pressureThresholdBreached <= 1",
                            "nextState": "Normal"
```

```
                            }
                        ],
                        "events": [
                            {
                                "eventName": "Overpressurized",
                                "actions": [
                                    {
                                        "setVariable": {
                                            "variableName":
 "pressureThresholdBreached",
                                            "value": "3"
                                        }
                                    }
                                ],
                                "condition":
 "$input.PressureInput.sensorData.pressure > 70"
                            },
                            {
                                "eventName": "Pressure Okay",
                                "actions": [
                                    {
                                        "setVariable": {
                                            "variableName":
 "pressureThresholdBreached",
                                            "value":
 "$variable.pressureThresholdBreached - 1"
                                        }
                                    }
                                ],
                                "condition":
 "$input.PressureInput.sensorData.pressure <= 70"
                            }
                        ]
                    },
                    "stateName": "Dangerous",
                    "onEnter": {
                        "events": [
                            {
                                "eventName": "Pressure Threshold Breached",
                                "actions": [
                                    {
                                        "sns": {
                                            "targetArn": "arn:aws:sns:us-
east-1:123456789012:underPressureAction"
```

```
                                    }
                                }
                            ],
                            "condition": "$variable.pressureThresholdBreached >
 1"
                        }
                    ]
                },
                "onExit": {
                    "events": [
                        {
                            "eventName": "Normal Pressure Restored",
                            "actions": [
                                {
                                    "sns": {
                                        "targetArn": "arn:aws:sns:us-
east-1:123456789012:pressureClearedAction"
                                    }
                                }
                            ],
                            "condition": "true"
                        }
                    ]
                }
            }
        ],
        "initialStateName": "Normal"
    }
}
}
```

Para obtener más información, consulte DescribeDetectorModel en la Referencia de la API de AWS IoT Events.

- Para obtener más información sobre la API, consulte DescribeDetectorModel en la Referencia de comandos de la AWS CLI.

`describe-detector`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-detector`.

AWS CLI

Para obtener información sobre un detector (instancia)

En el siguiente ejemplo de `describe-detector`, se muestran los detalles del detector especificado (instancia).

```
aws iotevents-data describe-detector \
    --detector-model-name motorDetectorModel \
    --key-value "Fulton-A32"
```

Salida:

```
{
    "detector": {
        "lastUpdateTime": 1560797852.776,
        "creationTime": 1560797852.775,
        "state": {
            "variables": [
                {
                    "name": "pressureThresholdBreached",
                    "value": "3"
                }
            ],
            "stateName": "Dangerous",
            "timers": []
        },
        "keyValue": "Fulton-A32",
        "detectorModelName": "motorDetectorModel",
        "detectorModelVersion": "1"
    }
}
```

Para obtener más información, consulte DescribeDetector en la Referencia de la API de AWS IoT Events.

- Para obtener más información sobre la API, consulte DescribeDetector en la Referencia de comandos de la AWS CLI.

`describe-input`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-input`.

AWS CLI

Para obtener información acerca de una entrada

En el ejemplo siguiente de `describe-input`, se muestran los detalles de la entrada especificada.

```
aws iotevents describe-input \
    --input-name PressureInput
```

Salida:

```
{
    "input": {
        "inputConfiguration": {
            "status": "ACTIVE",
            "inputArn": "arn:aws:iotevents:us-west-2:123456789012:input/
PressureInput",
            "lastUpdateTime": 1560795312.542,
            "creationTime": 1560795312.542,
            "inputName": "PressureInput",
            "inputDescription": "Pressure readings from a motor"
        },
        "inputDefinition": {
            "attributes": [
                {
                    "jsonPath": "sensorData.pressure"
                },
                {
                    "jsonPath": "motorid"
                }
            ]
        }
    }
}
```

Para obtener más información, consulte DescribeInput en la Referencia de la API de AWS IoT Events.

- Para obtener más información sobre la API, consulte DescribeInput en la Referencia de comandos de la AWS CLI.

describe-logging-options

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-logging-options`.

AWS CLI

Para obtener información sobre la configuración de registro

En el siguiente ejemplo de `describe-logging-options`, se recupera la configuración actual de las opciones de registro de AWS IoT Events.

```
aws iotevents describe-logging-options
```

Salida:

```
{
    "loggingOptions": {
        "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
        "enabled": false,
        "level": "ERROR"
    }
}
```

Para obtener más información, consulte DescribeLoggingOptions en la Referencia de la API de AWS IoT Events.

- Para obtener más información sobre la API, consulte DescribeLoggingOptions en la Referencia de comandos de la AWS CLI.

list-detector-model-versions

En el siguiente ejemplo de código, se muestra cómo utilizar `list-detector-model-versions`.

AWS CLI

Para obtener información acerca de las versiones de un modelo de detector

En el siguiente ejemplo de `list-detector-model-versions`, se muestra una lista de todas las versiones de un modelo de detector. Solo se devuelven los metadatos asociados a cada versión de modelo de detector.

```
aws iotevents list-detector-model-versions \
```

```
    --detector-model-name motorDetectorModel
```

Salida:

```
{
    "detectorModelVersionSummaries": [
        {
            "status": "ACTIVE",
            "lastUpdateTime": 1560796816.077,
            "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
            "creationTime": 1560796816.077,
            "detectorModelArn": "arn:aws:iotevents:us-
west-2:123456789012:detectorModel/motorDetectorModel",
            "detectorModelName": "motorDetectorModel",
            "detectorModelVersion": "1"
        }
    ]
}
```

Para obtener más información, consulte ListDetectorModelVersions en la Referencia de la API de AWS IoT Events.

- Para obtener más información sobre la API, consulte ListDetectorModelVersions en la Referencia de comandos de la AWS CLI.

`list-detector-models`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-detector-models`.

AWS CLI

Para obtener una lista de los modelos de detector

En el siguiente ejemplo de `list-detector-models`, se muestra una lista de los modelos de detector que ha creado. Solo se devuelven los metadatos asociados a cada modelo de detector.

```
aws iotevents list-detector-models
```

Salida:

```
{
    "detectorModelSummaries": [
```

```
        {
            "detectorModelName": "motorDetectorModel",
            "creationTime": 1552072424.212
            "detectorModelDescription": "Detect overpressure in a motor."
        }
    ]
}
```

Para obtener más información, consulte ListDetectorModels en la Referencia de la API de AWS IoT Events.

- Para obtener más información sobre la API, consulte ListDetectorModels en la Referencia de comandos de la AWS CLI.

`list-detectors`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-detectors`.

AWS CLI

Para obtener una lista de detectores para un modelo de detector

En el siguiente ejemplo de `list-detectors`, se muestra una lista de los detectores (las instancias de un modelo de detector) de su cuenta.

```
aws iotevents-data list-detectors \
    --detector-model-name motorDetectorModel
```

Salida:

```
{
    "detectorSummaries": [
        {
            "lastUpdateTime": 1558129925.2,
            "creationTime": 1552073155.527,
            "state": {
                "stateName": "Normal"
            },
            "keyValue": "Fulton-A32",
            "detectorModelName": "motorDetectorModel",
            "detectorModelVersion": "1"
        }
    ]
```

```
}
```

Para obtener más información, consulte ListDetectors en la Referencia de la API de AWS IoT Events.

- Para obtener más información sobre la API, consulte ListDetectors en la Referencia de comandos de la AWS CLI.

`list-inputs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-inputs`.

AWS CLI

Para enumerar las entradas

En el siguiente ejemplo de `list-inputs`, se muestra una lista de las entradas que ha creado en su cuenta.

```
aws iotevents list-inputs
```

Este comando no genera ninguna salida. Salida:

```
{
    {
        "status": "ACTIVE",
        "inputArn": "arn:aws:iotevents:us-west-2:123456789012:input/PressureInput",
        "lastUpdateTime": 1551742986.768,
        "creationTime": 1551742986.768,
        "inputName": "PressureInput",
        "inputDescription": "Pressure readings from a motor"
    }
}
```

Para obtener más información, consulte ListInputs en la Referencia de la API de AWS IoT Events.

- Para obtener información sobre la API, consulte ListInputs en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas asignadas a un recurso.

El siguiente ejemplo de `list-tags-for-resource` es una lista de los nombres de clave de las etiquetas y los valores que ha asignado al recurso.

```
aws iotevents list-tags-for-resource \
    --resource-arn "arn:aws:iotevents:us-west-2:123456789012:input/PressureInput"
```

Salida:

```
{
    "tags": [
        {
            "value": "motor",
            "key": "deviceType"
        }
    ]
}
```

Para obtener más información, consulte ListTagsForResource en la Referencia de la API de AWS IoT Events.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-logging-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-logging-options`.

AWS CLI

Para configurar las opciones de registro

En el siguiente ejemplo de `put-logging-options`, se definen o actualizan las opciones de registro de AWS IoT Events actuales. Si actualiza el valor de cualquier campo `loggingOptions` field, it can take up to one minute for the change to take effect. Also, if you change the policy attached to the role you specified in the ``roleArn` (por ejemplo, para corregir una política no válida), el cambio puede tardar hasta cinco minutos en surtir efecto.

```
aws iotevents put-logging-options \
    --cli-input-json file://logging-options.json
```

Contenido de `logging-options.json`:

```
{
    "loggingOptions": {
        "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
        "level": "DEBUG",
        "enabled": true,
        "detectorDebugOptions": [
            {
                "detectorModelName": "motorDetectorModel",
                "keyValue": "Fulton-A32"
            }
        ]
    }
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte PutLoggingOptions en la Referencia de la API de AWS IoT Events.

- Para obtener detalles sobre la API, consulte PutLoggingOptions en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para agregar etiquetas a un recurso

En el siguiente ejemplo de `tag-resource`, se agrega o modifica (si la clave `deviceType` ya existe) la etiqueta asociada al recurso especificado.

```
aws iotevents tag-resource \
    --cli-input-json file://pressureInput.tag.json
```

Contenido de `pressureInput.tag.json`:

```
{
    "resourceArn": "arn:aws:iotevents:us-west-2:123456789012:input/PressureInput",
    "tags": [
        {
            "key": "deviceType",
            "value": "motor"
        }
    ]
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte TagResource en la Referencia de la API de AWS IoT Events.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar etiquetas de un recurso

En el siguiente ejemplo de `untag-resource`, se elimina la etiqueta con el nombre de la clave especificado del recurso indicado.

```
aws iotevents untag-resource \
    --resource-arn arn:aws:iotevents:us-west-2:123456789012:input/PressureInput \
    --tagkeys deviceType
```

Este comando no genera ninguna salida.

Para obtener más información, consulte UntagResource en la Referencia de la API de AWS IoT Events.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-detector-model

En el siguiente ejemplo de código, se muestra cómo utilizar `update-detector-model`.

AWS CLI

Para actualizar un modelo de detector

En el siguiente ejemplo de `update-detector-model`, se actualiza el modelo de detector especificado. Los detectores (instancias) generados por la versión anterior se eliminan y, a continuación, se vuelven a crear a medida que llegan nuevas entradas.

```
aws iotevents update-detector-model \
    --cli-input-json file://motorDetectorModel.update.json
```

Contenido de `motorDetectorModel.update.json`:

```
{
    "detectorModelName": "motorDetectorModel",
    "detectorModelDefinition": {
        "states": [
            {
                "stateName": "Normal",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "init",
                            "condition": "true",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "pressureThresholdBreached",
                                        "value": "0"
                                    }
                                }
                            ]
                        }
                    ]
                },
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "Overpressurized",
```

```
                            "condition": "$input.PressureInput.sensorData.pressure >
 70",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "pressureThresholdBreached",
                                        "value":
 "$variable.pressureThresholdBreached + 3"
                                    }
                                }
                            ],
                            "nextState": "Dangerous"
                        }
                    ]
                }
            },
            {
                "stateName": "Dangerous",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "Pressure Threshold Breached",
                            "condition": "$variable.pressureThresholdBreached > 1",
                            "actions": [
                                {
                                    "sns": {
                                        "targetArn": "arn:aws:sns:us-
east-1:123456789012:underPressureAction"
                                    }
                                }
                            ]
                        }
                    ]
                },
                "onInput": {
                    "events": [
                        {
                            "eventName": "Overpressurized",
                            "condition": "$input.PressureInput.sensorData.pressure >
 70",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "pressureThresholdBreached",
```

```
                                        "value": "3"
                                    }
                                }
                            ]
                        },
                        {
                            "eventName": "Pressure Okay",
                            "condition": "$input.PressureInput.sensorData.pressure
 <= 70",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "pressureThresholdBreached",
                                        "value":
 "$variable.pressureThresholdBreached - 1"
                                    }
                                }
                            ]
                        }
                    ],
                    "transitionEvents": [
                        {
                            "eventName": "BackToNormal",
                            "condition": "$input.PressureInput.sensorData.pressure
 <= 70 && $variable.pressureThresholdBreached <= 1",
                            "nextState": "Normal"
                        }
                    ]
                },
                "onExit": {
                    "events": [
                        {
                            "eventName": "Normal Pressure Restored",
                            "condition": "true",
                            "actions": [
                                {
                                    "sns": {
                                        "targetArn": "arn:aws:sns:us-
east-1:123456789012:pressureClearedAction"
                                    }
                                }
                            ]
                        }
                    ]
```

```
                }
            }
        ],
        "initialStateName": "Normal"
    },
    "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole"
}
```

Salida:

```
{
    "detectorModelConfiguration": {
        "status": "ACTIVATING",
        "lastUpdateTime": 1560799387.719,
        "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
        "creationTime": 1560799387.719,
        "detectorModelArn": "arn:aws:iotevents:us-west-2:123456789012:detectorModel/
motorDetectorModel",
        "key": "motorid",
        "detectorModelName": "motorDetectorModel",
        "detectorModelVersion": "2"
    }
}
```

Para obtener más información, consulte UpdateDetectorModel en la Referencia de la API de AWS IoT Events.

- Para obtener más información sobre la API, consulte UpdateDetectorModel en la Referencia de comandos de la AWS CLI.

`update-input`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-input`.

AWS CLI

Para actualizar una entrada

En el siguiente ejemplo de `update-input`, se actualiza la entrada especificada con una descripción y definición nuevas.

```
aws iotevents update-input \
```

```
    --cli-input-json file://pressureInput.json
```

Contenido de `pressureInput.json`:

```
{
    "inputName": "PressureInput",
    "inputDescription": "Pressure readings from a motor",
    "inputDefinition": {
        "attributes": [
            { "jsonPath": "sensorData.pressure" },
            { "jsonPath": "motorid" }
        ]
    }
}
```

Salida:

```
{
    "inputConfiguration": {
        "status": "ACTIVE",
        "inputArn": "arn:aws:iotevents:us-west-2:123456789012:input/PressureInput",
        "lastUpdateTime": 1560795976.458,
        "creationTime": 1560795312.542,
        "inputName": "PressureInput",
        "inputDescription": "Pressure readings from a motor"
    }
}
```

Para obtener más información, consulte UpdateInput en la Referencia de la API de AWS IoT Events.

- Para obtener más información sobre la API, consulte UpdateInput en la Referencia de comandos de la AWS CLI.

AWS IoT Events-Data Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS IoT Events-Data.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`batch-put-message`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-put-message`.

AWS CLI

Para enviar mensajes (entradas) a AWS IoT Events

En el siguiente ejemplo de `batch-put-message`, se envía un conjunto de mensajes al sistema de AWS IoT Events. La carga útil de cada mensaje se transforma en la entrada que especifique (`inputName`) y se ingiere en cualquier detector que supervise dicha entrada. Si se envían varios mensajes, no se puede garantizar el orden en que se vayan a procesar dichos mensajes. Para garantizar un orden, debe enviar los mensajes de uno en uno y esperar una respuesta satisfactoria.

```
aws iotevents-data batch-put-message \
    --cli-binary-format raw-in-base64-out \
    --cli-input-json file://highPressureMessage.json
```

Contenido de `highPressureMessage.json`:

```
{
    "messages": [
        {
            "messageId": "00001",
            "inputName": "PressureInput",
            "payload": "{\"motorid\": \"Fulton-A32\", \"sensorData\": {\"pressure\":
 80, \"temperature\": 39} }"
        }
```

```
    ]
}
```

Salida:

```
{
    "BatchPutMessageErrorEntries": []
}
```

Para obtener más información, consulte BatchPutMessage en la Guía para desarrolladores de AWS IoT*.

- Para obtener más información sobre la API, consulte BatchPutMessage en la Referencia de comandos de la AWS CLI.

`batch-update-detector`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-update-detector`.

AWS CLI

Para actualizar un detector (instancia)

El siguiente ejemplo de `batch-update-detector` actualiza el estado, los valores de las variables y la configuración del temporizador de uno o más detectores (instancias) de un modelo de detector específico.

```
aws iotevents-data batch-update-detector \
    --cli-input-json file://budFulton-A32.json
```

Contenido de `budFulton-A32.json`:

```
{
    "detectors": [
        {
            "messageId": "00001",
            "detectorModelName": "motorDetectorModel",
            "keyValue": "Fulton-A32",
            "state": {
                "stateName": "Normal",
                "variables": [
                    {
```

```
                        "name": "pressureThresholdBreached",
                        "value": "0"
                    }
                ],
                "timers": [
                ]
            }
        }
    ]
}
```

Salida:

```
{
    "batchUpdateDetectorErrorEntries": []
}
```

Para obtener más información, consulte BatchUpdateDetector en la Guía para desarrolladores de AWS IoT*.

- Para obtener detalles sobre la API, consulte BatchUpdateDetector en la Referencia de comandos de la AWS CLI.

`create-detector-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-detector-model`.

AWS CLI

Para crear un modelo de detector

En el siguiente ejemplo de `create-detector-model`, se muestra cómo crear un modelo.

```
aws iotevents create-detector-model \
    --cli-input-json file://motorDetectorModel.json
```

Contenido de `motorDetectorModel.json`:

```
{
    "detectorModelName": "motorDetectorModel",
    "detectorModelDefinition": {
        "states": [
```

```
            {
                "stateName": "Normal",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "init",
                            "condition": "true",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "pressureThresholdBreached",
                                        "value": "0"
                                    }
                                }
                            ]
                        }
                    ]
                },
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "Overpressurized",
                            "condition": "$input.PressureInput.sensorData.pressure
&gt; 70",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "pressureThresholdBreached",
                                        "value":
"$variable.pressureThresholdBreached + 3"
                                    }
                                }
                            ],
                            "nextState": "Dangerous"
                        }
                    ]
                }
            },
            {
                "stateName": "Dangerous",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "Pressure Threshold Breached",
```

```
                            "condition": "$variable.pressureThresholdBreached &gt;
 1",
                            "actions": [
                                {
                                    "sns": {
                                        "targetArn": "arn:aws:sns:us-
east-1:123456789012:underPressureAction"
                                    }
                                }
                            ]
                        }
                    ]
                },
                "onInput": {
                    "events": [
                        {
                            "eventName": "Overpressurized",
                            "condition": "$input.PressureInput.sensorData.pressure
 &gt; 70",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "pressureThresholdBreached",
                                        "value": "3"
                                    }
                                }
                            ]
                        },
                        {
                            "eventName": "Pressure Okay",
                            "condition": "$input.PressureInput.sensorData.pressure
 &lt;= 70",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "pressureThresholdBreached",
                                        "value":
 "$variable.pressureThresholdBreached - 1"
                                    }
                                }
                            ]
                        }
                    ],
                    "transitionEvents": [
```

```
                        {
                            "eventName": "BackToNormal",
                            "condition": "$input.PressureInput.sensorData.pressure
 &lt;= 70 &amp;&amp; $variable.pressureThresholdBreached &lt;= 1",
                            "nextState": "Normal"
                        }
                    ]
                },
                "onExit": {
                    "events": [
                        {
                            "eventName": "Normal Pressure Restored",
                            "condition": "true",
                            "actions": [
                                {
                                    "sns": {
                                        "targetArn": "arn:aws:sns:us-
east-1:123456789012:pressureClearedAction"
                                    }
                                }
                            ]
                        }
                    ]
                }
            }
        ],
        "initialStateName": "Normal"
    },
    "key": "motorid",
    "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole"
}
```

Salida:

```
{
    "detectorModelConfiguration": {
        "status": "ACTIVATING",
        "lastUpdateTime": 1560796816.077,
        "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
        "creationTime": 1560796816.077,
        "detectorModelArn": "arn:aws:iotevents:us-west-2:123456789012:detectorModel/
motorDetectorModel",
        "key": "motorid",
```

```
        "detectorModelName": "motorDetectorModel",
        "detectorModelVersion": "1"
    }
}
```

Para obtener más información, consulte CreateDetectorModel en la Guía para desarrolladores de AWS IoT Events*.

- Para obtener más información sobre la API, consulte CreateDetectorModel en la Referencia de comandos de la AWS CLI.

`create-input`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-input`.

AWS CLI

Para crear una entrada

En el siguiente ejemplo de `create-input`, se crea una entrada.

```
aws iotevents create-input \
    --cli-input-json file://pressureInput.json
```

Contenido de `pressureInput.json`:

```
{
    "inputName": "PressureInput",
    "inputDescription": "Pressure readings from a motor",
    "inputDefinition": {
        "attributes": [
                { "jsonPath": "sensorData.pressure" },
                { "jsonPath": "motorid" }
            ]
    }
}
```

Salida:

```
{
```

```
    "inputConfiguration": {
        "status": "ACTIVE",
        "inputArn": "arn:aws:iotevents:us-west-2:123456789012:input/PressureInput",
        "lastUpdateTime": 1560795312.542,
        "creationTime": 1560795312.542,
        "inputName": "PressureInput",
        "inputDescription": "Pressure readings from a motor"
    }
}
```

Para obtener más información, consulte CreateInput en la Guía para desarrolladores de AWS IoT Events*.

- Para obtener más información sobre la API, consulte CreateInput en la Referencia de comandos de la AWS CLI.

`delete-detector-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-detector-model`.

AWS CLI

Para eliminar un modelo de detector

En el siguiente ejemplo de `delete-detector-model`, se muestra cómo eliminar un modelo de detector. También se eliminan todas las instancias activas del modelo de detector.

```
aws iotevents delete-detector-model \
    --detector-model-name motorDetectorModel*
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteDetectorModel en la Guía para desarrolladores de AWS IoT Events*.

- Para obtener más información sobre la API, consulte DeleteDetectorModel en la Referencia de comandos de la AWS CLI.

`delete-input`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-input`.

AWS CLI

Para eliminar una entrada

En el siguiente ejemplo de `delete-input`, se elimina una entrada.

```
aws iotevents delete-input \
    --input-name PressureInput
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteInput en la Guía para desarrolladores de AWS IoT Events*.

- Para obtener más información sobre la API, consulte DeleteInput en la Referencia de comandos de la AWS CLI.

`describe-detector-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-detector-model`.

AWS CLI

Para obtener información de un modelo de detector

En el siguiente ejemplo de `describe-detector-model`, se describe un modelo de detector. Cuando no se especifica el parámetro `version`, el comando devuelve información sobre la versión más reciente.

```
aws iotevents describe-detector-model \
    --detector-model-name motorDetectorModel
```

Salida:

```
{
    "detectorModel": {
        "detectorModelConfiguration": {
            "status": "ACTIVE",
            "lastUpdateTime": 1560796816.077,
            "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
            "creationTime": 1560796816.077,
            "detectorModelArn": "arn:aws:iotevents:us-
west-2:123456789012:detectorModel/motorDetectorModel",
```

```
            "key": "motorid",
            "detectorModelName": "motorDetectorModel",
            "detectorModelVersion": "1"
        },
        "detectorModelDefinition": {
            "states": [
                {
                    "onInput": {
                        "transitionEvents": [
                            {
                                "eventName": "Overpressurized",
                                "actions": [
                                    {
                                        "setVariable": {
                                            "variableName":
"pressureThresholdBreached",
                                            "value":
"$variable.pressureThresholdBreached + 3"
                                        }
                                    }
                                ],
                                "condition":
"$input.PressureInput.sensorData.pressure > 70",
                                "nextState": "Dangerous"
                            }
                        ],
                        "events": []
                    },
                    "stateName": "Normal",
                    "onEnter": {
                        "events": [
                            {
                                "eventName": "init",
                                "actions": [
                                    {
                                        "setVariable": {
                                            "variableName":
"pressureThresholdBreached",
                                            "value": "0"
                                        }
                                    }
                                ],
                                "condition": "true"
                            }
```

```
                    ]
                },
                "onExit": {
                    "events": []
                }
            },
            {
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "BackToNormal",
                            "actions": [],
                            "condition":
"$input.PressureInput.sensorData.pressure <= 70 &&
$variable.pressureThresholdBreached <= 1",
                            "nextState": "Normal"
                        }
                    ],
                    "events": [
                        {
                            "eventName": "Overpressurized",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName":
"pressureThresholdBreached",
                                        "value": "3"
                                    }
                                }
                            ],
                            "condition":
"$input.PressureInput.sensorData.pressure > 70"
                        },
                        {
                            "eventName": "Pressure Okay",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName":
"pressureThresholdBreached",
                                        "value":
"$variable.pressureThresholdBreached - 1"
                                    }
                                }
```

```
                                ],
                                "condition":
 "$input.PressureInput.sensorData.pressure <= 70"
                            }
                        ]
                    },
                    "stateName": "Dangerous",
                    "onEnter": {
                        "events": [
                            {
                                "eventName": "Pressure Threshold Breached",
                                "actions": [
                                    {
                                        "sns": {
                                            "targetArn": "arn:aws:sns:us-
east-1:123456789012:underPressureAction"
                                        }
                                    }
                                ],
                                "condition": "$variable.pressureThresholdBreached >
 1"
                            }
                        ]
                    },
                    "onExit": {
                        "events": [
                            {
                                "eventName": "Normal Pressure Restored",
                                "actions": [
                                    {
                                        "sns": {
                                            "targetArn": "arn:aws:sns:us-
east-1:123456789012:pressureClearedAction"
                                        }
                                    }
                                ],
                                "condition": "true"
                            }
                        ]
                    }
                }
            ],
            "initialStateName": "Normal"
        }
```

```
    }
}
```

Para obtener más información, consulte DescribeDetectorModel en la Guía para desarrolladores de AWS IoT Events*.

- Para obtener más información sobre la API, consulte DescribeDetectorModel en la Referencia de comandos de la AWS CLI.

`describe-detector`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-detector`.

AWS CLI

Para obtener información sobre un detector (instancia)

El siguiente ejemplo de `describe-detector` devuelve información acerca del detector especificado (instancia).

```
aws iotevents-data describe-detector \
    --detector-model-name motorDetectorModel \
    --key-value "Fulton-A32"
```

Salida:

```
{
    "detector": {
        "lastUpdateTime": 1560797852.776,
        "creationTime": 1560797852.775,
        "state": {
            "variables": [
                {
                    "name": "pressureThresholdBreached",
                    "value": "3"
                }
            ],
            "stateName": "Dangerous",
            "timers": []
        },
        "keyValue": "Fulton-A32",
        "detectorModelName": "motorDetectorModel",
```

```
        "detectorModelVersion": "1"
    }
}
```

Para obtener más información, consulte DescribeDetector en la Guía para desarrolladores de AWS IoT Events*.

- Para obtener más información sobre la API, consulte DescribeDetector en la Referencia de comandos de la AWS CLI.

`describe-input`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-input`.

AWS CLI

Para obtener información acerca de una entrada

En el siguiente ejemplo de `describe-input`, se recuperan los detalles de una entrada.

```
aws iotevents describe-input \
    --input-name PressureInput
```

Salida:

```
{
    "input": {
        "inputConfiguration": {
            "status": "ACTIVE",
            "inputArn": "arn:aws:iotevents:us-west-2:123456789012:input/
PressureInput",
            "lastUpdateTime": 1560795312.542,
            "creationTime": 1560795312.542,
            "inputName": "PressureInput",
            "inputDescription": "Pressure readings from a motor"
        },
        "inputDefinition": {
            "attributes": [
                {
                    "jsonPath": "sensorData.pressure"
                },
                {
```

```
                    "jsonPath": "motorid"
                }
            ]
        }
    }
}
```

Para obtener más información, consulte DescribeInput en la Guía para desarrolladores de AWS IoT Events*.

- Para obtener más información sobre la API, consulte DescribeInput en la Referencia de comandos de la AWS CLI.

`describe-logging-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-logging-options`.

AWS CLI

Para obtener información sobre la configuración de registro

El siguiente ejemplo de `describe-logging-options` recupera las opciones de registro de AWS IoT Events actuales.

```
aws iotevents describe-logging-options
```

Salida:

```
{
    "loggingOptions": {
        "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
        "enabled": false,
        "level": "ERROR"
    }
}
```

Para obtener más información, consulte DescribeLoggingOptions en la Guía para desarrolladores de AWS IoT Events*.

- Para obtener más información sobre la API, consulte DescribeLoggingOptions en la Referencia de comandos de la AWS CLI.

`list-detector-model-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-detector-model-versions`.

AWS CLI

Para obtener información acerca de las versiones de un modelo de detector

En el siguiente ejemplo de `list-detector-model-versions`, se muestra una lista de todas las versiones de un modelo de detector. Solo se devuelven los metadatos asociados a cada versión de modelo de detector.

```
aws iotevents list-detector-model-versions \
    --detector-model-name motorDetectorModel
```

Salida:

```
{
    "detectorModelVersionSummaries": [
        {
            "status": "ACTIVE",
            "lastUpdateTime": 1560796816.077,
            "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
            "creationTime": 1560796816.077,
            "detectorModelArn": "arn:aws:iotevents:us-
west-2:123456789012:detectorModel/motorDetectorModel",
            "detectorModelName": "motorDetectorModel",
            "detectorModelVersion": "1"
        }
    ]
}
```

Para obtener más información, consulte ListDetectorModelVersions en la Guía para desarrolladores de AWS IoT Events*.

- Para obtener más información sobre la API, consulte ListDetectorModelVersions en la Referencia de comandos de la AWS CLI.

`list-detector-models`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-detector-models`.

AWS CLI

Para obtener una lista de los modelos de detector

En el siguiente ejemplo de `list-detector-models`, se muestra una lista de los modelos de detector que ha creado. Solo se devuelven los metadatos asociados a cada modelo de detector.

```
aws iotevents list-detector-models
```

Salida:

```
{
    "detectorModelSummaries": [
        {
            "detectorModelName": "motorDetectorModel",
            "creationTime": 1552072424.212
            "detectorModelDescription": "Detect overpressure in a motor."
        }
    ]
}
```

Para obtener más información, consulte ListDetectorModels en la Guía para desarrolladores de AWS IoT Events*.

- Para obtener más información sobre la API, consulte ListDetectorModels en la Referencia de comandos de la AWS CLI.

`list-detectors`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-detectors`.

AWS CLI

Para obtener una lista de detectores para un modelo de detector

En el siguiente ejemplo de `list-detectors`, se muestra una lista de los detectores (las instancias de un modelo de detector).

```
aws iotevents-data list-detectors \
    --detector-model-name motorDetectorModel
```

Salida:

```
{
    "detectorSummaries": [
        {
            "lastUpdateTime": 1558129925.2,
            "creationTime": 1552073155.527,
            "state": {
                "stateName": "Normal"
            },
            "keyValue": "Fulton-A32",
            "detectorModelName": "motorDetectorModel",
            "detectorModelVersion": "1"
        }
    ]
}
```

Para obtener más información, consulte ListDetectors en la Guía para desarrolladores de AWS IoT Events*.

- Para obtener más información sobre la API, consulte ListDetectors en la Referencia de comandos de la AWS CLI.

`list-inputs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-inputs`.

AWS CLI

Para enumerar las entradas

En el siguiente ejemplo de `list-inputs`, se enumeran las entradas que ha creado.

```
aws iotevents list-inputs
```

Salida:

```
{
    "status": "ACTIVE",
    "inputArn": "arn:aws:iotevents:us-west-2:123456789012:input/PressureInput",
    "lastUpdateTime": 1551742986.768,
    "creationTime": 1551742986.768,
    "inputName": "PressureInput",
    "inputDescription": "Pressure readings from a motor"
```

```
}
```

Para obtener más información, consulte ListInputs en la Guía para desarrolladores de AWS IoT Events*.

- Para obtener información sobre la API, consulte ListInputs en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas asignadas a un recurso

El siguiente ejemplo de `list-tags-for-resource` es una lista las etiquetas (metadatos) que ha asignado al recurso.

```
aws iotevents list-tags-for-resource \
    --resource-arn "arn:aws:iotevents:us-west-2:123456789012:input/PressureInput"
```

Salida:

```
{
    "tags": [
        {
            "value": "motor",
            "key": "deviceType"
        }
    ]
}
```

Para obtener más información, consulte ListTagsForResource en la Guía para desarrolladores de AWS IoT Events*.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-logging-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-logging-options`.

AWS CLI

Para configurar las opciones de registro

En el siguiente ejemplo de `list-tags-for-resource`, se definen o actualizan las opciones de registro de AWS IoT Events actuales. Si actualiza el valor de cualquier campo `loggingOptions`, los cambios tardarán hasta un minuto en surtir efecto. Por otra parte, si cambia la política asociada al rol que ha especificado en el campo `roleArn` (por ejemplo, para corregir una política no válida), el cambio tardará hasta cinco minutos en surtir efecto.

```
aws iotevents put-logging-options \
    --cli-input-json file://logging-options.json
```

Contenido de `logging-options.json`:

```
{
    "loggingOptions": {
        "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
        "level": "DEBUG",
        "enabled": true,
        "detectorDebugOptions": [
            {
                "detectorModelName": "motorDetectorModel",
                "keyValue": "Fulton-A32"
            }
        ]
    }
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte PutLoggingOptions en la Guía para desarrolladores de AWS IoT Events*.

- Para obtener detalles sobre la API, consulte PutLoggingOptions en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para agregar etiquetas a un recurso

En el siguiente ejemplo de `tag-resource`, se agregan o modifican las etiquetas del recurso especificado. Las etiquetas son metadatos que puede utilizar para administrar un recurso.

```
aws iotevents tag-resource \
    --cli-input-json file://pressureInput.tag.json
```

Contenido de `pressureInput.tag.json`:

```
{
    "resourceArn": "arn:aws:iotevents:us-west-2:123456789012:input/PressureInput",
    "tags": [
        {
            "key": "deviceType",
            "value": "motor"
        }
    ]
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte TagResource en la Guía para desarrolladores de AWS IoT Events*.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar etiquetas de un recurso

En el siguiente ejemplo de `untag-resource`, se eliminan la etiquetas especificadas del recurso.

```
aws iotevents untag-resource \
    --cli-input-json file://pressureInput.untag.json
```

Contenido de `pressureInput.untag.json`:

```
{
    "resourceArn": "arn:aws:iotevents:us-west-2:123456789012:input/PressureInput",
    "tagKeys": [
            "deviceType"
    ]
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte UntagResource en la Guía para desarrolladores de AWS IoT Events*.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-detector-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-detector-model`.

AWS CLI

Para actualizar un modelo de detector

En el siguiente ejemplo de `update-detector-model`, se muestra cómo actualizar un modelo de detector. Los detectores (instancias) generados por la versión anterior se eliminan y, a continuación, se vuelven a crear a medida que llegan nuevas entradas.

```
aws iotevents update-detector-model \
    --cli-input-json file://motorDetectorModel.update.json
```

Contenido de motorDetectorModel.update.json:

```
{
  "detectorModelName": "motorDetectorModel",
  "detectorModelDefinition": {
    "states": [
      {
        "stateName": "Normal",
        "onEnter": {
          "events": [
```

```
            {
              "eventName": "init",
              "condition": "true",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "pressureThresholdBreached",
                    "value": "0"
                  }
                }
              ]
            }
          ]
        },
        "onInput": {
          "transitionEvents": [
            {
              "eventName": "Overpressurized",
              "condition": "$input.PressureInput.sensorData.pressure > 70",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "pressureThresholdBreached",
                    "value": "$variable.pressureThresholdBreached + 3"
                  }
                }
              ],
              "nextState": "Dangerous"
            }
          ]
        }
      },
      {
        "stateName": "Dangerous",
        "onEnter": {
          "events": [
            {
              "eventName": "Pressure Threshold Breached",
              "condition": "$variable.pressureThresholdBreached > 1",
              "actions": [
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-
east-1:123456789012:underPressureAction"
```

```
                }
              }
            ]
          }
        ]
      },
      "onInput": {
        "events": [
          {
            "eventName": "Overpressurized",
            "condition": "$input.PressureInput.sensorData.pressure > 70",
            "actions": [
              {
                "setVariable": {
                  "variableName": "pressureThresholdBreached",
                  "value": "3"
                }
              }
            ]
          },
          {
            "eventName": "Pressure Okay",
            "condition": "$input.PressureInput.sensorData.pressure <= 70",
            "actions": [
              {
                "setVariable": {
                  "variableName": "pressureThresholdBreached",
                  "value": "$variable.pressureThresholdBreached - 1"
                }
              }
            ]
          }
        ],
        "transitionEvents": [
          {
            "eventName": "BackToNormal",
            "condition": "$input.PressureInput.sensorData.pressure <= 70 &&
$variable.pressureThresholdBreached <= 1",
            "nextState": "Normal"
          }
        ]
      },
      "onExit": {
        "events": [
```

```
            {
              "eventName": "Normal Pressure Restored",
              "condition": "true",
              "actions": [
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-
east-1:123456789012:pressureClearedAction"
                  }
                }
              ]
            }
          ]
        }
      }
    ],
    "initialStateName": "Normal"
  },
  "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole"
}
```

Salida:

```
{
    "detectorModelConfiguration": {
        "status": "ACTIVATING",
        "lastUpdateTime": 1560799387.719,
        "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
        "creationTime": 1560799387.719,
        "detectorModelArn": "arn:aws:iotevents:us-west-2:123456789012:detectorModel/
motorDetectorModel",
        "key": "motorid",
        "detectorModelName": "motorDetectorModel",
        "detectorModelVersion": "2"
    }
}
```

Para obtener más información, consulte UpdateDetectorModel en la Guía para desarrolladores de AWS IoT Events*.

- Para obtener más información sobre la API, consulte UpdateDetectorModel en la Referencia de comandos de la AWS CLI.

update-input

En el siguiente ejemplo de código, se muestra cómo utilizar `update-input`.

AWS CLI

Para actualizar una entrada

En el siguiente ejemplo de `update-input`, se muestra cómo se actualiza una entrada.

```
aws iotevents update-input \
    --cli-input-json file://pressureInput.json
```

Contenido de `pressureInput.json`:

```
{
    "inputName": "PressureInput",
    "inputDescription": "Pressure readings from a motor",
    "inputDefinition": {
        "attributes": [
            { "jsonPath": "sensorData.pressure" },
            { "jsonPath": "motorid" }
        ]
    }
}
```

Salida:

```
{
    "inputConfiguration": {
        "status": "ACTIVE",
        "inputArn": "arn:aws:iotevents:us-west-2:123456789012:input/PressureInput",
        "lastUpdateTime": 1560795976.458,
        "creationTime": 1560795312.542,
        "inputName": "PressureInput",
        "inputDescription": "Pressure readings from a motor"
    }
}
```

Para obtener más información, consulte UpdateInput en la Guía para desarrolladores de AWS IoT Events*.

- Para obtener más información sobre la API, consulte UpdateInput en la Referencia de comandos de la AWS CLI.

AWS IoT Greengrass Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS IoT Greengrass.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-role-to-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-role-to-group`.

AWS CLI

Para asociar un rol con un grupo de Greengrass

En el siguiente ejemplo de `associate-role-to-group`, se asocia el rol de IAM especificado a un grupo de Greengrass. Las funciones y conectores de Lambda locales utilizan el rol de grupo para acceder a los servicios de AWS. Por ejemplo, su rol de grupo puede conceder los permisos necesarios para la integración de Registros de CloudWatch.

```
aws greengrass associate-role-to-group \
    --group-id 2494ee3f-7f8a-4e92-a78b-d205f808b84b \
    --role-arn arn:aws:iam::123456789012:role/GG-Group-Role
```

Salida:

```
{
    "AssociatedAt": "2019-09-10T20:03:30Z"
}
```

Para obtener más información, consulte Configuración del rol del grupo en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte AssociateRoleToGroup en la Referencia de comandos de la AWS CLI.

`associate-service-role-to-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-service-role-to-account`.

AWS CLI

Para asociar un rol de servicio a su cuenta de AWS

En el siguiente ejemplo de `associate-service-role-to-account`, se asocia un rol de servicio de IAM, especificado por su ARN, con AWS IoT Greengrass en su cuenta de AWS. Debe haber creado previamente el rol de servicio en IAM y debe asociarle un documento de política que permita a AWS IoT Greengrass asumir este rol.

```
aws greengrass associate-service-role-to-account \
    --role-arn "arn:aws:iam::123456789012:role/service-role/Greengrass_ServiceRole"
```

Salida:

```
{
    "AssociatedAt": "2019-06-25T18:12:45Z"
}
```

Para obtener más información, consulte Greengrass service role en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte AssociateServiceRoleToAccount en la Referencia de comandos de la AWS CLI.

`create-connector-definition-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-connector-definition-version`.

AWS CLI

Para crear una versión de definición de conector

En el siguiente ejemplo de `create-connector-definition-version`, se crea una versión de definición de conector y se asocia a la definición de conector especificada. Todos los conectores de una versión definen valores para sus parámetros.

```
aws greengrass create-connector-definition-version \
    --connector-definition-id "55d0052b-0d7d-44d6-b56f-21867215e118" \
    --connectors "[{\"Id\": \"MyTwilioNotificationsConnector\",
 \"ConnectorArn\": \"arn:aws:greengrass:us-west-2::/connectors/
TwilioNotifications/versions/2\", \"Parameters\": {\"TWILIO_ACCOUNT_SID
\": \"AC1a8d4204890840d7fc482aab38090d57\", \"TwilioAuthTokenSecretArn\":
 \"arn:aws:secretsmanager:us-west-2:123456789012:secret:greengrass-TwilioAuthToken-
ntSlp6\", \"TwilioAuthTokenSecretArn-ResourceId\": \"TwilioAuthToken\",
 \"DefaultFromPhoneNumber\": \"4254492999\"}}]"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
connectors/55d0052b-0d7d-44d6-b56f-21867215e118/versions/33f709a0-c825-49cb-9eea-
dc8964fbd635",
    "CreationTimestamp": "2019-06-24T20:46:30.134Z",
    "Id": "55d0052b-0d7d-44d6-b56f-21867215e118",
    "Version": "33f709a0-c825-49cb-9eea-dc8964fbd635"
}
```

- Para obtener información sobre la API, consulte CreateConnectorDefinitionVersion en la Referencia de comandos de la AWS CLI.

`create-connector-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-connector-definition`.

AWS CLI

Para crear una definición de conector

En el siguiente ejemplo de `create-connector-definition`, se crea una definición de conector y una versión inicial de la definición de conector. La versión inicial contiene un conector. Todos los conectores de una versión definen valores para sus parámetros.

```
aws greengrass create-connector-definition \
    --name MySNSConnector \
    --initial-version "{\"Connectors\": [{\"Id\":\"MySNSConnector\",\"ConnectorArn
\":\"arn:aws:greengrass:us-west-2::/connectors/SNS/versions/1\",\"Parameters\":
 {\"DefaultSNSArn\":\"arn:aws:sns:us-west-2:123456789012:GGConnectorTopic\"}}]}"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
connectors/b5c4ebfd-f672-49a3-83cd-31c7216a7bb8",
    "CreationTimestamp": "2019-06-19T19:30:01.300Z",
    "Id": "b5c4ebfd-f672-49a3-83cd-31c7216a7bb8",
    "LastUpdatedTimestamp": "2019-06-19T19:30:01.300Z",
    "LatestVersion": "63c57963-c7c2-4a26-a7e2-7bf478ea2623",
    "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/connectors/b5c4ebfd-f672-49a3-83cd-31c7216a7bb8/versions/63c57963-
c7c2-4a26-a7e2-7bf478ea2623",
    "Name": "MySNSConnector"
}
```

Para obtener más información, consulte Introducción a los conectores de Greengrass (CLI) en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte CreateConnectorDefinition en la Referencia de comandos de la AWS CLI.

`create-core-definition-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-core-definition-version`.

AWS CLI

Para crear una versión de definición de núcleo

En el siguiente ejemplo de `create-core-definition-version`, se crea una versión de definición de núcleo y se asocia a la definición de núcleo especificada. La versión solo puede contener un núcleo. Para poder crear un núcleo, debe crear y aprovisionar el elemento de AWS IoT correspondiente. Este proceso incluye los siguientes comandos de `iot`, que devuelven los valores de `ThingArn` y `CertificateArn` necesarios para el comando `create-core-definition-version`.

Cree el elemento de AWS IoT que corresponda al dispositivo de núcleo:

```
aws iot create-thing \
    --thing-name "MyCoreDevice"
```

Salida:

```
{
    "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MyCoreDevice",
    "thingName": "MyCoreDevice",
    "thingId": "cb419a19-9099-4515-9cec-e9b0e760608a"
}
```

Cree las claves públicas y privadas, así como el certificado del dispositivo de núcleo para el elemento. En este ejemplo, se usa el comando `create-keys-and-certificate` y se requieren permisos de escritura para el directorio actual. También puede utilizar el comando `create-certificate-from-csr`.

```
aws iot create-keys-and-certificate \
    --set-as-active \
    --certificate-pem-outfile "myCore.cert.pem" \
    --public-key-outfile "myCore.public.key" \
    --private-key-outfile "myCore.private.key"
```

Salida:

```
{
    "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/123a15ec415668c2349a76170b64ac0878231c1e21ec83c10e92a1EXAMPLExyz",
    "certificatePem": "-----BEGIN CERTIFICATE-----
\nMIIDWTCAkGgAwIBATgIUCgq6EGqou6zFqWgIZRndgQEFW+gwDQYJKoZIhvc...KdGewQS\n-----END
 CERTIFICATE-----\n",
    "keyPair": {
```

```
        "PublicKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBzrqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqKpRgnn6yq26U3y...wIDAQAB\n-----END
 PUBLIC KEY-----\n",
        "PrivateKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIABAKCAQEAqKpRgnn6yq26U3yt5YFZquyukfRjbMXDcNOK4rMCxDR...fvY4+te\n-----END
 RSA PRIVATE KEY-----\n"
    },
    "certificateId":
 "123a15ec415668c2349a76170b64ac0878231c1e21ec83c10e92a1EXAMPLExyz"
}
```

Cree una política de AWS IoT que permita las acciones de `iot` y `greengrass`. Para simplificar, la siguiente política permite acciones en todos los recursos, pero su política debería ser más restrictiva.

```
aws iot create-policy \
    --policy-name "Core_Devices" \
    --policy-document "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Action\":[\"iot:Publish\",\"iot:Subscribe\",\"iot:Connect
\",\"iot:Receive\"],\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":
[\"iot:GetThingShadow\",\"iot:UpdateThingShadow\",\"iot:DeleteThingShadow\"],
\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":[\"greengrass:*\"],\"Resource
\":[\"*\"]}]}"
```

Salida:

```
{
    "policyName": "Core_Devices",
    "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/Core_Devices",
    "policyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Action\":[\"iot:Publish\",\"iot:Subscribe\",\"iot:Connect
\",\"iot:Receive\"],\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":
[\"iot:GetThingShadow\",\"iot:UpdateThingShadow\",\"iot:DeleteThingShadow\"],
\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":[\"greengrass:*\"],\"Resource
\":[\"*\"]}]}",
    "policyVersionId": "1"
}
```

Asocie la política al certificado:

```
aws iot attach-policy \
```

```
    --policy-name "Core_Devices" \
    --target "arn:aws:iot:us-
west-2:123456789012:cert/123a15ec415668c2349a76170b64ac0878231c1e21ec83c10e92a1EXAMPLExyz"
```

Este comando no genera ninguna salida.

Asocie el elemento al certificado:

```
aws iot attach-thing-principal \
    --thing-name "MyCoreDevice" \
    --principal "arn:aws:iot:us-
west-2:123456789012:cert/123a15ec415668c2349a76170b64ac0878231c1e21ec83c10e92a1EXAMPLExyz"
```

Este comando no genera ninguna salida.

Cree la versión de la definición de núcleo:

```
aws greengrass create-core-definition-version \
    --core-definition-id "582efe12-b05a-409e-9a24-a2ba1bcc4a12" \
    --cores "[{\"Id\":\"MyCoreDevice\",\"ThingArn\":\"arn:aws:iot:us-
west-2:123456789012:thing/MyCoreDevice\",\"CertificateArn\":\"arn:aws:iot:us-
west-2:123456789012:cert/123a15ec415668c2349a76170b64ac0878231c1e21ec83c10e92a1EXAMPLExyz
\",\"SyncShadow\":true}]"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
cores/582efe12-b05a-409e-9a24-a2ba1bcc4a12/versions/3fdc1190-2ce5-44de-b98b-
eec8f9571014",
    "Version": "3fdc1190-2ce5-44de-b98b-eec8f9571014",
    "CreationTimestamp": "2019-09-18T00:15:09.838Z",
    "Id": "582efe12-b05a-409e-9a24-a2ba1bcc4a12"
}
```

Para obtener más información, consulte Configuración del software AWS IoT Greengrass Core en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte CreateCoreDefinitionVersion en la Referencia de comandos de la AWS CLI.

`create-core-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-core-definition`.

AWS CLI

Ejemplo 1: creación de una definición de núcleo vacía

En el siguiente ejemplo de `create-core-definition`, se crea una definición de núcleo de Greengrass vacía (sin versión inicial). Para poder utilizar el núcleo, debe utilizar el comando `create-core-definition-version` para proporcionar los demás parámetros del núcleo.

```
aws greengrass create-core-definition \
    --name cliGroup_Core
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/cores/
b5c08008-54cb-44bd-9eec-c121b04283b5",
    "CreationTimestamp": "2019-06-25T18:23:22.106Z",
    "Id": "b5c08008-54cb-44bd-9eec-c121b04283b5",
    "LastUpdatedTimestamp": "2019-06-25T18:23:22.106Z",
    "Name": "cliGroup_Core"
}
```

Ejemplo 2: creación de una definición de núcleo con una versión inicial

En el siguiente ejemplo de `create-core-definition`, se crea una definición de núcleo que especifica una versión de definición de núcleo inicial. La versión solo puede contener un núcleo. Para poder crear un núcleo, debe crear y aprovisionar el elemento de AWS IoT correspondiente. Este proceso incluye los siguientes comandos de `iot`, que devuelven los valores de `ThingArn` y `CertificateArn` necesarios para el comando `create-core-definition`.

Cree el elemento de AWS IoT que corresponda al dispositivo de núcleo:

```
aws iot create-thing \
    --thing-name "MyCoreDevice"
```

Salida:

```
{
```

```
    "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MyCoreDevice",
    "thingName": "MyCoreDevice",
    "thingId": "cb419a19-9099-4515-9cec-e9b0e760608a"
}
```

Cree las claves públicas y privadas, así como el certificado del dispositivo de núcleo para el elemento. En este ejemplo, se usa el comando `create-keys-and-certificate` y se requieren permisos de escritura para el directorio actual. También puede utilizar el comando `create-certificate-from-csr`.

```
aws iot create-keys-and-certificate \
    --set-as-active \
    --certificate-pem-outfile "myCore.cert.pem" \
    --public-key-outfile "myCore.public.key" \
    --private-key-outfile "myCore.private.key"
```

Salida:

```
{
    "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/123a15ec415668c2349a76170b64ac0878231c1e21ec83c10e92a1EXAMPLExyz",
    "certificatePem": "-----BEGIN CERTIFICATE-----
\nMIIDWTCAkGgAwIBATgIUCgq6EGqou6zFqWgIZRndgQEFW+gwDQYJKoZIhvc...KdGewQS\n-----END
 CERTIFICATE-----\n",
    "keyPair": {
        "PublicKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBzrqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqKpRgnn6yq26U3y...wIDAQAB\n-----END
 PUBLIC KEY-----\n",
        "PrivateKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIABAKCAQEAqKpRgnn6yq26U3yt5YFZquyukfRjbMXDcNOK4rMCxDR...fvY4+te\n-----END
 RSA PRIVATE KEY-----\n"
    },
    "certificateId":
 "123a15ec415668c2349a76170b64ac0878231c1e21ec83c10e92a1EXAMPLExyz"
}
```

Cree una política de AWS IoT que permita las acciones de `iot` y `greengrass`. Para simplificar, la siguiente política permite acciones en todos los recursos, pero su política debería ser más restrictiva.

```
aws iot create-policy \
```

```
    --policy-name "Core_Devices" \
    --policy-document "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Action\":[\"iot:Publish\",\"iot:Subscribe\",\"iot:Connect
\",\"iot:Receive\"],\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":
[\"iot:GetThingShadow\",\"iot:UpdateThingShadow\",\"iot:DeleteThingShadow\"],
\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":[\"greengrass:*\"],\"Resource
\":[\"*\"]}]}"
```

Salida:

```
{
    "policyName": "Core_Devices",
    "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/Core_Devices",
    "policyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Action\":[\"iot:Publish\",\"iot:Subscribe\",\"iot:Connect
\",\"iot:Receive\"],\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":
[\"iot:GetThingShadow\",\"iot:UpdateThingShadow\",\"iot:DeleteThingShadow\"],
\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":[\"greengrass:*\"],\"Resource
\":[\"*\"]}]}",
    "policyVersionId": "1"
}
```

Asocie la política al certificado:

```
aws iot attach-policy \
    --policy-name "Core_Devices" \
    --target "arn:aws:iot:us-
west-2:123456789012:cert/123a15ec415668c2349a76170b64ac0878231c1e21ec83c10e92a1EXAMPLExyz"
```

Este comando no genera ninguna salida.

Asocie el elemento al certificado:

```
aws iot attach-thing-principal \
    --thing-name "MyCoreDevice" \
    --principal "arn:aws:iot:us-
west-2:123456789012:cert/123a15ec415668c2349a76170b64ac0878231c1e21ec83c10e92a1EXAMPLExyz"
```

Este comando no genera ninguna salida.

Cree la definición del núcleo:

```
aws greengrass create-core-definition \
    --name "MyCores" \
    --initial-version "{\"Cores\":[{\"Id\":\"MyCoreDevice\",\"ThingArn\":
\"arn:aws:iot:us-west-2:123456789012:thing/MyCoreDevice\",\"CertificateArn\":
\"arn:aws:iot:us-
west-2:123456789012:cert/123a15ec415668c2349a76170b64ac0878231c1e21ec83c10e92a1EXAMPLExyz
\",\"SyncShadow\":true}]}"
```

Salida:

```
{
    "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/cores/582efe12-b05a-409e-9a24-a2ba1bcc4a12/versions/
cc87b5b3-8f4b-465d-944c-1d6de5dbfcdb",
    "Name": "MyCores",
    "LastUpdatedTimestamp": "2019-09-18T00:11:06.197Z",
    "LatestVersion": "cc87b5b3-8f4b-465d-944c-1d6de5dbfcdb",
    "CreationTimestamp": "2019-09-18T00:11:06.197Z",
    "Id": "582efe12-b05a-409e-9a24-a2ba1bcc4a12",
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
cores/582efe12-b05a-409e-9a24-a2ba1bcc4a12"
}
```

Para obtener más información, consulte Configuración del software AWS IoT Greengrass Core en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte CreateCoreDefinition en la Referencia de comandos de la AWS CLI.

`create-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-deployment`.

AWS CLI

Para crear una implementación para una versión de un grupo de Greengrass

En el siguiente ejemplo de `create-deployment`, se implementa la versión especificada de un grupo de Greengrass.

```
aws greengrass create-deployment \
    --deployment-type NewDeployment \
```

```
    --group-id "ce2e7d01-3240-4c24-b8e6-f6f6e7a9eeca" \
    --group-version-id "dc40c1e9-e8c8-4d28-a84d-a9cad5f599c9"
```

Salida:

```
{
    "DeploymentArn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
groups/ce2e7d01-3240-4c24-b8e6-f6f6e7a9eeca/deployments/bfceb608-4e97-45bc-
af5c-460144270308",
    "DeploymentId": "bfceb608-4e97-45bc-af5c-460144270308"
}
```

Para obtener más información, consulte Introducción a los conectores (CLI) en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte CreateDeployment en la Referencia de comandos de la AWS CLI.

`create-device-definition-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-device-definition-version`.

AWS CLI

Para crear una versión de definición de dispositivos

En el siguiente ejemplo de `create-device-definition-version`, se crea una versión de definición de dispositivo y se asocia a la definición de dispositivo especificada. La versión define dos dispositivos. Para poder crear un dispositivo de Greengrass, debe crear y aprovisionar primero el elemento de AWS IoT correspondiente. Este proceso incluye los siguientes comandos de `iot` que debe ejecutar para obtener la información necesaria para el comando de Greengrass:

Cree el elemento de AWS IoT que corresponda al dispositivo:

```
aws iot create-thing \
    --thing-name "InteriorTherm"
```

Salida:

```
{
```

```
    "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/InteriorTherm",
    "thingName": "InteriorTherm",
    "thingId": "01d4763c-78a6-46c6-92be-7add080394bf"
}
```

Cree las claves públicas y privadas, así como el certificado del dispositivo para el elemento. En este ejemplo, se usa el comando `create-keys-and-certificate` y se requieren permisos de escritura para el directorio actual. También puede utilizar el comando `create-certificate-from-csr`.

```
aws iot create-keys-and-certificate \
    --set-as-active \
    --certificate-pem-outfile "myDevice.cert.pem" \
    --public-key-outfile "myDevice.public.key" \
    --private-key-outfile "myDevice.private.key"
```

Salida:

```
{
    "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/66a415ec415668c2349a76170b64ac0878231c1e21ec83c10e92a18bd568eb92",
    "certificatePem": "-----BEGIN CERTIFICATE-----
\nMIIDWTCAkGgAwIBATgIUCgq6EGqou6zFqWgIZRndgQEFW+gwDQYJKoZIhvc...KdGewQS\n-----END
 CERTIFICATE-----\n",
    "keyPair": {
        "PublicKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBzrqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqKpRgnn6yq26U3y...wIDAQAB\n-----END
 PUBLIC KEY-----\n",
        "PrivateKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIABAKCAQEAqKpRgnn6yq26U3yt5YFZquyukfRjbMXDcNOK4rMCxDR...fvY4+te\n-----END
 RSA PRIVATE KEY-----\n"
    },
    "certificateId":
 "66a415ec415668c2349a76170b64ac0878231c1e21ec83c10e92a18bd568eb92"
}
```

Cree una política de AWS IoT que permita las acciones de `iot` y `greengrass`. Para simplificar, la siguiente política permite realizar acciones en todos los recursos, pero su política puede ser más restrictiva:

```
aws iot create-policy \
```

```
    --policy-name "GG_Devices" \
    --policy-document "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Action\":[\"iot:Publish\",\"iot:Subscribe\",\"iot:Connect
\",\"iot:Receive\"],\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":
[\"iot:GetThingShadow\",\"iot:UpdateThingShadow\",\"iot:DeleteThingShadow\"],
\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":[\"greengrass:*\"],\"Resource
\":[\"*\"]}]}"
```

Salida:

```
{
    "policyName": "GG_Devices",
    "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/GG_Devices",
    "policyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Action\":[\"iot:Publish\",\"iot:Subscribe\",\"iot:Connect
\",\"iot:Receive\"],\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":
[\"iot:GetThingShadow\",\"iot:UpdateThingShadow\",\"iot:DeleteThingShadow\"],
\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":[\"greengrass:*\"],\"Resource
\":[\"*\"]}]}",
    "policyVersionId": "1"
}
```

Asocie la política al certificado:

```
aws iot attach-policy \
    --policy-name "GG_Devices" \
    --target "arn:aws:iot:us-
west-2:123456789012:cert/66a415ec415668c2349a76170b64ac0878231c1e21ec83c10e92a18bd568eb92"
```

Asociación del elemento al certificado

```
aws iot attach-thing-principal \
    --thing-name "InteriorTherm" \
    --principal "arn:aws:iot:us-
west-2:123456789012:cert/66a415ec415668c2349a76170b64ac0878231c1e21ec83c10e92a18bd568eb92"
```

Después de crear y configurar el elemento de IoT como se muestra arriba, use los valores de `ThingArn` y `CertificateArn` de los primeros dos comandos del siguiente ejemplo.

```
aws greengrass create-device-definition-version \
    --device-definition-id "f9ba083d-5ad4-4534-9f86-026a45df1ccd" \
```

```
    --devices "[{\"Id\":\"InteriorTherm\",\"ThingArn\":\"arn:aws:iot:us-
west-2:123456789012:thing/InteriorTherm\",\"CertificateArn\":\"arn:aws:iot:us-
west-2:123456789012:cert/66a415ec415668c2349a76170b64ac0878231c1e21ec83c10e92a18bd568eb92\",
\"SyncShadow\":true},{\"Id\":\"ExteriorTherm\",\"ThingArn\":\"arn:aws:iot:us-
west-2:123456789012:thing/ExteriorTherm\",\"CertificateArn\":\"arn:aws:iot:us-
west-2:123456789012:cert/6c52ce1b47bde88a637e9ccdd45fe4e4c2c0a75a6866f8f63d980ee22fa51e02\",
\"SyncShadow\":true}]"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/devices/f9ba083d-5ad4-4534-9f86-026a45df1ccd/
versions/83c13984-6fed-447e-84d5-5b8aa45d5f71",
    "Version": "83c13984-6fed-447e-84d5-5b8aa45d5f71",
    "CreationTimestamp": "2019-09-11T00:15:09.838Z",
    "Id": "f9ba083d-5ad4-4534-9f86-026a45df1ccd"
}
```

- Para obtener información sobre la API, consulte CreateDeviceDefinitionVersion en la Referencia de comandos de la AWS CLI.

`create-device-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-device-definition`.

AWS CLI

Para crear una definición de dispositivo

En el siguiente ejemplo de `create-device-definition`, se crea una definición de dispositivo que especifica una versión de definición de dispositivo inicial. La versión inicial define dos dispositivos. Para poder crear un dispositivo de Greengrass, debe crear y aprovisionar primero el elemento de AWS IoT correspondiente. Este proceso incluye los siguientes comandos de `iot` que debe ejecutar para obtener la información necesaria para el comando de Greengrass:

Cree el elemento de AWS IoT que corresponda al dispositivo:

```
aws iot create-thing \
    --thing-name "InteriorTherm"
```

Salida:

```
{
    "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/InteriorTherm",
    "thingName": "InteriorTherm",
    "thingId": "01d4763c-78a6-46c6-92be-7add080394bf"
}
```

Cree las claves públicas y privadas, así como el certificado del dispositivo para el elemento. En este ejemplo, se usa el comando `create-keys-and-certificate` y se requieren permisos de escritura para el directorio actual. También puede utilizar el comando `create-certificate-from-csr`.

```
aws iot create-keys-and-certificate \
    --set-as-active \
    --certificate-pem-outfile "myDevice.cert.pem" \
    --public-key-outfile "myDevice.public.key" \
    --private-key-outfile "myDevice.private.key"
```

Salida:

```
{
    "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/66a415ec415668c2349a76170b64ac0878231c1e21ec83c10e92a18bd568eb92",
    "certificatePem": "-----BEGIN CERTIFICATE-----
\nMIIDWTCAkGgAwIBATgIUCgq6EGqou6zFqWgIZRndgQEFW+gwDQYJKoZIhvc...KdGewQS\n-----END
 CERTIFICATE-----\n",
    "keyPair": {
        "PublicKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBzrqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqKpRgnn6yq26U3y...wIDAQAB\n-----END
 PUBLIC KEY-----\n",
        "PrivateKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIABAKCAQEAqKpRgnn6yq26U3yt5YFZquyukfRjbMXDcNOK4rMCxDR...fvY4+te\n-----END
 RSA PRIVATE KEY-----\n"
    },
    "certificateId":
 "66a415ec415668c2349a76170b64ac0878231c1e21ec83c10e92a18bd568eb92"
}
```

Cree una política de AWS IoT que permita las acciones de `iot` y `greengrass`. Para simplificar, la siguiente política permite realizar acciones en todos los recursos, pero su política puede ser más restrictiva:

```
aws iot create-policy \
    --policy-name "GG_Devices" \
    --policy-document "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Action\":[\"iot:Publish\",\"iot:Subscribe\",\"iot:Connect
\",\"iot:Receive\"],\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":
[\"iot:GetThingShadow\",\"iot:UpdateThingShadow\",\"iot:DeleteThingShadow\"],
\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":[\"greengrass:*\"],\"Resource
\":[\"*\"]}]}"
```

Salida:

```
{
    "policyName": "GG_Devices",
    "policyArn": "arn:aws:iot:us-west-2:123456789012:policy/GG_Devices",
    "policyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Action\":[\"iot:Publish\",\"iot:Subscribe\",\"iot:Connect
\",\"iot:Receive\"],\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":
[\"iot:GetThingShadow\",\"iot:UpdateThingShadow\",\"iot:DeleteThingShadow\"],
\"Resource\":[\"*\"]},{\"Effect\":\"Allow\",\"Action\":[\"greengrass:*\"],\"Resource
\":[\"*\"]}]}",
    "policyVersionId": "1"
}
```

Asocie la política al certificado:

```
aws iot attach-policy \
    --policy-name "GG_Devices" \
    --target "arn:aws:iot:us-
west-2:123456789012:cert/66a415ec415668c2349a76170b64ac0878231c1e21ec83c10e92a18bd568eb92"
```

Asociación del elemento al certificado

```
aws iot attach-thing-principal \
    --thing-name "InteriorTherm" \
    --principal "arn:aws:iot:us-
west-2:123456789012:cert/66a415ec415668c2349a76170b64ac0878231c1e21ec83c10e92a18bd568eb92"
```

Después de crear y configurar el elemento de IoT como se muestra arriba, use los valores de `ThingArn` y `CertificateArn` de los primeros dos comandos del siguiente ejemplo.

```
aws greengrass create-device-definition \
    --name "Sensors" \
    --initial-version "{\"Devices\":[{\"Id\":\"InteriorTherm
\",\"ThingArn\":\"arn:aws:iot:us-west-2:123456789012:thing/
InteriorTherm\",\"CertificateArn\":\"arn:aws:iot:us-
west-2:123456789012:cert/66a415ec415668c2349a76170b64ac0878231c1e21ec83c10e92a18bd568eb92\",
\"SyncShadow\":true},{\"Id\":\"ExteriorTherm\",\"ThingArn\":\"arn:aws:iot:us-
west-2:123456789012:thing/ExteriorTherm\",\"CertificateArn\":\"arn:aws:iot:us-
west-2:123456789012:cert/6c52ce1b47bde88a637e9ccdd45fe4e4c2c0a75a6866f8f63d980ee22fa51e02\",
\"SyncShadow\":true}]}"
```

Salida:

```
{
    "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/devices/f9ba083d-5ad4-4534-9f86-026a45df1ccd/
versions/3b5cc510-58c1-44b5-9d98-4ad858ffa795",
    "Name": "Sensors",
    "LastUpdatedTimestamp": "2019-09-11T00:11:06.197Z",
    "LatestVersion": "3b5cc510-58c1-44b5-9d98-4ad858ffa795",
    "CreationTimestamp": "2019-09-11T00:11:06.197Z",
    "Id": "f9ba083d-5ad4-4534-9f86-026a45df1ccd",
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
devices/f9ba083d-5ad4-4534-9f86-026a45df1ccd"
}
```

- Para obtener información sobre la API, consulte CreateDeviceDefinition en la Referencia de comandos de la AWS CLI.

`create-function-definition-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-function-definition-version`.

AWS CLI

Para crear una versión de la definición de función

En el siguiente ejemplo de `create-function-definition-version`, se crea una nueva versión de la definición de función especificada. Esta versión especifica una única función cuyo ID es `Hello-World-function`, permite el acceso al sistema de archivos y especifica un tamaño máximo de memoria y un período de tiempo de espera.

```
aws greengrass create-function-definition-version \
    --cli-input-json "{\"FunctionDefinitionId\": \"e626e8c9-3b8f-4bf3-9cdc-
d26ecdeb9fa3\",\"Functions\": [{\"Id\": \"Hello-World-function\", \"FunctionArn\":
 \""arn:aws:lambda:us-
west-2:123456789012:function:Greengrass_HelloWorld_Counter:gghw-alias"\",
\"FunctionConfiguration\": {\"Environment\": {\"AccessSysfs\": true},\"Executable\":
 \"greengrassHelloWorldCounter.function_handler\",\"MemorySize\": 16000,\"Pinned\":
 false,\"Timeout\": 25}}]}"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/functions/e626e8c9-3b8f-4bf3-9cdc-d26ecdeb9fa3/
versions/74abd1cc-637e-4abe-8684-9a67890f4043",
    "CreationTimestamp": "2019-06-25T22:03:43.376Z",
    "Id": "e626e8c9-3b8f-4bf3-9cdc-d26ecdeb9fa3",
    "Version": "74abd1cc-637e-4abe-8684-9a67890f4043"
}
```

- Para obtener información sobre la API, consulte CreateFunctionDefinitionVersion en la Referencia de comandos de la AWS CLI.

`create-function-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-function-definition`.

AWS CLI

Para crear una definición de función de Lambda

En el siguiente ejemplo de `create-function-definition`, se crea una definición de función de Lambda y una versión inicial al proporcionar una lista de funciones de Lambda (en este caso, una lista con solo una función llamada `TempMonitorFunction`) y sus configuraciones. Para poder crear la definición de función, necesita el ARN de la función de Lambda. Para crear la

función y su alias, utilice los comandos `create-function` y `publish-version` de Lambda. El comando `create-function` de Lambda requiere el ARN del rol de ejecución, aunque AWS IoT Greengrass no utilice ese rol porque los permisos se especifican en el rol de grupo de Greengrass. Puede usar el comando `create-role` de IAM para crear un rol vacío y obtener un ARN para usarlo con `create-function` de Lambda, o usar un rol de ejecución existente.

```
aws greengrass create-function-definition \
    --name MyGreengrassFunctions \
    --initial-version "{\"Functions\": [{\"Id\": \"TempMonitorFunction\",
 \"FunctionArn\": \"arn:aws:lambda:us-
west-2:123456789012:function:TempMonitor:GG_TempMonitor\", \"FunctionConfiguration
\": {\"Executable\": \"temp_monitor.function_handler\", \"MemorySize\": 16000,
\"Timeout\": 5}}]}"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
functions/3b0d0080-87e7-48c6-b182-503ec743a08b",
    "CreationTimestamp": "2019-06-19T22:24:44.585Z",
    "Id": "3b0d0080-87e7-48c6-b182-503ec743a08b",
    "LastUpdatedTimestamp": "2019-06-19T22:24:44.585Z",
    "LatestVersion": "67f918b9-efb4-40b0-b87c-de8c9faf085b",
    "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/functions/3b0d0080-87e7-48c6-b182-503ec743a08b/versions/67f918b9-
efb4-40b0-b87c-de8c9faf085b",
    "Name": "MyGreengrassFunctions"
}
```

Para obtener más información, consulte Cómo configurar el acceso a recursos locales mediante la interfaz de la línea de comando de AWS en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte CreateFunctionDefinition en la Referencia de comandos de la AWS CLI.

`create-group-certificate-authority`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-group-certificate-authority`.

AWS CLI

Para crear una entidad de certificación (CA) para un grupo

En el siguiente ejemplo de `create-group-certificate-authority`, se crea o gira una CA para el grupo especificado.

```
aws greengrass create-group-certificate-authority \
    --group-id "8eaadd72-ce4b-4f15-892a-0cc4f3a343f1"
```

Salida:

```
{
    "GroupCertificateAuthorityArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/groups/8eaadd72-ce4b-4f15-892a-0cc4f3a343f1/certificateauthorities/
d31630d674c4437f6c5dbc0dca56312a902171ce2d086c38e509c8EXAMPLEcc5"
}
```

Para obtener más información, consulte AWS IoT Greengrass Security en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte CreateGroupCertificateAuthority en la Referencia de comandos de la AWS CLI.

`create-group-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-group-version`.

AWS CLI

Para crear una versión de un grupo de Greengrass

En el ejemplo siguiente de `create-group-version`, se crea una versión de grupo y se asocia al grupo especificado. La versión hace referencia a las versiones del núcleo, recurso, conector, función y suscripción que contienen las entidades que se incluirán en esta versión de grupo. Para poder crear la versión de grupo, debe crear estas entidades.

Para crear una definición de recurso con una versión inicial, utilice el comando `create-resource-definition`. Para crear una definición de conector con una versión inicial, utilice el comando `create-connector-definition`. Para crear una definición de función con una versión inicial, utilice el comando `create-function-definition`. Para crear una definición de

suscripción con una versión inicial, utilice el comando `create-subscription-definition`. Para recuperar el ARN de la última versión de definición de núcleo, utilice el comando `get-group-version` y especifique el ID de la última versión de grupo.

```
aws greengrass create-group-version \
    --group-id "ce2e7d01-3240-4c24-b8e6-f6f6e7a9eeca" \
    --core-definition-version-arn "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/cores/6a630442-8708-4838-ad36-eb98849d975e/
versions/6c87151b-1fb4-4cb2-8b31-6ee715d8f8ba" \
    --resource-definition-version-arn "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/resources/c8bb9ebc-c3fd-40a4-9c6a-568d75569d38/versions/
a5f94d0b-f6bc-40f4-bb78-7a1c5fe13ba1" \
    --connector-definition-version-arn "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/connectors/55d0052b-0d7d-44d6-b56f-21867215e118/
versions/78a3331b-895d-489b-8823-17b4f9f418a0" \
    --function-definition-version-arn "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/functions/3b0d0080-87e7-48c6-b182-503ec743a08b/
versions/67f918b9-efb4-40b0-b87c-de8c9faf085b" \
    --subscription-definition-version-arn "arn:aws:greengrass:us-
west-2:123456789012:/greengrass/definition/subscriptions/9d611d57-5d5d-44bd-a3b4-
feccbdd69112/versions/aa645c47-ac90-420d-9091-8c7ffa4f103f"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/groups/
ce2e7d01-3240-4c24-b8e6-f6f6e7a9eeca/versions/e10b0459-4345-4a09-88a4-1af1f5d34638",
    "CreationTimestamp": "2019-06-20T18:42:47.020Z",
    "Id": "ce2e7d01-3240-4c24-b8e6-f6f6e7a9eeca",
    "Version": "e10b0459-4345-4a09-88a4-1af1f5d34638"
}
```

Para obtener más información, consulte Información general del modelo de objetos del grupo de Greengrass de IoT de AWS en la Guía para desarrolladores de IoT AWSGreengrass.

- Para obtener información sobre la API, consulte CreateGroupVersion en la Referencia de comandos de la AWS CLI.

`create-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-group`.

AWS CLI

Para crear un grupo de Greengrass

En el siguiente ejemplo de `create-group`, se crea un grupo llamado `cli-created-group`.

```
aws greengrass create-group \
    --name cli-created-group
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
groups/4e22bd92-898c-436b-ade5-434d883ff749",
    "CreationTimestamp": "2019-06-25T18:07:17.688Z",
    "Id": "4e22bd92-898c-436b-ade5-434d883ff749",
    "LastUpdatedTimestamp": "2019-06-25T18:07:17.688Z",
    "Name": "cli-created-group"
}
```

Para obtener más información, consulte Información general del modelo de objetos del grupo de Greengrass de IoT de AWS en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte CreateGroup en la Referencia de comandos de la AWS CLI.

`create-logger-definition-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-logger-definition-version`.

AWS CLI

Para crear una versión de definición de registrador

En el siguiente ejemplo de `create-logger-definition-version`, se crea una versión de definición de registrador y se asocia a una definición de registrador. La versión define cuatro configuraciones de registro: 1) registros de componentes del sistema en el sistema de archivos del dispositivo de núcleo, 2) registros de funciones de Lambda definidas por el usuario en el sistema de archivos del dispositivo de núcleo, 3) registros de componentes del sistema en

Registros de Amazon CloudWatch y 4) registros de funciones Lambda definidas por el usuario en Registros de Amazon CloudWatch. Nota: Para la integración de Registros de CloudWatch, el rol de grupo debe conceder los permisos adecuados.

```
aws greengrass create-logger-definition-version \
    --logger-definition-id "a454b62a-5d56-4ca9-bdc4-8254e1662cb0" \
    --loggers "[{\"Id\":\"1\",\"Component\":\"GreengrassSystem\",\"Level\":\"ERROR
\",\"Space\":10240,\"Type\":\"FileSystem\"},{\"Id\":\"2\",\"Component\":\"Lambda
\",\"Level\":\"INFO\",\"Space\":10240,\"Type\":\"FileSystem\"},{\"Id\":\"3\",
\"Component\":\"GreengrassSystem\",\"Level\":\"WARN\",\"Type\":\"AWSCloudWatch\"},
{\"Id\":\"4\",\"Component\":\"Lambda\",\"Level\":\"INFO\",\"Type\":\"AWSCloudWatch
\"}]"
```

Salida:

```
{
 "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/loggers/
a454b62a-5d56-4ca9-bdc4-8254e1662cb0/versions/49aedb1e-01a3-4d39-9871-3a052573f1ea",
 "Version": "49aedb1e-01a3-4d39-9871-3a052573f1ea",
 "CreationTimestamp": "2019-07-24T00:04:48.523Z",
 "Id": "a454b62a-5d56-4ca9-bdc4-8254e1662cb0"
}
```

Para obtener más información, consulte Supervisión de los registros de AWS IoT Greengrass en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte CreateLoggerDefinitionVersion en la Referencia de comandos de la AWS CLI.

`create-logger-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-logger-definition`.

AWS CLI

Para crear una definición de registrador

En el siguiente ejemplo de `create-logger-definition`, se crea una definición de registrador que contiene una versión de definición de registrador inicial. La versión inicial define cuatro configuraciones de registro: 1) registros de componentes del sistema en el sistema de archivos del dispositivo de núcleo, 2) registros de funciones de Lambda definidas por el usuario en el

sistema de archivos del dispositivo de núcleo y 3) registros de funciones de Lambda definidas por el usuario en Registros de Amazon CloudWatch. Nota: Para la integración de Registros de CloudWatch, el rol de grupo debe conceder los permisos adecuados.

```
aws greengrass create-logger-definition \
    --name "LoggingConfigs" \
    --initial-version "{\"Loggers\":[{\"Id\":\"1\",\"Component\":\"GreengrassSystem
\",\"Level\":\"ERROR\",\"Space\":10240,\"Type\":\"FileSystem\"},{\"Id\":
\"2\",\"Component\":\"Lambda\",\"Level\":\"INFO\",\"Space\":10240,\"Type\":
\"FileSystem\"},{\"Id\":\"3\",\"Component\":\"Lambda\",\"Level\":\"INFO\",\"Type\":
\"AWSCloudWatch\"}]}"
```

Salida:

```
{
    "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/loggers/a454b62a-5d56-4ca9-bdc4-8254e1662cb0/versions/de1d9854-1588-4525-
b25e-b378f60f2322",
    "Name": "LoggingConfigs",
    "LastUpdatedTimestamp": "2019-07-23T23:52:17.165Z",
    "LatestVersion": "de1d9854-1588-4525-b25e-b378f60f2322",
    "CreationTimestamp": "2019-07-23T23:52:17.165Z",
    "Id": "a454b62a-5d56-4ca9-bdc4-8254e1662cb0",
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
loggers/a454b62a-5d56-4ca9-bdc4-8254e1662cb0"
}
```

Para obtener más información, consulte Supervisión de los registros de AWS IoT Greengrass en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte CreateLoggerDefinition en la Referencia de comandos de la AWS CLI.

`create-resource-definition-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-resource-definition-version`.

AWS CLI

Para crear una versión de una definición de recurso

En el siguiente ejemplo de `create-resource-definition-version`, se crea una nueva versión de un TwilioAuthToken.

```
aws greengrass create-resource-definition-version \
    --resource-definition-id "c8bb9ebc-c3fd-40a4-9c6a-568d75569d38" \
    --resources "[{\"Id\": \"TwilioAuthToken\",\"Name\": \"MyTwilioAuthToken
\",\"ResourceDataContainer\": {\"SecretsManagerSecretResourceData\": {\"ARN\":
 \"arn:aws:secretsmanager:us-west-2:123456789012:secret:greengrass-TwilioAuthToken-
ntSlp6\"}}}]"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
resources/c8bb9ebc-c3fd-40a4-9c6a-568d75569d38/versions/b3bcada0-5fb6-42df-
bf0b-1ee4f15e769e",
    "CreationTimestamp": "2019-06-24T21:17:25.623Z",
    "Id": "c8bb9ebc-c3fd-40a4-9c6a-568d75569d38",
    "Version": "b3bcada0-5fb6-42df-bf0b-1ee4f15e769e"
}
```

- Para obtener información sobre la API, consulte CreateResourceDefinitionVersion en la Referencia de comandos de la AWS CLI.

`create-resource-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-resource-definition`.

AWS CLI

Para crear una definición de recurso

En el siguiente ejemplo de `create-resource-definition`, se crea una definición de recurso que contiene una lista de los recursos que se utilizarán en un grupo de Greengrass. En este ejemplo, se incluye una versión inicial de la definición de recurso al proporcionar una lista de recursos. La lista incluye un recurso para un token de autorización de Twilio y el ARN para un secreto almacenado en AWS Secrets Manager. Para poder crear la definición del recurso, debe crear el secreto.

```
aws greengrass create-resource-definition \
```

```
    --name MyGreengrassResources \
    --initial-version "{\"Resources\": [{\"Id\": \"TwilioAuthToken
\",\"Name\": \"MyTwilioAuthToken\",\"ResourceDataContainer\":
 {\"SecretsManagerSecretResourceData\": {\"ARN\": \"arn:aws:secretsmanager:us-
west-2:123456789012:secret:greengrass-TwilioAuthToken-ntSlp6\"}}}]}"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
resources/c8bb9ebc-c3fd-40a4-9c6a-568d75569d38",
    "CreationTimestamp": "2019-06-19T21:51:28.212Z",
    "Id": "c8bb9ebc-c3fd-40a4-9c6a-568d75569d38",
    "LastUpdatedTimestamp": "2019-06-19T21:51:28.212Z",
    "LatestVersion": "a5f94d0b-f6bc-40f4-bb78-7a1c5fe13ba1",
    "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/resources/c8bb9ebc-c3fd-40a4-9c6a-568d75569d38/versions/a5f94d0b-
f6bc-40f4-bb78-7a1c5fe13ba1",
    "Name": "MyGreengrassResources"
}
```

Para obtener más información, consulte Cómo configurar el acceso a recursos locales mediante la interfaz de la línea de comando de AWS en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte CreateResourceDefinition en la Referencia de comandos de la AWS CLI.

`create-software-update-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-software-update-job`.

AWS CLI

Para crear un trabajo de actualización para el software de un núcleo

En el siguiente ejemplo de `create-software-update-job`, se crea un trabajo de actualización por vía inalámbrica (OTA) para actualizar el software de AWS IoT Greengrass Core en el núcleo cuyo nombre es `MyFirstGroup_Core`. Este comando requiere un rol de IAM que permita el acceso a los paquetes de actualización de software en Amazon S3 y que incluya `iot.amazonaws.com` como entidad de confianza.

```
aws greengrass create-software-update-job \
    --update-targets-architecture armv7l \
    --update-targets [\"arn:aws:iot:us-west-2:123456789012:thing/MyFirstGroup_Core
\"] \
    --update-targets-operating-system raspbian \
    --software-to-update core \
    --s3-url-signer-role arn:aws:iam::123456789012:role/OTA_signer_role \
    --update-agent-log-level WARN
```

Salida:

```
{
    "IotJobId": "GreengrassUpdateJob_30b353e3-3af7-4786-be25-4c446663c09e",
    "IotJobArn": "arn:aws:iot:us-west-2:123456789012:job/
GreengrassUpdateJob_30b353e3-3af7-4786-be25-4c446663c09e",
    "PlatformSoftwareVersion": "1.9.3"
}
```

Para obtener más información, consulte Actualizaciones de OTA del software de AWS IoT Greengrass Core en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte CreateSoftwareUpdateJob en la Referencia de comandos de la AWS CLI.

`create-subscription-definition-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-subscription-definition-version`.

AWS CLI

Para crear una versión nueva de una definición de suscripción

En el siguiente ejemplo de `create-subscription-definition-version`, se crea una versión nueva de una definición de suscripción que contiene tres suscripciones: una notificación de desencadenador, una entrada de temperatura y un estado de salida.

```
aws greengrass create-subscription-definition-version \
    --subscription-definition-id "9d611d57-5d5d-44bd-a3b4-feccbdd69112" \
    --subscriptions "[{\"Id\": \"TriggerNotification\", \"Source\":
 \"arn:aws:lambda:us-west-2:123456789012:function:TempMonitor:GG_TempMonitor
```

```
\", \"Subject\": \"twilio/txt\", \"Target\": \"arn:aws:greengrass:us-west-2::/
connectors/TwilioNotifications/versions/1\"},{\"Id\": \"TemperatureInput\", \"Source
\": \"cloud\", \"Subject\": \"temperature/input\", \"Target\": \"arn:aws:lambda:us-
west-2:123456789012:function:TempMonitor:GG_TempMonitor\"},{\"Id\": \"OutputStatus
\", \"Source\": \"arn:aws:greengrass:us-west-2::/connectors/TwilioNotifications/
versions/1\", \"Subject\": \"twilio/message/status\", \"Target\": \"cloud\"}]"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
subscriptions/9d611d57-5d5d-44bd-a3b4-feccbdd69112/versions/7b65dfae-50b6-4d0f-
b3e0-27728bfb0620",
    "CreationTimestamp": "2019-06-24T21:21:33.837Z",
    "Id": "9d611d57-5d5d-44bd-a3b4-feccbdd69112",
    "Version": "7b65dfae-50b6-4d0f-b3e0-27728bfb0620"
}
```

- Para obtener información sobre la API, consulte CreateSubscriptionDefinitionVersion en la Referencia de comandos de la AWS CLI.

`create-subscription-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-subscription-definition`.

AWS CLI

Para crear una definición de suscripción

En el siguiente ejemplo de `create-subscription-definition`, se crea una definición de suscripción y se especifica su versión inicial. La versión inicial contiene tres suscripciones: una para el tema de MQTT al que está suscrito el conector, otra para permitir que una función reciba lecturas de temperatura de AWS IoT y otra para permitir que AWS IoT reciba información de estado del conector. El ejemplo proporciona el ARN para el alias de la función de Lambda que se creó anteriormente mediante el comando `create-alias` de Lambda.

```
aws greengrass create-subscription-definition \
    --initial-version "{\"Subscriptions\": [{\"Id\":
 \"TriggerNotification\", \"Source\": \"arn:aws:lambda:us-
west-2:123456789012:function:TempMonitor:GG_TempMonitor\", \"Subject\":
 \"twilio/txt\", \"Target\": \"arn:aws:greengrass:us-west-2::/connectors/
```

```
TwilioNotifications/versions/1\"},{\"Id\": \"TemperatureInput\", \"Source\":
 \"cloud\", \"Subject\": \"temperature/input\", \"Target\": \"arn:aws:lambda:us-
west-2:123456789012:function:TempMonitor:GG_TempMonitor\"},{\"Id\": \"OutputStatus
\", \"Source\": \"arn:aws:greengrass:us-west-2::/connectors/TwilioNotifications/
versions/1\", \"Subject\": \"twilio/message/status\", \"Target\": \"cloud\"}]}"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
subscriptions/9d611d57-5d5d-44bd-a3b4-feccbdd69112",
    "CreationTimestamp": "2019-06-19T22:34:26.677Z",
    "Id": "9d611d57-5d5d-44bd-a3b4-feccbdd69112",
    "LastUpdatedTimestamp": "2019-06-19T22:34:26.677Z",
    "LatestVersion": "aa645c47-ac90-420d-9091-8c7ffa4f103f",
    "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/subscriptions/9d611d57-5d5d-44bd-a3b4-feccbdd69112/versions/aa645c47-
ac90-420d-9091-8c7ffa4f103f"
}
```

Para obtener más información, consulte Introducción a los conectores (CLI) en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte CreateSubscriptionDefinition en la Referencia de comandos de la AWS CLI.

`delete-connector-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-connector-definition`.

AWS CLI

Para eliminar una definición de conector

En el siguiente ejemplo de `delete-connector-definition`, se elimina la definición de conector de Greengrass especificada. Si elimina una definición de conector utilizada por un grupo, ese grupo no se podrá implementar correctamente.

```
aws greengrass delete-connector-definition \
    --connector-definition-id "b5c4ebfd-f672-49a3-83cd-31c7216a7bb8"
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteConnectorDefinition en la Referencia de comandos de la AWS CLI.

`delete-core-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-core-definition`.

AWS CLI

Para eliminar una definición de núcleo

En el siguiente ejemplo de `delete-core-definition`, se elimina la definición de núcleo de Greengrass especificada, incluidas todas las versiones. Si elimina un núcleo que está asociado a un grupo de Greengrass, ese grupo no se podrá implementar correctamente.

```
aws greengrass delete-core-definition \
    --core-definition-id "ff36cc5f-9f98-4994-b468-9d9b6dc52abd"
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteCoreDefinition en la Referencia de comandos de la AWS CLI.

`delete-device-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-device-definition`.

AWS CLI

Para eliminar una definición de dispositivo

En el siguiente ejemplo de `delete-device-definition`, se elimina la definición de dispositivo especificada, incluidas todas sus versiones. Si elimina una versión de definición de dispositivo utilizada por una versión de grupo, la versión de grupo no se podrá implementar correctamente.

```
aws greengrass delete-device-definition \
    --device-definition-id "f9ba083d-5ad4-4534-9f86-026a45df1ccd"
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteDeviceDefinition en la Referencia de comandos de la AWS CLI.

`delete-function-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-function-definition`.

AWS CLI

Para eliminar una definición de función

En el siguiente ejemplo de `delete-function-definition`, se elimina la definición de función de Greengrass especificada. Si elimina una definición de función utilizada por un grupo, ese grupo no se podrá implementar correctamente.

```
aws greengrass delete-function-definition \
    --function-definition-id "fd4b906a-dff3-4c1b-96eb-52ebfcfac06a"
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteFunctionDefinition en la Referencia de comandos de la AWS CLI.

`delete-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-group`.

AWS CLI

Para eliminar un grupo

En el siguiente ejemplo de `delete-group`, se elimina el grupo de Greengrass especificado.

```
aws greengrass delete-group \
    --group-id "4e22bd92-898c-436b-ade5-434d883ff749"
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteGroup en la Referencia de comandos de la AWS CLI.

`delete-logger-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-logger-definition`.

AWS CLI

Para eliminar una definición de registrador

En el siguiente ejemplo de `delete-logger-definition`, se elimina la definición de registrador especificada, incluidas todas sus versiones. Si elimina una versión de definición de registrador utilizada por una versión de grupo, la versión de grupo no se podrá implementar correctamente.

```
aws greengrass delete-logger-definition \
    --logger-definition-id "a454b62a-5d56-4ca9-bdc4-8254e1662cb0"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Supervisión de los registros de AWS IoT Greengrass en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte DeleteLoggerDefinition en la Referencia de comandos de la AWS CLI.

`delete-resource-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-resource-definition`.

AWS CLI

Para eliminar una definición de recurso

En el siguiente ejemplo de `delete-resource-definition`, se elimina la definición de recurso especificada, incluidas todas las versiones de recursos. Si elimina una definición de recurso utilizada por un grupo, ese grupo no se podrá implementar correctamente.

```
aws greengrass delete-resource-definition \
    --resource-definition-id "ad8c101d-8109-4b0e-b97d-9cc5802ab658"
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteResourceDefinition en la Referencia de comandos de la AWS CLI.

`delete-subscription-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-subscription-definition`.

AWS CLI

Para eliminar una definición de suscripción

En el siguiente ejemplo de `delete-subscription-definition`, se elimina la definición de suscripción de Greengrass especificada. Si elimina una suscripción utilizada por un grupo, ese grupo no se podrá implementar correctamente.

```
aws greengrass delete-subscription-definition \
    --subscription-definition-id "cd6f1c37-d9a4-4e90-be94-01a7404f5967"
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteSubscriptionDefinition en la Referencia de comandos de la AWS CLI.

`disassociate-role-from-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-role-from-group`.

AWS CLI

Para desasociar el rol de un grupo de Greengrass

En el siguiente ejemplo de `disassociate-role-from-group`, se desasocia el rol de IAM de un grupo de Greengrass especificado.

```
aws greengrass disassociate-role-from-group \
    --group-id 2494ee3f-7f8a-4e92-a78b-d205f808b84b
```

Salida:

```
{
    "DisassociatedAt": "2019-09-10T20:05:49Z"
}
```

Para obtener más información, consulte Configuración del rol del grupo en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte DisassociateRoleFromGroup en la Referencia de la comandos de AWS CLI.

`disassociate-service-role-from-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-service-role-from-account`.

AWS CLI

Para desasociar un rol de servicio de su cuenta de AWS

En el siguiente ejemplo de `disassociate-service-role-from-account`, se elimina el rol de servicio asociado a su cuenta de AWS. Si no utiliza el rol de servicio en ninguna región de AWS, utilice el comando `delete-role-policy` para separar la política administrada de `AWSGreengrassResourceAccessRolePolicy` del rol y, a continuación, utilice el comando `delete-role` para eliminar el rol.

```
aws greengrass disassociate-service-role-from-account
```

Salida:

```
{
    "DisassociatedAt": "2019-06-25T22:12:55Z"
}
```

Para obtener más información, consulte Greengrass service role en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte DisassociateServiceRoleFromAccount en la Referencia de comandos de la AWS CLI.

`get-associated-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-associated-role`.

AWS CLI

Para obtener el rol asociado a un grupo de Greengrass

En el siguiente ejemplo de `get-associated-role`, se obtiene el rol de IAM asociado al grupo de Greengrass especificado. Las funciones y conectores de Lambda locales utilizan el rol de grupo para acceder a los servicios de AWS.

```
aws greengrass get-associated-role \
    --group-id 2494ee3f-7f8a-4e92-a78b-d205f808b84b
```

Salida:

```
{
    "RoleArn": "arn:aws:iam::123456789012:role/GG-Group-Role",
    "AssociatedAt": "2019-09-10T20:03:30Z"
}
```

Para obtener más información, consulte Configuración del rol del grupo en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte GetAssociatedRole en la Referencia de comandos de la AWS CLI.

`get-bulk-deployment-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bulk-deployment-status`.

AWS CLI

Para comprobar el estado de la implementación por lotes

En el siguiente ejemplo de `get-bulk-deployment-status`, se recupera la información de estado para la operación de implementación por lotes especificada. En este ejemplo, el archivo que especifica los grupos que se implementarán tiene un registro de entrada no válido.

```
aws greengrass get-bulk-deployment-status \
    --bulk-deployment-id "870fb41b-6288-4e0c-bc76-a7ba4b4d3267"
```

Salida:

```
{
    "BulkDeploymentMetrics": {
        "InvalidInputRecords": 1,
        "RecordsProcessed": 1,
        "RetryAttempts": 0
    },
```

```
    "BulkDeploymentStatus": "Completed",
    "CreatedAt": "2019-06-25T16:11:33.265Z",
    "tags": {}
}
```

Para obtener más información, consulte Create Bulk Deployments for Groups en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte GetBulkDeploymentStatus en la Referencia de comandos de la AWS CLI.

`get-connectivity-info`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-connectivity-info`.

AWS CLI

Para obtener la información de conectividad para un núcleo de Greengrass

En el siguiente ejemplo de `get-connectivity-info`, se muestran los puntos de conexión que los dispositivos pueden usar para conectarse al núcleo de Greengrass especificado. La información de conectividad es una lista de direcciones IP o nombres de dominio, con los números de puerto correspondientes y los metadatos opcionales definidos por el cliente.

```
aws greengrass get-connectivity-info \
    --thing-name "MyGroup_Core"
```

Salida:

```
{
    "ConnectivityInfo": [
        {
            "Metadata": "",
            "PortNumber": 8883,
            "HostAddress": "127.0.0.1",
            "Id": "AUTOIP_127.0.0.1_0"
        },
        {
            "Metadata": "",
            "PortNumber": 8883,
            "HostAddress": "192.168.1.3",
```

```
            "Id": "AUTOIP_192.168.1.3_1"
        },
        {
            "Metadata": "",
            "PortNumber": 8883,
            "HostAddress": "::1",
            "Id": "AUTOIP_::1_2"
        },
        {
            "Metadata": "",
            "PortNumber": 8883,
            "HostAddress": "fe80::1e69:ed93:f5b:f6d",
            "Id": "AUTOIP_fe80::1e69:ed93:f5b:f6d_3"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetConnectivityInfo en la Referencia de comandos de la AWS CLI.

`get-connector-definition-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-connector-definition-version`.

AWS CLI

Para recuperar información sobre una versión específica de una definición de conector

En el siguiente ejemplo de `get-connector-definition-version`, se recupera información sobre la versión especificada de la definición de conector especificada. Para recuperar los ID de todas las versiones de la definición de conector, utilice el comando `list-connector-definition-versions`. Para recuperar el ID de la última versión agregada a la definición del conector, utilice el comando `get-connector-definition` y compruebe la propiedad `LatestVersion`.

```
aws greengrass get-connector-definition-version \
    --connector-definition-id "b5c4ebfd-f672-49a3-83cd-31c7216a7bb8" \
    --connector-definition-version-id "63c57963-c7c2-4a26-a7e2-7bf478ea2623"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
connectors/b5c4ebfd-f672-49a3-83cd-31c7216a7bb8/versions/63c57963-c7c2-4a26-
a7e2-7bf478ea2623",
    "CreationTimestamp": "2019-06-19T19:30:01.300Z",
    "Definition": {
        "Connectors": [
            {
                "ConnectorArn": "arn:aws:greengrass:us-west-2::/connectors/SNS/
versions/1",
                "Id": "MySNSConnector",
                "Parameters": {
                    "DefaultSNSArn": "arn:aws:sns:us-
west-2:123456789012:GGConnectorTopic"
                }
            }
        ]
    },
    "Id": "b5c4ebfd-f672-49a3-83cd-31c7216a7bb8",
    "Version": "63c57963-c7c2-4a26-a7e2-7bf478ea2623"
}
```

Para obtener más información, consulte Integrate with Services and Protocols Using Greengrass Connectors en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte GetConnectorDefinitionVersion en la Referencia de comandos de la AWS CLI.

`get-connector-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-connector-definition`.

AWS CLI

Para recuperar información sobre una definición de conector

En el siguiente ejemplo de `get-connector-definition`, se recupera información sobre la definición del conector especificada. Para recuperar los ID de las definiciones de conector, utilice el comando `list-connector-definitions`.

```
aws greengrass get-connector-definition \
    --connector-definition-id "b5c4ebfd-f672-49a3-83cd-31c7216a7bb8"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
connectors/b5c4ebfd-f672-49a3-83cd-31c7216a7bb8",
    "CreationTimestamp": "2019-06-19T19:30:01.300Z",
    "Id": "b5c4ebfd-f672-49a3-83cd-31c7216a7bb8",
    "LastUpdatedTimestamp": "2019-06-19T19:30:01.300Z",
    "LatestVersion": "63c57963-c7c2-4a26-a7e2-7bf478ea2623",
    "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/connectors/b5c4ebfd-f672-49a3-83cd-31c7216a7bb8/versions/63c57963-
c7c2-4a26-a7e2-7bf478ea2623",
    "Name": "MySNSConnector",
    "tags": {}
}
```

Para obtener más información, consulte Integrate with Services and Protocols Using Greengrass Connectors en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte GetConnectorDefinition en la Referencia de comandos de la AWS CLI.

`get-core-definition-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-core-definition-version`.

AWS CLI

Para recuperar detalles sobre una versión específica de la definición de núcleo de Greengrass

En el siguiente ejemplo de `get-core-definition-version`, se recupera información sobre la versión especificada de la definición de núcleo especificada. Para recuperar los ID de todas las versiones de la definición de núcleo, utilice el comando `list-core-definition-versions`. Para recuperar el ID de la última versión agregada a la definición de núcleo, utilice el comando `get-core-definition` y compruebe la propiedad `LatestVersion`.

```
aws greengrass get-core-definition-version \
    --core-definition-id "c906ed39-a1e3-4822-a981-7b9bd57b4b46"  \
    --core-definition-version-id "42aeeac3-fd9d-4312-a8fd-ffa9404a20e0"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/cores/
c906ed39-a1e3-4822-a981-7b9bd57b4b46/versions/42aeeac3-fd9d-4312-a8fd-ffa9404a20e0",
    "CreationTimestamp": "2019-06-18T16:21:21.351Z",
    "Definition": {
        "Cores": [
            {
                "CertificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/928dea7b82331b47c3ff77b0e763fc5e64e2f7c884e6ef391baed9b6b8e21b45",
                "Id": "1a39aac7-0885-4417-91f6-23e4cea6c511",
                "SyncShadow": false,
                "ThingArn": "arn:aws:iot:us-west-2:123456789012:thing/
GGGroup4Pi3_Core"
            }
        ]
    },
    "Id": "c906ed39-a1e3-4822-a981-7b9bd57b4b46",
    "Version": "42aeeac3-fd9d-4312-a8fd-ffa9404a20e0"
}
```

- Para obtener información sobre la API, consulte GetCoreDefinitionVersion en la Referencia de comandos de la AWS CLI.

`get-core-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-core-definition`.

AWS CLI

Para recuperar los detalles de una definición de núcleo de Greengrass

En el siguiente ejemplo de `get-core-definition`, se recupera información sobre la definición de núcleo especificada. Para recuperar los ID de sus definiciones de núcleo, utilice el comando `list-core-definitions`.

```
aws greengrass get-core-definition \
    --core-definition-id "c906ed39-a1e3-4822-a981-7b9bd57b4b46"
```

Salida:

```
{
```

```
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
cores/237d6916-27cf-457f-ba0c-e86cfb5d25cd",
    "CreationTimestamp": "2018-10-18T04:47:06.721Z",
    "Id": "237d6916-27cf-457f-ba0c-e86cfb5d25cd",
    "LastUpdatedTimestamp": "2018-10-18T04:47:06.721Z",
    "LatestVersion": "bd2cd6d4-2bc5-468a-8962-39e071e34b68",
    "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/cores/237d6916-27cf-457f-ba0c-e86cfb5d25cd/versions/
bd2cd6d4-2bc5-468a-8962-39e071e34b68",
    "tags": {}
}
```

- Para obtener información sobre la API, consulte GetCoreDefinition en la Referencia de comandos de la AWS CLI.

`get-deployment-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-deployment-status`.

AWS CLI

Para recuperar el estado de una implementación

En el siguiente ejemplo de `get-deployment-status`, se recupera el estado de la implementación especificada del grupo de Greengrass especificado. Para obtener el ID de implementación, utilice el comando `list-deployments` y especifique el ID del grupo.

```
aws greengrass get-deployment-status \
    --group-id "1013db12-8b58-45ff-acc7-704248f66731" \
    --deployment-id "1065b8a0-812b-4f21-9d5d-e89b232a530f"
```

Salida:

```
{
    "DeploymentStatus": "Success",
    "DeploymentType": "NewDeployment",
    "UpdatedAt": "2019-06-18T17:04:44.761Z"
}
```

- Para obtener información sobre la API, consulte GetDeploymentStatus en la Referencia de comandos de la AWS CLI.

get-device-definition-version

En el siguiente ejemplo de código, se muestra cómo utilizar `get-device-definition-version`.

AWS CLI

Para obtener una versión de definición de dispositivo

En el siguiente ejemplo de `get-device-definition-version`, se recupera información sobre la versión especificada de la definición de dispositivo especificada. Para recuperar los ID de todas las versiones de la definición de dispositivo, utilice el comando `list-device-definition-versions`. Para recuperar el ID de la última versión agregada a la definición de dispositivo, utilice el comando `get-device-definition` y compruebe la propiedad `LatestVersion`.

```
aws greengrass get-device-definition-version \
    --device-definition-id "f9ba083d-5ad4-4534-9f86-026a45df1ccd" \
    --device-definition-version-id "83c13984-6fed-447e-84d5-5b8aa45d5f71"
```

Salida:

```
{
    "Definition": {
        "Devices": [
            {
                "CertificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/6c52ce1b47bde88a637e9ccdd45fe4e4c2c0a75a6866f8f63d980ee22fa51e02",
                "ThingArn": "arn:aws:iot:us-west-2:123456789012:thing/
ExteriorTherm",
                "SyncShadow": true,
                "Id": "ExteriorTherm"
            },
            {
                "CertificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/66a415ec415668c2349a76170b64ac0878231c1e21ec83c10e92a18bd568eb92",
                "ThingArn": "arn:aws:iot:us-west-2:123456789012:thing/
InteriorTherm",
                "SyncShadow": true,
                "Id": "InteriorTherm"
            }
        ]
    },
    "Version": "83c13984-6fed-447e-84d5-5b8aa45d5f71",
    "CreationTimestamp": "2019-09-11T00:15:09.838Z",
```

```
    "Id": "f9ba083d-5ad4-4534-9f86-026a45df1ccd",
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/devices/f9ba083d-5ad4-4534-9f86-026a45df1ccd/
versions/83c13984-6fed-447e-84d5-5b8aa45d5f71"
}
```

- Para obtener información sobre la API, consulte GetDeviceDefinitionVersion en la Referencia de comandos de la AWS CLI.

`get-device-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-device-definition`.

AWS CLI

Para obtener una definición de dispositivo

En el siguiente ejemplo de `get-device-definition`, se recupera información sobre la definición de dispositivo especificada. Para recuperar los ID de las definiciones de dispositivos, utilice el comando `list-device-definitions`.

```
aws greengrass get-device-definition \
    --device-definition-id "f9ba083d-5ad4-4534-9f86-026a45df1ccd"
```

Salida:

```
{
    "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/devices/f9ba083d-5ad4-4534-9f86-026a45df1ccd/
versions/83c13984-6fed-447e-84d5-5b8aa45d5f71",
    "Name": "TemperatureSensors",
    "tags": {},
    "LastUpdatedTimestamp": "2019-09-11T00:19:03.698Z",
    "LatestVersion": "83c13984-6fed-447e-84d5-5b8aa45d5f71",
    "CreationTimestamp": "2019-09-11T00:11:06.197Z",
    "Id": "f9ba083d-5ad4-4534-9f86-026a45df1ccd",
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
devices/f9ba083d-5ad4-4534-9f86-026a45df1ccd"
}
```

- Para obtener información sobre la API, consulte GetDeviceDefinition en la Referencia de comandos de la AWS CLI.

get-function-definition-version

En el siguiente ejemplo de código, se muestra cómo utilizar `get-function-definition-version`.

AWS CLI

Para recuperar detalles sobre una versión específica de una función de Lambda

En el siguiente `get-function-definition-version`, se recupera información sobre la versión especificada de la definición de función especificada. Para recuperar los ID de todas las versiones de la definición de función, utilice el comando `list-function-definition-versions`. Para recuperar el ID de la última versión agregada a la definición de función, utilice el comando `get-function-definition` y compruebe la propiedad `LatestVersion`.

```
aws greengrass get-function-definition-version \
    --function-definition-id "063f5d1a-1dd1-40b4-9b51-56f8993d0f85" \
    --function-definition-version-id "9748fda7-1589-4fcc-ac94-f5559e88678b"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
functions/063f5d1a-1dd1-40b4-9b51-56f8993d0f85/versions/9748fda7-1589-4fcc-ac94-
f5559e88678b",
    "CreationTimestamp": "2019-06-18T17:04:30.776Z",
    "Definition": {
        "Functions": [
            {
                "FunctionArn": "arn:aws:lambda:::function:GGIPDetector:1",
                "FunctionConfiguration": {
                    "Environment": {},
                    "MemorySize": 32768,
                    "Pinned": true,
                    "Timeout": 3
                },
                "Id": "26b69bdb-e547-46bc-9812-84ec04b6cc8c"
            },
            {
                "FunctionArn": "arn:aws:lambda:us-
west-2:123456789012:function:Greengrass_HelloWorld:GG_HelloWorld",
                "FunctionConfiguration": {
```

```
                    "EncodingType": "json",
                    "Environment": {
                        "Variables": {}
                    },
                    "MemorySize": 16384,
                    "Pinned": true,
                    "Timeout": 25
                },
                "Id": "384465a8-eedf-48c6-b793-4c35f7bfae9b"
            }
        ]
    },
    "Id": "063f5d1a-1dd1-40b4-9b51-56f8993d0f85",
    "Version": "9748fda7-1589-4fcc-ac94-f5559e88678b"
}
```

- Para obtener información sobre la API, consulte GetFunctionDefinitionVersion en la Referencia de comandos de la AWS CLI.

`get-function-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-function-definition`.

AWS CLI

Para recuperar una definición de función

En el ejemplo siguiente de `get-function-definition`, se muestran los detalles para la definición de función especificada. Para recuperar los ID de las definiciones de función, utilice el comando `list-function-definitions`.

```
aws greengrass get-function-definition \
    --function-definition-id "063f5d1a-1dd1-40b4-9b51-56f8993d0f85"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
functions/063f5d1a-1dd1-40b4-9b51-56f8993d0f85",
    "CreationTimestamp": "2019-06-18T16:21:21.431Z",
    "Id": "063f5d1a-1dd1-40b4-9b51-56f8993d0f85",
    "LastUpdatedTimestamp": "2019-06-18T16:21:21.431Z",
```

```
    "LatestVersion": "9748fda7-1589-4fcc-ac94-f5559e88678b",
    "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/functions/063f5d1a-1dd1-40b4-9b51-56f8993d0f85/
versions/9748fda7-1589-4fcc-ac94-f5559e88678b",
    "tags": {}
}
```

- Para obtener información sobre la API, consulte GetFunctionDefinition en la Referencia de comandos de la AWS CLI.

`get-group-certificate-authority`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-group-certificate-authority`.

AWS CLI

Para recuperar la CA asociada a un grupo de Greengrass

En el siguiente ejemplo de `get-group-certificate-authority`, se recupera la entidad de certificación (CA) asociada al grupo de Greengrass especificado. Para obtener el ID de la entidad de certificación, utilice el comando `list-group-certificate-authorities` y especifique el ID del grupo.

```
aws greengrass get-group-certificate-authority \
    --group-id "1013db12-8b58-45ff-acc7-704248f66731" \
    --certificate-authority-
id "f0430e1736ea8ed30cc5d5de9af67a7e3586bad9ae4d89c2a44163f65fdd8cf6"
```

Salida:

```
{
    "GroupCertificateAuthorityArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/groups/1013db12-8b58-45ff-acc7-704248f66731/certificateauthorities/
f0430e1736ea8ed30cc5d5de9af67a7e3586bad9ae4d89c2a44163f65fdd8cf6",
    "GroupCertificateAuthorityId":
 "f0430e1736ea8ed30cc5d5de9af67a7e3586bad9ae4d89c2a44163f65fdd8cf6",
    "PemEncodedCertificate": "-----BEGIN CERTIFICATE-----
MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBWEXAMPLEGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDEXAMPLEEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAEXAMPLESBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jEXAMPLENMTEwNDI1MjA0NTIxWhcN
```

```
MTIwNDI0MjA0EXAMPLEBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWEXAMPLEDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWEXAMPLEgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5EXAMPLE8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CEXAMPLE93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswYEXAMPLEgpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKEXAMPLEAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----\n"
}
```

- Para obtener información sobre la API, consulte GetGroupCertificateAuthority en la Referencia de comandos de la AWS CLI.

`get-group-certificate-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-group-certificate-configuration`.

AWS CLI

Para recuperar la configuración de la entidad de certificación utilizada por el grupo de Greengrass

En el siguiente ejemplo de `get-group-certificate-configuration`, se recupera la configuración de la entidad de certificación (CA) usada por el grupo de Greengrass especificado.

```
aws greengrass get-group-certificate-configuration \
    --group-id "1013db12-8b58-45ff-acc7-704248f66731"
```

Salida:

```
{
    "CertificateAuthorityExpiryInMilliseconds": 2524607999000,
    "CertificateExpiryInMilliseconds": 604800000,
    "GroupId": "1013db12-8b58-45ff-acc7-704248f66731"
}
```

- Para obtener información sobre la API, consulte GetGroupCertificateConfiguration en la Referencia de comandos de la AWS CLI.

`get-group-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-group-version`.

AWS CLI

Para recuperar información sobre una versión de un grupo de Greengrass

En el siguiente ejemplo de `get-group-version`, se recupera información sobre la versión especificada del grupo especificado. Para recuperar los ID de todas las versiones del grupo, utilice el comando `list-group-versions`. Para recuperar el ID de la última versión agregada al grupo, utilice el comando `get-group` y compruebe la propiedad `LatestVersion`.

```
aws greengrass get-group-version \
    --group-id "1013db12-8b58-45ff-acc7-704248f66731"  \
    --group-version-id "115136b3-cfd7-4462-b77f-8741a4b00e5e"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
groups/1013db12-8b58-45ff-acc7-704248f66731/versions/115136b3-cfd7-4462-
b77f-8741a4b00e5e",
    "CreationTimestamp": "2019-06-18T17:04:30.915Z",
    "Definition": {
        "CoreDefinitionVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/cores/c906ed39-a1e3-4822-a981-7b9bd57b4b46/versions/42aeeac3-
fd9d-4312-a8fd-ffa9404a20e0",
        "FunctionDefinitionVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/functions/063f5d1a-1dd1-40b4-9b51-56f8993d0f85/
versions/9748fda7-1589-4fcc-ac94-f5559e88678b",
        "SubscriptionDefinitionVersionArn": "arn:aws:greengrass:us-
west-2:123456789012:/greengrass/definition/subscriptions/70e49321-83d5-45d2-
bc09-81f4917ae152/versions/88ae8699-12ac-4663-ba3f-4d7f0519140b"
    },
    "Id": "1013db12-8b58-45ff-acc7-704248f66731",
    "Version": "115136b3-cfd7-4462-b77f-8741a4b00e5e"
}
```

- Para obtener información sobre la API, consulte GetGroupVersion en la Referencia de comandos de la AWS CLI.

get-group

En el siguiente ejemplo de código, se muestra cómo utilizar `get-group`.

AWS CLI

Para recuperar información sobre un grupo de Greengrass

En el siguiente ejemplo de `get-group`, se recupera información sobre el grupo de Greengrass especificado. Para recuperar los ID de sus grupos, utilice el comando `list-groups`.

```
aws greengrass get-group \
    --group-id "1013db12-8b58-45ff-acc7-704248f66731"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
groups/1013db12-8b58-45ff-acc7-704248f66731",
    "CreationTimestamp": "2019-06-18T16:21:21.457Z",
    "Id": "1013db12-8b58-45ff-acc7-704248f66731",
    "LastUpdatedTimestamp": "2019-06-18T16:21:21.457Z",
    "LatestVersion": "115136b3-cfd7-4462-b77f-8741a4b00e5e",
    "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
groups/1013db12-8b58-45ff-acc7-704248f66731/versions/115136b3-cfd7-4462-
b77f-8741a4b00e5e",
    "Name": "GGGroup4Pi3",
    "tags": {}
}
```

- Para obtener información sobre la API, consulte GetGroup en la Referencia de comandos de la AWS CLI.

get-logger-definition-version

En el siguiente ejemplo de código, se muestra cómo utilizar `get-logger-definition-version`.

AWS CLI

Para recuperar información sobre una versión de una definición de registrador

En el siguiente ejemplo de `get-logger-definition-version`, se recupera información sobre la versión especificada de la definición de registrador especificada. Para recuperar los ID de todas las versiones de la definición de registrador, utilice el comando `list-logger-definition-versions`. Para recuperar el ID de la última versión agregada a la definición de registrador, utilice el comando `get-logger-definition` y compruebe la propiedad `LatestVersion`.

```
aws greengrass get-logger-definition-version \
    --logger-definition-id "49eeeb66-f1d3-4e34-86e3-3617262abf23" \
    --logger-definition-version-id "5e3f6f64-a565-491e-8de0-3c0d8e0f2073"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/loggers/49eeeb66-f1d3-4e34-86e3-3617262abf23/versions/5e3f6f64-
a565-491e-8de0-3c0d8e0f2073",
    "CreationTimestamp": "2019-05-08T16:10:13.866Z",
    "Definition": {
        "Loggers": []
    },
    "Id": "49eeeb66-f1d3-4e34-86e3-3617262abf23",
    "Version": "5e3f6f64-a565-491e-8de0-3c0d8e0f2073"
}
```

- Para obtener información sobre la API, consulte GetLoggerDefinitionVersion en la Referencia de comandos de la AWS CLI.

`get-logger-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-logger-definition`.

AWS CLI

Para recuperar información sobre una definición de registrador

En el siguiente ejemplo de `get-logger-definition`, se recupera información sobre la definición de registrador especificada. Para recuperar los ID de sus definiciones de registrador, utilice el comando `list-logger-definitions`.

```
aws greengrass get-logger-definition \
```

```
    --logger-definition-id "49eeeb66-f1d3-4e34-86e3-3617262abf23"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
loggers/49eeeb66-f1d3-4e34-86e3-3617262abf23",
    "CreationTimestamp": "2019-05-08T16:10:13.809Z",
    "Id": "49eeeb66-f1d3-4e34-86e3-3617262abf23",
    "LastUpdatedTimestamp": "2019-05-08T16:10:13.809Z",
    "LatestVersion": "5e3f6f64-a565-491e-8de0-3c0d8e0f2073",
    "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/loggers/49eeeb66-f1d3-4e34-86e3-3617262abf23/versions/5e3f6f64-
a565-491e-8de0-3c0d8e0f2073",
    "tags": {}
}
```

- Para obtener información sobre la API, consulte GetLoggerDefinition en la Referencia de comandos de la AWS CLI.

`get-resource-definition-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource-definition-version`.

AWS CLI

Para recuperar información sobre una versión específica de una definición de recurso

En el siguiente ejemplo de `get-resource-definition-version`, se recupera información sobre la versión especificada de la definición de recurso especificada. Para recuperar los ID de todas las versiones de la definición de recurso, utilice el comando `list-resource-definition-versions`. Para recuperar el ID de la última versión agregada a la definición de recurso, utilice el comando `get-resource-definition` y compruebe la propiedad `LatestVersion`.

```
aws greengrass get-resource-definition-version \
    --resource-definition-id "ad8c101d-8109-4b0e-b97d-9cc5802ab658" \
    --resource-definition-version-id "26e8829a-491a-464d-9c87-664bf6f6f2be"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/resources/ad8c101d-8109-4b0e-b97d-9cc5802ab658/
versions/26e8829a-491a-464d-9c87-664bf6f6f2be",
    "CreationTimestamp": "2019-06-19T16:40:59.392Z",
    "Definition": {
        "Resources": [
            {
                "Id": "26ff3f7b-839a-4217-9fdc-a218308b3963",
                "Name": "usb-port",
                "ResourceDataContainer": {
                    "LocalDeviceResourceData": {
                        "GroupOwnerSetting": {
                            "AutoAddGroupOwner": false
                        },
                        "SourcePath": "/dev/bus/usb"
                    }
                }
            }
        ]
    },
    "Id": "ad8c101d-8109-4b0e-b97d-9cc5802ab658",
    "Version": "26e8829a-491a-464d-9c87-664bf6f6f2be"
}
```

- Para obtener información sobre la API, consulte GetResourceDefinitionVersion en la Referencia de comandos de la AWS CLI.

`get-resource-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource-definition`.

AWS CLI

Para recuperar información sobre una definición de recurso

En el siguiente ejemplo de `get-resource-definition`, se recupera información sobre la definición de recurso especificada. Para recuperar los ID de sus definiciones de recurso, utilice el comando `list-resource-definitions`.

```
aws greengrass get-resource-definition \
```

```
    --resource-definition-id "ad8c101d-8109-4b0e-b97d-9cc5802ab658"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
resources/ad8c101d-8109-4b0e-b97d-9cc5802ab658",
    "CreationTimestamp": "2019-06-19T16:40:59.261Z",
    "Id": "ad8c101d-8109-4b0e-b97d-9cc5802ab658",
    "LastUpdatedTimestamp": "2019-06-19T16:40:59.261Z",
    "LatestVersion": "26e8829a-491a-464d-9c87-664bf6f6f2be",
    "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/resources/ad8c101d-8109-4b0e-b97d-9cc5802ab658/
versions/26e8829a-491a-464d-9c87-664bf6f6f2be",
    "tags": {}
}
```

- Para obtener información sobre la API, consulte GetResourceDefinition en la Referencia de comandos de la AWS CLI.

`get-service-role-for-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-role-for-account`.

AWS CLI

Para recuperar los detalles del rol de servicio asociado a su cuenta

En el siguiente ejemplo de `get-service-role-for-account`, se recupera información sobre el rol de servicio asociado a su cuenta de AWS.

```
aws greengrass get-service-role-for-account
```

Salida:

```
{
    "AssociatedAt": "2018-10-18T15:59:20Z",
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/Greengrass_ServiceRole"
}
```

Para obtener más información, consulte Greengrass service role en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte GetServiceRoleForAccount en la Referencia de comandos de la AWS CLI.

`get-subscription-definition-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-subscription-definition-version`.

AWS CLI

Para recuperar información sobre una versión específica de una definición de suscripción

En el siguiente ejemplo de `get-subscription-definition-version`, se recupera información sobre la versión especificada de la definición de suscripción especificada. Para recuperar los ID de todas las versiones de la definición de suscripción, utilice el comando `list-subscription-definition-versions`. Para recuperar el ID de la última versión agregada a la definición de suscripción, utilice el comando `get-subscription-definition` y compruebe la propiedad `LatestVersion`.

```
aws greengrass get-subscription-definition-version \
    --subscription-definition-id "70e49321-83d5-45d2-bc09-81f4917ae152" \
    --subscription-definition-version-id "88ae8699-12ac-4663-ba3f-4d7f0519140b"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
subscriptions/70e49321-83d5-45d2-bc09-81f4917ae152/versions/88ae8699-12ac-4663-
ba3f-4d7f0519140b",
    "CreationTimestamp": "2019-06-18T17:03:52.499Z",
    "Definition": {
        "Subscriptions": [
            {
                "Id": "692c4484-d89f-4f64-8edd-1a041a65e5b6",
                "Source": "arn:aws:lambda:us-
west-2:123456789012:function:Greengrass_HelloWorld:GG_HelloWorld",
                "Subject": "hello/world",
                "Target": "cloud"
            }
```

```
        ]
    },
    "Id": "70e49321-83d5-45d2-bc09-81f4917ae152",
    "Version": "88ae8699-12ac-4663-ba3f-4d7f0519140b"
}
```

- Para obtener información sobre la API, consulte GetSubscriptionDefinitionVersion en la Referencia de comandos de la AWS CLI.

`get-subscription-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-subscription-definition`.

AWS CLI

Para recuperar información sobre una definición de suscripción

En el siguiente ejemplo de `get-subscription-definition`, se recupera información sobre la definición de suscripción especificada. Para recuperar los ID de sus definiciones de suscripción, utilice el comando `list-subscription-definitions`.

```
aws greengrass get-subscription-definition \
    --subscription-definition-id "70e49321-83d5-45d2-bc09-81f4917ae152"
```

Salida:

```
{
    "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/definition/
subscriptions/70e49321-83d5-45d2-bc09-81f4917ae152",
    "CreationTimestamp": "2019-06-18T17:03:52.392Z",
    "Id": "70e49321-83d5-45d2-bc09-81f4917ae152",
    "LastUpdatedTimestamp": "2019-06-18T17:03:52.392Z",
    "LatestVersion": "88ae8699-12ac-4663-ba3f-4d7f0519140b",
    "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/subscriptions/70e49321-83d5-45d2-bc09-81f4917ae152/
versions/88ae8699-12ac-4663-ba3f-4d7f0519140b",
    "tags": {}
}
```

- Para obtener información sobre la API, consulte GetSubscriptionDefinition en la Referencia de comandos de la AWS CLI.

`get-thing-runtime-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-thing-runtime-configuration`.

AWS CLI

Para recuperar la configuración de tiempo de ejecución de un núcleo de Greengrass

En el siguiente ejemplo de `get-thing-runtime-configuration`, se recupera la configuración del tiempo de ejecución de un núcleo de Greengrass. Para poder recuperar la configuración del tiempo de ejecución, debe usar el comando `update-thing-runtime-configuration` para crear una configuración de tiempo de ejecución para el núcleo.

```
aws greengrass get-thing-runtime-configuration \
    --thing-name SampleGreengrassCore
```

Salida:

```
{
    "RuntimeConfiguration": {
        "TelemetryConfiguration": {
            "ConfigurationSyncStatus": "OutOfSync",
            "Telemetry": "On"
        }
    }
}
```

Para obtener más información, consulte Configuring telemetry settings en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte GetThingRuntimeConfiguration en la Referencia de comandos de la AWS CLI.

`list-bulk-deployment-detailed-reports`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-bulk-deployment-detailed-reports`.

AWS CLI

Para obtener información sobre las implementaciones individuales en una implementación por lotes

En el siguiente ejemplo de `list-bulk-deployment-detailed-reports`, se muestra información sobre las implementaciones individuales de una operación de implementación por lotes, incluido su estado.

```
aws greengrass list-bulk-deployment-detailed-reports \
    --bulk-deployment-id 42ce9c42-489b-4ed4-b905-8996aa50ef9d
```

Salida:

```
{
    "Deployments": [
        {
            "DeploymentType": "NewDeployment",
            "DeploymentStatus": "Success",
            "DeploymentId": "123456789012:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "DeploymentArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/groups/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333/
deployments/123456789012:123456789012:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "GroupArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/groups/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333/
versions/123456789012:a1b2c3d4-5678-90ab-cdef-EXAMPLE44444",
            "CreatedAt": "2020-01-21T21:34:16.501Z"
        },
        {
            "DeploymentType": "NewDeployment",
            "DeploymentStatus": "InProgress",
            "DeploymentId": "123456789012:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "DeploymentArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/groups/a1b2c3d4-5678-90ab-cdef-EXAMPLE55555/
deployments/123456789012:123456789012:a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "GroupArn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
groups/a1b2c3d4-5678-90ab-cdef-EXAMPLE55555/versions/a1b2c3d4-5678-90ab-cdef-
EXAMPLE66666",
            "CreatedAt": "2020-01-21T21:34:16.486Z"
        },
        ...
    ]
```

```
}
```

Para obtener más información, consulte Create Bulk Deployments for Groups en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte ListBulkDeploymentDetailedReports en la Referencia de comandos de la AWS CLI.

`list-bulk-deployments`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-bulk-deployments`.

AWS CLI

Para enumerar las implementaciones por lotes

En el siguiente ejemplo de `list-bulk-deployments`, se enumeran todos las implementaciones por lotes.

```
aws greengrass list-bulk-deployments
```

Salida:

```
{
    "BulkDeployments": [
        {
            "BulkDeploymentArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/bulk/deployments/870fb41b-6288-4e0c-bc76-a7ba4b4d3267",
            "BulkDeploymentId": "870fb41b-6288-4e0c-bc76-a7ba4b4d3267",
            "CreatedAt": "2019-06-25T16:11:33.265Z"
        }
    ]
}
```

Para obtener más información, consulte Create Bulk Deployments for Groups en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte ListBulkDeployments en la Referencia de comandos de la AWS CLI.

`list-connector-definition-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-connector-definition-versions`.

AWS CLI

Para enumerar las versiones disponibles para una definición de conector

En el siguiente ejemplo de `list-connector-definition-versions`, se enumeran las versiones disponibles para la definición de conector especificada. Utilice el comando `list-connector-definitions` para obtener el ID de definición de conector.

```
aws greengrass list-connector-definition-versions \
    --connector-definition-id "b5c4ebfd-f672-49a3-83cd-31c7216a7bb8"
```

Salida:

```
{
    "Versions": [
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/connectors/b5c4ebfd-f672-49a3-83cd-31c7216a7bb8/versions/63c57963-
c7c2-4a26-a7e2-7bf478ea2623",
            "CreationTimestamp": "2019-06-19T19:30:01.300Z",
            "Id": "b5c4ebfd-f672-49a3-83cd-31c7216a7bb8",
            "Version": "63c57963-c7c2-4a26-a7e2-7bf478ea2623"
        }
    ]
}
```

Para obtener más información, consulte Integrate with Services and Protocols Using Greengrass Connectors en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte ListConnectorDefinitionVersions en la Referencia de comandos de la AWS CLI.

`list-connector-definitions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-connector-definitions`.

AWS CLI

Para enumerar los conectores de Greengrass que están definidos

En el siguiente ejemplo de `list-connector-definitions`, se enumeran todos los conectores de Greengrass que están definidos para su cuenta de AWS.

```
aws greengrass list-connector-definitions
```

Salida:

```
{
    "Definitions": [
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/connectors/b5c4ebfd-f672-49a3-83cd-31c7216a7bb8",
            "CreationTimestamp": "2019-06-19T19:30:01.300Z",
            "Id": "b5c4ebfd-f672-49a3-83cd-31c7216a7bb8",
            "LastUpdatedTimestamp": "2019-06-19T19:30:01.300Z",
            "LatestVersion": "63c57963-c7c2-4a26-a7e2-7bf478ea2623",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/connectors/b5c4ebfd-f672-49a3-83cd-31c7216a7bb8/
versions/63c57963-c7c2-4a26-a7e2-7bf478ea2623",
            "Name": "MySNSConnector"
        }
    ]
}
```

Para obtener más información, consulte Integrate with Services and Protocols Using Greengrass Connectors en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte ListConnectorDefinitions en la Referencia de comandos de la AWS CLI.

`list-core-definition-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-core-definition-versions`.

AWS CLI

Para enumerar las versiones de una definición de núcleo de Greengrass

En el siguiente ejemplo de `list-core-definitions`, se enumeran todas las versiones de la definición de núcleo de Greengrass especificada. Puede usar el comando `list-core-definitions` para obtener el ID de la versión.

```
aws greengrass list-core-definition-versions \
    --core-definition-id "eaf280cb-138c-4d15-af36-6f681a1348f7"
```

Salida:

```
{
    "Versions": [
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/cores/eaf280cb-138c-4d15-af36-6f681a1348f7/versions/467c36e4-c5da-440c-
a97b-084e62593b4c",
            "CreationTimestamp": "2019-06-18T16:14:17.709Z",
            "Id": "eaf280cb-138c-4d15-af36-6f681a1348f7",
            "Version": "467c36e4-c5da-440c-a97b-084e62593b4c"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListCoreDefinitionVersions en la Referencia de comandos de la AWS CLI.

`list-core-definitions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-core-definitions`.

AWS CLI

Para enumerar las definiciones de núcleo de Greengrass

En el siguiente ejemplo de `list-core-definitions`, se enumeran todas las definiciones de núcleo de Greengrass para su cuenta de AWS.

```
aws greengrass list-core-definitions
```

Salida:

```
{
```

```
    "Definitions": [
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/cores/0507843c-c1ef-4f06-b051-817030df7e7d",
            "CreationTimestamp": "2018-10-17T04:30:32.786Z",
            "Id": "0507843c-c1ef-4f06-b051-817030df7e7d",
            "LastUpdatedTimestamp": "2018-10-17T04:30:32.786Z",
            "LatestVersion": "bcdf9e86-3793-491e-93af-3cdfbf4e22b7",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/cores/0507843c-c1ef-4f06-b051-817030df7e7d/versions/
bcdf9e86-3793-491e-93af-3cdfbf4e22b7"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/cores/31c22500-3509-4271-bafd-cf0655cda438",
            "CreationTimestamp": "2019-06-18T16:24:16.064Z",
            "Id": "31c22500-3509-4271-bafd-cf0655cda438",
            "LastUpdatedTimestamp": "2019-06-18T16:24:16.064Z",
            "LatestVersion": "2f350395-6d09-4c8a-8336-9ae5b57ace84",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/cores/31c22500-3509-4271-bafd-cf0655cda438/
versions/2f350395-6d09-4c8a-8336-9ae5b57ace84"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/cores/c906ed39-a1e3-4822-a981-7b9bd57b4b46",
            "CreationTimestamp": "2019-06-18T16:21:21.351Z",
            "Id": "c906ed39-a1e3-4822-a981-7b9bd57b4b46",
            "LastUpdatedTimestamp": "2019-06-18T16:21:21.351Z",
            "LatestVersion": "42aeeac3-fd9d-4312-a8fd-ffa9404a20e0",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/cores/c906ed39-a1e3-4822-a981-7b9bd57b4b46/versions/42aeeac3-
fd9d-4312-a8fd-ffa9404a20e0"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/cores/eaf280cb-138c-4d15-af36-6f681a1348f7",
            "CreationTimestamp": "2019-06-18T16:14:17.709Z",
            "Id": "eaf280cb-138c-4d15-af36-6f681a1348f7",
            "LastUpdatedTimestamp": "2019-06-18T16:14:17.709Z",
            "LatestVersion": "467c36e4-c5da-440c-a97b-084e62593b4c",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/cores/eaf280cb-138c-4d15-af36-6f681a1348f7/versions/467c36e4-
c5da-440c-a97b-084e62593b4c"
```

```
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListCoreDefinitions en la Referencia de comandos de la AWS CLI.

`list-deployments`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-deployments`.

AWS CLI

Para enumerar las implementaciones para un grupo de Greengrass

En el siguiente ejemplo de `list-deployments`, se enumeran las implementaciones del grupo de Greengrass especificado. Puede utilizar el comando `list-groups` para buscar el ID de grupo.

```
aws greengrass list-deployments \
    --group-id "1013db12-8b58-45ff-acc7-704248f66731"
```

Salida:

```
{
    "Deployments": [
        {
            "CreatedAt": "2019-06-18T17:04:32.702Z",
            "DeploymentId": "1065b8a0-812b-4f21-9d5d-e89b232a530f",
            "DeploymentType": "NewDeployment",
            "GroupArn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
groups/1013db12-8b58-45ff-acc7-704248f66731/versions/115136b3-cfd7-4462-
b77f-8741a4b00e5e"
        }
    ]
}
```

- Para obtener más información sobre la API, consulte ListDeployments en Referencia de comandos de la AWS CLI.

`list-device-definition-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-device-definition-versions`.

AWS CLI

Para enumerar las versiones de una definición de dispositivo

En el siguiente ejemplo de `list-device-definition-versions`, se muestran las versiones de las definiciones de dispositivos asociadas a la definición de dispositivo especificada.

```
aws greengrass list-device-definition-versions \
    --device-definition-id "f9ba083d-5ad4-4534-9f86-026a45df1ccd"
```

Salida:

```
{
    "Versions": [
        {
            "Version": "83c13984-6fed-447e-84d5-5b8aa45d5f71",
            "CreationTimestamp": "2019-09-11T00:15:09.838Z",
            "Id": "f9ba083d-5ad4-4534-9f86-026a45df1ccd",
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/devices/f9ba083d-5ad4-4534-9f86-026a45df1ccd/
versions/83c13984-6fed-447e-84d5-5b8aa45d5f71"
        },
        {
            "Version": "3b5cc510-58c1-44b5-9d98-4ad858ffa795",
            "CreationTimestamp": "2019-09-11T00:11:06.197Z",
            "Id": "f9ba083d-5ad4-4534-9f86-026a45df1ccd",
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/devices/f9ba083d-5ad4-4534-9f86-026a45df1ccd/
versions/3b5cc510-58c1-44b5-9d98-4ad858ffa795"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListDeviceDefinitionVersions en la Referencia de comandos de la AWS CLI.

`list-device-definitions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-device-definitions`.

AWS CLI

Para enumerar las definiciones de dispositivos

En el siguiente ejemplo de `list-device-definitions`, se muestran detalles sobre las definiciones de dispositivos en su cuenta de AWS en la región de AWS especificada.

```
aws greengrass list-device-definitions \
    --region us-west-2
```

Salida:

```
{
    "Definitions": [
        {
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/devices/50f3274c-3f0a-4f57-b114-6f46085281ab/versions/
c777b0f5-1059-449b-beaa-f003ebc56c34",
            "LastUpdatedTimestamp": "2019-06-14T15:42:09.059Z",
            "LatestVersion": "c777b0f5-1059-449b-beaa-f003ebc56c34",
            "CreationTimestamp": "2019-06-14T15:42:09.059Z",
            "Id": "50f3274c-3f0a-4f57-b114-6f46085281ab",
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/devices/50f3274c-3f0a-4f57-b114-6f46085281ab"
        },
        {
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/devices/e01951c9-6134-479a-969a-1a15cac11c40/
versions/514d57aa-4ee6-401c-9fac-938a9f7a51e5",
            "Name": "TestDeviceDefinition",
            "LastUpdatedTimestamp": "2019-04-16T23:17:43.245Z",
            "LatestVersion": "514d57aa-4ee6-401c-9fac-938a9f7a51e5",
            "CreationTimestamp": "2019-04-16T23:17:43.245Z",
            "Id": "e01951c9-6134-479a-969a-1a15cac11c40",
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/devices/e01951c9-6134-479a-969a-1a15cac11c40"
        },
        {
```

```
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/devices/f9ba083d-5ad4-4534-9f86-026a45df1ccd/
versions/83c13984-6fed-447e-84d5-5b8aa45d5f71",
            "Name": "TemperatureSensors",
            "LastUpdatedTimestamp": "2019-09-10T00:19:03.698Z",
            "LatestVersion": "83c13984-6fed-447e-84d5-5b8aa45d5f71",
            "CreationTimestamp": "2019-09-11T00:11:06.197Z",
            "Id": "f9ba083d-5ad4-4534-9f86-026a45df1ccd",
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/devices/f9ba083d-5ad4-4534-9f86-026a45df1ccd"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListDeviceDefinitions en la Referencia de comandos de la AWS CLI.

`list-function-definition-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-function-definition-versions`.

AWS CLI

Para enumerar todas las versiones de una función de Lambda

En el siguiente ejemplo de `list-function-definition-versions`, se muestran todas las versiones de la función de Lambda especificada. Puede utilizar el comando `list-function-definitions` para obtener el ID.

```
aws greengrass list-function-definition-versions \
    --function-definition-id "063f5d1a-1dd1-40b4-9b51-56f8993d0f85"
```

Salida:

```
{
    "Versions": [
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/functions/063f5d1a-1dd1-40b4-9b51-56f8993d0f85/
versions/9748fda7-1589-4fcc-ac94-f5559e88678b",
            "CreationTimestamp": "2019-06-18T17:04:30.776Z",
```

```
            "Id": "063f5d1a-1dd1-40b4-9b51-56f8993d0f85",
            "Version": "9748fda7-1589-4fcc-ac94-f5559e88678b"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/functions/063f5d1a-1dd1-40b4-9b51-56f8993d0f85/
versions/9b08df77-26f2-4c29-93d2-769715edcfec",
            "CreationTimestamp": "2019-06-18T17:02:44.087Z",
            "Id": "063f5d1a-1dd1-40b4-9b51-56f8993d0f85",
            "Version": "9b08df77-26f2-4c29-93d2-769715edcfec"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/functions/063f5d1a-1dd1-40b4-9b51-56f8993d0f85/
versions/4236239f-94f7-4b90-a2f8-2a24c829d21e",
            "CreationTimestamp": "2019-06-18T17:01:42.284Z",
            "Id": "063f5d1a-1dd1-40b4-9b51-56f8993d0f85",
            "Version": "4236239f-94f7-4b90-a2f8-2a24c829d21e"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/functions/063f5d1a-1dd1-40b4-9b51-56f8993d0f85/
versions/343408bb-549a-4fbe-b043-853643179a39",
            "CreationTimestamp": "2019-06-18T16:21:21.431Z",
            "Id": "063f5d1a-1dd1-40b4-9b51-56f8993d0f85",
            "Version": "343408bb-549a-4fbe-b043-853643179a39"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListFunctionDefinitionVersions en la Referencia de comandos de la AWS CLI.

`list-function-definitions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-function-definitions`.

AWS CLI

Para enumerar funciones de Lambda

En el siguiente ejemplo de `list-function-definitions`, se enumeran todas las funciones de Lambda definidas para su cuenta de AWS.

```
aws greengrass list-function-definitions
```

Salida:

```
{
    "Definitions": [
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/functions/017970a5-8952-46dd-b1c1-020b3ae8e960",
            "CreationTimestamp": "2018-10-17T04:30:32.884Z",
            "Id": "017970a5-8952-46dd-b1c1-020b3ae8e960",
            "LastUpdatedTimestamp": "2018-10-17T04:30:32.884Z",
            "LatestVersion": "4380b302-790d-4ed8-92bf-02e88afecb15",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/functions/017970a5-8952-46dd-b1c1-020b3ae8e960/
versions/4380b302-790d-4ed8-92bf-02e88afecb15"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/functions/063f5d1a-1dd1-40b4-9b51-56f8993d0f85",
            "CreationTimestamp": "2019-06-18T16:21:21.431Z",
            "Id": "063f5d1a-1dd1-40b4-9b51-56f8993d0f85",
            "LastUpdatedTimestamp": "2019-06-18T16:21:21.431Z",
            "LatestVersion": "9748fda7-1589-4fcc-ac94-f5559e88678b",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/functions/063f5d1a-1dd1-40b4-9b51-56f8993d0f85/
versions/9748fda7-1589-4fcc-ac94-f5559e88678b"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/functions/6598e653-a262-440c-9967-e2697f64da7b",
            "CreationTimestamp": "2019-06-18T16:24:16.123Z",
            "Id": "6598e653-a262-440c-9967-e2697f64da7b",
            "LastUpdatedTimestamp": "2019-06-18T16:24:16.123Z",
            "LatestVersion": "38bc6ccd-98a2-4ce7-997e-16c84748fae4",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/functions/6598e653-a262-440c-9967-e2697f64da7b/
versions/38bc6ccd-98a2-4ce7-997e-16c84748fae4"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/functions/c668df84-fad2-491b-95f4-655d2cad7885",
            "CreationTimestamp": "2019-06-18T16:14:17.784Z",
```

```
            "Id": "c668df84-fad2-491b-95f4-655d2cad7885",
            "LastUpdatedTimestamp": "2019-06-18T16:14:17.784Z",
            "LatestVersion": "37dd68c4-a64f-40ba-aa13-71fecc3ebded",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/functions/c668df84-fad2-491b-95f4-655d2cad7885/
versions/37dd68c4-a64f-40ba-aa13-71fecc3ebded"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListFunctionDefinitions en la Referencia de comandos de la AWS CLI.

`list-group-certificate-authorities`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-group-certificate-authorities`.

AWS CLI

Para enumerar las CA actuales para un grupo

En el siguiente ejemplo `list-group-certificate-authorities`, se enumeran las entidades de certificación (CA) actuales del grupo de Greengrass especificado.

```
aws greengrass list-group-certificate-authorities \
    --group-id "1013db12-8b58-45ff-acc7-704248f66731"
```

Salida:

```
{
    "GroupCertificateAuthorities": [
        {
            "GroupCertificateAuthorityArn": "arn:aws:greengrass:us-
west-2:123456789012:/greengrass/groups/1013db12-8b58-45ff-acc7-704248f66731/
certificateauthorities/
f0430e1736ea8ed30cc5d5de9af67a7e3586bad9ae4d89c2a44163f65fdd8cf6",
            "GroupCertificateAuthorityId":
 "f0430e1736ea8ed30cc5d5de9af67a7e3586bad9ae4d89c2a44163f65fdd8cf6"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListGroupCertificateAuthorities en la Referencia de comandos de la AWS CLI.

`list-group-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-group-versions`.

AWS CLI

Para enumerar las versiones de un grupo de Greengrass

En el siguiente ejemplo de `list-group-versions`, se enumeran las versiones del grupo de Greengrass especificado.

```
aws greengrass list-group-versions \
    --group-id "1013db12-8b58-45ff-acc7-704248f66731"
```

Salida:

```
{
    "Versions": [
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
groups/1013db12-8b58-45ff-acc7-704248f66731/versions/115136b3-cfd7-4462-
b77f-8741a4b00e5e",
            "CreationTimestamp": "2019-06-18T17:04:30.915Z",
            "Id": "1013db12-8b58-45ff-acc7-704248f66731",
            "Version": "115136b3-cfd7-4462-b77f-8741a4b00e5e"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/groups/1013db12-8b58-45ff-acc7-704248f66731/versions/4340669d-
d14d-44e3-920c-46c928750750",
            "CreationTimestamp": "2019-06-18T17:03:52.663Z",
            "Id": "1013db12-8b58-45ff-acc7-704248f66731",
            "Version": "4340669d-d14d-44e3-920c-46c928750750"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/groups/1013db12-8b58-45ff-acc7-704248f66731/
versions/1b06e099-2d5b-4f10-91b9-78c4e060f5da",
            "CreationTimestamp": "2019-06-18T17:02:44.189Z",
```

```
            "Id": "1013db12-8b58-45ff-acc7-704248f66731",
            "Version": "1b06e099-2d5b-4f10-91b9-78c4e060f5da"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
groups/1013db12-8b58-45ff-acc7-704248f66731/versions/2d3f27f1-3b43-4554-
ab7a-73ec30477efe",
            "CreationTimestamp": "2019-06-18T17:01:42.401Z",
            "Id": "1013db12-8b58-45ff-acc7-704248f66731",
            "Version": "2d3f27f1-3b43-4554-ab7a-73ec30477efe"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
groups/1013db12-8b58-45ff-acc7-704248f66731/versions/d20f7ae9-3444-4c1c-b025-
e2ede23cdd31",
            "CreationTimestamp": "2019-06-18T16:21:21.457Z",
            "Id": "1013db12-8b58-45ff-acc7-704248f66731",
            "Version": "d20f7ae9-3444-4c1c-b025-e2ede23cdd31"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListGroupVersions en la Referencia de comandos de la AWS CLI.

`list-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-groups`.

AWS CLI

Para enumerar los grupos de Greengrass

En el siguiente ejemplo de `list-groups`, se enumeran todos los grupos de Greengrass definidos en la cuenta de AWS.

```
aws greengrass list-groups
```

Salida:

```
{
```

```
    "Groups": [
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
groups/1013db12-8b58-45ff-acc7-704248f66731",
            "CreationTimestamp": "2019-06-18T16:21:21.457Z",
            "Id": "1013db12-8b58-45ff-acc7-704248f66731",
            "LastUpdatedTimestamp": "2019-06-18T16:21:21.457Z",
            "LatestVersion": "115136b3-cfd7-4462-b77f-8741a4b00e5e",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/groups/1013db12-8b58-45ff-acc7-704248f66731/versions/115136b3-cfd7-4462-
b77f-8741a4b00e5e",
            "Name": "GGGroup4Pi3"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
groups/1402daf9-71cf-4cfe-8be0-d5e80526d0d8",
            "CreationTimestamp": "2018-10-31T21:52:46.603Z",
            "Id": "1402daf9-71cf-4cfe-8be0-d5e80526d0d8",
            "LastUpdatedTimestamp": "2018-10-31T21:52:46.603Z",
            "LatestVersion": "749af901-60ab-456f-a096-91b12d983c29",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/groups/1402daf9-71cf-4cfe-8be0-d5e80526d0d8/versions/749af901-60ab-456f-
a096-91b12d983c29",
            "Name": "MyTestGroup"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
groups/504b5c8d-bbed-4635-aff1-48ec5b586db5",
            "CreationTimestamp": "2018-12-31T21:39:36.771Z",
            "Id": "504b5c8d-bbed-4635-aff1-48ec5b586db5",
            "LastUpdatedTimestamp": "2018-12-31T21:39:36.771Z",
            "LatestVersion": "46911e8e-f9bc-4898-8b63-59c7653636ec",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/groups/504b5c8d-bbed-4635-aff1-48ec5b586db5/versions/46911e8e-
f9bc-4898-8b63-59c7653636ec",
            "Name": "smp-ggrass-group"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListGroups en la Referencia de comandos de la AWS CLI.

`list-logger-definition-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-logger-definition-versions`.

AWS CLI

Para obtener una lista de versiones de una definición de registrador

En el siguiente ejemplo de `list-logger-definition-versions`, se obtiene una lista de todas las versiones de la definición de registrador especificada.

```
aws greengrass list-logger-definition-versions \
    --logger-definition-id "49eeeb66-f1d3-4e34-86e3-3617262abf23"
```

Salida:

```
{
    "Versions": [
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/loggers/49eeeb66-f1d3-4e34-86e3-3617262abf23/versions/5e3f6f64-
a565-491e-8de0-3c0d8e0f2073",
            "CreationTimestamp": "2019-05-08T16:10:13.866Z",
            "Id": "49eeeb66-f1d3-4e34-86e3-3617262abf23",
            "Version": "5e3f6f64-a565-491e-8de0-3c0d8e0f2073"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/loggers/49eeeb66-f1d3-4e34-86e3-3617262abf23/versions/3ec6d3af-eb85-48f9-
a16d-1c795fe696d7",
            "CreationTimestamp": "2019-05-08T16:10:13.809Z",
            "Id": "49eeeb66-f1d3-4e34-86e3-3617262abf23",
            "Version": "3ec6d3af-eb85-48f9-a16d-1c795fe696d7"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListLoggerDefinitionVersions en la Referencia de comandos de la AWS CLI.

`list-logger-definitions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-logger-definitions`.

AWS CLI

Para obtener una lista de definiciones de registrador

En el siguiente ejemplo de `list-logger-definitions`, se enumeran todas las definiciones de registrador para su cuenta de AWS.

```
aws greengrass list-logger-definitions
```

Salida:

```
{
    "Definitions": [
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/loggers/49eeeb66-f1d3-4e34-86e3-3617262abf23",
            "CreationTimestamp": "2019-05-08T16:10:13.809Z",
            "Id": "49eeeb66-f1d3-4e34-86e3-3617262abf23",
            "LastUpdatedTimestamp": "2019-05-08T16:10:13.809Z",
            "LatestVersion": "5e3f6f64-a565-491e-8de0-3c0d8e0f2073",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/loggers/49eeeb66-f1d3-4e34-86e3-3617262abf23/
versions/5e3f6f64-a565-491e-8de0-3c0d8e0f2073"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListLoggerDefinitions en la Referencia de comandos de la AWS CLI.

`list-resource-definition-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-definition-versions`.

AWS CLI

Para enumerar las versiones de una definición de recurso

En el siguiente ejemplo de `list-resource-definition-versions`, se enumeran las versiones para el recurso de Greengrass especificado.

```
aws greengrass list-resource-definition-versions \
    --resource-definition-id "ad8c101d-8109-4b0e-b97d-9cc5802ab658"
```

Salida:

```
{
    "Versions": [
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/resources/ad8c101d-8109-4b0e-b97d-9cc5802ab658/
versions/26e8829a-491a-464d-9c87-664bf6f6f2be",
            "CreationTimestamp": "2019-06-19T16:40:59.392Z",
            "Id": "ad8c101d-8109-4b0e-b97d-9cc5802ab658",
            "Version": "26e8829a-491a-464d-9c87-664bf6f6f2be"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/resources/ad8c101d-8109-4b0e-b97d-9cc5802ab658/
versions/432d92f6-12de-4ec9-a704-619a942a62aa",
            "CreationTimestamp": "2019-06-19T16:40:59.261Z",
            "Id": "ad8c101d-8109-4b0e-b97d-9cc5802ab658",
            "Version": "432d92f6-12de-4ec9-a704-619a942a62aa"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListResourceDefinitionVersions en la Referencia de comandos de la AWS CLI.

`list-resource-definitions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-definitions`.

AWS CLI

Para enumerar los recursos que están definidos

En el siguiente ejemplo de `list-resource-definitions`, se enumeran los recursos que están definidos para que los utilice AWS IoT Greengrass.

```
aws greengrass list-resource-definitions
```

Salida:

```
{
    "Definitions": [
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/resources/ad8c101d-8109-4b0e-b97d-9cc5802ab658",
            "CreationTimestamp": "2019-06-19T16:40:59.261Z",
            "Id": "ad8c101d-8109-4b0e-b97d-9cc5802ab658",
            "LastUpdatedTimestamp": "2019-06-19T16:40:59.261Z",
            "LatestVersion": "26e8829a-491a-464d-9c87-664bf6f6f2be",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/resources/ad8c101d-8109-4b0e-b97d-9cc5802ab658/
versions/26e8829a-491a-464d-9c87-664bf6f6f2be"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/resources/c8bb9ebc-c3fd-40a4-9c6a-568d75569d38",
            "CreationTimestamp": "2019-06-19T21:51:28.212Z",
            "Id": "c8bb9ebc-c3fd-40a4-9c6a-568d75569d38",
            "LastUpdatedTimestamp": "2019-06-19T21:51:28.212Z",
            "LatestVersion": "a5f94d0b-f6bc-40f4-bb78-7a1c5fe13ba1",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/resources/c8bb9ebc-c3fd-40a4-9c6a-568d75569d38/versions/
a5f94d0b-f6bc-40f4-bb78-7a1c5fe13ba1",
            "Name": "MyGreengrassResources"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListResourceDefinitions en la Referencia de comandos de la AWS CLI.

`list-subscription-definition-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-subscription-definition-versions`.

AWS CLI

Para enumerar las versiones de una definición de suscripción

En el siguiente ejemplo de `list-subscription-definition-versions` se enumeran todas las versiones de la suscripción especificada. Puede usar el comando `list-subscription-definitions` para buscar el ID de la suscripción.

```
aws greengrass list-subscription-definition-versions \
    --subscription-definition-id "70e49321-83d5-45d2-bc09-81f4917ae152"
```

Salida:

```
{
    "Versions": [
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/subscriptions/70e49321-83d5-45d2-bc09-81f4917ae152/
versions/88ae8699-12ac-4663-ba3f-4d7f0519140b",
            "CreationTimestamp": "2019-06-18T17:03:52.499Z",
            "Id": "70e49321-83d5-45d2-bc09-81f4917ae152",
            "Version": "88ae8699-12ac-4663-ba3f-4d7f0519140b"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/subscriptions/70e49321-83d5-45d2-bc09-81f4917ae152/versions/7e320ba3-
c369-4069-a2f0-90acb7f219d6",
            "CreationTimestamp": "2019-06-18T17:03:52.392Z",
            "Id": "70e49321-83d5-45d2-bc09-81f4917ae152",
            "Version": "7e320ba3-c369-4069-a2f0-90acb7f219d6"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListSubscriptionDefinitionVersions en la Referencia de comandos de la AWS CLI.

`list-subscription-definitions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-subscription-definitions`.

AWS CLI

Para obtener una lista de definiciones de suscripciones

En el siguiente ejemplo de `list-subscription-definitions`, se enumeran todas las suscripciones de AWS IoT Greengrass definidas en la cuenta de AWS.

```
aws greengrass list-subscription-definitions
```

Salida:

```
{
    "Definitions": [
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/subscriptions/70e49321-83d5-45d2-bc09-81f4917ae152",
            "CreationTimestamp": "2019-06-18T17:03:52.392Z",
            "Id": "70e49321-83d5-45d2-bc09-81f4917ae152",
            "LastUpdatedTimestamp": "2019-06-18T17:03:52.392Z",
            "LatestVersion": "88ae8699-12ac-4663-ba3f-4d7f0519140b",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/subscriptions/70e49321-83d5-45d2-bc09-81f4917ae152/
versions/88ae8699-12ac-4663-ba3f-4d7f0519140b"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/subscriptions/cd6f1c37-d9a4-4e90-be94-01a7404f5967",
            "CreationTimestamp": "2018-10-18T15:45:34.024Z",
            "Id": "cd6f1c37-d9a4-4e90-be94-01a7404f5967",
            "LastUpdatedTimestamp": "2018-10-18T15:45:34.024Z",
            "LatestVersion": "d1cf8fac-284f-4f6a-98fe-a2d36d089373",
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/subscriptions/cd6f1c37-d9a4-4e90-be94-01a7404f5967/versions/
d1cf8fac-284f-4f6a-98fe-a2d36d089373"
        },
        {
            "Arn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/subscriptions/fa81bc84-3f59-4377-a84b-5d0134da359b",
            "CreationTimestamp": "2018-10-22T17:09:31.429Z",
            "Id": "fa81bc84-3f59-4377-a84b-5d0134da359b",
            "LastUpdatedTimestamp": "2018-10-22T17:09:31.429Z",
            "LatestVersion": "086d1b08-b25a-477c-a16f-6f9b3a9c295a",
```

```
            "LatestVersionArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/definition/subscriptions/fa81bc84-3f59-4377-a84b-5d0134da359b/
versions/086d1b08-b25a-477c-a16f-6f9b3a9c295a"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListSubscriptionDefinitions en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas asociadas a un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se enumerar las etiquetas y sus valores asociados al recurso especificado.

```
aws greengrass list-tags-for-resource \
    --resource-arn "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/resources/ad8c101d-8109-4b0e-b97d-9cc5802ab658"
```

Salida:

```
{
    "tags": {
        "ResourceSubType": "USB",
        "ResourceType": "Device"
    }
}
```

Para obtener más información, consulte Tagging Your Greengrass Resources en la Guía para desarrolladores de AWS IoT Greengrass.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`reset-deployments`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-deployments`.

AWS CLI

Para limpiar la información de implementación para un grupo de Greengrass

En el siguiente ejemplo de `reset-deployments`, se limpian las implementaciones del grupo de Greengrass especificado. Al agregar `--force option`, la información de implementación se restablece sin esperar a que el dispositivo de núcleo responda.

```
aws greengrass reset-deployments \
    --group-id "1402daf9-71cf-4cfe-8be0-d5e80526d0d8" \
    --force
```

Salida:

```
{
    "DeploymentArn": "arn:aws:greengrass:us-west-2:123456789012:/
greengrass/groups/1402daf9-71cf-4cfe-8be0-d5e80526d0d8/
deployments/7dd4e356-9882-46a3-9e28-6d21900c011a",
    "DeploymentId": "7dd4e356-9882-46a3-9e28-6d21900c011a"
}
```

Para obtener más información, consulte Reset Deployments en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte ResetDeployments en la Referencia de comandos de la AWS CLI.

`start-bulk-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-bulk-deployment`.

AWS CLI

Para iniciar una operación de implementación por lotes

En el siguiente ejemplo `start-bulk-deployment`, se inicia una operación de implementación por lotes, usando un archivo almacenado en un bucket de S3 para especificar los grupos que se implementarán.

```
aws greengrass start-bulk-deployment \
    --cli-input-json "{\"InputFileUri\":\"https://gg-group-deployment1.s3-us-
west-2.amazonaws.com/MyBulkDeploymentInputFile.txt\", \"ExecutionRoleArn\":
\"arn:aws:iam::123456789012:role/ggCreateDeploymentRole\",\"AmznClientToken\":
\"yourAmazonClientToken\"}"
```

Salida:

```
{
    "BulkDeploymentArn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
bulk/deployments/870fb41b-6288-4e0c-bc76-a7ba4b4d3267",
    "BulkDeploymentId": "870fb41b-6288-4e0c-bc76-a7ba4b4d3267"
}
```

Para obtener más información, consulte Create Bulk Deployments for Groups en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte StartBulkDeployment en la Referencia de comandos de la AWS CLI.

`stop-bulk-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-bulk-deployment`.

AWS CLI

Para detener una implementación por lotes

En el siguiente ejemplo de `stop-bulk-deployment`, se detiene la implementación por lotes especificada. Si intenta detener una implementación por lotes que se ha completado, recibirá un error: `InvalidInputException: Cannot change state of finished execution.`

```
aws greengrass stop-bulk-deployment \
    --bulk-deployment-id "870fb41b-6288-4e0c-bc76-a7ba4b4d3267"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Create Bulk Deployments for Groups en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte StopBulkDeployment en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para aplicar etiquetas a un recurso

En el siguiente ejemplo de `tag-resource`, se aplican dos etiquetas, `ResourceType` y `ResourceSubType`, al recurso de Greengrass especificado. Esta operación puede agregar tanto etiquetas como valores nuevos, o actualizar el valor de las etiquetas existentes. Para eliminar una etiqueta, utilice el comando `untag-resource`.

```
aws greengrass tag-resource \
    --resource-arn "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
definition/resources/ad8c101d-8109-4b0e-b97d-9cc5802ab658" \
    --tags "ResourceType=Device,ResourceSubType=USB"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging Your Greengrass Resources en la Guía para desarrolladores de AWS IoT Greengrass.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar una etiqueta y su valor de un recurso

En el siguiente ejemplo de `untag-resource`, se quita la etiqueta cuya clave es `Category` del grupo de Greengrass especificado. Si la clave `Category` no existe para el recurso especificado, no se devuelve ningún error.

```
aws greengrass untag-resource \
    --resource-arn "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
groups/1013db12-8b58-45ff-acc7-704248f66731" \
    --tag-keys "Category"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging Your Greengrass Resources en la Guía para desarrolladores de AWS IoT Greengrass.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-connectivity-info

En el siguiente ejemplo de código, se muestra cómo utilizar `update-connectivity-info`.

AWS CLI

Para actualizar la información de conectividad para un núcleo de Greengrass

En el siguiente ejemplo de `update-connectivity-info`, se cambian los puntos de conexión que los dispositivos pueden usar para conectarse al núcleo de Greengrass especificado. La información de conectividad es una lista de direcciones IP o nombres de dominio, con los números de puerto correspondientes y los metadatos opcionales definidos por el cliente. Es posible que tenga que actualizar información de conectividad cuando la red local cambie.

```
aws greengrass update-connectivity-info \
    --thing-name "MyGroup_Core" \
    --connectivity-info "[{\"Metadata\":\"\",\"PortNumber\":8883,\"HostAddress\":
\"127.0.0.1\",\"Id\":\"localhost_127.0.0.1_0\"},{\"Metadata\":\"\",\"PortNumber
\":8883,\"HostAddress\":\"192.168.1.3\",\"Id\":\"localIP_192.168.1.3\"}]"
```

Salida:

```
{
    "Version": "312de337-59af-4cf9-a278-2a23bd39c300"
}
```

- Para obtener información sobre la API, consulte UpdateConnectivityInfo en la Referencia de comandos de la AWS CLI.

update-connector-definition

En el siguiente ejemplo de código, se muestra cómo utilizar `update-connector-definition`.

AWS CLI

Para actualizar el nombre para una definición de conector

En el siguiente ejemplo de `update-connector-definition`, se actualiza el nombre para la definición de conector especificada. Si desea actualizar los detalles del conector, utilice el comando `create-connector-definition-version` para crear una nueva versión.

```
aws greengrass update-connector-definition \
    --connector-definition-id "55d0052b-0d7d-44d6-b56f-21867215e118" \
    --name "GreengrassConnectors2019"
```

Para obtener más información, consulte Integrate with Services and Protocols Using Connectors en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte UpdateConnectorDefinition en la Referencia de comandos de la AWS CLI.

update-core-definition

En el siguiente ejemplo de código, se muestra cómo utilizar `update-core-definition`.

AWS CLI

Para actualizar una definición de núcleo

En el siguiente ejemplo de `update-core-definition`, se cambia el nombre de la definición de núcleo especificada. Solo puede actualizar la propiedad `name` de una definición de núcleo.

```
aws greengrass update-core-definition \
    --core-definition-id "582efe12-b05a-409e-9a24-a2ba1bcc4a12" \
    --name "MyCoreDevices"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración del software AWS IoT Greengrass Core en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte UpdateCoreDefinition en la Referencia de comandos de la AWS CLI.

`update-device-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-device-definition`.

AWS CLI

Para actualizar una definición de dispositivo

En el siguiente ejemplo de `update-device-definition`, se cambia el nombre de la definición de dispositivo especificada. Solo puede actualizar la propiedad `name` de una definición de dispositivo.

```
aws greengrass update-device-definition \
    --device-definition-id "f9ba083d-5ad4-4534-9f86-026a45df1ccd" \
    --name "TemperatureSensors"
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte UpdateDeviceDefinition en la Referencia de comandos de la AWS CLI.

`update-function-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-function-definition`.

AWS CLI

Para actualizar el nombre para una definición de función

En el siguiente ejemplo de `update-function-definition`, se actualiza el nombre para la definición de función especificada. Si desea actualizar los detalles de la función, utilice el comando `create-function-definition-version` para crear una versión nueva.

```
aws greengrass update-function-definition \
    --function-definition-id "e47952bd-dea9-4e2c-a7e1-37bbe8807f46" \
    --name ObsoleteFunction
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Run Local Lambda Functions en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte UpdateFunctionDefinition en la Referencia de comandos de la AWS CLI.

`update-group-certificate-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-group-certificate-configuration`.

AWS CLI

Para actualizar la caducidad de los certificados de un grupo

En el siguiente ejemplo de `update-group-certificate-configuration`, se establece un plazo de 10 días para los certificados generados para el grupo especificado.

```
aws greengrass update-group-certificate-configuration \
    --group-id "8eaadd72-ce4b-4f15-892a-0cc4f3a343f1" \
    --certificate-expiry-in-milliseconds 864000000
```

Salida:

```
{
    "CertificateExpiryInMilliseconds": 864000000,
    "CertificateAuthorityExpiryInMilliseconds": 2524607999000,
    "GroupId": "8eaadd72-ce4b-4f15-892a-0cc4f3a343f1"
}
```

Para obtener más información, consulte AWS IoT Greengrass Security en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre de la API, consulte UpdateGroupCertificateConfiguration en la Referencia de comandos de la AWS CLI.

`update-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-group`.

AWS CLI

Para actualizar el nombre del grupo

En el siguiente ejemplo de `update-group`, se actualiza el nombre del grupo de Greengrass especificado. Si desea actualizar los detalles del grupo, utilice el comando `create-group-version` para crear una versión nueva.

```
aws greengrass update-group \
    --group-id "1402daf9-71cf-4cfe-8be0-d5e80526d0d8" \
    --name TestGroup4of6
```

Para obtener más información, consulte Configure AWS IoT Greengrass on AWS IoT en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte UpdateGroup en la Referencia de comandos de la AWS CLI.

`update-logger-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-logger-definition`.

AWS CLI

Para actualizar una definición de registrador

En el siguiente ejemplo de `update-logger-definition`, se cambia el nombre de la definición de registrador especificada. Solo puede actualizar la propiedad `name` de una definición de registrador.

```
aws greengrass update-logger-definition \
    --logger-definition-id "a454b62a-5d56-4ca9-bdc4-8254e1662cb0" \
    --name "LoggingConfigsForSensors"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Supervisión de los registros de AWS IoT Greengrass en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte UpdateLoggerDefinition en la Referencia de comandos de la AWS CLI.

update-resource-definition

En el siguiente ejemplo de código, se muestra cómo utilizar update-resource-definition.

AWS CLI

Para actualizar el nombre de una definición de recurso

En el siguiente ejemplo de update-resource-definition, se actualiza el nombre para la definición de recurso especificada. Si desea cambiar los detalles del recurso, utilice el comando create-resource-definition-version para crear una versión nueva.

```
aws greengrass update-resource-definition \
    --resource-definition-id "c8bb9ebc-c3fd-40a4-9c6a-568d75569d38" \
    --name GreengrassConnectorResources
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Access Local Resources with Lambda Functions and Connectors en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte UpdateResourceDefinition en la Referencia de comandos de la AWS CLI.

update-subscription-definition

En el siguiente ejemplo de código, se muestra cómo utilizar update-subscription-definition.

AWS CLI

Para actualizar el nombre de una definición de suscripción

En el siguiente ejemplo de update-subscription-definition, se actualiza el nombre de la definición de suscripción especificada. Si desea cambiar los detalles de la suscripción, utilice el comando create-subscription-definition-version para crear una versión nueva.

```
aws greengrass update-subscription-definition \
    --subscription-definition-id "fa81bc84-3f59-4377-a84b-5d0134da359b" \
    --name "ObsoleteSubscription"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte el título en la guía.

- Para obtener información sobre la API, consulte UpdateSubscriptionDefinition en la Referencia de comandos de la AWS CLI.

`update-thing-runtime-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-thing-runtime-configuration`.

AWS CLI

Para activar la telemetría en la configuración del tiempo de ejecución de un núcleo de Greengrass

En el siguiente ejemplo de `update-thing-runtime-configuration`, se actualiza la configuración del tiempo de ejecución de un núcleo de Greengrass para activar la telemetría.

```
aws greengrass update-thing-runtime-configuration \
    --thing-name SampleGreengrassCore \
    --telemetry-configuration {\"Telemetry\":\"On\"}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuring telemetry settings en la Guía para desarrolladores de AWS IoT Greengrass.

- Para obtener información sobre la API, consulte UpdateThingRuntimeConfiguration en la Referencia de comandos de la AWS CLI.

AWS IoT Greengrass V2 Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS IoT Greengrass V2.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-service-role-to-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-service-role-to-account`.

AWS CLI

Para asociar el rol de servicio de Greengrass a su cuenta de AWS

En el siguiente ejemplo de `associate-service-role-to-account`, se asocia un rol de servicio a AWS IoT Greengrass para su cuenta de AWS.

```
aws greengrassv2 associate-service-role-to-account \
    --role-arn arn:aws:iam::123456789012:role/service-role/Greengrass_ServiceRole
```

Salida:

```
{
    "associatedAt": "2022-01-19T19:21:53Z"
}
```

Para obtener más información, consulte Greengrass service role en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte AssociateServiceRoleToAccount en la Referencia de comandos de la AWS CLI.

`batch-associate-client-device-with-core-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-associate-client-device-with-core-device`.

AWS CLI

Para asociar los dispositivos de cliente a un dispositivo de núcleo

En el siguiente ejemplo de `batch-associate-client-device-with-core-device`, se asocian dos dispositivos de cliente a un dispositivo de núcleo.

```
aws greengrassv2 batch-associate-client-device-with-core-device \
  --core-device-thing-name MyGreengrassCore \
  --entries thingName=MyClientDevice1 thingName=MyClientDevice2
```

Salida:

```
{
    "errorEntries": []
}
```

Para obtener más información, consulte Interact with local IoT devices en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte BatchAssociateClientDeviceWithCoreDevice en la Referencia de comandos de la AWS CLI.

`batch-disassociate-client-device-from-core-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-disassociate-client-device-from-core-device`.

AWS CLI

Para desasociar los dispositivos de cliente de un dispositivo de núcleo

En el siguiente ejemplo de `batch-disassociate-client-device-from-core-device`, se desasocian dos dispositivos de cliente de un dispositivo de núcleo.

```
aws greengrassv2 batch-disassociate-client-device-from-core-device \
  --core-device-thing-name MyGreengrassCore \
  --entries thingName=MyClientDevice1 thingName=MyClientDevice2
```

Salida:

```
{
    "errorEntries": []
}
```

Para obtener más información, consulte Interact with local IoT devices en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte BatchDisassociateClientDeviceFromCoreDevice en la Referencia de comandos de la AWS CLI.

`cancel-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-deployment`.

AWS CLI

Para cancelar una implementación

En el siguiente ejemplo de `cancel-deployment`, se detiene una implementación continua en un grupo de objetos.

```
aws greengrassv2 cancel-deployment \
    --deployment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "message": "SUCCESS"
}
```

Para obtener más información, consulte Cancel deployments en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte CancelDeployment en la Referencia de comandos de la AWS CLI.

`create-component-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-component-version`.

AWS CLI

Ejemplo 1: creación de una versión de componente a partir de una receta

En el siguiente ejemplo de `create-component-version`, se crea una versión de un componente de Hola, mundo a partir de un archivo de recetas.

```
aws greengrassv2 create-component-version \
    --inline-recipe fileb://com.example.HelloWorld-1.0.0.json
```

Contenido de `com.example.HelloWorld-1.0.0.json`:

```
{
    "RecipeFormatVersion": "2020-01-25",
    "ComponentName": "com.example.HelloWorld",
    "ComponentVersion": "1.0.0",
    "ComponentDescription": "My first AWS IoT Greengrass component.",
    "ComponentPublisher": "Amazon",
    "ComponentConfiguration": {
        "DefaultConfiguration": {
            "Message": "world"
        }
    },
    "Manifests": [
        {
            "Platform": {
                "os": "linux"
            },
            "Lifecycle": {
                "Run": "echo 'Hello {configuration:/Message}'"
            }
        }
    ]
}
```

Salida:

```
{
    "arn": "arn:aws:greengrass:us-
west-2:123456789012:components:com.example.HelloWorld:versions:1.0.0",
    "componentName": "com.example.HelloWorld",
    "componentVersion": "1.0.0",
    "creationTimestamp": "2021-01-07T16:24:33.650000-08:00",
    "status": {
        "componentState": "REQUESTED",
        "message": "NONE",
        "errors": {}
    }
}
```

Para obtener más información, consulte Create custom components y Upload components to deploy en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

Ejemplo 2: creación de una versión de componente a partir de una función de AWS Lambda

En el siguiente ejemplo de `create-component-version`, se crea una versión de un componente de Hola, mundo a partir de una función de AWS Lambda.

```
aws greengrassv2 create-component-version \
    --cli-input-json file://lambda-function-component.json
```

Contenido de `lambda-function-component.json`:

```
{
    "lambdaFunction": {
        "lambdaArn": "arn:aws:lambda:us-
west-2:123456789012:function:HelloWorldPythonLambda:1",
        "componentName": "com.example.HelloWorld",
        "componentVersion": "1.0.0",
        "componentLambdaParameters": {
            "eventSources": [
                {
                    "topic": "hello/world/+",
                    "type": "IOT_CORE"
                }
            ]
        }
    }
}
```

Salida:

```
{
    "arn": "arn:aws:greengrass:us-
west-2:123456789012:components:com.example.HelloWorld:versions:1.0.0",
    "componentName": "com.example.HelloWorld",
    "componentVersion": "1.0.0",
    "creationTimestamp": "2021-01-07T17:05:27.347000-08:00",
    "status": {
        "componentState": "REQUESTED",
        "message": "NONE",
        "errors": {}
    }
```

```
}
```

Para obtener más información, consulte Run AWS Lambda functions en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte CreateComponentVersion en la Referencia de comandos de la AWS CLI.

`create-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-deployment`.

AWS CLI

Ejemplo 1: creación de una implementación

En el siguiente ejemplo de `create-deployment`, se implementa la interfaz de la línea de comandos de AWS IoT Greengrass en un dispositivo de núcleo.

```
aws greengrassv2 create-deployment \
    --cli-input-json file://cli-deployment.json
```

Contenido de `cli-deployment.json`:

```
{
    "targetArn": "arn:aws:iot:us-west-2:123456789012:thing/MyGreengrassCore",
    "deploymentName": "Deployment for MyGreengrassCore",
    "components": {
        "aws.greengrass.Cli": {
            "componentVersion": "2.0.3"
        }
    },
    "deploymentPolicies": {
        "failureHandlingPolicy": "DO_NOTHING",
        "componentUpdatePolicy": {
            "timeoutInSeconds": 60,
            "action": "NOTIFY_COMPONENTS"
        },
        "configurationValidationPolicy": {
            "timeoutInSeconds": 60
        }
    },
    "iotJobConfiguration": {}
```

```
}
```

Salida:

```
{
    "deploymentId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Para obtener más información, consulte Create deployments en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

Ejemplo 2: creación de una implementación que actualice las configuraciones de los componentes

En el siguiente ejemplo de `create-deployment`, se implementa el componente del núcleo de AWS IoT Greengrass en un grupo de dispositivos de núcleo. Esta implementación aplica las siguientes actualizaciones de configuración para el componente del núcleo:

Restablezca la configuración de proxy de los dispositivos de destino en su configuración predeterminada sin proxy. Restablezca la configuración de MQTT de los dispositivos de destino a sus valores predeterminados. Establece las opciones de JVM para la JVM del núcleo. Establece el nivel de registro del núcleo.

```
aws greengrassv2 create-deployment \
    --cli-input-json file://nucleus-deployment.json
```

Contenido de `nucleus-deployment.json`:

```
{
    "targetArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/
MyGreengrassCoreGroup",
    "deploymentName": "Deployment for MyGreengrassCoreGroup",
    "components": {
        "aws.greengrass.Nucleus": {
            "componentVersion": "2.0.3",
            "configurationUpdate": {
                "reset": [
                    "/networkProxy",
                    "/mqtt"
                ],
                "merge": "{\"jvmOptions\":\"-Xmx64m\",\"logging\":{\"level\":\"WARN
\"}}"
```

```
            }
        }
    },
    "deploymentPolicies": {
        "failureHandlingPolicy": "ROLLBACK",
        "componentUpdatePolicy": {
            "timeoutInSeconds": 60,
            "action": "NOTIFY_COMPONENTS"
        },
        "configurationValidationPolicy": {
            "timeoutInSeconds": 60
        }
    },
    "iotJobConfiguration": {}
}
```

Salida:

```
{
    "deploymentId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "iotJobId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "iotJobArn": "arn:aws:iot:us-west-2:123456789012:job/a1b2c3d4-5678-90ab-cdef-
EXAMPLE22222"
}
```

Para obtener más información, consulte Create deployments y Update component configurations en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte CreateDeployment en la Referencia de comandos de la AWS CLI.

`delete-component`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-component`.

AWS CLI

Para eliminar la versión de un componente

En el siguiente ejemplo de `delete-component`, se elimina un componente de Hola, mundo.

```
aws greengrassv2 delete-component \
```

```
    --arn arn:aws:greengrass:us-
west-2:123456789012:components:com.example.HelloWorld:versions:1.0.0
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Manage components en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte DeleteComponent en la Referencia de comandos de la AWS CLI.

`delete-core-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-core-device`.

AWS CLI

Para eliminar un dispositivo de núcleo

En el siguiente ejemplo de `delete-core-device`, se elimina un dispositivo de núcleo de AWS IoT Greengrass.

```
aws greengrassv2 delete-core-device \
    --core-device-thing-name MyGreengrassCore
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uninstall the AWS IoT Greengrass Core software en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte DeleteCoreDevice en la Referencia de comandos de la AWS CLI.

`describe-component`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-component`.

AWS CLI

Para describir la versión de un componente

En el siguiente ejemplo de `describe-component`, se describe un componente de Hola, mundo.

```
aws greengrassv2 describe-component \
    --arn arn:aws:greengrass:us-
west-2:123456789012:components:com.example.HelloWorld:versions:1.0.0
```

Salida:

```
{
    "arn": "arn:aws:greengrass:us-
west-2:123456789012:components:com.example.HelloWorld:versions:1.0.0",
    "componentName": "com.example.HelloWorld",
    "componentVersion": "1.0.0",
    "creationTimestamp": "2021-01-07T17:12:11.133000-08:00",
    "publisher": "Amazon",
    "description": "My first AWS IoT Greengrass component.",
    "status": {
        "componentState": "DEPLOYABLE",
        "message": "NONE",
        "errors": {}
    },
    "platforms": [
        {
            "attributes": {
                "os": "linux"
            }
        }
    ]
}
```

Para obtener más información, consulte Manage components en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte DescribeComponent en la Referencia de comandos de la AWS CLI.

`disassociate-service-role-from-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-service-role-from-account`.

AWS CLI

Para desasociar el rol de servicio de Greengrass de su cuenta de AWS

En el siguiente ejemplo de `disassociate-service-role-from-account`, se desvincula el rol de servicio de Greengrass de AWS IoT Greengrass para su cuenta de AWS.

```
aws greengrassv2 disassociate-service-role-from-account
```

Salida:

```
{
    "disassociatedAt": "2022-01-19T19:26:09Z"
}
```

Para obtener más información, consulte Greengrass service role en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte DisassociateServiceRoleFromAccount en la Referencia de comandos de la AWS CLI.

`get-component-version-artifact`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-component-version-artifact`.

AWS CLI

Para obtener una URL con el fin de descargar un artefacto de componente

En el siguiente ejemplo de `get-component-version-artifact`, se obtiene una URL para descargar el archivo JAR del componente de la consola de depuración local.

```
aws greengrassv2 get-component-version-artifact \
    --arn arn:aws:greengrass:us-
west-2:aws:components:aws.greengrass.LocalDebugConsole:versions:2.0.3 \
    --artifact-name "Uvt6ZEzQ9TKiAuLbfXBX_APdY0TWks3uc46tHFHTzBM=/
aws.greengrass.LocalDebugConsole.jar"
```

Salida:

```
{
    "preSignedUrl": "https://evergreencomponentmanageme-
artifactbucket7410c9ef-g18n1iya8kwr.s3.us-west-2.amazonaws.com/public/
aws.greengrass.LocalDebugConsole/2.0.3/s3/ggv2-component-releases-prod-pdx/
```

```
EvergreenHttpDebugView/2ffc496ba41b39568968b22c582b4714a937193ee7687a45527238e696672521/
aws.greengrass.LocalDebugConsole/aws.greengrass.LocalDebugConsole.jar?X-Amz-
Security-Token=KwfLKSdEXAMPLE..."
}
```

Para obtener más información, consulte Manage components en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte GetComponentVersionArtifact en la Referencia de comandos de la AWS CLI.

`get-component`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-component`.

AWS CLI

Ejemplo 1: descarga de la receta de un componente en formato YAML (Linux, macOS o Unix)

En el siguiente ejemplo de `get-component`, se descarga la receta de un componente de Hola, mundo a un archivo en formato YAML. Este comando hace lo siguiente:

Utiliza los parámetros`--output` y `--query` para controlar la salida del comando. Estos parámetros extraen el blob de recetas de la salida del comando. Para obtener más información sobre la salida del comando, consulte Controlling Command Output en la Guía del usuario de la interfaz de línea de comandos de AWS. Utiliza la utilidad de `base64`. Esta utilidad descodifica el blob extraído en el texto original. El blob que devuelve un comando `get-component` correcto es texto codificado en base64. Debe descodificar este blob para obtener el texto original. Guarda el texto decodificado en un archivo. La sección final del comando (> `com.example.HelloWorld-1.0.0.json`) guarda el texto decodificado en un archivo.

```
aws greengrassv2 get-component \
    --arn arn:aws:greengrass:us-
west-2:123456789012:components:com.example.HelloWorld:versions:1.0.0 \
    --recipe-output-format YAML \
    --query recipe \
    --output text | base64 --decode > com.example.HelloWorld-1.0.0.json
```

Para obtener más información, consulte Manage components en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

Ejemplo 2: descarga de la receta de un componente en formato YAML (CMD de Windows)

En el siguiente ejemplo de `get-component`, se descarga la receta de un componente de Hola, mundo a un archivo en formato YAML. Este comando usa la utilidad `certutil`.

```
aws greengrassv2 get-component ^
    --arn arn:aws:greengrass:us-
west-2:675946970638:components:com.example.HelloWorld:versions:1.0.0 ^
    --recipe-output-format YAML ^
    --query recipe ^
    --output text > com.example.HelloWorld-1.0.0.yaml.b64

certutil -
decode com.example.HelloWorld-1.0.0.yaml.b64 com.example.HelloWorld-1.0.0.yaml
```

Para obtener más información, consulte Manage components en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

Ejemplo 3: descarga de la receta de un componente en formato YAML (Windows PowerShell)

En el siguiente ejemplo de `get-component`, se descarga la receta de un componente de Hola, mundo a un archivo en formato YAML. Este comando usa la utilidad `certutil`.

```
aws greengrassv2 get-component `
    --arn arn:aws:greengrass:us-
west-2:675946970638:components:com.example.HelloWorld:versions:1.0.0 `
    --recipe-output-format YAML `
    --query recipe `
    --output text > com.example.HelloWorld-1.0.0.yaml.b64

certutil -
decode com.example.HelloWorld-1.0.0.yaml.b64 com.example.HelloWorld-1.0.0.yaml
```

Para obtener más información, consulte Manage components en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte GetComponent en la Referencia de comandos de la AWS CLI.

`get-connectivity-info`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-connectivity-info`.

AWS CLI

Para obtener información de conectividad para un dispositivo de núcleo de Greengrass

En el siguiente ejemplo de `get-connectivity-info`, se obtiene información de conectividad para un dispositivo de núcleo de Greengrass. Los dispositivos de cliente utilizan esta información para conectarse al intermediario MQTT que se ejecuta en este dispositivo de núcleo.

```
aws greengrassv2 get-connectivity-info \
    --thing-name MyGreengrassCore
```

Salida:

```
{
    "connectivityInfo": [
        {
            "id": "localIP_192.0.2.0",
            "hostAddress": "192.0.2.0",
            "portNumber": 8883
        }
    ]
}
```

Para obtener más información, consulte Manage core device endpoints en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte GetConnectivityInfo en la Referencia de comandos de la AWS CLI.

`get-core-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-core-device`.

AWS CLI

Para obtener un dispositivo de núcleo

En el siguiente ejemplo de `get-core-device`, se obtiene información sobre un dispositivo de núcleo de AWS IoT Greengrass.

```
aws greengrassv2 get-core-device \
```

```
    --core-device-thing-name MyGreengrassCore
```

Salida:

```
{
    "coreDeviceThingName": "MyGreengrassCore",
    "coreVersion": "2.0.3",
    "platform": "linux",
    "architecture": "amd64",
    "status": "HEALTHY",
    "lastStatusUpdateTimestamp": "2021-01-08T04:57:58.838000-08:00",
    "tags": {}
}
```

Para obtener más información, consulte Check core device status en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte GetCoreDevice en la Referencia de comandos de la AWS CLI.

`get-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-deployment`.

AWS CLI

Para obtener una implementación

En el siguiente ejemplo de `get-deployment`, se obtiene información sobre la implementación del componente del núcleo de AWS IoT Greengrass en un grupo de dispositivos de núcleo.

```
aws greengrassv2 get-deployment \
    --deployment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "targetArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/
MyGreengrassCoreGroup",
    "revisionId": "14",
    "deploymentId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
    "deploymentName": "Deployment for MyGreengrassCoreGroup",
    "deploymentStatus": "ACTIVE",
    "iotJobId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "iotJobArn": "arn:aws:iot:us-west-2:123456789012:job/a1b2c3d4-5678-90ab-cdef-
EXAMPLE22222",
    "components": {
        "aws.greengrass.Nucleus": {
            "componentVersion": "2.0.3",
            "configurationUpdate": {
                "merge": "{\"jvmOptions\":\"-Xmx64m\",\"logging\":{\"level\":\"WARN
\"}}",
                "reset": [
                    "/networkProxy",
                    "/mqtt"
                ]
            }
        }
    },
    "deploymentPolicies": {
        "failureHandlingPolicy": "ROLLBACK",
        "componentUpdatePolicy": {
            "timeoutInSeconds": 60,
            "action": "NOTIFY_COMPONENTS"
        },
        "configurationValidationPolicy": {
            "timeoutInSeconds": 60
        }
    },
    "iotJobConfiguration": {},
    "creationTimestamp": "2021-01-07T17:21:20.691000-08:00",
    "isLatestForTarget": false,
    "tags": {}
}
```

Para obtener más información, consulte Deploy components to devices en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte GetDeployment en la Referencia de comandos de la AWS CLI.

`get-service-role-for-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-role-for-account`.

AWS CLI

Para obtener el rol de servicio de Greengrass para su cuenta de AWS

En el siguiente ejemplo de `get-service-role-for-account`, se obtiene el rol de servicio asociado a AWS IoT Greengrass para su cuenta de AWS.

```
aws greengrassv2 get-service-role-for-account
```

Salida:

```
{
    "associatedAt": "2022-01-19T19:21:53Z",
    "roleArn": "arn:aws:iam::123456789012:role/service-role/Greengrass_ServiceRole"
}
```

Para obtener más información, consulte Greengrass service role en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte GetServiceRoleForAccount en la Referencia de comandos de la AWS CLI.

`list-client-devices-associated-with-core-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-client-devices-associated-with-core-device`.

AWS CLI

Para enumerar los dispositivos cliente asociados a un dispositivo de núcleo

En el siguiente ejemplo de `list-client-devices-associated-with-core-device`, se enumeran todos los dispositivos de cliente asociados a un dispositivo de núcleo.

```
aws greengrassv2 list-client-devices-associated-with-core-device \
  --core-device-thing-name MyTestGreengrassCore
```

Salida:

```
{
    "associatedClientDevices": [
        {
```

```
            "thingName": "MyClientDevice2",
            "associationTimestamp": "2021-07-12T16:33:55.843000-07:00"
        },
        {
            "thingName": "MyClientDevice1",
            "associationTimestamp": "2021-07-12T16:33:55.843000-07:00"
        }
    ]
}
```

Para obtener más información, consulte Interact with local IoT devices en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte ListClientDevicesAssociatedWithCoreDevice en la Referencia de comandos de la AWS CLI.

`list-component-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-component-versions`.

AWS CLI

Para enumerar las versiones disponibles del componente

En el siguiente ejemplo de `list-component-versions`, se enumeran todas las versiones de un componente de Hola, mundo.

```
aws greengrassv2 list-component-versions \
    --arn arn:aws:greengrass:us-
west-2:123456789012:components:com.example.HelloWorld
```

Salida:

```
{
    "componentVersions": [
        {
            "componentName": "com.example.HelloWorld",
            "componentVersion": "1.0.1",
            "arn": "arn:aws:greengrass:us-
west-2:123456789012:components:com.example.HelloWorld:versions:1.0.1"
        },
        {
```

```
            "componentName": "com.example.HelloWorld",
            "componentVersion": "1.0.0",
            "arn": "arn:aws:greengrass:us-
west-2:123456789012:components:com.example.HelloWorld:versions:1.0.0"
        }
    ]
}
```

Para obtener más información, consulte Manage components en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte ListComponentVersions en la Referencia de comandos de la AWS CLI.

`list-components`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-components`.

AWS CLI

Para enumerar componentes

En el siguiente ejemplo de `list-components`, se muestra cada componente y su versión más reciente definida en su cuenta de AWS en la región actual.

```
aws greengrassv2 list-components
```

Salida:

```
{
    "components": [
        {
            "arn": "arn:aws:greengrass:us-
west-2:123456789012:components:com.example.HelloWorld",
            "componentName": "com.example.HelloWorld",
            "latestVersion": {
                "arn": "arn:aws:greengrass:us-
west-2:123456789012:components:com.example.HelloWorld:versions:1.0.1",
                "componentVersion": "1.0.1",
                "creationTimestamp": "2021-01-08T16:51:07.352000-08:00",
                "description": "My first AWS IoT Greengrass component.",
                "publisher": "Amazon",
```

```
                "platforms": [
                    {
                        "attributes": {
                            "os": "linux"
                        }
                    }
                ]
            }
        }
    ]
}
```

Para obtener más información, consulte Manage components en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener detalles de la API, consulte ListComponents en la Referencia de comandos de la AWS CLI.

`list-core-devices`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-core-devices`.

AWS CLI

Para enumerar los dispositivos de núcleo

En el siguiente ejemplo de `list-core-devices`, se muestran los dispositivos de núcleo de AWS IoT Greengrass de su cuenta de AWS en la región actual.

```
aws greengrassv2 list-core-devices
```

Salida:

```
{
    "coreDevices": [
        {
            "coreDeviceThingName": "MyGreengrassCore",
            "status": "HEALTHY",
            "lastStatusUpdateTimestamp": "2021-01-08T04:57:58.838000-08:00"
        }
    ]
}
```

Para obtener más información, consulte Check core device status en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte ListCoreDevices en la Referencia de comandos de la AWS CLI.

`list-deployments`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-deployments`.

AWS CLI

Para enumerar implementaciones

En el siguiente ejemplo de `list-deployments`, se muestra la versión más reciente de cada implementación definida en su cuenta de AWS en la región actual.

```
aws greengrassv2 list-deployments
```

Salida:

```
{
    "deployments": [
        {
            "targetArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/
MyGreengrassCoreGroup",
            "revisionId": "14",
            "deploymentId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "deploymentName": "Deployment for MyGreengrassCoreGroup",
            "creationTimestamp": "2021-01-07T17:21:20.691000-08:00",
            "deploymentStatus": "ACTIVE",
            "isLatestForTarget": false
        },
        {
            "targetArn": "arn:aws:iot:us-west-2:123456789012:thing/
MyGreengrassCore",
            "revisionId": "1",
            "deploymentId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "deploymentName": "Deployment for MyGreengrassCore",
            "creationTimestamp": "2021-01-06T16:10:42.407000-08:00",
            "deploymentStatus": "COMPLETED",
            "isLatestForTarget": false
```

```
        }
    ]
}
```

Para obtener más información, consulte Deploy components to devices en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener más información sobre la API, consulte ListDeployments en Referencia de comandos de la AWS CLI.

`list-effective-deployments`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-effective-deployments`.

AWS CLI

Para enumerar los trabajos de implementación

En el siguiente ejemplo de `list-effective-deployments`, se enumeran las implementaciones que se aplican a un dispositivo de núcleo de AWS IoT Greengrass.

```
aws greengrassv2 list-effective-deployments \
    --core-device-thing-name MyGreengrassCore
```

Salida:

```
{
    "effectiveDeployments": [
        {
            "deploymentId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "deploymentName": "Deployment for MyGreengrassCore",
            "iotJobId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "targetArn": "arn:aws:iot:us-west-2:123456789012:thing/
MyGreengrassCore",
            "coreDeviceExecutionStatus": "COMPLETED",
            "reason": "SUCCESSFUL",
            "creationTimestamp": "2021-01-06T16:10:42.442000-08:00",
            "modifiedTimestamp": "2021-01-08T17:21:27.830000-08:00"
        },
        {
            "deploymentId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "deploymentName": "Deployment for MyGreengrassCoreGroup",
```

```
            "iotJobId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE44444",
            "iotJobArn": "arn:aws:iot:us-west-2:123456789012:job/a1b2c3d4-5678-90ab-
cdef-EXAMPLE44444",
            "targetArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/
MyGreengrassCoreGroup",
            "coreDeviceExecutionStatus": "SUCCEEDED",
            "reason": "SUCCESSFUL",
            "creationTimestamp": "2021-01-07T17:19:20.394000-08:00",
            "modifiedTimestamp": "2021-01-07T17:21:20.721000-08:00"
        }
    ]
}
```

Para obtener más información, consulte Check core device status en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte ListEffectiveDeployments en la Referencia de comandos de la AWS CLI.

`list-installed-components`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-installed-components`.

AWS CLI

Para enumerar los componentes instalados en un dispositivo de núcleo

En el siguiente ejemplo de `list-installed-components`, se muestran los componentes que están instalados en un dispositivo de núcleo de AWS IoT Greengrass.

```
aws greengrassv2 list-installed-components \
    --core-device-thing-name MyGreengrassCore
```

Salida:

```
{
    "installedComponents": [
        {
            "componentName": "aws.greengrass.Cli",
            "componentVersion": "2.0.3",
            "lifecycleState": "RUNNING",
            "isRoot": true
```

```
        },
        {
            "componentName": "aws.greengrass.Nucleus",
            "componentVersion": "2.0.3",
            "lifecycleState": "FINISHED",
            "isRoot": true
        }
    ]
}
```

Para obtener más información, consulte Check core device status en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte ListInstalledComponents en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se muestran todas las etiquetas de un dispositivo de núcleo de AWS IoT Greengrass.

```
aws greengrassv2 list-tags-for-resource \
    --resource-arn arn:aws:greengrass:us-
west-2:123456789012:coreDevices:MyGreengrassCore
```

Salida:

```
{
    "tags": {
        "Owner": "richard-roe"
    }
}
```

Para obtener más información, consulte Tag your resources en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Cómo añadir una etiqueta a un recurso

En el siguiente ejemplo de `tag-resource`, se agrega una etiqueta de propietario a un dispositivo de núcleo de AWS IoT Greengrass. Puede usar esta etiqueta para controlar el acceso al dispositivo de núcleo en función de quién sea su propietario.

```
aws greengrassv2 tag-resource \
    --resource-arn arn:aws:greengrass:us-
west-2:123456789012:coreDevices:MyGreengrassCore \
    --tags Owner=richard-roe
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tag your resources en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar una etiqueta de un recurso

En el siguiente ejemplo de `untag-resource`, se elimina una etiqueta de propietario de un dispositivo de núcleo de AWS IoT Greengrass.

```
aws iotsitewise untag-resource \
```

```
    --resource-arn arn:aws:greengrass:us-
west-2:123456789012:coreDevices:MyGreengrassCore \
    --tag-keys Owner
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tag your resources en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-connectivity-info

En el siguiente ejemplo de código, se muestra cómo utilizar `update-connectivity-info`.

AWS CLI

Para actualizar la información de conectividad para un dispositivo de núcleo de Greengrass

En el siguiente ejemplo de `update-connectivity-info`, se obtiene información de conectividad para un dispositivo de núcleo de Greengrass. Los dispositivos de cliente utilizan esta información para conectarse al intermediario MQTT que se ejecuta en este dispositivo de núcleo.

```
aws greengrassv2 update-connectivity-info \
    --thing-name MyGreengrassCore \
    --cli-input-json file://core-device-connectivity-info.json
```

Contenido de `core-device-connectivity-info.json`:

```
{
    "connectivityInfo": [
        {
            "hostAddress": "192.0.2.0",
            "portNumber": 8883,
            "id": "localIP_192.0.2.0"
        }
    ]
}
```

Salida:

```
{
    "version": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Para obtener más información, consulte Manage core device endpoints en la Guía para desarrolladores de AWS IoT Greengrass, versión 2.

- Para obtener información sobre la API, consulte UpdateConnectivityInfo en la Referencia de comandos de la AWS CLI.

Publicación de AWS IoT Jobs SDK Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Publicación de AWS IoT Jobs SDK.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`describe-job-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-job-execution`.

AWS CLI

Para obtener los detalles de una ejecución de trabajo

En el siguiente ejemplo de `describe-job-execution`, se recuperan los detalles de la última ejecución del trabajo y el objeto especificados.

```
aws iot-jobs-data describe-job-execution \
    --job-id SampleJob \
```

```
    --thing-name MotionSensor1 \
    --endpoint-url https://1234567890abcd.jobs.iot.us-west-2.amazonaws.com
```

Salida:

```
{
    "execution": {
        "approximateSecondsBeforeTimedOut": 88,
        "executionNumber": 2939653338,
        "jobId": "SampleJob",
        "lastUpdatedAt": 1567701875.743,
        "queuedAt": 1567701902.444,
        "status": "QUEUED",
        "thingName": "MotionSensor1 ",
        "versionNumber": 3
   }
}
```

Para obtener más información, consulte los Devices and Jobs en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DescribeJobExecution en la Referencia de comandos de la AWS CLI.

`get-pending-job-executions`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-pending-job-executions`.

AWS CLI

Para obtener la lista de todos los trabajos que no tienen un estado terminal para un objeto

En el siguiente ejemplo de `get-pending-job-executions`, se muestra una lista de todos los trabajos que no tienen un estado terminal para el objeto especificado.

```
aws iot-jobs-data get-pending-job-executions \
    --thing-name MotionSensor1
    --endpoint-url https://1234567890abcd.jobs.iot.us-west-2.amazonaws.com
```

Salida:

```
{
```

```
    "inProgressJobs": [
    ],
    "queuedJobs": [
        {
            "executionNumber": 2939653338,
            "jobId": "SampleJob",
            "lastUpdatedAt": 1567701875.743,
            "queuedAt": 1567701902.444,
            "versionNumber": 3
      }
    ]
}
```

Para obtener más información, consulte los Devices and Jobs en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetPendingJobExecutions en la Referencia de comandos de la AWS CLI.

`start-next-pending-job-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-next-pending-job-execution`.

AWS CLI

Para obtener e iniciar la siguiente ejecución de trabajos pendiente para un objeto

En el siguiente ejemplo de `start-next-pending-job-execution`, se recupera e inicia la siguiente ejecución de trabajo cuyo estado es IN_PROGRESS o QUEUED para el objeto especificado.

```
aws iot-jobs-data start-next-pending-job-execution \
    --thing-name MotionSensor1
    --endpoint-url https://1234567890abcd.jobs.iot.us-west-2.amazonaws.com
```

Salida:

```
{
    "execution": {
        "approximateSecondsBeforeTimedOut": 88,
        "executionNumber": 2939653338,
```

```
        "jobId": "SampleJob",
        "lastUpdatedAt": 1567714853.743,
        "queuedAt": 1567701902.444,
        "startedAt": 1567714871.690,
        "status": "IN_PROGRESS",
        "thingName": "MotionSensor1 ",
        "versionNumber": 3
    }
}
```

Para obtener más información, consulte los Devices and Jobs en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte StartNextPendingJobExecution en la Referencia de comandos de la AWS CLI.

`update-job-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-job-execution`.

AWS CLI

Para actualizar el estado de una ejecución de trabajo

En el siguiente ejemplo de `update-job-execution`, se actualiza el estado de un trabajo y un objeto especificados.

```
aws iot-jobs-data update-job-execution \
    --job-id SampleJob \
    --thing-name MotionSensor1 \
    --status REMOVED \
    --endpoint-url https://1234567890abcd.jobs.iot.us-west-2.amazonaws.com
```

Salida:

```
{
    "executionState": {
        "status": "REMOVED",
        "versionNumber": 3
    },
}
```

Para obtener más información, consulte los Devices and Jobs en la Guía para desarrolladores de AWS IoT.

- Para obtener información acerca de la API, consulte UpdateJobExecution en la Referencia de comandos de la AWS CLI.

AWS IoT SiteWise Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS IoT SiteWise.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-assets`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-assets`.

AWS CLI

Para asociar un activo secundario a un activo principal

En el siguiente ejemplo de `associate-assets`, se asocia un activo de turbina eólica a un activo de parque eólico, donde el modelo de activos de turbina eólica existe como jerarquía en el modelo de activos de parque eólico.

```
aws iotsitewise associate-assets \
    --asset-id a1b2c3d4-5678-90ab-cdef-44444EXAMPLE \
    --hierarchy-id a1b2c3d4-5678-90ab-cdef-77777EXAMPLE \
    --child-asset-id a1b2c3d4-5678-90ab-cdef-33333EXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Associating assets en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte AssociateAssets en la Referencia de comandos de la AWS CLI.

`batch-associate-project-assets`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-associate-project-assets`.

AWS CLI

Para asociar un activo a un proyecto

En el siguiente ejemplo de `batch-associate-project-assets`, se asocia un activo de parque eólico a un proyecto.

```
aws iotsitewise batch-associate-project-assets \
    --project-id a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE \
    --asset-ids a1b2c3d4-5678-90ab-cdef-44444EXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adding assets to projects en la Guía de la aplicación AWS IoT SiteWise Monitor.

- Para obtener información sobre la API, consulte BatchAssociateProjectAssets en la Referencia de comandos de la AWS CLI.

`batch-disassociate-project-assets`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-disassociate-project-assets`.

AWS CLI

Para desasociar un activo de un proyecto

En el siguiente ejemplo de `batch-disassociate-project-assets`, se desvincula un activo de parque eólico de un proyecto.

```
aws iotsitewise batch-disassociate-project-assets \
    --project-id a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE \
    --asset-ids a1b2c3d4-5678-90ab-cdef-44444EXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adding assets to projects en la Guía de la aplicación AWS IoT SiteWise Monitor.

- Para obtener información sobre la API, consulte BatchDisassociateProjectAssets en la Referencia de comandos de la AWS CLI.

batch-put-asset-property-value

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-put-asset-property-value`.

AWS CLI

Para enviar datos a propiedades de los activos

En el siguiente ejemplo de `batch-put-asset-property-value`, se envían datos de potencia y temperatura a las propiedades de los activos identificadas por los alias de las propiedades.

```
aws iotsitewise batch-put-asset-property-value \
    --cli-input-json file://batch-put-asset-property-value.json
```

Contenido de `batch-put-asset-property-value.json`:

```
{
    "entries": [
        {
            "entryId": "1575691200-company-windfarm-3-turbine-7-power",
            "propertyAlias": "company-windfarm-3-turbine-7-power",
            "propertyValues": [
                {
                    "value": {
                        "doubleValue": 4.92
                    },
                    "timestamp": {
                        "timeInSeconds": 1575691200
                    },
                    "quality": "GOOD"
```

```
                }
            ]
        },
        {
            "entryId": "1575691200-company-windfarm-3-turbine-7-temperature",
            "propertyAlias": "company-windfarm-3-turbine-7-temperature",
            "propertyValues": [
                {
                    "value": {
                        "integerValue": 38
                    },
                    "timestamp": {
                        "timeInSeconds": 1575691200
                    }
                }
            ]
        }
    ]
}
```

Salida:

```
{
    "errorEntries": []
}
```

Para obtener más información, consulte Ingesting data using the AWS IoT SiteWise API en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte BatchPutAssetPropertyValue en la Referencia de comandos de la AWS CLI.

`create-access-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-access-policy`.

AWS CLI

Ejemplo 1: concesión a un usuario de acceso administrativo a un portal

En el siguiente ejemplo de `create-access-policy`, se crea una política de acceso que concede a un usuario acceso administrativo a un portal web de una empresa de parques eólicos.

```
aws iotsitewise create-access-policy \
    --cli-input-json file://create-portal-administrator-access-policy.json
```

Contenido de `create-portal-administrator-access-policy.json`:

```
{
    "accessPolicyIdentity": {
        "user": {
            "id": "a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-bbbbbEXAMPLE"
        }
    },
    "accessPolicyPermission": "ADMINISTRATOR",
    "accessPolicyResource": {
        "portal": {
            "id": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE"
        }
    }
}
```

Salida:

```
{
    "accessPolicyId": "a1b2c3d4-5678-90ab-cdef-cccccEXAMPLE",
    "accessPolicyArn": "arn:aws:iotsitewise:us-west-2:123456789012:access-policy/
a1b2c3d4-5678-90ab-cdef-cccccEXAMPLE"
}
```

Para obtener más información, consulte Adding or removing portal administrators en la Guía del usuario de AWS IoT SiteWise.

Ejemplo 2: concesión al usuario acceso de solo lectura a un proyecto

En el siguiente ejemplo de `create-access-policy`, se crea una política de acceso que concede a un usuario acceso de solo lectura a un proyecto de parque eólico.

```
aws iotsitewise create-access-policy \
    --cli-input-json file://create-project-viewer-access-policy.json
```

Contenido de `create-project-viewer-access-policy.json`:

```
{
```

```
    "accessPolicyIdentity": {
        "user": {
            "id": "a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-bbbbbEXAMPLE"
        }
    },
    "accessPolicyPermission": "VIEWER",
    "accessPolicyResource": {
        "project": {
            "id": "a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE"
        }
    }
}
```

Salida:

```
{
    "accessPolicyId": "a1b2c3d4-5678-90ab-cdef-dddddEXAMPLE",
    "accessPolicyArn": "arn:aws:iotsitewise:us-west-2:123456789012:access-policy/
a1b2c3d4-5678-90ab-cdef-dddddEXAMPLE"
}
```

Para obtener más información, consulte Assigning project viewers en la Guía de la aplicación AWS IoT SiteWise Monitor.

- Para obtener información sobre la API, consulte CreateAccessPolicy en la Referencia de comandos de la AWS CLI.

`create-asset-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-asset-model`.

AWS CLI

Para crear un modelo de activos

En el siguiente ejemplo de `create-asset-model`, se crea un modelo de activos que define una turbina eólica con las siguientes propiedades:

Número de serie: es el número de serie de una turbina eólica. Potencia generada: es el flujo de datos de energía generada por una turbina eólica. Temperatura C: es el flujo de datos de temperatura de una turbina eólica en grados Celsius. Temperatura F: son los puntos de datos de temperatura asignados desde Celsius a Fahrenheit.

```
aws iotsitewise create-asset-model \
    --cli-input-json file://create-wind-turbine-model.json
```

Contenido de `create-wind-turbine-model.json`:

```
{
    "assetModelName": "Wind Turbine Model",
    "assetModelDescription": "Represents a wind turbine",
    "assetModelProperties": [
        {
            "name": "Serial Number",
            "dataType": "STRING",
            "type": {
                "attribute": {}
            }
        },
        {
            "name": "Generated Power",
            "dataType": "DOUBLE",
            "unit": "kW",
            "type": {
                "measurement": {}
            }
        },
        {
            "name": "Temperature C",
            "dataType": "DOUBLE",
            "unit": "Celsius",
            "type": {
                "measurement": {}
            }
        },
        {
            "name": "Temperature F",
            "dataType": "DOUBLE",
            "unit": "Fahrenheit",
            "type": {
                "transform": {
                    "expression": "temp_c * 9 / 5 + 32",
                    "variables": [
                        {
                            "name": "temp_c",
                            "value": {
```

```
                                "propertyId": "Temperature C"
                            }
                        }
                    ]
                }
            }
        },
        {
            "name": "Total Generated Power",
            "dataType": "DOUBLE",
            "unit": "kW",
            "type": {
                "metric": {
                    "expression": "sum(power)",
                    "variables": [
                        {
                            "name": "power",
                            "value": {
                                "propertyId": "Generated Power"
                            }
                        }
                    ],
                    "window": {
                        "tumbling": {
                            "interval": "1h"
                        }
                    }
                }
            }
        }
    ]
}
```

Salida:

```
{
    "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
    "assetModelArn": "arn:aws:iotsitewise:us-west-2:123456789012:asset-model/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
    "assetModelStatus": {
        "state": "CREATING"
    }
}
```

Para obtener más información, consulte Defining asset models en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte CreateAssetModel en la Referencia de comandos de la AWS CLI.

`create-asset`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-asset`.

AWS CLI

Para crear un activo

En el siguiente ejemplo de `create-asset`, se crea un activo de turbina eólica a partir de un modelo de activos de turbina eólica.

```
aws iotsitewise create-asset \
    --asset-model-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --asset-name "Wind Turbine 1"
```

Salida:

```
{
    "assetId": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
    "assetArn": "arn:aws:iotsitewise:us-west-2:123456789012:asset/
a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
    "assetStatus": {
        "state": "CREATING"
    }
}
```

Para obtener más información, consulte Creating assets en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte CreateAsset en la Referencia de comandos de la AWS CLI.

`create-dashboard`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-dashboard`.

AWS CLI

Para crear un panel

En el siguiente ejemplo de `create-dashboard`, se crea un panel con un gráfico de líneas que muestra la potencia total generada por un parque eólico.

```
aws iotsitewise create-dashboard \
    --project-id a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE \
    --dashboard-name "Wind Farm" \
    --dashboard-definition file://create-wind-farm-dashboard.json
```

Contenido de `create-wind-farm-dashboard.json`:

```
{
    "widgets": [
        {
            "type": "monitor-line-chart",
            "title": "Generated Power",
            "x": 0,
            "y": 0,
            "height": 3,
            "width": 3,
            "metrics": [
                {
                    "label": "Power",
                    "type": "iotsitewise",
                    "assetId": "a1b2c3d4-5678-90ab-cdef-44444EXAMPLE",
                    "propertyId": "a1b2c3d4-5678-90ab-cdef-99999EXAMPLE"
                }
            ]
        }
    ]
}
```

Salida:

```
{
    "dashboardId": "a1b2c3d4-5678-90ab-cdef-fffffEXAMPLE",
    "dashboardArn": "arn:aws:iotsitewise:us-west-2:123456789012:dashboard/
a1b2c3d4-5678-90ab-cdef-fffffEXAMPLE"
}
```

Para obtener más información, consulte Creating dashboards (CLI) en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte CreateDashboard en la Referencia de comandos de la AWS CLI.

`create-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-gateway`.

AWS CLI

Para crear una puerta de enlace

En el siguiente ejemplo de `create-gateway`, se crea una puerta de enlace que se ejecuta en AWS IoT Greengrass.

```
aws iotsitewise create-gateway \
    --gateway-name ExampleCorpGateway \
    --gateway-platform greengrass={groupArn=arn:aws:greengrass:us-
west-2:123456789012:/greengrass/groups/a1b2c3d4-5678-90ab-cdef-1b1b1EXAMPLE}
```

Salida:

```
{
    "gatewayId": "a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE",
    "gatewayArn": "arn:aws:iotsitewise:us-west-2:123456789012:gateway/
a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE"
}
```

Para obtener más información, consulte Configuring a gateway en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte CreateGateway en la Referencia de comandos de la AWS CLI.

`create-portal`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-portal`.

AWS CLI

Para crear un portal

En el siguiente ejemplo de `create-portal`, se crea un portal web para una empresa de parques eólicos. Solo puede crear portales en la misma región en la que haya activado el AWS Single Sign-On.

```
aws iotsitewise create-portal \
    --portal-name WindFarmPortal \
    --portal-description "A portal that contains wind farm projects for Example
 Corp." \
    --portal-contact-email support@example.com \
    --role-arn arn:aws:iam::123456789012:role/service-role/
MySiteWiseMonitorServiceRole
```

Salida:

```
{
    "portalId": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
    "portalArn": "arn:aws:iotsitewise:us-west-2:123456789012:portal/
a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
    "portalStartUrl": "https://a1b2c3d4-5678-90ab-cdef-
aaaaaEXAMPLE.app.iotsitewise.aws",
    "portalStatus": {
        "state": "CREATING"
    },
    "ssoApplicationId": "ins-a1b2c3d4-EXAMPLE"
}
```

Para obtener más información, consulte Getting started with AWS IoT SiteWise Monitor en la Guía del usuario de AWS IoT SiteWise y Enabling AWS SSO en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte CreatePortal en la Referencia de comandos de AWS CLI.

`create-project`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-project`.

AWS CLI

Para crear un proyecto

En el siguiente ejemplo de `create-project`, se crea un proyecto de parques eólicos.

```
aws iotsitewise create-project \
    --portal-id a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE \
    --project-name "Wind Farm 1" \
    --project-description "Contains asset visualizations for Wind Farm #1 for
 Example Corp."
```

Salida:

```
{
    "projectId": "a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE",
    "projectArn": "arn:aws:iotsitewise:us-west-2:123456789012:project/
a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE"
}
```

Para obtener más información, consulte Creating projects en la Guía de la aplicación AWS IoT SiteWise Monitor.

- Para obtener información sobre la API, consulte CreateProject en la Referencia de comandos de la AWS CLI.

`delete-access-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-access-policy`.

AWS CLI

Para revocar el acceso de un usuario a un proyecto o portal

En el siguiente ejemplo de `delete-access-policy`, se elimina una política de acceso que concede a un usuario acceso administrativo a un portal.

```
aws iotsitewise delete-access-policy \
    --access-policy-id a1b2c3d4-5678-90ab-cdef-cccccEXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adding or removing portal administrators en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte DeleteAccessPolicy en la Referencia de comandos de la AWS CLI.

`delete-asset-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-asset-model`.

AWS CLI

Para eliminar un modelo de activos

En el siguiente ejemplo de `delete-asset-model`, se elimina un modelo de activos de turbina eólica.

```
aws iotsitewise delete-asset-model \
    --asset-model-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE
```

Salida:

```
{
    "assetModelStatus": {
        "state": "DELETING"
    }
}
```

Para obtener más información, consulte Deleting asset models en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte DeleteAssetModel en la Referencia de comandos de la AWS CLI.

`delete-asset`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-asset`.

AWS CLI

Para eliminar un activo

En el siguiente ejemplo de `delete-asset`, se elimina un activo de turbina eólica.

```
aws iotsitewise delete-asset \
    --asset-id a1b2c3d4-5678-90ab-cdef-33333EXAMPLE
```

Salida:

```
{
    "assetStatus": {
        "state": "DELETING"
    }
}
```

Para obtener más información, consulte Deleting assets en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte DeleteAsset en la Referencia de comandos de la AWS CLI.

`delete-dashboard`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-dashboard`.

AWS CLI

Para eliminar un panel

En el siguiente ejemplo de `delete-dashboard`, se elimina el panel de una turbina eólica.

```
aws iotsitewise delete-dashboard \
    --dashboard-id a1b2c3d4-5678-90ab-cdef-fffffEXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting dashboards en la Guía de la aplicación AWS IoT SiteWise Monitor.

- Para obtener información sobre la API, consulte DeleteDashboard en la Referencia de comandos de la AWS CLI.

`delete-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-gateway`.

AWS CLI

Para eliminar una puerta de enlace

En el siguiente ejemplo de `delete-gateway`, se elimina una puerta de enlace.

```
aws iotsitewise delete-gateway \
    --gateway-id a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Ingesting data using a gateway en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte DeleteGateway en la Referencia de comandos de AWS CLI.

`delete-portal`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-portal`.

AWS CLI

Para eliminar un portal

En el siguiente ejemplo de `delete-portal`, se elimina un portal web para una empresa de parques eólicos.

```
aws iotsitewise delete-portal \
    --portal-id a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE
```

Salida:

```
{
    "portalStatus": {
        "state": "DELETING"
    }
```

```
}
```

Para obtener más información, consulte Deleting a portal en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte DeletePortal en la Referencia de comandos de la AWS CLI.

`delete-project`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-project`.

AWS CLI

Para eliminar un proyecto

En el siguiente ejemplo de `delete-project`, se elimina un proyecto de parques eólicos.

```
aws iotsitewise delete-project \
    --project-id a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting projects en la Guía de la aplicación AWS IoT SiteWise Monitor.

- Para obtener información sobre la API, consulte DeleteProject en la Referencia de comandos de la AWS CLI.

`describe-access-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-access-policy`.

AWS CLI

Para describir una política de acceso

En el siguiente ejemplo de `describe-access-policy`, se describe una política de acceso que concede a un usuario acceso administrativo a un portal web de una empresa de parques eólicos.

```
aws iotsitewise describe-access-policy \
```

```
    --access-policy-id a1b2c3d4-5678-90ab-cdef-cccccEXAMPLE
```

Salida:

```
{
    "accessPolicyId": "a1b2c3d4-5678-90ab-cdef-cccccEXAMPLE",
    "accessPolicyArn": "arn:aws:iotsitewise:us-west-2:123456789012:access-policy/
a1b2c3d4-5678-90ab-cdef-cccccEXAMPLE",
    "accessPolicyIdentity": {
        "user": {
            "id": "a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-bbbbbEXAMPLE"
        }
    },
    "accessPolicyResource": {
        "portal": {
            "id": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE"
        }
    },
    "accessPolicyPermission": "ADMINISTRATOR",
    "accessPolicyCreationDate": "2020-02-20T22:35:15.552880124Z",
    "accessPolicyLastUpdateDate": "2020-02-20T22:35:15.552880124Z"
}
```

Para obtener más información, consulte Adding or removing portal administrators en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte DescribeAccessPolicy en la Referencia de comandos de la AWS CLI.

`describe-asset-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-asset-model`.

AWS CLI

Para describir un modelo de activos

En el siguiente ejemplo de `describe-asset-model`, se describe un modelo de activos de parque eólico.

```
aws iotsitewise describe-asset-model \
    --asset-model-id a1b2c3d4-5678-90ab-cdef-22222EXAMPLE
```

Salida:

```
{
    "assetModelId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
    "assetModelArn": "arn:aws:iotsitewise:us-west-2:123456789012:asset-model/
a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
    "assetModelName": "Wind Farm Model",
    "assetModelDescription": "Represents a wind farm that comprises many wind
 turbines",
    "assetModelProperties": [
        {
            "id": "a1b2c3d4-5678-90ab-cdef-99999EXAMPLE",
            "name": "Total Generated Power",
            "dataType": "DOUBLE",
            "unit": "kW",
            "type": {
                "metric": {
                    "expression": "sum(power)",
                    "variables": [
                        {
                            "name": "power",
                            "value": {
                                "propertyId": "a1b2c3d4-5678-90ab-
cdef-66666EXAMPLE",
                                "hierarchyId": "a1b2c3d4-5678-90ab-
cdef-77777EXAMPLE"
                            }
                        }
                    ],
                    "window": {
                        "tumbling": {
                            "interval": "1h"
                        }
                    }
                }
            }
        },
        {
            "id": "a1b2c3d4-5678-90ab-cdef-88888EXAMPLE",
            "name": "Region",
            "dataType": "STRING",
            "type": {
                "attribute": {
                    "defaultValue": " "
```

```
                }
            }
        }
    ],
    "assetModelHierarchies": [
        {
            "id": "a1b2c3d4-5678-90ab-cdef-77777EXAMPLE",
            "name": "Wind Turbines",
            "childAssetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
        }
    ],
    "assetModelCreationDate": 1575671284.0,
    "assetModelLastUpdateDate": 1575671988.0,
    "assetModelStatus": {
        "state": "ACTIVE"
    }
}
```

Para obtener más información, consulte Describing a specific asset model en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte DescribeAssetModel en la Referencia de comandos de la AWS CLI.

`describe-asset-property`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-asset-property`.

AWS CLI

Para describir una propiedad de un activo

En el siguiente ejemplo de `describe-asset-property`, se describe la propiedad de potencia total generada de un activo de parque eólico.

```
aws iotsitewise describe-asset-property \
    --asset-id a1b2c3d4-5678-90ab-cdef-44444EXAMPLE \
    --property-id a1b2c3d4-5678-90ab-cdef-99999EXAMPLE
```

Salida:

```
{
```

```
    "assetId": "a1b2c3d4-5678-90ab-cdef-44444EXAMPLE",
    "assetName": "Wind Farm 1",
    "assetModelId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
    "assetProperty": {
        "id": "a1b2c3d4-5678-90ab-cdef-99999EXAMPLE",
        "name": "Total Generated Power",
        "notification": {
            "topic": "$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-
cdef-22222EXAMPLE/assets/a1b2c3d4-5678-90ab-cdef-44444EXAMPLE/properties/
a1b2c3d4-5678-90ab-cdef-99999EXAMPLE",
            "state": "DISABLED"
        },
        "dataType": "DOUBLE",
        "unit": "kW",
        "type": {
            "metric": {
                "expression": "sum(power)",
                "variables": [
                    {
                        "name": "power",
                        "value": {
                            "propertyId": "a1b2c3d4-5678-90ab-cdef-66666EXAMPLE",
                            "hierarchyId": "a1b2c3d4-5678-90ab-cdef-77777EXAMPLE"
                        }
                    }
                ],
                "window": {
                    "tumbling": {
                        "interval": "1h"
                    }
                }
            }
        }
    }
}
```

Para obtener más información, consulte Describing a specific asset property en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte DescribeAssetProperty en la Referencia de comandos de la AWS CLI.

describe-asset

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-asset`.

AWS CLI

Para describir un activo

En el siguiente ejemplo de `describe-asset`, se describe un activo de parque eólico.

```
aws iotsitewise describe-asset \
    --asset-id a1b2c3d4-5678-90ab-cdef-44444EXAMPLE
```

Salida:

```
{
    "assetId": "a1b2c3d4-5678-90ab-cdef-44444EXAMPLE",
    "assetArn": "arn:aws:iotsitewise:us-west-2:123456789012:asset/
a1b2c3d4-5678-90ab-cdef-44444EXAMPLE",
    "assetName": "Wind Farm 1",
    "assetModelId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
    "assetProperties": [
        {
            "id": "a1b2c3d4-5678-90ab-cdef-88888EXAMPLE",
            "name": "Region",
            "dataType": "STRING"
        },
        {
            "id": "a1b2c3d4-5678-90ab-cdef-99999EXAMPLE",
            "name": "Total Generated Power",
            "dataType": "DOUBLE",
            "unit": "kW"
        }
    ],
    "assetHierarchies": [
        {
            "id": "a1b2c3d4-5678-90ab-cdef-77777EXAMPLE",
            "name": "Wind Turbines"
        }
    ],
    "assetCreationDate": 1575672453.0,
    "assetLastUpdateDate": 1575672453.0,
    "assetStatus": {
```

```
        "state": "ACTIVE"
    }
}
```

Para obtener más información, consulte Describing a specific asset en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte DescribeAsset en la Referencia de comandos de la AWS CLI.

`describe-dashboard`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-dashboard`.

AWS CLI

Para describir un panel

En el siguiente ejemplo de `describe-dashboard`, se describe el panel de parque eólico especificado.

```
aws iotsitewise describe-dashboard \
    --dashboard-id a1b2c3d4-5678-90ab-cdef-fffffEXAMPLE
```

Salida:

```
{
    "dashboardId": "a1b2c3d4-5678-90ab-cdef-fffffEXAMPLE",
    "dashboardArn": "arn:aws:iotsitewise:us-west-2:123456789012:dashboard/
a1b2c3d4-5678-90ab-cdef-fffffEXAMPLE",
    "dashboardName": "Wind Farm",
    "projectId": "a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE",
    "dashboardDefinition": "{\"widgets\":[{\"type\":\"monitor-line-chart\",\"title
\":\"Generated Power\",\"x\":0,\"y\":0,\"height\":3,\"width\":3,\"metrics\":
[{\"label\":\"Power\",\"type\":\"iotsitewise\",\"assetId\":\"a1b2c3d4-5678-90ab-
cdef-44444EXAMPLE\",\"propertyId\":\"a1b2c3d4-5678-90ab-cdef-99999EXAMPLE\"}]}]}",
    "dashboardCreationDate": "2020-05-01T20:32:12.228476348Z",
    "dashboardLastUpdateDate": "2020-05-01T20:32:12.228476348Z"
}
```

Para obtener más información, consulte Viewing dashboards en la Guía de la aplicación AWS IoT SiteWise Monitor.

- Para obtener información sobre la API, consulte DescribeDashboard en la Referencia de comandos de la AWS CLI.

`describe-gateway-capability-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-gateway-capability-configuration`.

AWS CLI

Para describir la capacidad de una puerta de enlace

En el siguiente ejemplo de `describe-gateway-capability-configuration`, se describe una capacidad de origen OPC-UA.

```
aws iotsitewise describe-gateway-capability-configuration \
    --gateway-id a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE \
    --capability-namespace "iotsitewise:opcuacollector:1"
```

Salida:

```
{
    "gatewayId": "a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE",
    "capabilityNamespace": "iotsitewise:opcuacollector:1",
    "capabilityConfiguration": "{\"sources\":[{\"name\":\"Wind Farm #1\",
\"endpoint\":{\"certificateTrust\":{\"type\":\"TrustAny\"},\"endpointUri
\":\"opc.tcp://203.0.113.0:49320\",\"securityPolicy\":\"BASIC256\",
\"messageSecurityMode\":\"SIGN_AND_ENCRYPT\",\"identityProvider\":
{\"type\":\"Username\",\"usernameSecretArn\":\"arn:aws:secretsmanager:us-
east-1:123456789012:secret:greengrass-factory1-auth-3QNDmM\"},\"nodeFilterRules\":
[]},\"measurementDataStreamPrefix\":\"\"}]}",
    "capabilitySyncStatus": "IN_SYNC"
}
```

Para obtener más información, consulte Configuring data sources en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte DescribeGatewayCapabilityConfiguration en la Referencia de comandos de la AWS CLI.

describe-gateway

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-gateway`.

AWS CLI

Para describir una puerta de enlace

En el siguiente ejemplo de `describe-gateway`, se describe una puerta de enlace.

```
aws iotsitewise describe-gateway \
    --gateway-id a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE
```

Salida:

```
{
    "gatewayId": "a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE",
    "gatewayName": "ExampleCorpGateway",
    "gatewayArn": "arn:aws:iotsitewise:us-west-2:123456789012:gateway/
a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE",
    "gatewayPlatform": {
        "greengrass": {
            "groupArn": "arn:aws:greengrass:us-west-2:123456789012:/greengrass/
groups/a1b2c3d4-5678-90ab-cdef-1b1b1EXAMPLE"
        }
    },
    "gatewayCapabilitySummaries": [
        {
            "capabilityNamespace": "iotsitewise:opcuacollector:1",
            "capabilitySyncStatus": "IN_SYNC"
        }
    ],
    "creationDate": 1588369971.457,
    "lastUpdateDate": 1588369971.457
}
```

Para obtener más información, consulte Ingesting data using a gateway en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte DescribeGateway en la Referencia de comandos de la AWS CLI.

`describe-logging-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-logging-options`.

AWS CLI

Para recuperar las opciones de registro actuales de AWS IoT SiteWise

En el siguiente ejemplo de `describe-logging-options`, se recuperan las opciones de registro actuales de AWS IoT SiteWise para su cuenta de AWS en la región actual.

```
aws iotsitewise describe-logging-options
```

Salida:

```
{
    "loggingOptions": {
        "level": "INFO"
    }
}
```

Para obtener más información, consulte Monitoring AWS IoT SiteWise with Amazon CloudWatch Logs en la Guía del usuario de AWS IoT SiteWise.

- Para obtener más información sobre la API, consulte DescribeLoggingOptions en la Referencia de comandos de la AWS CLI.

`describe-portal`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-portal`.

AWS CLI

Para describir un portal

En el siguiente ejemplo de `describe-portal`, se describe un portal web para una empresa de parques eólicos.

```
aws iotsitewise describe-portal \
    --portal-id a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE
```

Salida:

```
{
    "portalId": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
    "portalArn": "arn:aws:iotsitewise:us-west-2:123456789012:portal/
a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
    "portalName": "WindFarmPortal",
    "portalDescription": "A portal that contains wind farm projects for Example
 Corp.",
    "portalClientId": "E-a1b2c3d4e5f6_a1b2c3d4e5f6EXAMPLE",
    "portalStartUrl": "https://a1b2c3d4-5678-90ab-cdef-
aaaaaEXAMPLE.app.iotsitewise.aws",
    "portalContactEmail": "support@example.com",
    "portalStatus": {
        "state": "ACTIVE"
    },
    "portalCreationDate": "2020-02-04T23:01:52.90248068Z",
    "portalLastUpdateDate": "2020-02-04T23:01:52.90248078Z",
    "roleArn": "arn:aws:iam::123456789012:role/MySiteWiseMonitorServiceRole"
}
```

Para obtener más información, consulte Administering your portals en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte DescribePortal en la Referencia de comandos de la AWS CLI.

`describe-project`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-project`.

AWS CLI

Para describir un proyecto

En el siguiente ejemplo de `describe-project`, se describe un proyecto de parque eólico.

```
aws iotsitewise describe-project \
    --project-id a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE
```

Salida:

```
{
    "projectId": "a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE",
    "projectArn": "arn:aws:iotsitewise:us-west-2:123456789012:project/
a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE",
    "projectName": "Wind Farm 1",
    "portalId": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
    "projectDescription": "Contains asset visualizations for Wind Farm #1 for
 Example Corp.",
    "projectCreationDate": "2020-02-20T21:58:43.362246001Z",
    "projectLastUpdateDate": "2020-02-20T21:58:43.362246095Z"
}
```

Para obtener más información, consulte Viewing project details en la Guía de la aplicación AWS IoT SiteWise Monitor.

- Para obtener información sobre la API, consulte DescribeProject en la Referencia de comandos de la AWS CLI.

`disassociate-assets`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-assets`.

AWS CLI

Para desasociar un activo secundario de un activo principal

En el siguiente ejemplo de `disassociate-assets`, se desvincula un activo de turbina eólica de un activo de parque eólico.

```
aws iotsitewise disassociate-assets \
    --asset-id a1b2c3d4-5678-90ab-cdef-44444EXAMPLE \
    --hierarchy-id a1b2c3d4-5678-90ab-cdef-77777EXAMPLE \
    --child-asset-id a1b2c3d4-5678-90ab-cdef-33333EXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Associating assets en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte DisassociateAssets en la Referencia de comandos de la AWS CLI.

`get-asset-property-aggregates`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-asset-property-aggregates`.

AWS CLI

Para recuperar el promedio agregado y los valores de recuento de una propiedad de un activo

En el siguiente ejemplo de `get-asset-property-aggregates`, se recupera la potencia total media de un activo de turbina eólica y el recuento de los puntos de datos de potencia total durante un período de una hora.

```
aws iotsitewise get-asset-property-aggregates \
    --asset-id a1b2c3d4-5678-90ab-cdef-33333EXAMPLE \
    --property-id a1b2c3d4-5678-90ab-cdef-66666EXAMPLE \
    --start-date 1580849400 \
    --end-date 1580853000 \
    --aggregate-types AVERAGE COUNT \
    --resolution 1h
```

Salida:

```
{
    "aggregatedValues": [
        {
            "timestamp": 1580850000.0,
            "quality": "GOOD",
            "value": {
                "average": 8723.46538886233,
                "count": 12.0
            }
        }
    ]
}
```

Para obtener más información, consulte Querying asset property aggregates en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte GetAssetPropertyAggregates en la Referencia de comandos de la AWS CLI.

`get-asset-property-value-history`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-asset-property-value-history`.

AWS CLI

Para recuperar los valores históricos de una propiedad de un activo

En el siguiente ejemplo de `get-asset-property-value-history`, se recuperan los valores de potencia total de un activo de turbina eólica durante un período de 20 minutos.

```
aws iotsitewise get-asset-property-value-history \
    --asset-id a1b2c3d4-5678-90ab-cdef-33333EXAMPLE \
    --property-id a1b2c3d4-5678-90ab-cdef-66666EXAMPLE \
    --start-date 1580851800 \
    --end-date 1580853000
```

Salida:

```
{
    "assetPropertyValueHistory": [
        {
            "value": {
                "doubleValue": 7217.787046814844
            },
            "timestamp": {
                "timeInSeconds": 1580852100,
                "offsetInNanos": 0
            },
            "quality": "GOOD"
        },
        {
            "value": {
                "doubleValue": 6941.242811875451
            },
            "timestamp": {
                "timeInSeconds": 1580852400,
                "offsetInNanos": 0
            },
            "quality": "GOOD"
        },
        {
```

```
            "value": {
                "doubleValue": 6976.797662266717
            },
            "timestamp": {
                "timeInSeconds": 1580852700,
                "offsetInNanos": 0
            },
            "quality": "GOOD"
        },
        {
            "value": {
                "doubleValue": 6890.8677520453875
            },
            "timestamp": {
                "timeInSeconds": 1580853000,
                "offsetInNanos": 0
            },
            "quality": "GOOD"
        }
    ]
}
```

Para obtener más información, consulte Querying historical asset property values en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte GetAssetPropertyValueHistory en la Referencia de comandos de la AWS CLI.

`get-asset-property-value`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-asset-property-value`.

AWS CLI

Para recuperar el valor actual de una propiedad de un activo

En el siguiente ejemplo de `get-asset-property-value`, se recupera la potencia total actual de un activo de turbina eólica.

```
aws iotsitewise get-asset-property-value \
    --asset-id a1b2c3d4-5678-90ab-cdef-33333EXAMPLE \
    --property-id a1b2c3d4-5678-90ab-cdef-66666EXAMPLE
```

Salida:

```
{
    "propertyValue": {
        "value": {
            "doubleValue": 6890.8677520453875
        },
        "timestamp": {
            "timeInSeconds": 1580853000,
            "offsetInNanos": 0
        },
        "quality": "GOOD"
    }
}
```

Para obtener más información, consulte Querying current asset property values en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte GetAssetPropertyValue en la Referencia de comandos de la AWS CLI.

`list-access-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-access-policies`.

AWS CLI

Para enumerar todas las políticas de acceso

En el siguiente ejemplo de `list-access-policies`, se enumeran todas las políticas de acceso de un usuario que es administrador del portal.

```
aws iotsitewise list-access-policies \
    --identity-type USER \
    --identity-id a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-bbbbbEXAMPLE
```

Salida:

```
{
    "accessPolicySummaries": [
        {
            "id": "a1b2c3d4-5678-90ab-cdef-cccccEXAMPLE",
```

```
            "identity": {
                "user": {
                    "id": "a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-bbbbbEXAMPLE"
                }
            },
            "resource": {
                "portal": {
                    "id": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE"
                }
            },
            "permission": "ADMINISTRATOR"
        }
    ]
}
```

Para obtener más información, consulte Administering your portals en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte ListAccessPolicies en la Referencia de comandos de la AWS CLI.

`list-asset-models`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-asset-models`.

AWS CLI

Para enumerar todos los modelos de activos

En el siguiente ejemplo de `list-asset-models`, se enumeran todos los modelos de activos que se definen en la cuenta de AWS en la región actual.

```
aws iotsitewise list-asset-models
```

Salida:

```
{
    "assetModelSummaries": [
        {
            "id": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
            "arn": "arn:aws:iotsitewise:us-west-2:123456789012:asset-model/
a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
```

```
            "name": "Wind Farm Model",
            "description": "Represents a wind farm that comprises many wind
 turbines",
            "creationDate": 1575671284.0,
            "lastUpdateDate": 1575671988.0,
            "status": {
                "state": "ACTIVE"
            }
        },
        {
            "id": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "arn": "arn:aws:iotsitewise:us-west-2:123456789012:asset-model/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "name": "Wind Turbine Model",
            "description": "Represents a wind turbine manufactured by Example Corp",
            "creationDate": 1575671207.0,
            "lastUpdateDate": 1575686273.0,
            "status": {
                "state": "ACTIVE"
            }
        }
    ]
}
```

Para obtener más información, consulte Listing all asset models en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte ListAssetModels en la Referencia de comandos de la AWS CLI.

`list-assets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-assets`.

AWS CLI

Ejemplo 1: enumeración de todos los activos de nivel superior

En el siguiente ejemplo de `list-assets`, se enumeran todos los activos que ocupan el nivel superior del árbol jerárquico de activos y están definidos en su cuenta de AWS en la región actual.

```
aws iotsitewise list-assets \
```

```
    --filter TOP_LEVEL
```

Salida:

```
{
    "assetSummaries": [
        {
            "id": "a1b2c3d4-5678-90ab-cdef-44444EXAMPLE",
            "arn": "arn:aws:iotsitewise:us-west-2:123456789012:asset/
a1b2c3d4-5678-90ab-cdef-44444EXAMPLE",
            "name": "Wind Farm 1",
            "assetModelId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
            "creationDate": 1575672453.0,
            "lastUpdateDate": 1575672453.0,
            "status": {
                "state": "ACTIVE"
            },
            "hierarchies": [
                {
                    "id": "a1b2c3d4-5678-90ab-cdef-77777EXAMPLE",
                    "name": "Wind Turbines"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Listing assets en la Guía del usuario de AWS IoT SiteWise.

Ejemplo 2: enumeración de todos los activos en función de un modelo de activos

En el siguiente ejemplo de `list-assets`, se enumeran todos los activos según un modelo de activos y que están definidos en su cuenta de AWS en la región actual.

```
aws iotsitewise list-assets \
    --asset-model-id a1b2c3d4-5678-90ab-cdef-11111EXAMPLE
```

Salida:

```
{
    "assetSummaries": [
```

```
        {
            "id": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
            "arn": "arn:aws:iotsitewise:us-west-2:123456789012:asset/
a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
            "name": "Wind Turbine 1",
            "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "creationDate": 1575671550.0,
            "lastUpdateDate": 1575686308.0,
            "status": {
                "state": "ACTIVE"
            },
            "hierarchies": []
        }
    ]
}
```

Para obtener más información, consulte Listing assets en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte ListAssets en la Referencia de comandos de la AWS CLI.

`list-associated-assets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-associated-assets`.

AWS CLI

Para enumerar todos los activos asociados a un activo en una jerarquía específica

En el siguiente ejemplo de `list-associated-assets`, se enumeran todos los activos de turbinas eólicas asociados al activo de parque eólico especificado.

```
aws iotsitewise list-associated-assets \
    --asset-id a1b2c3d4-5678-90ab-cdef-44444EXAMPLE \
    --hierarchy-id a1b2c3d4-5678-90ab-cdef-77777EXAMPLE
```

Salida:

```
{
    "assetSummaries": [
        {
```

```
            "id": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
            "arn": "arn:aws:iotsitewise:us-west-2:123456789012:asset/
a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
            "name": "Wind Turbine 1",
            "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "creationDate": 1575671550.0,
            "lastUpdateDate": 1575686308.0,
            "status": {
                "state": "ACTIVE"
            },
            "hierarchies": []
        }
    ]
}
```

Para obtener más información, consulte Listing assets associated to a specific asset en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte ListAssociatedAssets en la Referencia de comandos de la AWS CLI.

`list-dashboards`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-dashboards`.

AWS CLI

Para enumerar todos los paneles de un proyecto

En el siguiente ejemplo de `list-dashboards`, se enumeran todos los paneles que están definidos en un proyecto.

```
aws iotsitewise list-dashboards \
    --project-id a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE
```

Salida:

```
{
    "dashboardSummaries": [
        {
            "id": "a1b2c3d4-5678-90ab-cdef-fffffEXAMPLE",
            "name": "Wind Farm",
```

```
            "creationDate": "2020-05-01T20:32:12.228476348Z",
            "lastUpdateDate": "2020-05-01T20:32:12.228476348Z"
        }
    ]
}
```

Para obtener más información, consulte Viewing dashboards en la Guía de la aplicación AWS IoT SiteWise Monitor.

- Para obtener detalles sobre la API, consulte ListDashboards en la Referencia de comandos de la AWS CLI.

`list-gateways`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-gateways`.

AWS CLI

Para enumerar todas las puertas de enlace

En el siguiente ejemplo de `list-gateways`, se enumeran todas las puertas de enlace que se definen en la cuenta de AWS en la región actual.

```
aws iotsitewise list-gateways
```

Salida:

```
{
    "gatewaySummaries": [
        {
            "gatewayId": "a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE",
            "gatewayName": "ExampleCorpGateway",
            "gatewayCapabilitySummaries": [
                {
                    "capabilityNamespace": "iotsitewise:opcuacollector:1",
                    "capabilitySyncStatus": "IN_SYNC"
                }
            ],
            "creationDate": 1588369971.457,
            "lastUpdateDate": 1588369971.457
        }
    ]
```

```
}
```

Para obtener más información, consulte Ingesting data using a gateway en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte ListGateways en la Referencia de comandos de la AWS CLI.

`list-portals`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-portals`.

AWS CLI

Para enumerar todos los portales

En el siguiente ejemplo de `list-portals`, se enumeran todos los portales que se definen en la cuenta de AWS en la región actual.

```
aws iotsitewise list-portals
```

Salida:

```
{
    "portalSummaries": [
        {
            "id": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
            "name": "WindFarmPortal",
            "description": "A portal that contains wind farm projects for Example
 Corp.",
            "startUrl": "https://a1b2c3d4-5678-90ab-cdef-
aaaaaEXAMPLE.app.iotsitewise.aws",
            "creationDate": "2020-02-04T23:01:52.90248068Z",
            "lastUpdateDate": "2020-02-04T23:01:52.90248078Z",
            "roleArn": "arn:aws:iam::123456789012:role/service-role/
MySiteWiseMonitorServiceRole"
        }
    ]
}
```

Para obtener más información, consulte Administering your portals en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte ListPortals en la Referencia de comandos de la AWS CLI.

`list-project-assets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-project-assets`.

AWS CLI

Para enumerar todos los activos asociados a un proyecto

En el siguiente ejemplo de `list-project-assets`, se enumeran todos los activos que están asociados a un proyecto de parque eólico.

```
aws iotsitewise list-projects \
    --project-id a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE
```

Salida:

```
{
    "assetIds": [
        "a1b2c3d4-5678-90ab-cdef-44444EXAMPLE"
    ]
}
```

Para obtener más información, consulte Adding assets to projects en la Guía de la aplicación AWS IoT SiteWise Monitor.

- Para obtener información sobre la API, consulte ListProjectAssets en la Referencia de comandos de la AWS CLI.

`list-projects`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-projects`.

AWS CLI

Para enumerar todos los proyectos de un portal

En el siguiente ejemplo de `list-projects`, se enumeran todos los proyectos que están definidos en un portal.

```
aws iotsitewise list-projects \
    --portal-id a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE
```

Salida:

```
{
    "projectSummaries": [
        {
            "id": "a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE",
            "name": "Wind Farm 1",
            "description": "Contains asset visualizations for Wind Farm #1 for
 Example Corp.",
            "creationDate": "2020-02-20T21:58:43.362246001Z",
            "lastUpdateDate": "2020-02-20T21:58:43.362246095Z"
        }
    ]
}
```

Para obtener más información, consulte Viewing project details en la Guía de la aplicación AWS IoT SiteWise Monitor.

- Para obtener detalles sobre la API, consulte ListProjects en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar todas las etiquetas de un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran todas las etiquetas de un activo de turbina eólica.

```
aws iotsitewise list-tags-for-resource \
    --resource-arn arn:aws:iotsitewise:us-west-2:123456789012:asset/
a1b2c3d4-5678-90ab-cdef-33333EXAMPLE
```

Salida:

```
{
    "tags": {
        "Owner": "richard-roe"
    }
}
```

Para obtener más información, consulte Tagging your resources en la Guía del usuario de AWS IoT SiteWise.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-logging-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-logging-options`.

AWS CLI

Para especificar el nivel de registro

En el siguiente ejemplo de `put-logging-options`, se habilita el registro de niveles de `INFO` en AWS IoT SiteWise. Otros niveles incluyen `DEBUG` y `OFF`.

```
aws iotsitewise put-logging-options \
    --logging-options level=INFO
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Monitoring AWS IoT SiteWise with Amazon CloudWatch Logs en la Guía del usuario de AWS IoT SiteWise.

- Para obtener detalles sobre la API, consulte PutLoggingOptions en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Cómo añadir una etiqueta a un recurso

En el siguiente ejemplo de `tag-resource`, se añade una etiqueta de propietario a un activo de turbina eólica. Esto le permite controlar el acceso al activo en función de quién sea su propietario.

```
aws iotsitewise tag-resource \
    --resource-arn arn:aws:iotsitewise:us-west-2:123456789012:asset/
a1b2c3d4-5678-90ab-cdef-33333EXAMPLE \
    --tags Owner=richard-roe
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging your resources en la Guía del usuario de AWS IoT SiteWise.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar una etiqueta de un recurso

En el siguiente ejemplo de `untag-resource`, se elimina una etiqueta de propietario de un activo de turbina eólica.

```
aws iotsitewise untag-resource \
    --resource-arn arn:aws:iotsitewise:us-west-2:123456789012:asset/
a1b2c3d4-5678-90ab-cdef-33333EXAMPLE \
    --tag-keys Owner
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging your resources en la Guía del usuario de AWS IoT SiteWise.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-access-policy

En el siguiente ejemplo de código, se muestra cómo utilizar update-access-policy.

AWS CLI

Para conceder a un lector del proyecto la propiedad de un proyecto

En el siguiente ejemplo de update-access-policy, se actualiza una política de acceso que otorga a un lector del proyecto la propiedad de un proyecto.

```
aws iotsitewise update-access-policy \
    --access-policy-id a1b2c3d4-5678-90ab-cdef-dddddEXAMPLE \
    --cli-input-json file://update-project-viewer-access-policy.json
```

Contenido de update-project-viewer-access-policy.json:

```
{
    "accessPolicyIdentity": {
        "user": {
            "id": "a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-bbbbbEXAMPLE"
        }
    },
    "accessPolicyPermission": "ADMINISTRATOR",
    "accessPolicyResource": {
        "project": {
            "id": "a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE"
        }
    }
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Assigning project owners en la Guía de la aplicación AWS IoT SiteWise Monitor.

- Para obtener información acerca de la API, consulte UpdateAccessPolicy en la Referencia de comandos de la AWS CLI.

update-asset-model

En el siguiente ejemplo de código, se muestra cómo utilizar update-asset-model.

AWS CLI

Para actualizar un modelo de activos

En el siguiente ejemplo de `update-asset-model`, se actualiza la descripción de un modelo de activos de parque eólico. Este ejemplo incluye los ID y las definiciones existentes del modelo, ya que `update-asset-model` sobrescribe el modelo existente con el nuevo modelo.

```
aws iotsitewise update-asset-model \
    --cli-input-json file://update-wind-farm-model.json
```

Contenido de `update-wind-farm-model.json`:

```
{
    "assetModelName": "Wind Farm Model",
    "assetModelDescription": "Represents a wind farm that comprises many wind
 turbines",
    "assetModelProperties": [
        {
            "id": "a1b2c3d4-5678-90ab-cdef-88888EXAMPLE",
            "name": "Region",
            "dataType": "STRING",
            "type": {
                "attribute": {}
            }
        },
        {
            "id": "a1b2c3d4-5678-90ab-cdef-99999EXAMPLE",
            "name": "Total Generated Power",
            "dataType": "DOUBLE",
            "unit": "kW",
            "type": {
                "metric": {
                    "expression": "sum(power)",
                    "variables": [
                        {
                            "name": "power",
                            "value": {
                                "hierarchyId": "a1b2c3d4-5678-90ab-
cdef-77777EXAMPLE",
                                "propertyId": "a1b2c3d4-5678-90ab-cdef-66666EXAMPLE"
                            }
                        }
```

```
                    ],
                    "window": {
                        "tumbling": {
                            "interval": "1h"
                        }
                    }
                }
            }
        }
    ],
    "assetModelHierarchies": [
        {
            "id": "a1b2c3d4-5678-90ab-cdef-77777EXAMPLE",
            "name": "Wind Turbines",
            "childAssetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
        }
    ]
}
```

Salida:

```
{
    "assetModelId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
    "assetModelArn": "arn:aws:iotsitewise:us-west-2:123456789012:asset-model/
a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
    "assetModelStatus": {
        "state": "CREATING"
    }
}
```

Para obtener más información, consulte Updating asset models en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte UpdateAssetModel en la Referencia de comandos de la AWS CLI.

`update-asset-property`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-asset-property`.

AWS CLI

Ejemplo 1: actualización del alias de una propiedad de un activo

En el siguiente ejemplo de `update-asset-property`, se actualiza el alias de la propiedad de potencia de un activo de turbina eólica.

```
aws iotsitewise update-asset-property \
    --asset-id a1b2c3d4-5678-90ab-cdef-33333EXAMPLE \
    --property-id a1b2c3d4-5678-90ab-cdef-55555EXAMPLE \
    --property-alias "/examplecorp/windfarm/1/turbine/1/power" \
    --property-notification-state DISABLED
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Mapping industrial data streams to asset properties en la Guía del usuario de AWS IoT SiteWise.

Ejemplo 2: activación de notificaciones de propiedad de activo

En el siguiente ejemplo de `update-asset-property`, se habilitan las notificaciones de actualización de propiedades de un activo para la propiedad de potencia de un activo de turbina eólica. Las actualizaciones del valor de la propiedad se publican en el tema MQTT `$aws/sitewise/asset-models/<assetModelId>/assets/<assetId>/properties/<propertyId>`, donde cada ID se sustituye por el ID de propiedad, activo y modelo de la propiedad del activo.

```
aws iotsitewise update-asset-property \
    --asset-id a1b2c3d4-5678-90ab-cdef-33333EXAMPLE \
    --property-id a1b2c3d4-5678-90ab-cdef-66666EXAMPLE \
    --property-notification-state ENABLED \
    --property-alias "/examplecorp/windfarm/1/turbine/1/power"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Interacting with other services en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte UpdateAssetProperty en la Referencia de comandos de la AWS CLI.

`update-asset`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-asset`.

AWS CLI

Para actualizar el nombre de un activo

En el siguiente ejemplo de `update-asset`, se actualiza el nombre de un activo de turbina eólica.

```
aws iotsitewise update-asset \
    --asset-id a1b2c3d4-5678-90ab-cdef-33333EXAMPLE \
    --asset-name "Wind Turbine 2"
```

Salida:

```
{
    "assetStatus": {
        "state": "UPDATING"
    }
}
```

Para obtener más información, consulte Updating assets en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte UpdateAsset en la Referencia de comandos de la AWS CLI.

`update-dashboard`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-dashboard`.

AWS CLI

Para actualizar un panel

En el siguiente ejemplo de `update-dashboard`, se modifica el título de un gráfico de líneas de un panel que muestra la potencia total generada para un parque eólico.

```
aws iotsitewise update-dashboard \
    --project-id a1b2c3d4-5678-90ab-cdef-fffffEXAMPLE \
    --dashboard-name "Wind Farm" \
    --dashboard-definition file://update-wind-farm-dashboard.json
```

Contenido de `update-wind-farm-dashboard.json`:

```
{
    "widgets": [
        {
            "type": "monitor-line-chart",
            "title": "Total Generated Power",
            "x": 0,
            "y": 0,
            "height": 3,
            "width": 3,
            "metrics": [
                {
                    "label": "Power",
                    "type": "iotsitewise",
                    "assetId": "a1b2c3d4-5678-90ab-cdef-44444EXAMPLE",
                    "propertyId": "a1b2c3d4-5678-90ab-cdef-99999EXAMPLE"
                }
            ]
        }
    ]
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creating dashboards (CLI) en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte UpdateDashboard en la Referencia de comandos de la AWS CLI.

`update-gateway-capability-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-gateway-capability-configuration`.

AWS CLI

Para actualizar la capacidad de una puerta de enlace

En el siguiente ejemplo de `update-gateway-capability-configuration`, se configura el origen OPC-UA con las siguientes propiedades:

Confía en cualquier certificado. Utiliza el algoritmo Basic256 para proteger los mensajes. Utiliza el modo SignAndEncrypt para proteger las conexiones. Utiliza las credenciales de autenticación almacenadas en un secreto de AWS Secrets Manager.

```
aws iotsitewise update-gateway-capability-configuration \
    --gateway-id a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE \
    --capability-namespace "iotsitewise:opcuacollector:1" \
    --capability-configuration file://opc-ua-capability-configuration.json
```

Contenido de `opc-ua-capability-configuration.json`:

```
{
    "sources": [
        {
            "name": "Wind Farm #1",
            "endpoint": {
                "certificateTrust": {
                    "type": "TrustAny"
                },
                "endpointUri": "opc.tcp://203.0.113.0:49320",
                "securityPolicy": "BASIC256",
                "messageSecurityMode": "SIGN_AND_ENCRYPT",
                "identityProvider": {
                    "type": "Username",
                    "usernameSecretArn": "arn:aws:secretsmanager:us-
west-2:123456789012:secret:greengrass-windfarm1-auth-1ABCDE"
                },
                "nodeFilterRules": []
            },
            "measurementDataStreamPrefix": ""
        }
    ]
}
```

Salida:

```
{
    "capabilityNamespace": "iotsitewise:opcuacollector:1",
    "capabilitySyncStatus": "OUT_OF_SYNC"
}
```

Para obtener más información, consulte Configuring data sources en la Guía del usuario de AWS IoT SiteWise.

- Para obtener detalles sobre la API, consulte UpdateGatewayCapabilityConfiguration en la Referencia de comandos de la AWS CLI.

`update-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-gateway`.

AWS CLI

Para actualizar el nombre de una puerta de enlace

En el siguiente ejemplo de `update-gateway`, se actualiza el nombre de una puerta de enlace.

```
aws iotsitewise update-gateway \
    --gateway-id a1b2c3d4-5678-90ab-cdef-1a1a1EXAMPLE \
    --gateway-name ExampleCorpGateway1
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Ingesting data using a gateway en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte UpdateGateway en la Referencia de comandos de la AWS CLI.

`update-portal`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-portal`.

AWS CLI

Para actualizar los detalles de un portal

En el siguiente ejemplo de `update-portal`, se actualiza un portal web para una empresa de parques eólicos.

```
aws iotsitewise update-portal \
```

```
    --portal-id a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE \
    --portal-name WindFarmPortal \
    --portal-description "A portal that contains wind farm projects for Example
 Corp." \
    --portal-contact-email support@example.com \
    --role-arn arn:aws:iam::123456789012:role/MySiteWiseMonitorServiceRole
```

Salida:

```
{
    "portalStatus": {
        "state": "UPDATING"
    }
}
```

Para obtener más información, consulte Administering your portals en la Guía del usuario de AWS IoT SiteWise.

- Para obtener información sobre la API, consulte UpdatePortal en la Referencia de comandos de la AWS CLI.

`update-project`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-project`.

AWS CLI

Para actualizar los detalles de un proyecto

En el siguiente ejemplo de `update-project`, se actualiza un proyecto de parque eólico.

```
aws iotsitewise update-project \
    --project-id a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE \
    --project-name "Wind Farm 1" \
    --project-description "Contains asset visualizations for Wind Farm #1 for
 Example Corp."
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Changing project details en la Guía de la aplicación AWS IoT SiteWise Monitor.

- Para obtener información sobre la API, consulte UpdateProject en la Referencia de comandos de la AWS CLI.

AWS IoT Things Graph Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS IoT Things Graph.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-entity-to-thing`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-entity-to-thing`.

AWS CLI

Para asociar un objeto con un dispositivo

En el siguiente ejemplo de `associate-entity-to-thing`, se asocia un objeto a un dispositivo. En el ejemplo se utiliza un dispositivo sensor de movimiento que se encuentra en el espacio de nombres público.

```
aws iotthingsgraph associate-entity-to-thing \
    --thing-name "MotionSensorName" \
    --entity-id "urn:tdm:aws/examples:Device:HCSR501MotionSensor"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creating and Uploading Models en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte AssociateEntityToThing en la Referencia de comandos de la AWS CLI.

`create-flow-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-flow-template`.

AWS CLI

Para crear un flujo

En el siguiente ejemplo de `create-flow-template`, se crea un flujo (flujo de trabajo). El valor de `MyFlowDefinition` es el GraphQL que modela el flujo.

```
aws iotthingsgraph create-flow-template \
    --definition language=GRAPHQL,text="MyFlowDefinition"
```

Salida:

```
{
    "summary": {
        "createdAt": 1559248067.545,
        "id": "urn:tdm:us-west-2/123456789012/default:Workflow:MyFlow",
        "revisionNumber": 1
    }
}
```

Para obtener más información, consulte Working with Flows en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte CreateFlowTemplate en la Referencia de comandos de la AWS CLI.

`create-system-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-system-instance`.

AWS CLI

Para crear una instancia de sistema

En el siguiente ejemplo de `create-system-instance`, se crea una instancia del sistema. El valor de `MySystemInstanceDefinition` es el GraphQL que modela la instancia del sistema.

```
aws iotthingsgraph create-system-instance -\
    -definition language=GRAPHQL,text="MySystemInstanceDefinition" \
    --target CLOUD \
    --flow-actions-role-arn myRoleARN
```

Salida:

```
{
    "summary": {
        "id": "urn:tdm:us-west-2/123456789012/default:Deployment:Room218",
        "arn": "arn:aws:iotthingsgraph:us-west-2:123456789012:Deployment/default/
Room218",
        "status": "NOT_DEPLOYED",
        "target": "CLOUD",
        "createdAt": 1559249315.208,
        "updatedAt": 1559249315.208
    }
}
```

Para obtener más información, consulte Working with Systems and Flow Configurations en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte CreateSystemInstance en la Referencia de comandos de la AWS CLI.

`create-system-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-system-template`.

AWS CLI

Para crear un sistema

En el siguiente ejemplo de `create-system-template`, se crea un sistema. El valor de MySystemDefinition es el GraphQL que modela el sistema.

```
aws iotthingsgraph create-system-template \
    --definition language=GRAPHQL,text="MySystemDefinition"
```

Salida:

```
{
    "summary": {
        "createdAt": 1559249776.254,
        "id": "urn:tdm:us-west-2/123456789012/default:System:MySystem",
        "arn": "arn:aws:iotthingsgraph:us-west-2:123456789012:System/default/
MySystem",
        "revisionNumber": 1
    }
}
```

Para obtener más información, consulte Creating Systems en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte CreateSystemTemplate en la Referencia de comandos de la AWS CLI.

`delete-flow-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-flow-template`.

AWS CLI

Para eliminar un flujo

En el siguiente ejemplo de `delete-flow-template`, se elimina un flujo (flujo de trabajo).

```
aws iotthingsgraph delete-flow-template \
    --id "urn:tdm:us-west-2/123456789012/default:Workflow:MyFlow"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Lifecycle Management for AWS IoT Things Graph Entities, Flows, Systems, and Deployments en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte DeleteFlowTemplate en la Referencia de comandos de la AWS CLI.

`delete-namespace`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-namespace`.

AWS CLI

Para eliminar un espacio de nombres

En el siguiente ejemplo de `delete-namespace`, se elimina un espacio de nombres.

```
aws iotthingsgraph delete-namespace
```

Salida:

```
{
   "namespaceArn": "arn:aws:iotthingsgraph:us-west-2:123456789012",
   "namespaceName": "us-west-2/123456789012/default"
}
```

Para obtener más información, consulte Lifecycle Management for AWS IoT Things Graph Entities, Flows, Systems, and Deployments en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte DeleteNamespace en la Referencia de comandos de la AWS CLI.

`delete-system-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-system-instance`.

AWS CLI

Para eliminar una instancia de sistema

En el siguiente ejemplo de `delete-system-instance`, se elimina una instancia del sistema.

```
aws iotthingsgraph delete-system-instance \
    --id "urn:tdm:us-west-2/123456789012/default:Deployment:Room218"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Lifecycle Management for AWS IoT Things Graph Entities, Flows, Systems, and Deployments en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte DeleteSystemInstance en la Referencia de comandos de la AWS CLI.

`delete-system-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-system-template`.

AWS CLI

Para eliminar un sistema

En el siguiente ejemplo de `delete-system-template`, se elimina un sistema.

```
aws iotthingsgraph delete-system-template \
    --id "urn:tdm:us-west-2/123456789012/default:System:MySystem"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Lifecycle Management for AWS IoT Things Graph Entities, Flows, Systems, and Deployments en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte DeleteSystemTemplate en la Referencia de comandos de la AWS CLI.

`deploy-system-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `deploy-system-instance`.

AWS CLI

Para implementar una instancia de sistema

En el siguiente ejemplo de `delete-system-template`, se implementa una instancia del sistema.

```
aws iotthingsgraph deploy-system-instance \
    --id "urn:tdm:us-west-2/123456789012/default:Deployment:Room218"
```

Salida:

```
{
   "summary": {
      "arn": "arn:aws:iotthingsgraph:us-west-2:123456789012:Deployment:Room218",
      "createdAt": 1559249776.254,
      "id": "urn:tdm:us-west-2/123456789012/default:Deployment:Room218",
```

```
        "status": "DEPLOYED_IN_TARGET",
        "target": "CLOUD",
        "updatedAt": 1559249776.254
    }
}
```

Para obtener más información, consulte Working with Systems and Flow Configurations en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte DeploySystemInstance en la Referencia de comandos de la AWS CLI.

`deprecate-flow-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `deprecate-flow-template`.

AWS CLI

Para dar de baja un flujo

En el siguiente ejemplo de `deprecate-flow-template`, se da de baja un flujo (flujo de trabajo).

```
aws iotthingsgraph deprecate-flow-template \
    --id "urn:tdm:us-west-2/123456789012/default:Workflow:MyFlow"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Lifecycle Management for AWS IoT Things Graph Entities, Flows, Systems, and Deployments en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte DeprecateFlowTemplate en la Referencia de comandos de la AWS CLI.

`deprecate-system-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `deprecate-system-template`.

AWS CLI

Para dar de baja un sistema

En el siguiente ejemplo de `deprecate-system-template`, se da de baja un sistema.

```
aws iotthingsgraph deprecate-system-template \
    --id "urn:tdm:us-west-2/123456789012/default:System:MySystem"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Lifecycle Management for AWS IoT Things Graph Entities, Flows, Systems, and Deployments en la Guía del usuario de AWS IoT Things Graph.

- Para obtener más información sobre la API, consulte DeprecateSystemTemplate en la Referencia de comandos de la AWS CLI.

`describe-namespace`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-namespace`.

AWS CLI

Para obtener una descripción de su espacio de nombres

En el siguiente ejemplo de `describe-namespace`, se obtiene una descripción del espacio de nombres.

```
aws iotthingsgraph describe-namespace
```

Salida:

```
{
    "namespaceName": "us-west-2/123456789012/default",
    "trackingNamespaceName": "aws",
    "trackingNamespaceVersion": 1,
    "namespaceVersion": 5
}
```

Para obtener más información, consulte Namespaces en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte DescribeNamespace en la Referencia de comandos de la AWS CLI.

`dissociate-entity-from-thing`

En el siguiente ejemplo de código, se muestra cómo utilizar `dissociate-entity-from-thing`.

AWS CLI

Para desasociar un objeto de un dispositivo

En el siguiente ejemplo de `dissociate-entity-from-thing`, se desvincula un objeto de un dispositivo.

```
aws iotthingsgraph dissociate-entity-from-thing \
    --thing-name "MotionSensorName" \
    --entity-type "DEVICE"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creating and Uploading Models en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte DissociateEntityFromThing en la Referencia de la comandos de la AWS CLI.

`get-entities`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-entities`.

AWS CLI

Para obtener definiciones de las entidades

En el siguiente ejemplo de `get-entities`, se obtiene una definición de un modelo de dispositivo.

```
aws iotthingsgraph get-entities \
    --ids "urn:tdm:aws/examples:DeviceModel:MotionSensor"
```

Salida:

```
{
```

```
    "descriptions": [
        {
            "id": "urn:tdm:aws/examples:DeviceModel:MotionSensor",
            "type": "DEVICE_MODEL",
            "createdAt": 1559256190.599,
            "definition": {
                "language": "GRAPHQL",
                "text": "##\n# Specification of motion sensor devices interface.\n##
\ntype MotionSensor @deviceModel(id: \"urn:tdm:aws/examples:deviceModel:MotionSensor
\",\n        capability: \"urn:tdm:aws/examples:capability:MotionSensorCapability\")
 {ignore:void}"
            }
        }
    ]
}
```

Para obtener más información, consulte Creating and Uploading Models en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte GetEntities en la Referencia de comandos de la AWS CLI.

`get-flow-template-revisions`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-flow-template-revisions`.

AWS CLI

Para obtener información de las revisiones de un flujo

En el siguiente ejemplo de `get-flow-template-revisions`, se obtiene información de revisión de un flujo (flujo de trabajo).

```
aws iotthingsgraph get-flow-template-revisions \
    --id urn:tdm:us-west-2/123456789012/default:Workflow:MyFlow
```

Salida:

```
{
    "summaries": [
        {
            "id": "urn:tdm:us-west-2/123456789012/default:Workflow:MyFlow",
```

```
            "revisionNumber": 1,
            "createdAt": 1559247540.292
        }
    ]
}
```

Para obtener más información, consulte Working with Flows en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte GetFlowTemplateRevisions en la Referencia de comandos de la AWS CLI.

`get-flow-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-flow-template`.

AWS CLI

Para obtener una definición de flujo

En el siguiente ejemplo de `get-flow-template`, se obtiene una definición de un flujo (flujo de trabajo).

```
aws iotthingsgraph get-flow-template \
    --id "urn:tdm:us-west-2/123456789012/default:Workflow:MyFlow"
```

Salida:

```
{
    "description": {
        "summary": {
            "id": "urn:tdm:us-west-2/123456789012/default:Workflow:MyFlow",
            "revisionNumber": 1,
            "createdAt": 1559247540.292
        },
        "definition": {
            "language": "GRAPHQL",
            "text": "{\nquery MyFlow($camera: string!, $screen: string!)
 @workflowType(id: \"urn:tdm:us-west-2/123456789012/default:Workflow:MyFlow\")
 @annotation(type: \"tgc:FlowEvent\", id: \"sledged790c1b2bcd949e09da0c9bfc077f79d
\", x: 1586, y: 653) @triggers(definition: \"{MotionSensor(description:
 \\\"\\\") @position(x: 1045, y: 635.6666564941406) {\\n  condition(expr:
```

```
 \\\"devices[name == \\\\\\\"motionSensor\\\\\\\"].events[name == \\\
\\\\"StateChanged\\\\\\\"].lastEvent\\\")\\n  action(expr: \\\"\\\")\
\n}}\") {\n  variables {\n    cameraResult @property(id: \"urn:tdm:aws/
examples:property:CameraStateProperty\")\n  }\n  steps {\n    step(name: \"Camera
\", outEvent: [\"sledged790c1b2bcd949e09da0c9bfc077f79d\"]) @position(x: 1377,
 y: 638.6666564941406) {\n      DeviceActivity(deviceModel: \"urn:tdm:aws/
examples:deviceModel:Camera\", out: \"cameraResult\", deviceId: \"${camera}\")
 {\n        capture\n      }\n    }\n    step(name: \"Screen\", inEvent:
 [\"sledged790c1b2bcd949e09da0c9bfc077f79d\"]) @position(x: 1675.6666870117188,
 y: 637.9999847412109) {\n      DeviceActivity(deviceModel: \"urn:tdm:aws/
examples:deviceModel:Screen\", deviceId: \"${screen}\") {\n        display(imageUrl:
 \"${cameraResult.lastClickedImage}\")\n      }\n    }\n  }\n}\n}"
        },
        "validatedNamespaceVersion": 5
    }
}
```

Para obtener más información, consulte Working with Flows en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte GetFlowTemplate en la Referencia de comandos de la AWS CLI.

`get-namespace-deletion-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-namespace-deletion-status`.

AWS CLI

Para obtener el estado de la tarea de eliminación del espacio de nombres

En el siguiente ejemplo de `get-namespace-deletion-status`, se obtiene el estado de la tarea de eliminación del espacio de nombres.

```
aws iotthingsgraph get-namespace-deletion-status
```

Salida:

```
{
   "namespaceArn": "arn:aws:iotthingsgraph:us-west-2:123456789012",
   "namespaceName": "us-west-2/123456789012/default"
   "status": "SUCCEEDED "
```

```
}
```

Para obtener más información, consulte Namespaces en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte GetNamespaceDeletionStatus en la Referencia de comandos de la AWS CLI.

`get-system-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-system-instance`.

AWS CLI

Para obtener una instancia de sistema

En el siguiente ejemplo de `get-system-instance`, se obtiene una definición de una instancia del sistema.

```
aws iotthingsgraph get-system-instance \
    --id "urn:tdm:us-west-2/123456789012/default:Deployment:Room218"
```

Salida:

```
{
    "description": {
        "summary": {
            "id": "urn:tdm:us-west-2/123456789012/default:Deployment:Room218",
            "arn": "arn:aws:iotthingsgraph:us-west-2:123456789012:Deployment/
default/Room218",
            "status": "NOT_DEPLOYED",
            "target": "CLOUD",
            "createdAt": 1559249315.208,
            "updatedAt": 1559249315.208
        },
        "definition": {
            "language": "GRAPHQL",
            "text": "{\r\nquery Room218 @deployment(id: \"urn:tdm:us-
west-2/123456789012/default:Deployment:Room218\", systemId: \"urn:tdm:us-
west-2/123456789012/default:System:SecurityFlow\") {\r\n    motionSensor(deviceId:
 \"MotionSensorName\")\r\n    screen(deviceId: \"ScreenName\")\r\n
 camera(deviceId: \"CameraName\") \r\n    triggers {MotionEventTrigger(description:
```

```
 \"a trigger\") {  \r\n    condition(expr: \"devices[name ==
 'motionSensor'].events[name == 'StateChanged'].lastEvent\") \r\n    action(expr:
 \"ThingsGraph.startFlow('SecurityFlow', bindings[name == 'camera'].deviceId,
 bindings[name == 'screen'].deviceId)\")\r\n    }\r\n   }\r\n  }\r\n  }"
        },
        "metricsConfiguration": {
            "cloudMetricEnabled": false
        },
        "validatedNamespaceVersion": 5,
        "flowActionsRoleArn": "arn:aws:iam::123456789012:role/ThingsGraphRole"
    }
}
```

Para obtener más información, consulte Working with Systems and Flow Configurations en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte GetSystemInstance en la Referencia de comandos de la AWS CLI.

`get-system-template-revisions`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-system-template-revisions`.

AWS CLI

Para obtener información de las revisiones de un flujo

En el siguiente ejemplo de `get-system-template-revisions`, se obtiene información de revisión sobre un sistema.

```
aws iotthingsgraph get-system-template-revisions \
    --id "urn:tdm:us-west-2/123456789012/default:System:MySystem"
```

Salida:

```
{
    "summaries": [
        {
            "id": "urn:tdm:us-west-2/123456789012/default:System:MySystem",
            "arn": "arn:aws:iotthingsgraph:us-west-2:123456789012:System/default/
MySystem",
            "revisionNumber": 1,
```

```
            "createdAt": 1559247540.656
        }
    ]
}
```

Para obtener más información, consulte Working with Systems and Flow Configurations en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte GetSystemTemplateRevisions en la Referencia de comandos de la AWS CLI.

`get-system-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-system-template`.

AWS CLI

Para obtener un sistema

En el siguiente ejemplo de `get-system-template`, se obtiene una definición de un sistema.

```
aws iotthingsgraph get-system-template \
    --id "urn:tdm:us-west-2/123456789012/default:System:MySystem"
```

Salida:

```
{
    "description": {
        "summary": {
            "id": "urn:tdm:us-west-2/123456789012/default:System:MySystem",
            "arn": "arn:aws:iotthingsgraph:us-west-2:123456789012:System/default/
MyFlow",
            "revisionNumber": 1,
            "createdAt": 1559247540.656
        },
        "definition": {
            "language": "GRAPHQL",
            "text": "{\ntype MySystem @systemType(id: \"urn:tdm:us-
west-2/123456789012/default:System:MySystem\", description: \"\") {\n  camera:
 Camera @thing(id: \"urn:tdm:aws/examples:deviceModel:Camera\")\n  screen:
 Screen @thing(id: \"urn:tdm:aws/examples:deviceModel:Screen\")\n  motionSensor:
 MotionSensor @thing(id: \"urn:tdm:aws/examples:deviceModel:MotionSensor
```

```
\")\n  MyFlow: MyFlow @workflow(id: \"urn:tdm:us-west-2/123456789012/
default:Workflow:MyFlow\")\n}\n}"
        },
        "validatedNamespaceVersion": 5
    }
}
```

Para obtener más información, consulte Working with Systems and Flow Configurations en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte GetSystemTemplate en la Referencia de comandos de la AWS CLI.

`get-upload-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-upload-status`.

AWS CLI

Para obtener el estado de la carga de la entidad

En el siguiente ejemplo de `get-upload-status`, se obtiene el estado de la operación de carga de la entidad. El valor de `MyUploadId` es el valor de ID devuelto por la operación `upload-entity-definitions`.

```
aws iotthingsgraph get-upload-status \
    --upload-id "MyUploadId"
```

Salida:

```
{
    "namespaceName": "us-west-2/123456789012/default",
    "namespaceVersion": 5,
    "uploadId": "f6294f1e-b109-4bbe-9073-f451a2dda2da",
    "uploadStatus": "SUCCEEDED"
}
```

Para obtener más información, consulte Modeling Entities en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte GetUploadStatus en la Referencia de comandos de la AWS CLI.

`list-flow-execution-messages`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-flow-execution-messages`.

AWS CLI

Para obtener información sobre los eventos de la ejecución de un flujo

En el siguiente ejemplo de `list-flow-execution-messages`, se obtiene información sobre los eventos de una ejecución de flujo.

```
aws iotthingsgraph list-flow-execution-messages \
    --flow-execution-id "urn:tdm:us-west-2/123456789012/
default:Workflow:SecurityFlow_2019-05-11T19:39:55.317Z_MotionSensor_69b151ad-
a611-42f5-ac21-fe537f9868ad"
```

Salida:

```
{
    "messages": [
        {
         "eventType": "EXECUTION_STARTED",
         "messageId": "f6294f1e-b109-4bbe-9073-f451a2dda2da",
         "payload": "Flow execution started",
         "timestamp": 1559247540.656
        }
    ]
}
```

Para obtener más información, consulte Working with Flows en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte ListFlowExecutionMessages en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar todas las etiquetas de un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran todas las etiquetas de un recurso de AWS IoT Things Graph.

```
aws iotthingsgraph list-tags-for-resource \
    --resource-arn "arn:aws:iotthingsgraph:us-west-2:123456789012:Deployment/default/Room218"
```

Salida:

```
{
   "tags": [
      {
         "key": "Type",
         "value": "Residential"
      }
   ]
}
```

Para obtener más información, consulte Tagging Your AWS IoT Things Graph Resources en la Guía del usuario de AWS IoT Things Graph.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`search-entities`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-entities`.

AWS CLI

Para buscar entidades

En el siguiente ejemplo de `search-entities`, se buscan todas las entidades del tipo `EVENT`.

```
aws iotthingsgraph search-entities \
    --entity-types "EVENT"
```

Salida:

```
{
```

```
    "descriptions": [
        {
            "id": "urn:tdm:aws/examples:Event:MotionSensorEvent",
            "type": "EVENT",
            "definition": {
                "language": "GRAPHQL",
                "text": "##\n# Description of events emitted by motion
 sensor.\n##\ntype MotionSensorEvent @eventType(id: \"urn:tdm:aws/
examples:event:MotionSensorEvent\",\n            payload: \"urn:tdm:aws/
examples:property:MotionSensorStateProperty\") {ignore:void}"
            }
        },
        {
            "id": "urn:tdm:us-west-2/123456789012/
default:Event:CameraClickedEventV2",
            "type": "EVENT",
            "definition": {
                "language": "GRAPHQL",
                "text": "type CameraClickedEventV2 @eventType(id: \"urn:tdm:us-
west-2/123456789012/default:event:CameraClickedEventV2\",\r\npayload:
 \"urn:tdm:aws:Property:Boolean\"){ignore:void}"
            }
        },
        {
            "id": "urn:tdm:us-west-2/123456789012/
default:Event:MotionSensorEventV2",
            "type": "EVENT",
            "definition": {
                "language": "GRAPHQL",
                "text": "# Event emitted by the motion sensor.\r\ntype
 MotionSensorEventV2 @eventType(id: \"urn:tdm:us-west-2/123456789012/
default:event:MotionSensorEventV2\",\r\npayload: \"urn:tdm:us-west-2/123456789012/
default:property:MotionSensorStateProperty2\") {ignore:void}"
            }
        }
    ],
    "nextToken": "urn:tdm:us-west-2/123456789012/default:Event:MotionSensorEventV2"
}
```

Para obtener más información, consulte la AWS IoT Things Graph Data Model Reference en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte SearchEntities en la Referencia de comandos de la AWS CLI.

`search-flow-executions`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-flow-executions`.

AWS CLI

Para buscar ejecuciones de flujos

En el siguiente ejemplo de `search-flow-executions`, se buscan todas las ejecuciones de un flujo en una instancia del sistema especificada.

```
aws iotthingsgraph search-flow-executions \
    --system-instance-id "urn:tdm:us-west-2/123456789012/default:Deployment:Room218"
```

Salida:

```
{
   "summaries": [
      {
         "createdAt": 1559247540.656,
         "flowExecutionId": "f6294f1e-b109-4bbe-9073-f451a2dda2da",
         "flowTemplateId": "urn:tdm:us-west-2/123456789012/default:Workflow:MyFlow",
         "status": "RUNNING ",
         "systemInstanceId": "urn:tdm:us-west-2/123456789012/
default:System:MySystem",
         "updatedAt": 1559247540.656
      }
   ]
}
```

Para obtener más información, consulte Working with Systems and Flow Configurations en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte SearchFlowExecutions en la Referencia de comandos de la AWS CLI.

`search-flow-templates`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-flow-templates`.

AWS CLI

Para buscar flujos (o flujos de trabajo)

En el siguiente ejemplo de `search-flow-templates`, se buscan todos los flujos (flujos de trabajo) que contienen el modelo de dispositivo de cámara.

```
aws iotthingsgraph search-flow-templates \
    --filters name="DEVICE_MODEL_ID",value="urn:tdm:aws/examples:DeviceModel:Camera"
```

Salida:

```
{
    "summaries": [
        {
            "id": "urn:tdm:us-west-2/123456789012/default:Workflow:MyFlow",
            "revisionNumber": 1,
            "createdAt": 1559247540.292
        },
        {
            "id": "urn:tdm:us-west-2/123456789012/default:Workflow:SecurityFlow",
            "revisionNumber": 3,
            "createdAt": 1548283099.27
        }
    ]
}
```

Para obtener más información, consulte Working with Flows en la Guía del usuario de AWS IoT Things Graph.

- Para obtener más información sobre la API, consulte SearchFlowTemplates en la Referencia de comandos de la AWS CLI.

`search-system-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-system-instances`.

AWS CLI

Para buscar instancias de sistema

En el siguiente ejemplo de `search-system-instances`, se buscan todas las instancias del sistema que contienen el sistema especificado.

```
aws iotthingsgraph search-system-instances \
```

```
    --filters name="SYSTEM_TEMPLATE_ID",value="urn:tdm:us-west-2/123456789012/
default:System:SecurityFlow"
```

Salida:

```
{
    "summaries": [
        {
            "id": "urn:tdm:us-west-2/123456789012/
default:Deployment:DeploymentForSample",
            "arn": "arn:aws:iotthingsgraph:us-west-2:123456789012:Deployment/
default/DeploymentForSample",
            "status": "NOT_DEPLOYED",
            "target": "GREENGRASS",
            "greengrassGroupName": "ThingsGraphGrnGr",
            "createdAt": 1555716314.707,
            "updatedAt": 1555716314.707
        },
        {
            "id": "urn:tdm:us-west-2/123456789012/
default:Deployment:MockDeployment",
            "arn": "arn:aws:iotthingsgraph:us-west-2:123456789012:Deployment/
default/MockDeployment",
            "status": "DELETED_IN_TARGET",
            "target": "GREENGRASS",
            "greengrassGroupName": "ThingsGraphGrnGr",
            "createdAt": 1549416462.049,
            "updatedAt": 1549416722.361,
            "greengrassGroupId": "01d04b07-2a51-467f-9d03-0c90b3cdcaaf",
            "greengrassGroupVersionId": "7365aed7-2d3e-4d13-aad8-75443d45eb05"
        },
        {
            "id": "urn:tdm:us-west-2/123456789012/
default:Deployment:MockDeployment2",
            "arn": "arn:aws:iotthingsgraph:us-west-2:123456789012:Deployment/
default/MockDeployment2",
            "status": "DEPLOYED_IN_TARGET",
            "target": "GREENGRASS",
            "greengrassGroupName": "ThingsGraphGrnGr",
            "createdAt": 1549572385.774,
            "updatedAt": 1549572418.408,
            "greengrassGroupId": "01d04b07-2a51-467f-9d03-0c90b3cdcaaf",
            "greengrassGroupVersionId": "bfa70ab3-2bf7-409c-a4d4-bc8328ae5b86"
```

```
        },
        {
            "id": "urn:tdm:us-west-2/123456789012/default:Deployment:Room215",
            "arn": "arn:aws:iotthingsgraph:us-west-2:123456789012:Deployment/
default/Room215",
            "status": "NOT_DEPLOYED",
            "target": "GREENGRASS",
            "greengrassGroupName": "ThingsGraphGG",
            "createdAt": 1547056918.413,
            "updatedAt": 1547056918.413
        },
        {
            "id": "urn:tdm:us-west-2/123456789012/default:Deployment:Room218",
            "arn": "arn:aws:iotthingsgraph:us-west-2:123456789012:Deployment/
default/Room218",
            "status": "NOT_DEPLOYED",
            "target": "CLOUD",
            "createdAt": 1559249315.208,
            "updatedAt": 1559249315.208
        }
    ]
}
```

Para obtener más información, consulte Working with Systems and Flow Configurations en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte SearchSystemInstances en la Referencia de comandos de la AWS CLI.

`search-system-templates`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-system-templates`.

AWS CLI

Para buscar un sistema

En el siguiente ejemplo de `search-system-templates`, se buscan todos los sistemas que contienen el flujo especificado.

```
aws iotthingsgraph search-system-templates \
```

```
    --filters name="FLOW_TEMPLATE_ID",value="urn:tdm:us-west-2/123456789012/
default:Workflow:SecurityFlow"
```

Salida:

```
{
    "summaries": [
        {
            "id": "urn:tdm:us-west-2/123456789012/default:System:SecurityFlow",
            "arn": "arn:aws:iotthingsgraph:us-west-2:123456789012:System/default/
SecurityFlow",
            "revisionNumber": 1,
            "createdAt": 1548283099.433
        }
    ]
}
```

Para obtener más información, consulte Working with Flows en la Guía del usuario de AWS IoT Things Graph.

- Para obtener más información sobre la API, consulte SearchSystemTemplates en la Referencia de comandos de la AWS CLI.

`search-things`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-things`.

AWS CLI

Para buscar objetos asociados a dispositivos y modelos de dispositivos

En el siguiente ejemplo de `search-things`, se buscan todos los objetos asociados al dispositivo HCSR501MotionSensor.

```
aws iotthingsgraph search-things \
    --entity-id "urn:tdm:aws/examples:Device:HCSR501MotionSensor"
```

Salida:

```
{
    "things": [
        {
```

```
            "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MotionSensor1",
            "thingName": "MotionSensor1"
        },
        {
            "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/TG_MS",
            "thingName": "TG_MS"
        }
    ]
}
```

Para obtener más información, consulte Creating and Uploading Models en la Guía del usuario de AWS IoT Things Graph.

- Para obtener más información sobre la API, consulte SearchThings en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para crear una etiqueta para un recurso

En el siguiente ejemplo de `tag-resource`, se crea una etiqueta de un recurso especificado.

```
aws iotthingsgraph tag-resource \
    --resource-arn "arn:aws:iotthingsgraph:us-west-2:123456789012:Deployment/
default/Room218" \
    --tags key="Type",value="Residential"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging Your AWS IoT Things Graph Resources en la Guía del usuario de AWS IoT Things Graph.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`undeploy-system-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `undeploy-system-instance`.

AWS CLI

Para anular la implementación de una instancia de sistema de su destino

En el siguiente ejemplo de `undeploy-system-instance`, se elimina una instancia del sistema de su destino.

```
aws iotthingsgraph undeploy-system-instance \
    --id "urn:tdm:us-west-2/123456789012/default:Deployment:Room215"
```

Salida:

```
{
    "summary": {
        "id": "urn:tdm:us-west-2/123456789012/default:Deployment:Room215",
        "arn": "arn:aws:iotthingsgraph:us-west-2:123456789012:Deployment/default/
Room215",
        "status": "PENDING_DELETE",
        "target": "GREENGRASS",
        "greengrassGroupName": "ThingsGraphGrnGr",
        "createdAt": 1553189694.255,
        "updatedAt": 1559344549.601,
        "greengrassGroupId": "01d04b07-2a51-467f-9d03-0c90b3cdcaaf",
        "greengrassGroupVersionId": "731b371d-d644-4b67-ac64-3934e99b75d7"
    }
}
```

Para obtener más información, consulte Lifecycle Management for AWS IoT Things Graph Entities, Flows, Systems, and Deployments en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte UndeploySystemInstance en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar una etiqueta de un recurso

En el siguiente ejemplo de `untag-resource`, se elimina una etiqueta del recurso especificado.

```
aws iotthingsgraph untag-resource \
    --resource-arn "arn:aws:iotthingsgraph:us-west-2:123456789012:Deployment/
default/Room218" \
    --tag-keys "Type"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging Your AWS IoT Things Graph Resources en la Guía del usuario de AWS IoT Things Graph.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-flow-template

En el siguiente ejemplo de código, se muestra cómo utilizar `update-flow-template`.

AWS CLI

Para actualizar un flujo

En el siguiente ejemplo de `update-flow-template`, se actualiza un flujo (flujo de trabajo). El valor de `MyFlowDefinition` es el GraphQL que modela el flujo.

```
aws iotthingsgraph update-flow-template \
    --id "urn:tdm:us-west-2/123456789012/default:Workflow:MyFlow" \
    --definition language=GRAPHQL,text="MyFlowDefinition"
```

Salida:

```
{
    "summary": {
        "createdAt": 1559248067.545,
        "id": "urn:tdm:us-west-2/123456789012/default:Workflow:MyFlow",
        "revisionNumber": 2
    }
}
```

Para obtener más información, consulte Working with Flows en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información acerca de la API, consulte UpdateFlowTemplate en la Referencia de comandos de la AWS CLI.

`update-system-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-system-template`.

AWS CLI

Para actualizar un sistema

En el siguiente ejemplo de `update-system-template`, se actualiza un sistema. El valor de `MySystemDefinition` es el GraphQL que modela el sistema.

```
aws iotthingsgraph update-system-template \
    --id "urn:tdm:us-west-2/123456789012/default:System:MySystem" \
    --definition language=GRAPHQL,text="MySystemDefinition"
```

Salida:

```
{
    "summary": {
        "createdAt": 1559249776.254,
        "id": "urn:tdm:us-west-2/123456789012/default:System:MySystem",
        "arn": "arn:aws:iotthingsgraph:us-west-2:123456789012:System/default/
MySystem",
        "revisionNumber": 2
    }
}
```

Para obtener más información, consulte Creating Systems en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte UpdateSystemTemplate en la Referencia de comandos de la AWS CLI.

`upload-entity-definitions`

En el siguiente ejemplo de código, se muestra cómo utilizar `upload-entity-definitions`.

AWS CLI

Para cargar definiciones de entidades

En el siguiente ejemplo de `upload-entity-definitions`, se cargan las definiciones de entidades en su espacio de nombres. El valor de `MyEntityDefinitions` es el GraphQL que modela las entidades.

```
aws iotthingsgraph upload-entity-definitions \
    --document language=GRAPHQL,text="MyEntityDefinitions"
```

Salida:

```
{
    "uploadId": "f6294f1e-b109-4bbe-9073-f451a2dda2da"
}
```

Para obtener más información, consulte Modeling Entities en la Guía del usuario de AWS IoT Things Graph.

- Para obtener información sobre la API, consulte UploadEntityDefinitions en la Referencia de comandos de la AWS CLI.

AWS IoT Wireless Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS IoT Wireless.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-aws-account-with-partner-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-aws-account-with-partner-account`.

AWS CLI

Para asociar una cuenta de socio a su cuenta de AWS

El siguiente ejemplo de `associate-aws-account-with-partner-account`, se asocian las siguientes credenciales de la cuenta de Sidewalk a su cuenta de AWS.

```
aws iotwireless associate-aws-account-with-partner-account \
    --sidewalk
 AmazonId="12345678901234",AppServerPrivateKey="a123b45c6d78e9f012a34cd5e6a7890b12c3d45e6f78
```

Salida:

```
{
    "Sidewalk": {
        "AmazonId": "12345678901234",
        "AppServerPrivateKey":
 "a123b45c6d78e9f012a34cd5e6a7890b12c3d45e6f78a1b234c56d7e890a1234"
    }
}
```

Para obtener más información, consulte Integración de Amazon Sidewalk para AWS IoT Core en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte AssociateAwsAccountWithPartnerAccount en la Referencia de comandos de la AWS CLI.

`associate-wireless-device-with-thing`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-wireless-device-with-thing`.

AWS CLI

Para asociar un objeto a un dispositivo inalámbrico

En el siguiente ejemplo de `associate-wireless-device-with-thing`, se asocia un objeto al dispositivo inalámbrico que tiene el ID especificado.

```
aws iotwireless associate-wireless-device-with-thing \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d" \
    --thing-arn "arn:aws:iot:us-east-1:123456789012:thing/MyIoTWirelessThing"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Agregar las puertas de enlace y dispositivos inalámbricos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte AssociateWirelessDeviceWithThing en la Referencia de comandos de la AWS CLI.

`associate-wireless-gateway-with-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-wireless-gateway-with-certificate`.

AWS CLI

Para asociar el certificado a la puerta de enlace inalámbrica

`associate-wireless-gateway-with-certificate` asocia una puerta de enlace inalámbrica a un certificado.

```
aws iotwireless associate-wireless-gateway-with-certificate \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d" \
    --iot-certificate-
id "a123b45c6d78e9f012a34cd5e6a7890b12c3d45e6f78a1b234c56d7e890a1234"
```

Salida:

```
{
    "IotCertificateId":
 "a123b45c6d78e9f012a34cd5e6a7890b12c3d45e6f78a1b234c56d7e890a1234"
}
```

Para obtener más información, consulte Agregar las puertas de enlace y dispositivos inalámbricos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte AssociateWirelessGatewayWithCertificate en la Referencia de comandos de la AWS CLI.

`associate-wireless-gateway-with-thing`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-wireless-gateway-with-thing`.

AWS CLI

Para asociar un objeto a una puerta de enlace inalámbrica

En el siguiente ejemplo de `associate-wireless-gateway-with-thing`, se asocia un objeto a una puerta de enlace inalámbrica.

```
aws iotwireless associate-wireless-gateway-with-thing \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d" \
    --thing-arn "arn:aws:iot:us-east-1:123456789012:thing/MyIoTWirelessThing"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Agregar las puertas de enlace y dispositivos inalámbricos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte AssociateWirelessGatewayWithThing en la Referencia de comandos de la AWS CLI.

`create-destination`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-destination`.

AWS CLI

Para crear un destino inalámbrico de IoT

En el siguiente ejemplo de `create-destination`, se crea un destino para asignar un mensaje de dispositivo a una regla de AWS IoT. Antes de ejecutar este comando, debe haber creado un rol de IAM que otorgue a AWS IoT Core para LoRaWAN los permisos necesarios para enviar datos a la regla de AWS de IoT.

```
aws iotwireless create-destination \
    --name IoTWirelessDestination \
```

```
    --expression-type RuleName \
    --expression IoTWirelessRule \
    --role-arn arn:aws:iam::123456789012:role/IoTWirelessDestinationRole
```

Salida:

```
{
    "Arn": "arn:aws:iotwireless:us-east-1:123456789012:Destination/
IoTWirelessDestination",
    "Name": "IoTWirelessDestination"
}
```

Para obtener más información, consulte Agregar destinos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateDestination en la Referencia de comandos de la AWS CLI.

`create-device-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-device-profile`.

AWS CLI

Para crear un nuevo perfil de dispositivo

En el siguiente ejemplo de `create-device-profile`, se crea un nuevo perfil de dispositivo inalámbrico de IoT.

```
aws iotwireless create-device-profile
```

Salida:

```
{
    "Arn": "arn:aws:iotwireless:us-east-1:123456789012:DeviceProfile/12345678-
a1b2-3c45-67d8-e90fa1b2c34d",
    "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
}
```

Para obtener más información, consulte Agregar perfiles a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateDeviceProfile en la Referencia de comandos de la AWS CLI.

`create-service-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-service-profile`.

AWS CLI

Para crear un nuevo perfil de servicio

En el siguiente ejemplo de `create-service-profile`, se crea un nuevo perfil de servicio inalámbrico de IoT.

```
aws iotwireless create-service-profile
```

Salida:

```
{
    "Arn": "arn:aws:iotwireless:us-east-1:123456789012:ServiceProfile/12345678-
a1b2-3c45-67d8-e90fa1b2c34d",
    "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
}
```

Para obtener más información, consulte Agregar perfiles a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateServiceProfile en la Referencia de comandos de la AWS CLI.

`create-wireless-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-wireless-device`.

AWS CLI

Para crear un dispositivo inalámbrico de IoT

En el siguiente ejemplo de `create-wireless-device`, se crea un recurso de dispositivo inalámbrico del tipo LoRaWAN.

```
aws iotwireless create-wireless-device \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "Description": "My LoRaWAN wireless device"
    "DestinationName": "IoTWirelessDestination"
    "LoRaWAN": {
        "DeviceProfileId": "ab0c23d3-b001-45ef-6a01-2bc3de4f5333",
        "ServiceProfileId": "fe98dc76-cd12-001e-2d34-5550432da100",
        "OtaaV1_1": {
            "AppKey": "3f4ca100e2fc675ea123f4eb12c4a012",
            "JoinEui": "b4c231a359bc2e3d",
            "NwkKey": "01c3f004a2d6efffe32c4eda14bcd2b4"
        },
        "DevEui": "ac12efc654d23fc2"
    },
    "Name": "SampleIoTWirelessThing"
    "Type": LoRaWAN
}
```

Salida:

```
{
    "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:WirelessDevice/1ffd32c8-8130-4194-96df-622f072a315f",
    "Id": "1ffd32c8-8130-4194-96df-622f072a315f"
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateWirelessDevice en la Referencia de comandos de la AWS CLI.

`create-wireless-gateway-task-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-wireless-gateway-task-definition`.

AWS CLI

Para crear una definición de la tarea de puerta de enlace inalámbrica

`create-wireless-gateway-task-definition` crea tareas automáticamente con esta definición de tarea para todas las puertas de enlace con la versión actual especificada.

```
aws iotwireless create-wireless-gateway-task-definition \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "AutoCreateTasks": true,
    "Name": "TestAutoUpdate",
    "Update":{
        "UpdateDataSource" : "s3://cupsalphagafirmwarebin/station",
        "UpdateDataRole" : "arn:aws:iam::001234567890:role/SDK_Test_Role",
        "LoRaWAN" :{
            "CurrentVersion" :{
                "PackageVersion" : "1.0.0",
                "Station" : "2.0.5",
                "Model" : "linux"
            },
            "UpdateVersion" :{
                "PackageVersion" : "1.0.1",
                "Station" : "2.0.5",
                "Model" : "minihub"
            }
        }
    }
}
```

Salida:

```
{
    "Id": "b7d3baad-25c7-35e7-a4e1-1683a0d61da9"
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateWirelessGatewayTaskDefinition en la Referencia de comandos de la AWS CLI.

`create-wireless-gateway-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-wireless-gateway-task`.

AWS CLI

Para crear la tarea para una puerta de enlace inalámbrica

En el siguiente ejemplo de `create-wireless-gateway-task`, se crea una tarea para una puerta de enlace inalámbrica.

```
aws iotwireless create-wireless-gateway-task \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d" \
    --wireless-gateway-task-definition-id "aa000102-0304-b0cd-ef56-a1b23cde456a"
```

Salida:

```
{
    "WirelessGatewayTaskDefinitionId": "aa204003-0604-30fb-ac82-a4f95aaf450a",
    "Status": "Success"
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateWirelessGatewayTask en la Referencia de comandos de la AWS CLI.

`create-wireless-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-wireless-gateway`.

AWS CLI

Para crear una puerta de enlace inalámbrica

En el siguiente ejemplo de `create-wireless-gateway`, se crea una puerta de enlace de dispositivo para LoRaWAN inalámbrica.

```
aws iotwireless create-wireless-gateway \
    --lorawan GatewayEui="a1b2c3d4567890ab",RfRegion="US915" \
    --name "myFirstLoRaWANGateway" \
    --description "Using my first LoRaWAN gateway"
```

Salida:

```
{
    "Arn": "arn:aws:iotwireless:us-east-1:123456789012:WirelessGateway/12345678-
a1b2-3c45-67d8-e90fa1b2c34d",
    "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte CreateWirelessGateway en la Referencia de comandos de la AWS CLI.

`delete-destination`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-destination`.

AWS CLI

Para eliminar un destino inalámbrico de IoT

En el siguiente ejemplo de `delete-destination`, se elimina el recurso de destino inalámbrico con el nombre `IoTWirelessDestination` que ha creado.

```
aws iotwireless delete-destination \
    --name "IoTWirelessDestination"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Agregar destinos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteDestination en la Referencia de comandos de la AWS CLI.

`delete-device-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-device-profile`.

AWS CLI

Para eliminar un perfil de dispositivo

En el siguiente ejemplo de `delete-device-profile`, se elimina un perfil de dispositivo con el ID especificado que ha creado.

```
aws iotwireless delete-device-profile \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Agregar perfiles a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteDeviceProfile en la Referencia de comandos de la AWS CLI.

`delete-service-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-service-profile`.

AWS CLI

Para eliminar un perfil de servicio

En el siguiente ejemplo de `delete-service-profile`, se elimina un perfil de servicio con el ID especificado que ha creado.

```
aws iotwireless delete-service-profile \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Agregar perfiles a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteServiceProfile en la Referencia de comandos de la AWS CLI.

`delete-wireless-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-wireless-device`.

AWS CLI

Para eliminar un dispositivo inalámbrico

En el siguiente ejemplo de `delete-wireless-device`, se elimina el dispositivo inalámbrico que tiene el ID especificado.

```
aws iotwireless delete-wireless-device \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteWirelessDevice en la Referencia de comandos de la AWS CLI.

`delete-wireless-gateway-task-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-wireless-gateway-task-definition`.

AWS CLI

Para eliminar una definición de tarea de puerta de enlace inalámbrica

En el siguiente ejemplo de `delete-wireless-gateway-task-definition`, se elimina la definición de tarea de puerta de enlace inalámbrica que ha creado con el siguiente ID.

```
aws iotwireless delete-wireless-gateway-task-definition \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteWirelessGatewayTaskDefinition en la Referencia de comandos de la AWS CLI.

`delete-wireless-gateway-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-wireless-gateway-task`.

AWS CLI

Para eliminar una tarea de puerta de enlace inalámbrica

En el siguiente ejemplo de `delete-wireless-gateway-task`, se elimina la tarea de puerta de enlace inalámbrica que tiene el ID especificado.

```
aws iotwireless delete-wireless-gateway-task \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteWirelessGatewayTask en la Referencia de comandos de la AWS CLI.

`delete-wireless-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-wireless-gateway`.

AWS CLI

Para eliminar una puerta de enlace inalámbrica

En el siguiente ejemplo de `delete-wireless-gateway`, se elimina la puerta de enlace inalámbrica que tiene el ID especificado.

```
aws iotwireless delete-wireless-gateway \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DeleteWirelessGateway en la Referencia de comandos de la AWS CLI.

`disassociate-aws-account-from-partner-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-aws-account-from-partner-account`.

AWS CLI

Para desasociar la cuenta de socio de la cuenta de AWS

En el siguiente ejemplo de `disassociate-aws-account-from-partner-account`, se desasocia una cuenta de socio de su cuenta de AWS asociada actualmente.

```
aws iotwireless disassociate-aws-account-from-partner-account \
    --partner-account-id "12345678901234" \
    --partner-type "Sidewalk"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Agregar las puertas de enlace y dispositivos inalámbricos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DisassociateAwsAccountFromPartnerAccount en la Referencia de comandos de la AWS CLI.

`disassociate-wireless-device-from-thing`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-wireless-device-from-thing`.

AWS CLI

Para desasociar el objeto del dispositivo inalámbrico

En el siguiente ejemplo de `disassociate-wireless-device-from-thing`, se desvincula un dispositivo inalámbrico del dispositivo con el que está asociado actualmente.

```
aws iotwireless disassociate-wireless-device-from-thing \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Agregar las puertas de enlace y dispositivos inalámbricos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DisassociateWirelessDeviceFromThing en la Referencia de comandos de la AWS CLI.

`disassociate-wireless-gateway-from-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-wireless-gateway-from-certificate`.

AWS CLI

Para asociar el certificado a la puerta de enlace inalámbrica

En el siguiente ejemplo de `disassociate-wireless-gateway-from-certificate`, se desvincula una puerta de enlace inalámbrica del certificado con el que está asociado actualmente.

```
aws iotwireless disassociate-wireless-gateway-from-certificate \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Agregar las puertas de enlace y dispositivos inalámbricos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DisassociateWirelessGatewayFromCertificate en la Referencia de comandos de la AWS CLI.

`disassociate-wireless-gateway-from-thing`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-wireless-gateway-from-thing`.

AWS CLI

Para desasociar el objeto de la puerta de enlace inalámbrica

En el siguiente ejemplo de `disassociate-wireless-gateway-from-thing`, se desvincula una puerta de enlace inalámbrica del objeto con el que está asociado actualmente.

```
aws iotwireless disassociate-wireless-gateway-from-thing \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Agregar las puertas de enlace y dispositivos inalámbricos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte DisassociateWirelessGatewayFromThing en la Referencia de comandos de la AWS CLI.

`get-destination`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-destination`.

AWS CLI

Para obtener información sobre un destino inalámbrico de IoT

En el siguiente ejemplo de `get-destination`, se obtiene información sobre el recurso de destino con el nombre `IoTWirelessDestination` que ha creado.

```
aws iotwireless get-destination \
    --name "IoTWirelessDestination"
```

Salida:

```
{
```

```
    "Arn": "arn:aws:iotwireless:us-east-1:123456789012:Destination/
IoTWirelessDestination",
    "Name": "IoTWirelessDestination",
    "Expression": "IoTWirelessRule",
    "ExpressionType": "RuleName",
    "RoleArn": "arn:aws:iam::123456789012:role/IoTWirelessDestinationRole"
}
```

Para obtener más información, consulte Agregar destinos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetDestination en la Referencia de comandos de la AWS CLI.

`get-device-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-device-profile`.

AWS CLI

Para obtener información sobre un perfil de dispositivo

En el siguiente ejemplo de `get-device-profile`, se obtiene información sobre el perfil del dispositivo con el ID especificado que ha creado.

```
aws iotwireless get-device-profile \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
```

Salida:

```
{
    "Arn": "arn:aws:iotwireless:us-east-1:123456789012:DeviceProfile/12345678-
a1b2-3c45-67d8-e90fa1b2c34d",
    "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d",
    "LoRaWAN": {
    "MacVersion": "1.0.3",
    "MaxDutyCycle": 10,
    "Supports32BitFCnt": false,
    "RegParamsRevision": "RP002-1.0.1",
    "SupportsJoin": true,
    "RfRegion": "US915",
```

```
    "MaxEirp": 13,
    "SupportsClassB": false,
    "SupportsClassC": false
    }
}
```

Para obtener más información, consulte Agregar perfiles a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetDeviceProfile en la Referencia de comandos de la AWS CLI.

`get-partner-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-partner-account`.

AWS CLI

Para obtener la información de la cuenta de socio

En el siguiente ejemplo de `get-partner-account`, se obtiene información sobre la cuenta de Sidewalk que tiene el siguiente ID.

```
aws iotwireless get-partner-account \
    --partner-account-id "12345678901234" \
    --partner-type "Sidewalk"
```

Salida:

```
{
    "Sidewalk": {
        "AmazonId": "12345678901234",
        "Fingerprint":
 "a123b45c6d78e9f012a34cd5e6a7890b12c3d45e6f78a1b234c56d7e890a1234"
    },
    "AccountLinked": false
}
```

Para obtener más información, consulte Integración de Amazon Sidewalk para AWS IoT Core en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetPartnerAccount en la Referencia de comandos de la AWS CLI.

`get-service-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-endpoint`.

AWS CLI

Para obtener el punto de conexión de servicio

En el siguiente ejemplo de `get-service-endpoint`, se obtiene el punto de conexión específico de la cuenta para el protocolo CUPS.

```
aws iotwireless get-service-endpoint
```

Salida:

```
{
    "ServiceType": "CUPS",
    "ServiceEndpoint": "https://A1RMKZ37ACAGOT.cups.lorawan.us-
east-1.amazonaws.com:443",
    "ServerTrust": "-----BEGIN CERTIFICATE-----\n
    MIIESTCCAzGgAwIBAgITBn+UV4WH6Kx33rJTMlu8mYtWDTANBgkqhkiG9w0BAQsF\n
    ADA5MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGQW1hem9uMRkwFwYDVQQDExBBbWF6\n
    b24gUm9vdCBDQSAxMB4XDTE1MTAyMjAwMDAwMFoXDTI1MTAxOTAwMDAwMFowRjEL\n
    MAkGA1UEBhMCVVMxDzANBgNVBAoTBkFtYXpvbjEVMBMGA1UECxMMU2VydmVyIENB\n
    IDFCMQ8wDQYDVQQDEwZBbWF6b24wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK\n
    AoIBAQDCThZn3c68asg3Wuw6MLAd5tES6BIoSMzoKcG5blPVo+sDORrMd4f2AbnZ\n
    cMzPa43j4wNxhplty6aUKk4T1qe9BOwKFjwK6zmxxLVYo7bHViXsPlJ6qOMpFge5\n
    blDP+18x+B26A0piiQOuPkfyDyeR4xQghfj66Yo19V+emU3nazfvpFA+ROz6WoVm\n
    B5x+F2pV8xeKNR7u6azDdU5YVX1TawprmxRC1+WsAYmz6qP+z8ArDITC2FMVy2fw\n
    0IjKOtEXc/VfmtTFch5+AfGYMGMqqvJ6LcXiAhqG5TI+Dr0RtM88k+8XUBCeQ8IG\n
    KuANaL7TiItKZYxK1MMuTJtV9IblAgMBAAGjggE7MIIBNzASBgNVHRMBAf8ECDAG\n
    AQH/AgEAMA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUWaRmBlKge5WSPKOUByeW\n
    dFv5PdAwHwYDVR0jBBgwFoAUhBjMhTTsvAyUlC4IWZzHshBOCggwewYIKwYBBQUH\n
    AQEEbzBtMC8GCCsGAQUFBzABhiNodHRwOi8vb2NzcC5yb290Y2ExLmFtYXpvbnRy\n
    dXN0LmNvbTA6BggrBgEFBQcwAoYuaHR0cDovL2NydC5yb290Y2ExLmFtYXpvbnRy\n
    dXN0LmNvbS9yb290Y2ExLmNlcjA/BgNVHR8EODA2MDSgMqAwhi5odHRwOi8vY3Js\n
    LnJvb3RjYTEuYW1hem9udHJ1c3QuY29tL3Jvb3RjYTEuY3JsMBMGA1UdIAQMMAow\n
    CAYGZ4EMAQIBMA0GCSqGSIb3DQEBCwUAA4IBAQCFkr41u3nPo4FCHOTjY3NTOVI1\n
    59Gt/a6ZiqyJEi+752+a1U5y6iAwYfmXss2lJwJFqMp2PphKg5625kXg8kP2CN5t\n
```

```
    6G7bMQcT8C8xDZNtYTd7WPD8UZiRKAJPBXa30/AbwuZe0GaFEQ8ugcYQgSn+IGBI\n
    8/LwhBNTZTUVEWuCUUBVV18YtbAiPq3yXqMB48Oz+ctBWuZSkbvkNodPLamkB2g1\n
    upRyzQ7qDn1X8nn8N8V7YJ6y68AtkHcNSRAnpTitxBKjtKPISLMVCx7i4hncxHZS\n
    yLyKQXhw2W2Xs0qLeC1etA+jTGDK4UfLeC0SF7FSi8o5LL21L8IzApar2pR/\n
    -----END CERTIFICATE-----\n"
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetServiceEndpoint en la Referencia de comandos de la AWS CLI.

`get-service-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-profile`.

AWS CLI

Para obtener información sobre un perfil de servicio

En el siguiente ejemplo de `get-service-profile`, se obtiene información sobre el perfil de servicio con el ID especificado que ha creado.

```
aws iotwireless get-service-profile \
    --id "12345678-a1b2-3c45-67d8-e90fa1b2c34d"
```

Salida:

```
{
    "Arn": "arn:aws:iotwireless:us-east-1:651419225604:ServiceProfile/538185bb-
d7e7-4b95-96a0-c51aa4a5b9a0",
    "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d",
    "LoRaWAN": {
        "HrAllowed": false,
        "NwkGeoLoc": false,
        "DrMax": 15,
        "UlBucketSize": 4096,
        "PrAllowed": false,
        "ReportDevStatusBattery": false,
        "DrMin": 0,
        "DlRate": 60,
```

```
        "AddGwMetadata": false,
        "ReportDevStatusMargin": false,
        "MinGwDiversity": 1,
        "RaAllowed": false,
        "DlBucketSize": 4096,
        "DevStatusReqFreq": 24,
        "TargetPer": 5,
        "UlRate": 60
    }
}
```

Para obtener más información, consulte Agregar perfiles a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetServiceProfile en la Referencia de comandos de la AWS CLI.

`get-wireless-device-statistics`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-wireless-device-statistics`.

AWS CLI

Para obtener información sobre el funcionamiento de un dispositivo inalámbrico

En el siguiente ejemplo de `get-wireless-device-statistics`, se obtiene información sobre el funcionamiento de un dispositivo inalámbrico.

```
aws iotwireless get-wireless-device-statistics \
    --wireless-device-id "1ffd32c8-8130-4194-96df-622f072a315f"
```

Salida:

```
{
    "WirelessDeviceId": "1ffd32c8-8130-4194-96df-622f072a315f"
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetWirelessDeviceStatistics en la Referencia de comandos de la AWS CLI.

`get-wireless-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-wireless-device`.

AWS CLI

Para obtener información sobre el dispositivo inalámbrico

En el siguiente ejemplo de `get-wireless-device`, se genera una lista de los widgets disponibles en la cuenta de AWS.

```
aws iotwireless get-wireless-device \
    --identifier "1ffd32c8-8130-4194-96df-622f072a315f" \
    --identifier-type WirelessDeviceID
```

Salida:

```
{
    "Name": "myLoRaWANDevice",
    "ThingArn": "arn:aws:iot:us-east-1:123456789012:thing/44b87eb4-9bce-423d-
b5fc-973f5ecc358b",
    "DestinationName": "IoTWirelessDestination",
    "Id": "1ffd32c8-8130-4194-96df-622f072a315f",
    "ThingName": "44b87eb4-9bce-423d-b5fc-973f5ecc358b",
    "Type": "LoRaWAN",
    "LoRaWAN": {
        "DeviceProfileId": "ab0c23d3-b001-45ef-6a01-2bc3de4f5333",
        "ServiceProfileId": "fe98dc76-cd12-001e-2d34-5550432da100",
        "OtaaV1_1": {
            "AppKey": "3f4ca100e2fc675ea123f4eb12c4a012",
            "JoinEui": "b4c231a359bc2e3d",
            "NwkKey": "01c3f004a2d6efffe32c4eda14bcd2b4"
        },
        "DevEui": "ac12efc654d23fc2"
    },
    "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:WirelessDevice/1ffd32c8-8130-4194-96df-622f072a315f",
    "Description": "My LoRaWAN wireless device"
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetWirelessDevice en la Referencia de comandos de la AWS CLI.

`get-wireless-gateway-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-wireless-gateway-certificate`.

AWS CLI

Para obtener el ID de un certificado asociado a una puerta de enlace inalámbrica

En el siguiente ejemplo de `get-wireless-gateway-certificate`, se obtiene el ID del certificado asociado a una puerta de enlace inalámbrica que tiene el ID especificado.

```
aws iotwireless get-wireless-gateway-certificate \
    --id "6c44ab31-8b4d-407a-bed3-19b6c7cda551"
```

Salida:

```
{
    "IotCertificateId":
 "8ea4aeae3db34c78cce75d9abd830356869ead6972997e0603e5fd032c804b6f"
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetWirelessGatewayCertificate en la Referencia de comandos de la AWS CLI.

`get-wireless-gateway-firmware-information`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-wireless-gateway-firmware-information`.

AWS CLI

Para obtener información sobre el firmware de una puerta de enlace inalámbrica

En el siguiente ejemplo de `get-wireless-gateway-firmware-information`, se obtiene la versión del firmware y otra información sobre una puerta de enlace inalámbrica.

```
aws iotwireless get-wireless-gateway-firmware-information \
    --id "3039b406-5cc9-4307-925b-9948c63da25b"
```

Salida:

```
{
    "LoRaWAN" :{
        "CurrentVersion" :{
            "PackageVersion" : "1.0.0",
            "Station" : "2.0.5",
            "Model" : "linux"
        }
    }
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetWirelessGatewayFirmwareInformation en la Referencia de comandos de la AWS CLI.

`get-wireless-gateway-statistics`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-wireless-gateway-statistics`.

AWS CLI

Para obtener información sobre la puerta de enlace inalámbrica

En el siguiente ejemplo `get-wireless-gateway-statistics`, se obtiene información operativa sobre una puerta de enlace inalámbrica.

```
aws iotwireless get-wireless-gateway-statistics \
    --wireless-gateway-id "3039b406-5cc9-4307-925b-9948c63da25b"
```

Salida:

```
{
    "WirelessGatewayId": "3039b406-5cc9-4307-925b-9948c63da25b"
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetWirelessGatewayStatistics en la Referencia de comandos de la AWS CLI.

`get-wireless-gateway-task-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-wireless-gateway-task-definition`.

AWS CLI

Para obtener información sobre la definición de tareas de puerta de enlace inalámbricas

En el siguiente ejemplo de `get-wireless-gateway-task-definition`, se obtiene información sobre la definición de tareas inalámbricas con el ID especificado.

```
aws iotwireless get-wireless-gateway-task-definition \
    --id "b7d3baad-25c7-35e7-a4e1-1683a0d61da9"
```

Salida:

```
{
    "AutoCreateTasks": true,
    "Name": "TestAutoUpdate",
    "Update":{
        "UpdateDataSource" : "s3://cupsalphagafirmwarebin/station",
        "UpdateDataRole" : "arn:aws:iam::001234567890:role/SDK_Test_Role",
        "LoRaWAN" :{
            "CurrentVersion" :{
                "PackageVersion" : "1.0.0",
                "Station" : "2.0.5",
                "Model" : "linux"
            },
            "UpdateVersion" :{
```

```
                "PackageVersion" : "1.0.1",
                "Station" : "2.0.5",
                "Model" : "minihub"
            }
        }
    }
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetWirelessGatewayTaskDefinition en la Referencia de comandos de la AWS CLI.

`get-wireless-gateway-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-wireless-gateway-task`.

AWS CLI

Para obtener información sobre la tarea de puerta de enlace inalámbrica

En el siguiente ejemplo de `get-wireless-gateway-task`, se obtiene información sobre la tarea de puerta de enlace inalámbrica con el ID especificado.

```
aws iotwireless get-wireless-gateway-task \
    --id "11693a46-6866-47c3-a031-c9a616e7644b"
```

Salida:

```
{
    "WirelessGatewayId": "6c44ab31-8b4d-407a-bed3-19b6c7cda551",
    "WirelessGatewayTaskDefinitionId": "b7d3baad-25c7-35e7-a4e1-1683a0d61da9",
    "Status": "Success"
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetWirelessGatewayTask en la Referencia de comandos de la AWS CLI.

`get-wireless-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-wireless-gateway`.

AWS CLI

Para obtener información sobre la puerta de enlace inalámbrica

En el siguiente ejemplo de `get-wireless-gateway`, se obtiene información sobre la puerta de enlace inalámbrica `myFirstLoRaWANGateway`.

```
aws iotwireless get-wireless-gateway \
    --identifier "12345678-a1b2-3c45-67d8-e90fa1b2c34d" \
    --identifier-type WirelessGatewayId
```

Salida:

```
{
    "Description": "My first LoRaWAN gateway",
    "ThingArn": "arn:aws:iot:us-east-1:123456789012:thing/a1b2c3d4-5678-90ab-
cdef-12ab345c67de",
    "LoRaWAN": {
        "RfRegion": "US915",
        "GatewayEui": "a1b2c3d4567890ab"
    },
    "ThingName": "a1b2c3d4-5678-90ab-cdef-12ab345c67de",
    "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d",
    "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:WirelessGateway/6c44ab31-8b4d-407a-bed3-19b6c7cda551",
    "Name": "myFirstLoRaWANGateway"
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte GetWirelessGateway en la Referencia de comandos de la AWS CLI.

`list-destinations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-destinations`.

AWS CLI

Para enumerar los destinos inalámbricos

En el siguiente ejemplo de `list-destinations`, se enumeran los destinos disponibles registrados en su cuenta de AWS.

```
aws iotwireless list-destinations
```

Salida:

```
{
    "DestinationList": [
        {
            "Arn": "arn:aws:iotwireless:us-east-1:123456789012:Destination/
IoTWirelessDestination",
            "Name": "IoTWirelessDestination",
            "Expression": "IoTWirelessRule",
            "Description": "Destination for messages processed using
 IoTWirelessRule",
            "RoleArn": "arn:aws:iam::123456789012:role/IoTWirelessDestinationRole"
        },
        {
            "Arn": "arn:aws:iotwireless:us-east-1:123456789012:Destination/
IoTWirelessDestination2",
            "Name": "IoTWirelessDestination2",
            "Expression": "IoTWirelessRule2",
            "RoleArn": "arn:aws:iam::123456789012:role/IoTWirelessDestinationRole"
        }
    ]
}
```

Para obtener más información, consulte Agregar destinos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListDestinations en la Referencia de comandos de la AWS CLI.

`list-device-profiles`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-device-profiles`.

AWS CLI

Para enumerar los perfiles de los dispositivos

En el siguiente ejemplo de `list-device-profiles`, se enumeran los perfiles de dispositivo disponibles registrados en su cuenta de AWS.

```
aws iotwireless list-device-profiles
```

Salida:

```
{
    "DeviceProfileList": [
        {
            "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d",
            "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:DeviceProfile/12345678-a1b2-3c45-67d8-e90fa1b2c34d"
        },
        {
            "Id": "a1b2c3d4-5678-90ab-cdef-12ab345c67de",
            "Arn": "arn:aws:iotwireless:us-east-1:123456789012:DeviceProfile/
a1b2c3d4-5678-90ab-cdef-12ab345c67de"
        }
    ]
}
```

Para obtener más información, consulte Agregar perfiles a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListDeviceProfiles en la Referencia de comandos de la AWS CLI.

`list-partner-accounts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-partner-accounts`.

AWS CLI

Para enumerar las cuentas de los socios

En el siguiente ejemplo de `list-partner-accounts`, se enumeran las cuentas de socios disponibles asociadas con su cuenta de AWS.

```
aws iotwireless list-partner-accounts
```

Salida:

```
{
    "Sidewalk": [
        {
            "AmazonId": "78965678771228",
            "Fingerprint":
 "bd96d8ef66dbfd2160eb60e156849e82ad7018b8b73c1ba0b4fc65c32498ee35"
        },
        {
            "AmazonId": "89656787651228",
            "Fingerprint":
 "bc5e99e151c07be14be7e6603e4489c53f858b271213a36ebe3370777ba06e9b"
        }
    ]
}
```

Para obtener más información, consulte Integración de Amazon Sidewalk para AWS IoT Core en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListPartnerAccounts en la Referencia de comandos de la AWS CLI.

`list-service-profiles`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-service-profiles`.

AWS CLI

Para enumerar los perfiles de los servicios

En el siguiente ejemplo de `list-service-profiles`, se enumeran los perfiles de servicio disponibles registrados en su cuenta de AWS.

```
aws iotwireless list-service-profiles
```

Salida:

```
{
```

```
    "ServiceProfileList": [
        {
            "Id": "12345678-a1b2-3c45-67d8-e90fa1b2c34d",
            "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:ServiceProfile/538185bb-d7e7-4b95-96a0-c51aa4a5b9a0"
        },
        {
            "Id": "a1b2c3d4-5678-90ab-cdef-12ab345c67de",
            "Arn": "arn:aws:iotwireless:us-east-1:123456789012:ServiceProfile/
ea8bc823-5d13-472e-8d26-9550737d8100"
        }
    ]
}
```

Para obtener más información, consulte Agregar perfiles a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListServiceProfiles en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas asignadas al recurso

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran las etiquetas asignadas a un recurso de destino inalámbrico.

```
aws iotwireless list-tags-for-resource \
    --resource-arn "arn:aws:iotwireless:us-east-1:123456789012:Destination/
IoTWirelessDestination"
```

Salida:

```
{
    "Tags": [
        {
            "Value": "MyValue",
```

```
            "Key": "MyTag"
        }
    ]
}
```

Para obtener más información, consulte Describa sus recursos de AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWSIoT.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-wireless-devices`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-wireless-devices`.

AWS CLI

Para ver una lista de los dispositivos inalámbricos disponibles

En el siguiente ejemplo de `list-wireless-devices`, se enumeran los dispositivos inalámbricos disponibles registrados en su cuenta de AWS.

```
aws iotwireless list-wireless-devices
```

Salida:

```
{
    "WirelessDeviceList": [
        {
            "Name": "myLoRaWANDevice",
            "DestinationName": "IoTWirelessDestination",
            "Id": "1ffd32c8-8130-4194-96df-622f072a315f",
            "Type": "LoRaWAN",
            "LoRaWAN": {
                "DevEui": "ac12efc654d23fc2"
            },
            "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:WirelessDevice/1ffd32c8-8130-4194-96df-622f072a315f"
        }
    ]
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListWirelessDevices en la Referencia de comandos de la AWS CLI.

`list-wireless-gateway-task-definitions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-wireless-gateway-task-definitions`.

AWS CLI

Para enumerar las definiciones de tareas de puertas de enlace inalámbricas

En el siguiente ejemplo de `list-wireless-gateway-task-definitions`, se enumeran las definiciones de tareas de puerta de enlace inalámbrica disponibles registradas en su cuenta de AWS.

```
aws iotwireless list-wireless-gateway-task-definitions
```

Salida:

```
{
    "TaskDefinitions": [
        {
            "Id": "b7d3baad-25c7-35e7-a4e1-1683a0d61da9",
            "LoRaWAN" :
                {
                "CurrentVersion" :{
                    "PackageVersion" : "1.0.0",
                    "Station" : "2.0.5",
                    "Model" : "linux"
                },
                "UpdateVersion" :{
                    "PackageVersion" : "1.0.1",
                    "Station" : "2.0.5",
                    "Model" : "minihub"
                }
            }
        }
    ]
```

```
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListWirelessGatewayTaskDefinitions en la Referencia de comandos de la AWS CLI.

`list-wireless-gateways`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-wireless-gateways`.

AWS CLI

Para enumerar las puertas de enlace inalámbricas

En el siguiente ejemplo de `list-wireless-gateways`, se enumeran las puertas de enlace inalámbricas disponibles en su cuenta de AWS.

```
aws iotwireless list-wireless-gateways
```

Salida:

```
{
    "WirelessGatewayList": [
        {
            "Description": "My first LoRaWAN gateway",
            "LoRaWAN": {
                "RfRegion": "US915",
                "GatewayEui": "dac632ebc01d23e4"
            },
            "Id": "3039b406-5cc9-4307-925b-9948c63da25b",
            "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:WirelessGateway/3039b406-5cc9-4307-925b-9948c63da25b",
            "Name": "myFirstLoRaWANGateway"
        },
        {
            "Description": "My second LoRaWAN gateway",
            "LoRaWAN": {
                "RfRegion": "US915",
                "GatewayEui": "cda123fffe92ecd2"
            },
```

```
            "Id": "3285bdc7-5a12-4991-84ed-dadca65e342e",
            "Arn": "arn:aws:iotwireless:us-
east-1:123456789012:WirelessGateway/3285bdc7-5a12-4991-84ed-dadca65e342e",
            "Name": "mySecondLoRaWANGateway"
        }
    ]
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte ListWirelessGateways en la Referencia de comandos de la AWS CLI.

`send-data-to-wireless-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `send-data-to-wireless-device`.

AWS CLI

Para enviar datos al dispositivo inalámbrico

En el siguiente ejemplo de `send-data-to-wireless-device`, se envía una trama de datos de la aplicación descifrada al dispositivo inalámbrico.

```
aws iotwireless send-data-to-wireless-device \
    --id "11aa5eae-2f56-4b8e-a023-b28d98494e49" \
    --transmit-mode "1" \
    --payload-data "SGVsbG8gVG8gRGV2c2lt" \
    --wireless-metadata LoRaWAN={FPort=1}
```

Salida:

```
{
    MessageId: "6011dd36-0043d6eb-0072-0008"
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener más información sobre la API, consulte SendDataToWirelessDevice en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para especificar una clave y valor de etiqueta para un recurso

En el siguiente ejemplo de `tag-resource`, se etiqueta el destino inalámbrico `IoTWirelessDestination` con la clave `MyTag` y el valor `MyValue`.

```
aws iotwireless tag-resource \
    --resource-arn "arn:aws:iotwireless:us-east-1:651419225604:Destination/
IoTWirelessDestination" \
    --tags Key="MyTag",Value="MyValue"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Describa sus recursos de AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWSIoT.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`test-wireless-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `test-wireless-device`.

AWS CLI

Para probar el dispositivo inalámbrico

En el siguiente ejemplo de `test-wireless-device`, se envían los datos de enlace ascendente `Hello` a un dispositivo con un ID especificado.

```
aws iotwireless test-wireless-device \
    --id "11aa5eae-2f56-4b8e-a023-b28d98494e49"
```

Salida:

```
{
    Result: "Test succeeded. one message is sent with payload: hello"
```

```
}
```

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información acerca de la API, consulte TestWirelessDevice en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para quitar una o varias etiquetas de un recurso

En el siguiente ejemplo de `untag-resource`, se elimina la etiqueta `MyTag` y su valor del destino inalámbrico `IoTWirelessDestination`.

```
aws iotwireless untag-resource \
    --resource-arn "arn:aws:iotwireless:us-east-1:123456789012:Destination/
IoTWirelessDestination" \
    --tag-keys "MyTag"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Describa sus recursos de AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWSIoT.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-destination`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-destination`.

AWS CLI

Para actualizar las propiedades de un destino

En el siguiente ejemplo de `update-destination`, se actualiza la propiedad de descripción de un destino inalámbrico.

```
aws iotwireless update-destination \
    --name "IoTWirelessDestination" \
    --description "Destination for messages processed using IoTWirelessRule"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Agregar destinos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte UpdateDestination en la Referencia de comandos de la AWS CLI.

`update-partner-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-partner-account`.

AWS CLI

Para actualizar las propiedades de una cuenta de socio

`update-partner-account` actualiza la `AppServerPrivateKey` de la cuenta que tiene el ID especificado.

```
aws iotwireless update-partner-account \
    --partner-account-id "78965678771228" \
    --partner-type "Sidewalk" \
    --sidewalk
 AppServerPrivateKey="f798ab4899346a88599180fee9e14fa1ada7b6df989425b7c6d2146dd6c815bb"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Integración de Amazon Sidewalk para AWS IoT Core en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte UpdatePartnerAccount en la Referencia de comandos de la AWS CLI.

`update-wireless-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-wireless-device`.

AWS CLI

Para actualizar las propiedades de un dispositivo inalámbrico

En el siguiente ejemplo de `update-wireless-device`, se actualizan las propiedades de un dispositivo inalámbrico registrado en su cuenta de AWS.

```
aws iotwireless update-wireless-device \
    --id "1ffd32c8-8130-4194-96df-622f072a315f" \
    --destination-name IoTWirelessDestination2 \
    --description "Using my first LoRaWAN device"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte UpdateWirelessDevice en la Referencia de comandos de la AWS CLI.

`update-wireless-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-wireless-gateway`.

AWS CLI

Para actualizar la puerta de enlace inalámbrica

En el siguiente ejemplo de `update-wireless-gateway`, se actualiza la descripción de una puerta de enlace inalámbrica.

```
aws iotwireless update-wireless-gateway \
    --id "3285bdc7-5a12-4991-84ed-dadca65e342e" \
    --description "Using my LoRaWAN gateway"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Conexión de puertas de enlace y dispositivos a AWS IoT Core para LoRaWAN en la Guía para desarrolladores de AWS IoT.

- Para obtener información sobre la API, consulte UpdateWirelessGateway en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon IVS que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon IVS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`batch-get-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-channel`.

AWS CLI

Para obtener información de configuración de canal sobre varios canales

En el siguiente ejemplo de `batch-get-channel`, se enumera información sobre los canales especificados.

```
aws ivs batch-get-channel \
    --arns arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh \
        arn:aws:ivs:us-west-2:123456789012:channel/efghEFGHijkl
```

Salida:

```
{
    "channels": [
        {
            "arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
            "authorized": false,
            "containerFormat": "TS",
            "ingestEndpoint": "a1b2c3d4e5f6.global-contribute.live-video.net",
```

```
            "insecureIngest": false,
            "latencyMode": "LOW",
            "multitrackInputConfiguration": {
                "enabled": false,
                "maximumResolution": "FULL_HD",
                "policy": "ALLOW"
            },
            "name": "channel-1",
            "playbackUrl": "https://a1b2c3d4e5f6.us-west-2.playback.live-video.net/
api/video/v1/us-west-2.123456789012.channel-1.abcdEFGH.m3u8",
            "preset": "",
            "playbackRestrictionPolicyArn": "",
            "recordingConfigurationArn": "arn:aws:ivs:us-
west-2:123456789012:recording-configuration/ABCD12cdEFgh",
            "srt": {
                "endpoint": "a1b2c3d4e5f6.srt.live-video.net",
                "passphrase":
 "AB1C2defGHijkLMNo3PqQRstUvwxyzaBCDEfghh4ijklMN5opqrStuVWxyzAbCDEfghIJ"
            },
            "tags": {},
            "type": "STANDARD"
        },
        {
            "arn": "arn:aws:ivs:us-west-2:123456789012:channel/efghEFGHijkl",
            "authorized": false,
            "containerFormat": "FRAGMENTED_MP4",
            "ingestEndpoint": "a1b2c3d4e5f6.global-contribute.live-video.net",
            "insecureIngest": false,
            "latencyMode": "LOW",
            "multitrackInputConfiguration": {
                "enabled": true,
                "maximumResolution": "FULL_HD",
                "policy": "ALLOW"
            },
            "name": "channel-2",
            "playbackUrl": "https://a1b2c3d4e5f6.us-west-2.playback.live-video.net/
api/video/v1/us-west-2.123456789012.channel-2.abcdEFGH.m3u8",
            "preset": "",
            "playbackRestrictionPolicyArn": "arn:aws:ivs:us-
west-2:123456789012:playback-restriction-policy/ABcdef34ghIJ"",
            "recordingConfigurationArn": "",
            "srt": {
                "endpoint": "a1b2c3d4e5f6.srt.live-video.net",
```

```
                "passphrase":
 "BA1C2defGHijkLMNo3PqQRstUvwxyzaBCDEfghh4ijklMN5opqrStuVWxyzAbCDEfghIJ"
            },
            "tags": {},
            "type": "STANDARD"
        }
    ]
}
```

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener detalles sobre la API, consulte BatchGetChannel en la Referencia de comandos de la AWS CLI.

`batch-get-stream-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-stream-key`.

AWS CLI

Para obtener información sobre varias claves de transmisión

En el siguiente ejemplo de `batch-get-stream-key`, se obtiene información de las claves de transmisión especificadas.

```
aws ivs batch-get-stream-key \
    --arns arn:aws:ivs:us-west-2:123456789012:stream-key/skSKABCDefgh \
       arn:aws:ivs:us-west-2:123456789012:stream-key/skSKIJKLmnop
```

Salida:

```
{
    "streamKeys": [
        {
            "arn": "arn:aws:ivs:us-west-2:123456789012:stream-key/skSKABCDefgh",
            "value": "sk_us-west-2_abcdABCDefgh_567890abcdef",
            "channelArn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
            "tags": {}
        },
        {
```

```
            "arn": "arn:aws:ivs:us-west-2:123456789012:stream-key/skSKIJKLmnop",
            "value": "sk_us-west-2_abcdABCDefgh_567890ghijkl",
            "channelArn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
            "tags": {}
        }
    ]
}
```

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener detalles sobre la API, consulte BatchGetStreamKey en la Referencia de comandos de la AWS CLI.

`batch-start-viewer-session-revocation`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-start-viewer-session-revocation`.

AWS CLI

Para revocar las sesiones de los espectadores para varios pares de canal-ARN e ID de espectador

En el siguiente ejemplo de `batch-start-viewer-session-revocation`, se realiza la revocación de la sesión en varios pares de canal-ARN e ID-observador simultáneamente. La solicitud puede completarse con normalidad, pero devuelve valores en el campo de errores si quien llama no tiene permiso para revocar una sesión específica.

```
aws ivs batch-start-viewer-session-revocation \
    --viewer-sessions '[{"channelArn":"arn:aws:ivs:us-west-2:123456789012:channel/
abcdABCDefgh1","viewerId":"abcdefg1","viewerSessionVersionsLessThanOrEqualTo":1234567890},
 \
     {"channelArn":"arn:aws:ivs:us-west-2:123456789012:channel/
abcdABCDefgh2","viewerId":"abcdefg2","viewerSessionVersionsLessThanOrEqualTo":1234567890}]'
```

Salida:

```
{
    "errors": [
        {
```

```
            "channelArn": "arn:aws:ivs:us-west-2:123456789012:channel/
abcdABCDefgh1",
            "viewerId": "abcdefg1",
            "code": "403",
            "message": "not authorized",
        },
        {
            "channelArn": "arn:aws:ivs:us-west-2:123456789012:channel/
abcdABCDefgh2",
            "viewerId": "abcdefg2",
            "code": "403",
            "message": "not authorized",
        }
    ]
}
```

Para obtener más información, consulte Configuración de canales privados en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener detalles sobre la API, consulte BatchStartViewerSessionRevocation en la Referencia de comandos de la AWS CLI.

`create-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-channel`.

AWS CLI

Ejemplo 1: crear un canal sin grabación

En el siguiente ejemplo de `create-channel`, se crea un nuevo canal y una clave de transmisión asociada para iniciar la transmisión.

```
aws ivs create-channel \
    --name 'test-channel' \
    --no-insecure-ingest
```

Salida:

```
{
    "channel": {
```

```
        "arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "authorized": false,
        "containerFormat": "TS",
        "name": "test-channel",
        "latencyMode": "LOW",
        "multitrackInputConfiguration": {
            "enabled": false,
            "maximumResolution": "FULL_HD",
            "policy": "ALLOW"
        },
        "playbackRestrictionPolicyArn": "",
        "recordingConfigurationArn": "",
        "srt": {
            "endpoint": "a1b2c3d4e5f6.srt.live-video.net",
            "passphrase":
 "AB1C2defGHijkLMNo3PqQRstUvwxyzaBCDEfghh4ijklMN5opqrStuVWxyzAbCDEfghIJ"
        },
        "ingestEndpoint": "a1b2c3d4e5f6.global-contribute.live-video.net",
        "insecureIngest": false,
        "playbackUrl": "https://a1b2c3d4e5f6.us-west-2.playback.live-video.net/api/
video/v1/us-west-2.123456789012.channel.abcdEFGH.m3u8",
        "preset": "",
        "tags": {},
        "type": "STANDARD"
    },
    "streamKey": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:stream-key/g1H2I3j4k5L6",
        "value": "sk_us-west-2_abcdABCDefgh_567890abcdef",
        "channelArn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "tags": {}
    }
}
```

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

Ejemplo 2: crear un canal con la grabación habilitada, mediante el recurso RecordingConfiguration especificado por su ARN

En el siguiente ejemplo de `create-channel`, se crea un nuevo canal y una clave de transmisión asociada para iniciar la transmisión y se configura la grabación para el canal:

```
aws ivs create-channel \
```

```
    --name test-channel-with-recording \
    --insecure-ingest \
    --recording-configuration-arn 'arn:aws:ivs:us-west-2:123456789012:recording-
configuration/ABCD12cdEFgh'
```

Salida:

```
{
    "channel": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "containerFormat": "TS",
        "name": "test-channel-with-recording",
        "latencyMode": "LOW",
        "multitrackInputConfiguration": {
            "enabled": false,
            "maximumResolution": "FULL_HD",
            "policy": "ALLOW"
        },
        "type": "STANDARD",
        "playbackRestrictionPolicyArn": "",
        "recordingConfigurationArn": "arn:aws:ivs:us-west-2:123456789012:recording-
configuration/ABCD12cdEFgh",
        "srt": {
            "endpoint": "a1b2c3d4e5f6.srt.live-video.net",
            "passphrase":
 "BA1C2defGHijkLMNo3PqQRstUvwxyzaBCDEfghh4ijklMN5opqrStuVWxyzAbCDEfghIJ"
        },
        "ingestEndpoint": "a1b2c3d4e5f6.global-contribute.live-video.net",
        "insecureIngest": true,
        "playbackUrl": "https://a1b2c3d4e5f6.us-west-2.playback.live-video.net/api/
video/v1/us-west-2.123456789012.channel.abcdEFGH.m3u8",
        "preset": "",
        "authorized": false,
        "tags": {},
        "type": "STANDARD"
    },
    "streamKey": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:stream-key/abcdABCDefgh",
        "value": "sk_us-west-2_abcdABCDefgh_567890abcdef",
        "channelArn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "tags": {}
    }
}
```

Para obtener más información, consulte Record to Amazon S3 en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

Ejemplo 3: crear un canal con una política de restricción de reproducción especificada por su ARN

En el siguiente ejemplo de `create-channel`, se crea un nuevo canal y una clave de transmisión asociada para iniciar la transmisión y se configura la política de restricción de reproducción para el canal:

```
aws ivs create-channel \
    --name test-channel-with-playback-restriction-policy\
    --insecure-ingest \
    --playback-restriction-policy-arn 'arn:aws:ivs:us-west-2:123456789012:playback-restriction-policy/ABcdef34ghIJ'
```

Salida:

```
{
    "channel": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "containerFormat": "TS",
        "name": "test-channel-with-playback-restriction-policy",
        "latencyMode": "LOW",
        "multitrackInputConfiguration": {
            "enabled": false,
            "maximumResolution": "FULL_HD",
            "policy": "ALLOW"
        },
        "type": "STANDARD",
        "playbackRestrictionPolicyArn": "arn:aws:ivs:us-
west-2:123456789012:playback-restriction-policy/ABcdef34ghIJ",
        "recordingConfigurationArn": "",
        "srt": {
            "endpoint": "a1b2c3d4e5f6.srt.live-video.net",
            "passphrase":
 "AB1C2edfGHijkLMNo3PqQRstUvwxyzaBCDEfghh4ijklMN5opqrStuVWxyzAbCDEfghIJ"
        },
        "ingestEndpoint": "a1b2c3d4e5f6.global-contribute.live-video.net",
        "insecureIngest": true,
        "playbackUrl": "https://a1b2c3d4e5f6.us-west-2.playback.live-video.net/api/
video/v1/us-west-2.123456789012.channel.abcdEFGH.m3u8",
```

```
        "preset": "",
        "authorized": false,
        "tags": {},
        "type": "STANDARD"
    },
    "streamKey": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:stream-key/abcdABCDefgh",
        "value": "sk_us-west-2_abcdABCDefgh_567890abcdef",
        "channelArn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "tags": {}
    }
}
```

Para obtener más información, consulte Contenido y espectadores no deseados en IVS en la Guía del usuario de Guía de Transmisión de baja latencia de Amazon IVS.

Ejemplo 4: creación de un canal con la función multipista habilitada

En el siguiente ejemplo de `create-channel`, se crea un nuevo canal y una clave de transmisión asociada para iniciar la transmisión, y se habilita la multipista.

```
aws ivs create-channel \
    --name 'test-channel' \
    --no-insecure-ingest \
    --container-format 'FRAGMENTED_MP4' \
    --multitrack-input-configuration '{"enabled": true,"maximumResolution":
 "FULL_HD","policy": "ALLOW"}'
```

Salida:

```
{
    "channel": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "authorized": false,
        "containerFormat": "FRAGMENTED_MP4",
        "name": "test-channel",
        "latencyMode": "LOW",
        "multitrackInputConfiguration": {
            "enabled": true,
            "maximumResolution": "FULL_HD",
            "policy": "ALLOW"
        },
```

```
        "playbackRestrictionPolicyArn": "",
        "recordingConfigurationArn": "",
        "srt": {
            "endpoint": "a1b2c3d4e5f6.srt.live-video.net",
            "passphrase":
 "AB1C2defGHijkLMNo3PqQRstUvwxyzaBCDEfghh4ijklMN5opqrStuVWxyzAbCDEfghIJ"
        },
        "ingestEndpoint": "a1b2c3d4e5f6.global-contribute.live-video.net",
        "insecureIngest": false,
        "playbackUrl": "https://a1b2c3d4e5f6.us-west-2.playback.live-video.net/api/
video/v1/us-west-2.123456789012.channel.abcdEFGH.m3u8",
        "preset": "",
        "tags": {},
        "type": "STANDARD"
    },
    "streamKey": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:stream-key/g1H2I3j4k5L6",
        "value": "sk_us-west-2_abcdABCDefgh_567890abcdef",
        "channelArn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "tags": {}
    }
}
```

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte CreateChannel en la Referencia de comandos de la AWS CLI.

`create-playback-restriction-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-playback-restriction-policy`.

AWS CLI

Para crear una política de restricción de la reproducción

En el siguiente ejemplo de `create-playback-restriction-policy`, se crea una nueva política de restricción de reproducción.

```
aws ivs create-playback-restriction-policy \
```

```
    --name "test-playback-restriction-policy" \
    --enable-strict-origin-enforcement \
    --tags "key1=value1, key2=value2" \
    --allowed-countries US MX \
    --allowed-origins https://www.website1.com https://www.website2.com
```

Salida:

```
{
    "playbackRestrictionPolicy": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:playback-restriction-policy/
ABcdef34ghIJ",
        "allowedCountries": [
            "US",
            "MX"
        ],
        "allowedOrigins": [
            "https://www.website1.com",
            "https://www.website2.com"
        ],
        "enableStrictOriginEnforcement": true,
        "name": "test-playback-restriction-policy",
        "tags": {
            "key1": "value1",
            "key2": "value2"
        }
    }
}
```

Para obtener más información, consulte Contenido y espectadores no deseados en IVS en la Guía del usuario de Guía de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte CreatePlaybackRestrictionPolicy en la Referencia de comandos de la AWS CLI.

`create-recording-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-recording-configuration`.

AWS CLI

Para crear un recurso RecordingConfiguration

En el siguiente ejemplo de `create-recording-configuration`, se crea un recurso RecordingConfiguration para activar grabación en Amazon S3.

```
aws ivs create-recording-configuration \
    --name "test-recording-config" \
    --recording-reconnect-window-seconds 60 \
    --tags "key1=value1, key2=value2" \
    --rendition-configuration renditionSelection="CUSTOM",renditions="HD" \
    --thumbnail-configuration
 recordingMode="INTERVAL",targetIntervalSeconds=1,storage="LATEST",resolution="LOWEST_RESOLU
 \
    --destination-configuration s3={bucketName=demo-recording-bucket}
```

Salida:

```
{
    "recordingConfiguration": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:recording-configuration/
ABcdef34ghIJ",
        "name": "test-recording-config",
        "destinationConfiguration": {
            "s3": {
                "bucketName": "demo-recording-bucket"
            }
        },
        "state": "CREATING",
        "tags": {
            "key1": "value1",
            "key2": "value2"
        },
        "thumbnailConfiguration": {
            "recordingMode": "INTERVAL",
            "targetIntervalSeconds": 1,
            "resolution": "LOWEST_RESOLUTION",
            "storage": [
                "LATEST"
            ]
        },
        "recordingReconnectWindowSeconds": 60,
        "renditionConfiguration": {
            "renditionSelection": "CUSTOM",
            "renditions": [
                "HD"
```

```
            ]
        }
    }
}
```

Para obtener más información, consulte Record to Amazon S3 en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte CreateRecordingConfiguration en la Referencia de comandos de la AWS CLI.

`create-stream-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-stream-key`.

AWS CLI

Para crear una clave de transmisión

En el siguiente ejemplo de `create-stream-key`, se crea una clave de transmisión para un ARN (Nombre de recurso de Amazon) específico.

```
aws ivs create-stream-key \
    --channel-arn arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh
```

Salida:

```
{
    "streamKey": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:stream-key/abcdABCDefgh",
        "value": "sk_us-west-2_abcdABCDefgh_567890abcdef",
        "channelArn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "tags": {}
    }
}
```

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte CreateStreamKey en la Referencia de comandos de la AWS CLI.

`delete-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-channel`.

AWS CLI

Para eliminar un canal y las claves de transmisión asociadas

En el siguiente ejemplo de `delete-channel`, se elimina el canal con el ARN (Amazon Resource Name) especificado.

```
aws ivs delete-channel \
    --arn arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte DeleteChannel en la Referencia de comandos de la AWS CLI.

`delete-playback-key-pair`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-playback-key-pair`.

AWS CLI

Para eliminar un par de claves de reproducción especificado

En el siguiente ejemplo de `delete-playback-key-pair`, se devuelve la huella digital del par de claves especificado.

```
aws ivs delete-playback-key-pair \
    --arn arn:aws:ivs:us-west-2:123456789012:playback-key/abcd1234efgh
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de canales privados en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte DeletePlaybackKeyPair en la Referencia de comandos de la AWS CLI.

`delete-playback-restriction-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-playback-restriction-policy`.

AWS CLI

Para eliminar una política de restricción de la reproducción

En el siguiente ejemplo de `delete-playback-restriction-policy`, se elimina la política de restricción de reproducción con el ARN (Amazon Resource Name) de política especificado.

```
aws ivs delete-playback-restriction-policy \
    --arn "arn:aws:ivs:us-west-2:123456789012:playback-restriction-policy/
ABcdef34ghIJ"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Contenido y espectadores no deseados en IVS en la Guía del usuario de Guía de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte DeletePlaybackRestrictionPolicy en la Referencia de comandos de la AWS CLI.

`delete-recording-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-recording-configuration`.

AWS CLI

Para eliminar el recurso RecordingConfiguration especificado por su ARN

En el siguiente ejemplo de `delete-recording-configuration`, se elimina el recurso RecordingConfiguration con el ARN especificado.

```
aws ivs delete-recording-configuration \
    --arn "arn:aws:ivs:us-west-2:123456789012:recording-configuration/ABcdef34ghIJ"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Record to Amazon S3 en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte DeleteRecordingConfiguration en la Referencia de comandos de la AWS CLI.

`delete-stream-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-stream-key`.

AWS CLI

Para eliminar una clave de transmisión

En el siguiente ejemplo de `delete-stream-key`, se elimina la clave de transmisión de un ARN (Amazon Resource Name) específico, por lo que ya no se puede utilizar para la transmisión.

```
aws ivs delete-stream-key \
    --arn arn:aws:ivs:us-west-2:123456789012:stream-key/g1H2I3j4k5L6
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte DeleteStreamKey en la Referencia de comandos de la AWS CLI.

`get-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-channel`.

AWS CLI

Para obtener la información de configuración de un canal

En el siguiente ejemplo de `get-channel`, se obtiene la configuración del canal para un ARN (Nombre de recurso de Amazon) de canal específico.

```
aws ivs get-channel \
    --arn 'arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh'
```

Salida:

```
{
    "channel": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "authorized": false,
        "containerFormat": "TS",
        "ingestEndpoint": "a1b2c3d4e5f6.global-contribute.live-video.net",
        "insecureIngest": false,
        "latencyMode": "LOW",
        "multitrackInputConfiguration": {
            "enabled": false,
            "maximumResolution": "FULL_HD",
            "policy": "ALLOW"
        },
        "name": "channel-1",
        "playbackRestrictionPolicyArn": "",
        "playbackUrl": "https://a1b2c3d4e5f6.us-west-2.playback.live-video.net/api/
video/v1/us-west-2.123456789012.channel.abcdEFGH.m3u8",
        "preset": "",
        "recordingConfigurationArn": "",
        "srt": {
            "endpoint": "a1b2c3d4e5f6.srt.live-video.net",
            "passphrase":
 "AB1C2defGHijkLMNo3PqQRstUvwxyzaBCDEfghh4ijklMN5opqrStuVWxyzAbCDEfghIJ"
        },
        "tags": {}
        "type": "STANDARD",
    }
}
```

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para ver los detalles de la API, consulte GetChannel en la Referencia de comandos de la AWS CLI.

`get-playback-key-pair`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-playback-key-pair`.

AWS CLI

Para obtener un par de claves de reproducción especificado

En el siguiente ejemplo de `get-playback-key-pair`, se devuelve la huella digital del par de claves especificado.

```
aws ivs get-playback-key-pair \
    --arn arn:aws:ivs:us-west-2:123456789012:playback-key/abcd1234efgh
```

Salida:

```
{
    "keyPair": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:playback-key/abcd1234efgh",
        "name": "my-playback-key",
        "fingerprint": "0a:1b:2c:ab:cd:ef:34:56:70:b1:b2:71:01:2a:a3:72",
        "tags": {}
    }
}
```

Para obtener más información, consulte Configuración de canales privados en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte GetPlaybackKeyPair en la Referencia de comandos de la AWS CLI.

`get-playback-restriction-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-playback-restriction-policy`.

AWS CLI

Para obtener la información de configuración de una política de restricción de reproducción

En el siguiente ejemplo de `get-playback-restriction-policy`, se obtiene la configuración de la política de restricción de reproducción con el ARN (Nombre de recurso de Amazon) de política especificado.

```
aws ivs get-playback-restriction-policy \
    --arn "arn:aws:ivs:us-west-2:123456789012:playback-restriction-policy/
ABcdef34ghIJ"
```

Salida:

```
{
    "playbackRestrictionPolicy": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:playback-restriction-policy/
ABcdef34ghIJ",
        "allowedCountries": [
            "US",
            "MX"
        ],
        "allowedOrigins": [
            "https://www.website1.com",
            "https://www.website2.com"
        ],
        "enableStrictOriginEnforcement": true,
        "name": "test-playback-restriction-policy",
        "tags": {
            "key1": "value1",
            "key2": "value2"
        }
    }
}
```

Para obtener más información, consulte Contenido y espectadores no deseados en IVS en la Guía del usuario de Guía de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte GetPlaybackRestrictionPolicy en la Referencia de comandos de la AWS CLI.

`get-recording-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-recording-configuration`.

AWS CLI

Para obtener información sobre un recurso RecordingConfiguration

En el siguiente ejemplo de `get-recording-configuration`, se obtiene información del recurso RecordingConfiguration con el ARN especificado.

```
aws ivs get-recording-configuration \
    --arn "arn:aws:ivs:us-west-2:123456789012:recording-configuration/ABcdef34ghIJ"
```

Salida:

```
{
    "recordingConfiguration": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:recording-configuration/
ABcdef34ghIJ",
        "destinationConfiguration": {
            "s3": {
                "bucketName": "demo-recording-bucket"
            }
        },
        "name": "test-recording-config",
        "recordingReconnectWindowSeconds": 60,
        "state": "ACTIVE",
        "tags": {
            "key1" : "value1",
            "key2" : "value2"
        },
        "thumbnailConfiguration": {
            "recordingMode": "INTERVAL",
            "targetIntervalSeconds": 1,
            "resolution": "LOWEST_RESOLUTION",
            "storage": [
                "LATEST"
            ]
        },
        "renditionConfiguration": {
            "renditionSelection": "CUSTOM",
            "renditions": [
                "HD"
            ]
        }
    }
}
```

Para obtener más información, consulte Record to Amazon S3 en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte GetRecordingConfiguration en la Referencia de comandos de la AWS CLI.

`get-stream-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-stream-key`.

AWS CLI

Para obtener información acerca de un flujo

En el siguiente ejemplo de `get-stream-key`, se obtiene información sobre la clave de transmisión especificada.

```
aws ivs get-stream-key \
    --arn arn:aws:ivs:us-west-2:123456789012:stream-key/skSKABCDefgh --region=us-
west-2
```

Salida:

```
{
    "streamKey": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:stream-key/skSKABCDefgh",
        "value": "sk_us-west-2_abcdABCDefgh_567890abcdef",
        "channelArn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "tags": {}
    }
}
```

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte GetStreamKey en la Referencia de comandos de la AWS CLI.

`get-stream-session`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-stream-session`.

AWS CLI

Para obtener los metadatos de una transmisión específica

En el siguiente ejemplo de `get-stream-session`, se obtiene la configuración de metadatos para el nombre de recurso de Amazon (ARN) de canal y de transmisión especificados; si no se proporciona `streamId`, se selecciona la transmisión más reciente del canal.

```
aws ivs get-stream-session \
```

```
    --channel-arn 'arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh' \
    --stream-id 'mystream'
```

Salida:

```
{
    "streamSession": {
        "streamId": "mystream1",
        "startTime": "2023-06-26T19:09:28+00:00",
        "channel": {
            "arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
            "name": "mychannel",
            "latencyMode": "LOW",
            "type": "STANDARD",
            "recordingConfigurationArn": "arn:aws:ivs:us-
west-2:123456789012:recording-configuration/ABcdef34ghIJ",
            "ingestEndpoint": "a1b2c3d4e5f6.global-contribute.live-video.net",
            "playbackUrl": "url-string",
            "authorized": false,
            "insecureIngest": false,
            "preset": ""
        },
        "ingestConfiguration": {
            "audio": {
                "channels": 2,
                "codec": "mp4a.40.2",
                "sampleRate": 8000,
                "targetBitrate": 46875,
                "track": "Track0"
            },
            "video": {
                "avcProfile": "Baseline",
                "avcLevel": "4.2",
                "codec": "avc1.42C02A",
                "encoder": "Lavf58.45.100",
                "level": "4.2",
                "profile": "Baseline",
                "targetBitrate": 8789062,
                "targetFramerate": 60,
                "track": "Track0",
                "videoHeight": 1080,
                "videoWidth": 1920
            }
```

```
        },
        "ingestConfigurations": {
            "audioConfigurations": [
                {
                    "channels": 2,
                    "codec": "mp4a.40.2",
                    "sampleRate": 8000,
                    "targetBitrate": 46875,
                    "track": "Track0"
                }
            ],
            "videoConfigurations": [
                {
                    "codec": "avc1.42C02A",
                    "encoder": "Lavf58.45.100",
                    "level": "4.2",
                    "profile": "Baseline",
                    "targetBitrate": 8789062,
                    "targetFramerate": 60,
                    "track": "Track0",
                    "videoHeight": 1080,
                    "videoWidth": 1920
                }
            ]
        },
        "recordingConfiguration": {
            "arn": "arn:aws:ivs:us-west-2:123456789012:recording-configuration/
ABcdef34ghIJ",
            "name": "test-recording-config",
            "destinationConfiguration": {
                "s3": {
                    "bucketName": "demo-recording-bucket"
                }
            },
            "state": "ACTIVE",
            "tags": {
                "key1": "value1",
                "key2": "value2"
            },
            "thumbnailConfiguration": {
                "recordingMode": "INTERVAL",
                "targetIntervalSeconds": 1,
                "resolution": "LOWEST_RESOLUTION",
                "storage": [
```

```
                    "LATEST"
                ]
            },
            "recordingReconnectWindowSeconds": 60,
            "renditionConfiguration": {
                "renditionSelection": "CUSTOM",
                "renditions": [
                    "HD"
                ]
            }
        },
        "truncatedEvents": [
            {
                "code": "StreamTakeoverInvalidPriority",
                "name": "Stream Takeover Failure",
                "type": "IVS Stream State Change",
                "eventTime": "2023-06-26T19:09:48+00:00"
            },
            {
                "name": "Stream Takeover",
                "type": "IVS Stream State Change",
                "eventTime": "2023-06-26T19:09:47+00:00"
            },
            {
                "name": "Recording Start",
                "type": "IVS Recording State Change",
                "eventTime": "2023-06-26T19:09:35+00:00"
            },
            {
                "name": "Stream Start",
                "type": "IVS Stream State Change",
                "eventTime": "2023-06-26T19:09:34+00:00"
            },
            {
                "name": "Session Created",
                "type": "IVS Stream State Change",
                "eventTime": "2023-06-26T19:09:28+00:00"
            }
        ]
    }
}
```

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte GetStreamSession en la Referencia de comandos de la AWS CLI.

`get-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-stream`.

AWS CLI

Para obtener información acerca de un flujo

En el siguiente ejemplo de `get-stream`, se obtiene información sobre la transmisión para el canal especificado.

```
aws ivs get-stream \
    --channel-arn arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh
```

Salida:

```
{
    "stream": {
        "channelArn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "playbackUrl": "https://a1b2c3d4e5f6.us-west-2.playback.live-video.net/api/
video/v1/us-west-2.123456789012.channel.abcdEFGH.m3u8",
        "startTime": "2020-05-05T21:55:38Z",
        "state": "LIVE",
        "health": "HEALTHY",
        "streamId": "st-ABCDEfghij01234KLMN5678",
        "viewerCount": 1
    }
}
```

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte GetStream en la Referencia de comandos de AWS CLI.

`import-playback-key-pair`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-playback-key-pair`.

AWS CLI

Para importar la parte pública de un nuevo par de claves

En el siguiente ejemplo de `import-playback-key-pair`, se importa la clave pública especificada (como una cadena en formato PEM) y se devuelve el ARN y la huella digital del nuevo par de claves.

```
aws ivs import-playback-key-pair \
    --name "my-playback-key" \
    --public-key-material "G1lbnQxOTA3BgNVBAMMMFdoeSBhcmUgeW91IGRl..."
```

Salida:

```
{
    "keyPair": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:playback-key/abcd1234efgh",
        "name": "my-playback-key",
        "fingerprint": "0a:1b:2c:ab:cd:ef:34:56:70:b1:b2:71:01:2a:a3:72",
        "tags": {}
    }
}
```

Para obtener más información, consulte Configuración de canales privados en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener detalles sobre la API, consulte ImportPlaybackKeyPair en la Referencia de comandos de la AWS CLI.

`list-channels`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-channels`.

AWS CLI

Ejemplo 1: obtener información resumida de todos los canales

En el siguiente ejemplo de `list-channels`, se enumeran todos los canales de su cuenta de AWS.

```
aws ivs list-channels
```

Salida:

```
{
    "channels": [
        {
            "arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
            "name": "channel-1",
            "latencyMode": "LOW",
            "authorized": false,
            "insecureIngest": false,
            "preset": "",
            "playbackRestrictionPolicyArn": "",
            "recordingConfigurationArn": "arn:aws:ivs:us-
west-2:123456789012:recording-configuration/ABCD12cdEFgh",
            "tags": {},
            "type": "STANDARD"
        },
        {
            "arn": "arn:aws:ivs:us-west-2:123456789012:channel/efghEFGHijkl",
            "name": "channel-2",
            "latencyMode": "LOW",
            "authorized": false,
            "preset": "",
            "playbackRestrictionPolicyArn": "arn:aws:ivs:us-
west-2:123456789012:playback-restriction-policy/ABcdef34ghIJ",
            "recordingConfigurationArn": "",
            "tags": {},
            "type": "STANDARD"
        }
    ]
}
```

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

Ejemplo 2: obtener información resumida de todos los canales, filtrada por el ARN de RecordingConfiguration especificado

En el siguiente ejemplo de `list-channels`, se enumeran todos los canales de su cuenta de AWS que están asociados al ARN de RecordingConfiguration especificado.

```
aws ivs list-channels \
    --filter-by-recording-configuration-arn "arn:aws:ivs:us-
west-2:123456789012:recording-configuration/ABCD12cdEFgh"
```

Salida:

```
{
    "channels": [
        {
            "arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
            "name": "channel-1",
            "latencyMode": "LOW",
            "authorized": false,
            "insecureIngest": false,
            "preset": "",
            "playbackRestrictionPolicyArn": "",
            "recordingConfigurationArn": "arn:aws:ivs:us-
west-2:123456789012:recording-configuration/ABCD12cdEFgh",
            "tags": {},
            "type": "STANDARD"
        }
    ]
}
```

Para obtener más información, consulte Record to Amazon S3 en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

Ejemplo 3: obtener información resumida de todos los canales, filtrada por el ARN de PlaybackRestrictionPolicy especificado

En el siguiente ejemplo de `list-channels`, se enumeran todos los canales de su cuenta de AWS que están asociados al ARN de PlaybackRestrictionPolicy especificado.

```
aws ivs list-channels \
    --filter-by-playback-restriction-policy-arn "arn:aws:ivs:us-
west-2:123456789012:playback-restriction-policy/ABcdef34ghIJ"
```

Salida:

```
{
    "channels": [
        {
            "arn": "arn:aws:ivs:us-west-2:123456789012:channel/efghEFGHijkl",
            "name": "channel-2",
            "latencyMode": "LOW",
            "authorized": false,
            "preset": "",
            "playbackRestrictionPolicyArn": "arn:aws:ivs:us-
west-2:123456789012:playback-restriction-policy/ABcdef34ghIJ",
            "recordingConfigurationArn": "",
            "tags": {},
            "type": "STANDARD"
        }
    ]
}
```

Para obtener más información, consulte Contenido y espectadores no deseados en IVS en la Guía del usuario de Guía de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte ListChannels en la Referencia de comandos de la AWS CLI.

`list-playback-key-pairs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-playback-key-pairs`.

AWS CLI

Para obtener información resumida sobre todos los pares de claves de reproducción

En el siguiente ejemplo de `list-playback-key-pairs`, se obtiene información sobre todos los pares de claves.

```
aws ivs list-playback-key-pairs
```

Salida:

```
{
    "keyPairs": [
        {
            "arn": "arn:aws:ivs:us-west-2:123456789012:playback-key/abcd1234efgh",
```

```
            "name": "test-key-0",
            "tags": {}
        },
        {
            "arn": "arn:aws:ivs:us-west-2:123456789012:playback-key/ijkl5678mnop",
            "name": "test-key-1",
            "tags": {}
        }
    ]
}
```

Para obtener más información, consulte Configuración de canales privados en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte ListPlaybackKeyPairs en la Referencia de comandos de la AWS CLI.

`list-playback-restriction-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-playback-restriction-policies`.

AWS CLI

Para obtener información resumida sobre todas las políticas de restricción de reproducción

En el siguiente ejemplo de `list-playback-restriction-policies`, se enumeran todas las políticas de restricción de reproducción de su cuenta de AWS.

```
aws ivs list-playback-restriction-policies
```

Salida:

```
{
    "playbackRestrictionPolicies": [
        {
            "arn": "arn:aws:ivs:us-west-2:123456789012:playback-restriction-policy/
ABcdef34ghIJ",
            "allowedCountries": [
                "US",
                "MX"
            ],
```

```
            "allowedOrigins": [
                "https://www.website1.com",
                "https://www.website2.com"
            ],
            "enableStrictOriginEnforcement": true,
            "name": "test-playback-restriction-policy",
            "tags": {
                "key1": "value1",
                "key2": "value2"
            }
        }
    ]
}
```

Para obtener más información, consulte Contenido y espectadores no deseados en IVS en la Guía del usuario de Guía de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte ListPlaybackRestrictionPolicies en la Referencia de comandos de la AWS CLI.

`list-recording-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-recording-configurations`.

AWS CLI

Para enumerar todos los recursos RecordingConfiguration creados en esta cuenta

En el siguiente ejemplo de `list-recording-configurations`, se obtiene información de todos los recursos RecordingConfiguration de su cuenta.

```
aws ivs list-recording-configurations
```

Salida:

```
{
    "recordingConfigurations": [
        {
            "arn": "arn:aws:ivs:us-west-2:123456789012:recording-configuration/
ABcdef34ghIJ",
            "name": "test-recording-config-1",
            "destinationConfiguration": {
```

```
                "s3": {
                    "bucketName": "demo-recording-bucket-1"
                }
            },
            "state": "ACTIVE",
            "tags": {}
        },
        {
            "arn": "arn:aws:ivs:us-west-2:123456789012:recording-configuration/
CD12abcdGHIJ",
            "name": "test-recording-config-2",
            "destinationConfiguration": {
                "s3": {
                    "bucketName": "demo-recording-bucket-2"
                }
            },
            "state": "ACTIVE",
            "tags": {}
        }
    ]
}
```

Para obtener más información, consulte Record to Amazon S3 en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener más información sobre la API, consulte ListRecordingConfigurations en Referencia de comandos de la AWS CLI.

`list-stream-keys`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-stream-keys`.

AWS CLI

Para obtener una lista de claves de transmisión

En el siguiente ejemplo de `list-stream-keys`, se enumeran todas las claves de transmisión de un ARN (Nombre de recurso de Amazon) especificado.

```
aws ivs list-stream-keys \
    --channel-arn arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh
```

Salida:

```
{
    "streamKeys": [
        {
            "arn": "arn:aws:ivs:us-west-2:123456789012:stream-key/abcdABCDefgh",
            "channelArn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
            "tags": {}
        }
    ]
}
```

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener detalles de la API, consulte ListStreamKeys en la Referencia de comandos de la AWS CLI.

`list-stream-sessions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-stream-sessions`.

AWS CLI

Para obtener un resumen de las transmisiones actuales y anteriores de un canal específico en la región de AWS actual

En el siguiente ejemplo de `list-stream-sessions`, se proporciona información resumida de las transmisiones de un ARN (Nombre de recurso de Amazon) de canal específico.

```
aws ivs list-stream-sessions \
    --channel-arn arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh \
    --max-results 25 \
    --next-token ""
```

Salida:

```
{
    "nextToken": "set-2",
    "streamSessions": [
        {
            "startTime": 1641578182,
            "endTime": 1641579982,
```

```
            "hasErrorEvent": false,
            "streamId": "mystream"
        }
        ...
    ]
}
```

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte ListStreamSessions en la Referencia de comandos de la AWS CLI.

`list-streams`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-streams`.

AWS CLI

Para obtener una lista de las transmisiones en directo y su estado

En el siguiente ejemplo de `list-streams`, se enumeran todas las transmisiones en directo de la cuenta de AWS.

```
aws ivs list-streams
```

Salida:

```
{
   "streams": [
        {
            "channelArn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
            "state": "LIVE",
            "health": "HEALTHY",
            "streamId": "st-ABCDEfghij01234KLMN5678",
            "viewerCount": 1
        }
    ]
}
```

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte ListStreams en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar todas las etiquetas de un recurso de AWS (por ejemplo, channel, stream key)

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran todas las etiquetas de un ARN (Nombre de recurso de Amazon) de recurso específico.

```
aws ivs list-tags-for-resource \
    --resource-arn arn:aws:ivs:us-west-2:12345689012:channel/abcdABCDefgh
```

Salida:

```
{
    "tags":
    {
        "key1": "value1",
        "key2": "value2"
    }
}
```

Para obtener más información, consulte Tagging en la Referencia de la API de Amazon Interactive Video Service.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-metadata`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-metadata`.

AWS CLI

Para insertar metadatos en la transmisión activa para un canal específico

En el siguiente ejemplo de `put-metadata`, se insertan los metadatos indicados en la transmisión del canal especificado.

```
aws ivs put-metadata \
    --channel-arn arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh \
    --metadata '{"my": "metadata"}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener más información sobre la API, consulte PutMetadata en la Referencia de comandos de la AWS CLI.

`start-viewer-session-revocation`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-viewer-session-revocation`.

AWS CLI

Para revocar las sesiones de los espectadores para varios pares de canal-ARN y ID-de espectador

En el siguiente ejemplo de `start-viewer-session-revocation`, se inicia el proceso de revocación de la sesión del observador asociada a un ARN de canal e ID de observador específicos hasta el número de versión de sesión especificado. Si no se proporciona la versión, el valor predeterminado es 0.

```
aws ivs batch-start-viewer-session-revocation \
    --channel-arn arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh \
    --viewer-id abcdefg \
    --viewer-session-versions-less-than-or-equal-to 1234567890
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de canales privados en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte StartViewerSessionRevocation en la Referencia de comandos de la AWS CLI.

`stop-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-stream`.

AWS CLI

Para detener una transmisión específica

En el siguiente ejemplo de `stop-stream`, se detiene la transmisión en el canal especificado.

```
aws ivs stop-stream \
    --channel-arn arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte StopStream en la Referencia de comandos de AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para agregar o actualizar todas las etiquetas de un recurso de AWS (por ejemplo, channel, stream key)

En el siguiente ejemplo de `tag-resource`, se agregan o actualizan las etiquetas de un ARN (Nombre de recurso de Amazon) de recurso específico.

```
aws ivs tag-resource \
    --resource-arn arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh \
    --tags "tagkey1=tagvalue1, tagkey2=tagvalue2"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging en la Referencia de la API de Amazon Interactive Video Service.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar todas las etiquetas de un recurso de AWS (por ejemplo, channel, stream key)

En el siguiente ejemplo de `untag-resource`, se eliminan etiquetas específicas de un ARN (Nombre de recurso de Amazon) de recurso específico.

```
aws ivs untag-resource \
    --resource-arn arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh \
    --tag-keys "tagkey1, tagkey2"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging en la Referencia de la API de Amazon Interactive Video Service.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-channel`.

AWS CLI

Ejemplo 1: actualizar la información de configuración de un canal

En el siguiente ejemplo de `update-channel`, se actualiza la configuración del canal para un ARN de canal específico para cambiar el nombre de canal. Esto no afecta a la transmisión en curso de este canal; debe detener y reiniciar la transmisión para que los cambios surtan efecto.

```
aws ivs update-channel \
```

```
    --arn 'arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh' \
    --name 'channel-1' \
    --insecure-ingest
```

Salida:

```
{
    "channel": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "name": "channel-1",
        "latencyMode": "LOW",
        "containerFormat": "TS",
        "multitrackInputConfiguration": {
            "enabled": false,
            "maximumResolution": "FULL_HD",
            "policy": "ALLOW"
        },
        "type": "STANDARD",
        "playbackRestrictionPolicyArn": "",
        "recordingConfigurationArn": "",
        "srt": {
            "endpoint": "a1b2c3d4e5f6.srt.live-video.net",
            "passphrase":
 "AB1C2defGHijkLMNo3PqQRstUvwxyzaBCDEfghh4ijklMN5opqrStuVWxyzAbCDEfghIJ"
        },
        "ingestEndpoint": "a1b2c3d4e5f6.global-contribute.live-video.net",
        "insecureIngest": true,
        "playbackUrl": "https://a1b2c3d4e5f6.us-west-2.playback.live-video.net/api/
video/v1/us-west-2.123456789012.channel.abcdEFGH.m3u8",
        "preset": "",
        "authorized": false,
        "tags": {}
}
```

Para obtener más información, consulte Create a Channel en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

Ejemplo 2: actualizar la configuración de un canal para permitir la grabación

En el siguiente ejemplo de `update-channel`, se actualiza la configuración del canal para un ARN de canal específico para activar la grabación. Esto no afecta a la transmisión en curso de este canal; debe detener y reiniciar la transmisión para que los cambios surtan efecto.

```
aws ivs update-channel \
    --arn 'arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh' \
    --no-insecure-ingest \
    --recording-configuration-arn 'arn:aws:ivs:us-west-2:123456789012:recording-
configuration/ABCD12cdEFgh'
```

Salida:

```
{
    "channel": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "name": "test-channel-with-recording",
        "latencyMode": "LOW",
        "containerFormat": "TS",
        "multitrackInputConfiguration": {
            "enabled": false,
            "maximumResolution": "FULL_HD",
            "policy": "ALLOW"
        },
        "type": "STANDARD",
        "playbackRestrictionPolicyArn": "",
        "recordingConfigurationArn": "arn:aws:ivs:us-west-2:123456789012:recording-
configuration/ABCD12cdEFgh",
        "srt": {
            "endpoint": "a1b2c3d4e5f6.srt.live-video.net",
            "passphrase":
 "BA1C2defGHijkLMNo3PqQRstUvwxyzaBCDEfghh4ijklMN5opqrStuVWxyzAbCDEfghIJ"
        },
        "ingestEndpoint": "a1b2c3d4e5f6.global-contribute.live-video.net",
        "insecureIngest": false,
        "playbackUrl": "https://a1b2c3d4e5f6.us-west-2.playback.live-video.net/api/
video/v1/us-west-2.123456789012.channel.abcdEFGH.m3u8",
        "preset": "",
        "authorized": false,
        "tags": {}
    }
}
```

Para obtener más información, consulte Record to Amazon S3 en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

Ejemplo 3: actualizar la configuración de un canal para deshabilitar la grabación

En el siguiente ejemplo de `update-channel`, se actualiza la configuración del canal para un ARN de canal específico para desactivar la grabación. Esto no afecta a la transmisión en curso de este canal; debe detener y reiniciar la transmisión para que los cambios surtan efecto.

```
aws ivs update-channel \
    --arn 'arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh' \
    --recording-configuration-arn ''
```

Salida:

```
{
    "channel": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "name": "test-channel-with-recording",
        "latencyMode": "LOW",
        "containerFormat": "TS",
        "multitrackInputConfiguration": {
            "enabled": false,
            "maximumResolution": "FULL_HD",
            "policy": "ALLOW"
        },
        "type": "STANDARD",
        "playbackRestrictionPolicyArn": "",
        "recordingConfigurationArn": "",
        "srt": {
            "endpoint": "a1b2c3d4e5f6.srt.live-video.net",
            "passphrase":
 "AB1C2edfGHijkLMNo3PqQRstUvwxyzaBCDEfghh4ijklMN5opqrStuVWxyzAbCDEfghIJ"
        },
        "ingestEndpoint": "a1b2c3d4e5f6.global-contribute.live-video.net",
        "insecureIngest": false,
        "playbackUrl": "https://a1b2c3d4e5f6.us-west-2.playback.live-video.net/api/
video/v1/us-west-2.123456789012.channel.abcdEFGH.m3u8",
        "preset": "",
        "authorized": false,
        "tags": {}
    }
}
```

Para obtener más información, consulte Record to Amazon S3 en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

Ejemplo 4: actualizar la configuración de un canal para habilitar la restricción de reproducción

En el siguiente ejemplo de `update-channel`, se actualiza la configuración del canal para un ARN de canal específico para activar la política de restricción de reproducción. Esto no afecta a la transmisión en curso de este canal; debe detener y reiniciar la transmisión para que los cambios surtan efecto.

```
aws ivs update-channel \
    --arn 'arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh' \
    --no-insecure-ingest \
    --playback-restriction-policy-arn 'arn:aws:ivs:us-west-2:123456789012:playback-restriction-policy/ABcdef34ghIJ'
```

Salida:

```
{
    "channel": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "name": "test-channel-with-playback-restriction-policy",
        "latencyMode": "LOW",
        "containerFormat": "TS",
        "multitrackInputConfiguration": {
            "enabled": false,
            "maximumResolution": "FULL_HD",
            "policy": "ALLOW"
        },
        "type": "STANDARD",
        "playbackRestrictionPolicyArn": "arn:aws:ivs:us-
west-2:123456789012:playback-restriction-policy/ABcdef34ghIJ",
        "recordingConfigurationArn": "",
        "srt": {
            "endpoint": "a1b2c3d4e5f6.srt.live-video.net",
            "passphrase":
 "AB1C2defGHijkLMNo3PqQRstUvwxyzaCBDEfghh4ijklMN5opqrStuVWxyzAbCDEfghIJ"
        },
        "ingestEndpoint": "a1b2c3d4e5f6.global-contribute.live-video.net",
        "insecureIngest": false,
        "playbackUrl": "https://a1b2c3d4e5f6.us-west-2.playback.live-video.net/api/
video/v1/us-west-2.123456789012.channel.abcdEFGH.m3u8",
        "preset": "",
        "authorized": false,
        "tags": {}
    }
```

```
}
```

Para obtener más información, consulte Contenido y espectadores no deseados en IVS en la Guía del usuario de Guía de Transmisión de baja latencia de Amazon IVS.

Ejemplo 5: actualizar la configuración de un canal para deshabilitar la restricción de reproducción

En el siguiente ejemplo de `update-channel`, se actualiza la configuración del canal para un ARN de canal específico para desactivar la restricción de reproducción. Esto no afecta a la transmisión en curso de este canal; debe detener y reiniciar la transmisión para que los cambios surtan efecto.

```
aws ivs update-channel \
    --arn 'arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh' \
    --playback-restriction-policy-arn ''
```

Salida:

```
{
    "channel": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "name": "test-channel-with-playback-restriction-policy",
        "latencyMode": "LOW",
        "containerFormat": "TS",
        "multitrackInputConfiguration": {
            "enabled": false,
            "maximumResolution": "FULL_HD",
            "policy": "ALLOW"
        },
        "type": "STANDARD",
        "playbackRestrictionPolicyArn": "",
        "recordingConfigurationArn": "",
        "srt": {
            "endpoint": "a1b2c3d4e5f6.srt.live-video.net",
            "passphrase":
 "AB1C2defGHijkLMNo3PqQRstUvwxyzaBCDeFghh4ijklMN5opqrStuVWxyzAbCDEfghIJ"
        },
        "ingestEndpoint": "a1b2c3d4e5f6.global-contribute.live-video.net",
        "insecureIngest": false,
        "playbackUrl": "https://a1b2c3d4e5f6.us-west-2.playback.live-video.net/api/
video/v1/us-west-2.123456789012.channel.abcdEFGH.m3u8",
        "preset": "",
```

```
        "authorized": false,
        "tags": {}
    }
}
```

Para obtener más información, consulte Contenido y espectadores no deseados en IVS en la Guía del usuario de Guía de Transmisión de baja latencia de Amazon IVS.

Ejemplo 6: actualización de la configuración de un canal para permitir la multipista

En el siguiente ejemplo de `update-channel`, se actualiza la configuración del canal para un ARN de canal específico para habilitar la multipista. Esto no afecta a la transmisión en curso de este canal; debe detener y reiniciar la transmisión para que los cambios surtan efecto.

```
aws ivs update-channel \
    --arn 'arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh' \
    --container-format 'FRAGMENTED_MP4' \
    --multitrack-input-configuration '{"enabled": true,"maximumResolution":
 "FULL_HD","policy": "ALLOW"}'
```

Salida:

```
{
    "channel": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "containerFormat": "FRAGMENTED_MP4",
        "name": "test-channel-with-multitrack",
        "latencyMode": "LOW",
        "multitrackInputConfiguration": {
            "enabled": true,
            "maximumResolution": "FULL_HD",
            "policy": "ALLOW"
        },
        "type": "STANDARD",
        "playbackRestrictionPolicyArn": "",
        "recordingConfigurationArn": "",
        "srt": {
            "endpoint": "a1b2c3d4e5f6.srt.live-video.net",
            "passphrase":
 "AB1C2defGHijkLMNo3PqQRstUvwxyzaCBDEfghh4ijklMN5opqrStuVWxyzAbCDEfghIJ"
        },
        "ingestEndpoint": "a1b2c3d4e5f6.global-contribute.live-video.net",
```

```
        "insecureIngest": false,
        "playbackUrl": "https://a1b2c3d4e5f6.us-west-2.playback.live-video.net/api/
video/v1/us-west-2.123456789012.channel.abcdEFGH.m3u8",
        "preset": "",
        "authorized": false,
        "tags": {}
    }
}
```

Para obtener más información, consulte Contenido y espectadores no deseados en IVS en la Guía del usuario de Guía de Transmisión de baja latencia de Amazon IVS.

Ejemplo 7: actualización de la configuración de un canal para desactivar la restricción de reproducción

En el siguiente ejemplo de `update-channel`, se actualiza la configuración del canal para un ARN de canal específico para desactivar la multipista. Esto no afecta a la transmisión en curso de este canal; debe detener y reiniciar la transmisión para que los cambios surtan efecto.

```
aws ivs update-channel \
    --arn 'arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh' \
    --container-format 'TS' \
    --multitrack-input-configuration '{"enabled": false}'
```

Salida:

```
{
    "channel": {
        ""arn": "arn:aws:ivs:us-west-2:123456789012:channel/abcdABCDefgh",
        "containerFormat": "TS",
        "name": "test-channel-with-multitrack",
        "latencyMode": "LOW",
        "multitrackInputConfiguration": {
            "enabled": false,
            "maximumResolution": "FULL_HD",
            "policy": "ALLOW"
        },
        "type": "STANDARD",
        "playbackRestrictionPolicyArn": "",
        "recordingConfigurationArn": "",
        "srt": {
            "endpoint": "a1b2c3d4e5f6.srt.live-video.net",
```

```
            "passphrase":
 "AB1C2defGHijkLMNo3PqQRstUvwxyzaCBDEfghh4ijklMN5opqrStuVWxyzAbCDEfghIJ"
        },
        "ingestEndpoint": "a1b2c3d4e5f6.global-contribute.live-video.net",
        "insecureIngest": false,
        "playbackUrl": "https://a1b2c3d4e5f6.us-west-2.playback.live-video.net/api/
video/v1/us-west-2.123456789012.channel.abcdEFGH.m3u8",
        "preset": "",
        "authorized": false,
        "tags": {}
    }
}
```

Para obtener más información, consulte Contenido y espectadores no deseados en IVS en la Guía del usuario de Guía de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte UpdateChannel en la Referencia de comandos de la AWS CLI.

`update-playback-restriction-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-playback-restriction-policy`.

AWS CLI

Para actualizar una política de restricción de reproducción

En el siguiente ejemplo de `update-playback-restriction-policy`, se actualiza la política de restricción de reproducción con el ARN de política especificado para deshabilitar la aplicación estricta del origen. Esto no afecta a la transmisión en curso del canal asociado; debe detener y reiniciar la transmisión para que los cambios surtan efecto.

```
aws ivs update-playback-restriction-policy \
    --arn "arn:aws:ivs:us-west-2:123456789012:playback-restriction-policy/
ABcdef34ghIJ" \
    --no-enable-strict-origin-enforcement
```

Salida:

```
{
```

```
    "playbackRestrictionPolicy": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:playback-restriction-policy/
ABcdef34ghIJ",
        "allowedCountries": [
            "US",
            "MX"
        ],
        "allowedOrigins": [
            "https://www.website1.com",
            "https://www.website2.com"
        ],
        "enableStrictOriginEnforcement": false,
        "name": "test-playback-restriction-policy",
        "tags": {
            "key1": "value1",
            "key2": "value2"
        }
    }
}
```

Para obtener más información, consulte Contenido y espectadores no deseados en IVS en la Guía del usuario de Guía de Transmisión de baja latencia de Amazon IVS.

- Para obtener detalles sobre la API, consulte UpdatePlaybackRestrictionPolicy en la Referencia de comandos de la AWS CLI.

Ejemplos de Chat de Amazon IVS que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Chat de Amazon IVS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-chat-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-chat-token`.

AWS CLI

Para crear un token de chat

En el siguiente ejemplo de `create-chat-token`, se crea un token de chat cifrado que se utiliza para establecer una conexión WebSocket individual a una sala. El token es válido durante un minuto. Una conexión (sesión) establecida con el token es válida durante el tiempo especificado.

```
aws ivschat create-chat-token \
    --roomIdentifier "arn:aws:ivschat:us-west-2:12345689012:room/g1H2I3j4k5L6", \
    --userId" "11231234" \
    --capabilities "SEND_MESSAGE", \
    --sessionDurationInMinutes" 30
```

Salida:

```
{
    "token": "ACEGmnoq#1rstu2...BDFH3vxwy!4hlm!#5",
    "sessionExpirationTime": "2022-03-16T04:44:09+00:00"
    "state": "CREATING",
    "tokenExpirationTime": "2022-03-16T03:45:09+00:00"
}
```

Para obtener más información, consulte el Step 3: Authenticate and Authorize Chat Clients en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte CreateChatToken en la Referencia de comandos de la AWS CLI.

`create-logging-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-logging-configuration`.

AWS CLI

Para crear un recurso LoggingConfiguration de chat

En el siguiente ejemplo de `create-logging-configuration`, se crea un recurso LoggingConfiguration que permite a los clientes almacenar y registrar los mensajes enviados.

```
aws ivschat create-logging-configuration \
    --destination-configuration s3={bucketName=demo-logging-bucket} \
    --name "test-logging-config" \
    --tags "key1=value1, key2=value2"
```

Salida:

```
{
    "arn": "arn:aws:ivschat:us-west-2:123456789012:logging-configuration/
ABcdef34ghIJ",
    "createTime": "2022-09-14T17:48:00.653000+00:00",
    "destinationConfiguration": {
        "s3": {
            "bucketName": "demo-logging-bucket"
        }
    },
    "id": "ABcdef34ghIJ",
    "name": "test-logging-config",
    "state": "ACTIVE",
    "tags": { "key1" : "value1", "key2" : "value2" },
    "updateTime": "2022-09-14T17:48:01.104000+00:00"
}
```

Para obtener más información, consulte Introducción al Chat de Amazon IVS en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte CreateLoggingConfiguration en la Referencia de comandos de la AWS CLI.

`create-room`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-room`.

AWS CLI

Para crear una sala

En el siguiente ejemplo de `create-room`, se crea una nueva sala.

```
aws ivschat create-room \
    --name "test-room-1" \
    --logging-configuration-identifiers "arn:aws:ivschat:us-
west-2:123456789012:logging-configuration/ABcdef34ghIJ" \
    --maximum-message-length 256 \
    --maximum-message-rate-per-second 5
```

Salida:

```
{
    "arn": "arn:aws:ivschat:us-west-2:12345689012:room/g1H2I3j4k5L6",
    "id": "g1H2I3j4k5L6",
    "createTime": "2022-03-16T04:44:09+00:00",
    "loggingConfigurationIdentifiers": ["arn:aws:ivschat:us-
west-2:123456789012:logging-configuration/ABcdef34ghIJ"],
    "maximumMessageLength": 256,
    "maximumMessageRatePerSecond": 5,
    "name": "test-room-1",
    "tags": {}
    "updateTime": "2022-03-16T07:22:09+00:00"
}
```

Para obtener más información, consulte Paso 2: crear una sala de chat en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte CreateRoom en la Referencia de comandos de la AWS CLI.

`delete-logging-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-logging-configuration`.

AWS CLI

Para eliminar un recurso LoggingConfiguration de chat

En el siguiente ejemplo de `delete-logging-configuration`, se elimina el recurso LoggingConfiguration del ARN especificado.

```
aws ivschat delete-logging-configuration \
```

```
    --identifier "arn:aws:ivschat:us-west-2:123456789012:logging-configuration/
ABcdef34ghIJ"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Introducción al Chat de Amazon IVS en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte DeleteLoggingConfiguration en la Referencia de comandos de la AWS CLI.

`delete-message`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-message`.

AWS CLI

Para eliminar mensajes de una sala específica

En el siguiente ejemplo de `delete-message`, se envía un evento a la sala especificada, que indica a los clientes que eliminen el mensaje especificado, es decir, que lo retiren de la vista y que lo eliminen del historial de chat del cliente.

```
aws ivschat delete-message \
    --roomIdentifier "arn:aws:ivschat:us-west-2:12345689012:room/g1H2I3j4k5L6" \
    --id "ABC123def456" \
    --reason "Message contains profanity"
```

Salida:

```
{
    "id": "12345689012"
}
```

Para obtener más información, consulte Introducción al Chat de Amazon IVS en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte DeleteMessage en la Referencia de comandos de la AWS CLI.

`delete-room`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-room`.

AWS CLI

Para eliminar una sala

En el siguiente ejemplo de `delete-room`, se elimina la sala especificada. Los clientes que están conectados a la sala se desconectarán. Si se ejecuta correctamente, devuelve HTTP 204 con un cuerpo de respuesta vacío.

```
aws ivschat delete-room \
    --identifier "arn:aws:ivschat:us-west-2:12345689012:room/g1H2I3j4k5L6"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Introducción al Chat de Amazon IVS en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte DeleteRoom en la Referencia de comandos de la AWS CLI.

`disconnect-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `disconnect-user`.

AWS CLI

Para desconectar a un usuario de una sala

En el siguiente ejemplo de `disconnect-user`, se desconectan todas las conexiones del usuario especificado de la sala indicada. Si se ejecuta correctamente, devuelve HTTP 200 con un cuerpo de respuesta vacío.

```
aws ivschat disconnect-user \
    --roomIdentifier "arn:aws:ivschat:us-west-2:12345689012:room/g1H2I3j4k5L6" \
    --userId "ABC123def456" \
    --reason "Violated terms of service"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Introducción al Chat de Amazon IVS en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener más información sobre la API, consulte DisconnectUser en la Referencia de comandos de la AWS CLI.

`get-logging-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-logging-configuration`.

AWS CLI

Para obtener información sobre un recurso LoggingConfiguration

En el siguiente ejemplo de `get-logging-configuration`, se obtiene información del recurso LoggingConfiguration del ARN especificado.

```
aws ivschat get-logging-configuration \
    --identifier "arn:aws:ivschat:us-west-2:123456789012:logging-configuration/
ABcdef34ghIJ"
```

Salida:

```
{
    "arn": "arn:aws:ivschat:us-west-2:123456789012:logging-configuration/
ABcdef34ghIJ",
    "createTime": "2022-09-14T17:48:00.653000+00:00",
    "destinationConfiguration": {
        "s3": {
            "bucketName": "demo-logging-bucket"
        }
    },
    "id": "ABcdef34ghIJ",
    "name": "test-logging-config",
    "state": "ACTIVE",
    "tags": { "key1" : "value1", "key2" : "value2" },
    "updateTime": "2022-09-14T17:48:01.104000+00:00"
}
```

Para obtener más información, consulte Introducción al Chat de Amazon IVS en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte GetLoggingConfiguration en la Referencia de comandos de la AWS CLI.

`get-room`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-room`.

AWS CLI

Para obtener la sala especificada

En el siguiente ejemplo de `get-room`, se obtiene información de la sala especificada.

```
aws ivschat get-room \
    --identifier "arn:aws:ivschat:us-west-2:12345689012:room/g1H2I3j4k5L6"
```

Salida:

```
{
    "arn": "arn:aws:ivschat:us-west-2:12345689012:room/g1H2I3j4k5L6",
    "createTime": "2022-03-16T04:44:09+00:00",
    "id": "g1H2I3j4k5L6",
    "loggingConfigurationIdentifiers": ["arn:aws:ivschat:us-
west-2:123456789012:logging-configuration/ABcdef34ghIJ"],
    "maximumMessageLength": 256,
    "maximumMessageRatePerSecond": 5,
    "name": "test-room-1",
    "tags": {},
    "updateTime": "2022-03-16T07:22:09+00:00"
}
```

Para obtener más información, consulte Introducción al Chat de Amazon IVS en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte GetRoom en la Referencia de comandos de la AWS CLI.

`list-logging-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-logging-configurations`.

AWS CLI

Para obtener información resumida sobre todas las configuraciones de registro del usuario en la región de AWS en la que se procesa la solicitud de la API

En el siguiente ejemplo de `list-logging-configurations`, se enumera información sobre todos los recursos LoggingConfiguration para el usuario en la región de AWS en la que se procesa la solicitud de la API.

```
aws ivschat list-logging-configurations \
    --max-results 2 \
    --next-token ""
```

Salida:

```
{
    "nextToken": "set-2",
    "loggingConfigurations": [
        {
            "arn": "arn:aws:ivschat:us-west-2:123456789012:logging-configuration/
ABcdef34ghIJ",
            "createTime": "2022-09-14T17:48:00.653000+00:00",
            "destinationConfiguration": {
                "s3": {
                    "bucketName": "demo-logging-bucket"
                }
            },
            "id": "ABcdef34ghIJ",
            "name": "test-logging-config",
            "state": "ACTIVE",
            "tags": { "key1" : "value1", "key2" : "value2" },
            "updateTime": "2022-09-14T17:48:01.104000+00:00"
        }
        ...
    ]
}
```

Para obtener más información, consulte Introducción al Chat de Amazon IVS en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener más información sobre la API, consulte ListLoggingConfigurations en la Referencia de comandos de la AWS CLI.

`list-rooms`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-rooms`.

AWS CLI

Para obtener información resumida sobre todas las salas de la región actual

En el siguiente ejemplo de `list-rooms`, se obtiene información resumida sobre todas las salas de la región de AWS en la que se procesa la solicitud. Los resultados se muestran en orden descendente de updateTime.

```
aws ivschat list-rooms \
    --logging-configuration-identifier "arn:aws:ivschat:us-
west-2:123456789012:logging-configuration/ABcdef34ghIJ" \
    --max-results 10 \
    --next-token ""
```

Salida:

```
{
    "nextToken": "page3",
    "rooms": [
        {
            "arn:aws:ivschat:us-west-2:12345689012:room/g1H2I3j4k5L6",
            "createTime": "2022-03-16T04:44:09+00:00",
            "id": "g1H2I3j4k5L6",
            "loggingConfigurationIdentifiers": ["arn:aws:ivschat:us-
west-2:123456789012:logging-configuration/ABcdef34ghIJ"],
            "name": "test-room-1",
            "tags": {},
            "updateTime": "2022-03-16T07:22:09+00:00"
        }
    ]
}
```

Para obtener más información, consulte Introducción al Chat de Amazon IVS en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte ListRooms en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar todas las etiquetas de un recurso de AWS (por ejemplo, Room)

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran todas las etiquetas de un ARN (Nombre de recurso de Amazon) de recurso específico.

```
aws ivschat list-tags-for-resource \
    --resource-arn arn:aws:ivschat:us-west-2:12345689012:room/g1H2I3j4k5L6
```

Salida:

```
{
    "tags":
    {
        "key1": "value1",
        "key2": "value2"
    }
}
```

Para obtener más información, consulte Tagging en la Referencia de la API de Amazon Interactive Video Service.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`send-event`

En el siguiente ejemplo de código, se muestra cómo utilizar `send-event`.

AWS CLI

Para enviar un evento a una sala

En el siguiente ejemplo de `send-event`, se envía el evento dado a la sala especificada.

```
aws ivschat send-event \
```

```
    --roomIdentifier "arn:aws:ivschat:us-west-2:12345689012:room/g1H2I3j4k5L6" \
    --eventName "SystemMessage" \
    --attributes \
        "msgType"="user-notification", \
        "msgText"="This chat room will close in 15 minutes."
```

Salida:

```
{
    "id": "12345689012"
}
```

Para obtener más información, consulte Introducción al Chat de Amazon IVS en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener más información sobre la API, consulte SendEvent en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para agregar o actualizar todas las etiquetas de un recurso de AWS (por ejemplo, Room)

En el siguiente ejemplo de `tag-resource`, se agregan o actualizan las etiquetas de un ARN (Nombre de recurso de Amazon) de recurso específico. Si se ejecuta correctamente, devuelve HTTP 200 con un cuerpo de respuesta vacío.

```
aws ivschat tag-resource \
    --resource-arn arn:aws:ivschat:us-west-2:12345689012:room/g1H2I3j4k5L6 \
    --tags "tagkey1=tagkeyvalue1, tagkey2=tagkeyvalue2"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging en la Referencia de la API de Amazon Interactive Video Service.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar las etiquetas de un recurso de AWS (por ejemplo, Room)

En el siguiente ejemplo de `untag-resource`, se eliminan etiquetas específicas de un ARN (Nombre de recurso de Amazon) de recurso específico. Si se ejecuta correctamente, devuelve HTTP 200 con un cuerpo de respuesta vacío.

```
aws ivschat untag-resource \
    --resource-arn arn:aws:ivschat:us-west-2:12345689012:room/g1H2I3j4k5L6 \
    --tag-keys "tagkey1, tagkey2"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging en la Referencia de la API de Amazon Interactive Video Service.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-logging-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-logging-configuration`.

AWS CLI

Para actualizar una configuración de registro de una sala

En el siguiente ejemplo de `update-logging-configuration`, se actualiza un recurso LoggingConfiguration con los datos proporcionados.

```
aws ivschat update-logging-configuration \
    --destination-configuration s3={bucketName=demo-logging-bucket} \
    --identifier "arn:aws:ivschat:us-west-2:123456789012:logging-configuration/
ABcdef34ghIJ" \
    --name "test-logging-config"
```

Salida:

```
{
    "arn": "arn:aws:ivschat:us-west-2:123456789012:logging-configuration/
ABcdef34ghIJ",
    "createTime": "2022-09-14T17:48:00.653000+00:00",
    "destinationConfiguration": {
        "s3": {
            "bucketName": "demo-logging-bucket"
        }
    },
    "id": "ABcdef34ghIJ",
    "name": "test-logging-config",
    "state": "ACTIVE",
    "tags": { "key1" : "value1", "key2" : "value2" },
    "updateTime": "2022-09-14T17:48:01.104000+00:00"
}
```

Para obtener más información, consulte Introducción al Chat de Amazon IVS en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información acerca de la API, consulte UpdateLoggingConfiguration en la Referencia de comandos de la AWS CLI.

`update-room`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-room`.

AWS CLI

Para actualizar la configuración de una sala

En el siguiente de ejemplo de `update-room`, se actualiza la configuración de la sala indicada para los datos especificados.

```
aws ivschat update-room \
    --identifier "arn:aws:ivschat:us-west-2:12345689012:room/g1H2I3j4k5L6" \
    --logging-configuration-identifiers "arn:aws:ivschat:us-
west-2:123456789012:logging-configuration/ABcdef34ghIJ" \
    --name "chat-room-a" \
    --maximum-message-length 256 \
    --maximum-message-rate-per-second 5
```

Salida:

```
{
    "arn": "arn:aws:ivschat:us-west-2:12345689012:room/g1H2I3j4k5L6",
    "createTime": "2022-03-16T04:44:09+00:00",
    "id": "g1H2I3j4k5L6",
    "loggingConfigurationIdentifiers": ["arn:aws:ivschat:us-
west-2:123456789012:logging-configuration/ABcdef34ghIJ"],
    "maximumMessageLength": 256,
    "maximumMessageRatePerSecond": 5,
    "name": "chat-room-a",
    "tags": {},
    "updateTime": "2022-03-16T07:22:09+00:00"
}
```

Para obtener más información, consulte Introducción al Chat de Amazon IVS en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte UpdateRoom en la Referencia de comandos de la AWS CLI.

Ejemplos de Transmisión en tiempo real de Amazon IVS que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Transmisión en tiempo real de Amazon IVS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-encoder-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-encoder-configuration`.

AWS CLI

Para crear una configuración de codificador de composición

En el siguiente ejemplo de `create-encoder-configuration`, se crea una configuración de codificador de composición con las propiedades especificadas.

```
aws ivs-realtime create-encoder-configuration \
    --name test-ec --video bitrate=3500000,framerate=30.0,height=1080,width=1920
```

Salida:

```
{
    "encoderConfiguration": {
        "arn": "arn:aws:ivs:ap-northeast-1:123456789012:encoder-configuration/
ABabCDcdEFef",
        "name": "test-ec",
        "tags": {},
        "video": {
            "bitrate": 3500000,
            "framerate": 30,
            "height": 1080,
            "width": 1920
        }
    }
}
```

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener información sobre la API, consulte CreateEncoderConfiguration en la Referencia de comandos de la AWS CLI.

`create-ingest-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-ingest-configuration`.

AWS CLI

Creación de una configuración de ingesta

En el siguiente ejemplo de `create-ingest-configuration`, se crea una configuración de ingesta mediante el protocolo RTMPS.

```
aws ivs-realtime create-ingest-configuration \
    --name ingest1 \
    --ingest-protocol rtmps
```

Salida:

```
{
    "ingestConfiguration": {
        "name": "ingest1",
        "arn": "arn:aws:ivs:us-west-2:123456789012:ingest-configuration/
AbCdEfGh1234",
        "ingestProtocol": "RTMPS",
        "streamKey": "rt_123456789012_us-
west-2_AbCdEfGh1234_abcd1234efgh5678ijkl9012MNOP34",
        "stageArn": "",
        "participantId": "xyZ654abC321",
        "state": "INACTIVE",
        "userId": "",
        "tags": {}
    }
}
```

Para obtener más información, consulte Ingesta de transmisiones de IVS | Transmisión en tiempo real en la Guía del usuario de Servicio de vídeos interactivos de Amazon.

- Para obtener información sobre la API, consulte CreateIngestConfiguration en la Referencia de comandos de la AWS CLI.

`create-participant-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-participant-token`.

AWS CLI

Para crear un token de participante de la fase

En el siguiente ejemplo de `create-participant-token`, se crea un token de participante para la etapa especificada.

```
aws ivs-realtime create-participant-token \
    --stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --user-id bob
```

Salida:

```
{
    "participantToken": {
        "expirationTime": "2023-03-07T09:47:43+00:00",
        "participantId": "ABCDEfghij01234KLMN6789",
        "token": "abcd1234defg5678"
    }
}
```

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener información sobre la API, consulte CreateParticipantToken en la Referencia de comandos de la AWS CLI.

`create-stage`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-stage`.

AWS CLI

Ejemplo 1: crear un escenario

En el siguiente ejemplo de `create-stage`, se crea un token de fase y un token de participante de la fase para un usuario especificado.

```
aws ivs-realtime create-stage \
    --name stage1 \
    --participant-token-configurations userId=alice
```

Salida:

```
{
    "participantTokens": [
        {
```

```
            "participantId": "ABCDEfghij01234KLMN5678",
            "token": "a1b2c3d4567890ab",
            "userId": "alice"
        }
    ],
    "stage": {
        "activeSessionId": "st-a1b2c3d4e5f6g",
        "arn": "arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh",
        "autoParticipantRecordingConfiguration": {
            "storageConfigurationArn": "",
            "mediaTypes": [
                "AUDIO_VIDEO"
            ],
            "thumbnailConfiguration": {
                "targetIntervalSeconds": 60,
                "storage": [
                    "SEQUENTIAL"
                ],
                "recordingMode": "DISABLED"
            },
            "recordingReconnectWindowSeconds": 0,
            "hlsConfiguration": {
                "targetSegmentDurationSeconds": 6
            },
            "recordParticipantReplicas": true
        },
        "endpoints": {
            "events": "wss://global.events.live-video.net",
            "rtmp": "rtmp://9x0y8z7s6t5u.global-contribute-staging.live-video.net/
app/",
            "rtmps": "rtmps://9x0y8z7s6t5u.global-contribute-staging.live-
video.net:443/app/",
            "whip": "https://9x0y8z7s6t5u.global-bm.whip.live-video.net"
        },
        "name": "stage1",
        "tags": {}
    }
}
```

Para obtener más información, consulte Habilitación de varios hosts en un flujo de Amazon IVS en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

Ejemplo 2: crear una fase y configurar una grabación de participante individual

En el siguiente ejemplo de `create-stage`, se crea una fase y se configura la grabación de cada participante individual.

```
aws ivs-realtime create-stage \
    --name stage1 \
    --auto-participant-recording-configuration '{"mediaTypes":
 ["AUDIO_VIDEO"],"storageConfigurationArn": "arn:aws:ivs:us-
west-2:123456789012:storage-configuration/abcdABCDefgh",
 "recordingReconnectWindowSeconds": 100, \
        "hlsConfiguration": {"targetSegmentDurationSeconds": 5}}'
```

Salida:

```
{
    "stage": {
        "activeSessionId": "st-a1b2c3d4e5f6g",
        "arn": "arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh",
        "autoParticipantRecordingConfiguration": {
            "storageConfigurationArn": "arn:aws:ivs:us-west-2:123456789012:storage-
configuration/abcdABCDefgh"
            "mediaTypes": [
                "AUDIO_VIDEO"
            ],
            "thumbnailConfiguration": {
                "targetIntervalSeconds": 60,
                "storage": [
                    "SEQUENTIAL"
                ],
                "recordingMode": "DISABLED"
            },
            "recordingReconnectWindowSeconds": 100,
            "hlsConfiguration": {
                "targetSegmentDurationSeconds": 5
            },
            "recordParticipantReplicas": true
        },
        "endpoints": {
            "events": "wss://global.events.live-video.net",
            "rtmp": "rtmp://9x0y8z7s6t5u.global-contribute-staging.live-video.net/
app/",
            "rtmps": "rtmps://9x0y8z7s6t5u.global-contribute-staging.live-
video.net:443/app/",
            "whip": "https://9x0y8z7s6t5u.global-bm.whip.live-video.net"
```

```
        },
        "name": "stage1",
        "tags": {}
    }
}
```

Para obtener más información, consulte Habilitación de varios hosts en un flujo de Amazon IVS en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

Ejemplo 3: creación de una etapa y configuración de una grabación de participante individual con grabación de miniaturas habilitada

En el siguiente ejemplo de `create-stage`, se crea una etapa y se configura la grabación de cada participante individual con grabación de miniaturas habilitada.

```
aws ivs-realtime create-stage \
    --name stage1 \
    --auto-participant-recording-configuration '{"mediaTypes":
 ["AUDIO_VIDEO"],"storageConfigurationArn": "arn:aws:ivs:us-
west-2:123456789012:storage-configuration/abcdABCDefgh", \
        "thumbnailConfiguration": {"recordingMode": "INTERVAL","storage":
 ["SEQUENTIAL"],"targetIntervalSeconds": 60}}'
```

Salida:

```
{
    "stage": {
        "activeSessionId": "st-a1b2c3d4e5f6g",
        "arn": "arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh",
        "autoParticipantRecordingConfiguration": {
            "storageConfigurationArn": "arn:aws:ivs:us-west-2:123456789012:storage-
configuration/abcdABCDefgh",
            "mediaTypes": [
                "AUDIO_VIDEO"
            ],
            "thumbnailConfiguration": {
                "targetIntervalSeconds": 60,
                "storage": [
                    "SEQUENTIAL"
                ],
                "recordingMode": "INTERVAL"
            },
            "recordingReconnectWindowSeconds": 0,
```

```
            "hlsConfiguration": {
                "targetSegmentDurationSeconds": 6
            },
            "recordParticipantReplicas": true
        },
        "endpoints": {
            "events": "wss://global.events.live-video.net",
            "rtmp": "rtmp://9x0y8z7s6t5u.global-contribute-staging.live-video.net/
app/",
            "rtmps": "rtmps://9x0y8z7s6t5u.global-contribute-staging.live-
video.net:443/app/",
            "whip": "https://9x0y8z7s6t5u.global-bm.whip.live-video.net"
        },
        "name": "stage1",
        "tags": {}
    }
}
```

Para obtener más información, consulte Habilitación de varios hosts en un flujo de Amazon IVS en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte CreateStage en la Referencia de comandos de la AWS CLI.

`create-storage-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-storage-configuration`.

AWS CLI

Para crear una configuración de almacenamiento de composición

En el siguiente ejemplo de `create-storage-configuration`, se crea una configuración de almacenamiento de composición con las propiedades especificadas.

```
aws ivs-realtime create-storage-configuration \
    --name "test-sc" --s3 "bucketName=amzn-s3-demo-bucket"
```

Salida:

```
{
    "storageConfiguration": {
```

```
        "arn": "arn:aws:ivs:ap-northeast-1:123456789012:storage-configuration/
ABabCDcdEFef",
        "name": "test-sc",
        "s3": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "tags": {}
    }
}
```

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener información sobre la API, consulte CreateStorageConfiguration en la Referencia de comandos de la AWS CLI.

`delete-encoder-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-encoder-configuration`.

AWS CLI

Para eliminar una configuración de codificador de composición

En el siguiente ejemplo de `delete-encoder-configuration`, se elimina la configuración del codificador de composición especificada por el ARN (Nombre de recurso de Amazon) indicado.

```
aws ivs-realtime delete-encoder-configuration \
    --arn "arn:aws:ivs:ap-northeast-1:123456789012:encoder-configuration/
ABabCDcdEFef"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener información sobre la API, consulte DeleteEncoderConfiguration en la Referencia de comandos de la AWS CLI.

`delete-ingest-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-ingest-configuration`.

AWS CLI

Ejemplo 1: eliminación de una configuración de ingesta inactiva

En el siguiente ejemplo de `delete-ingest-configuration`, se elimina la configuración de ingesta inactiva para un nombre de recurso de Amazon (ARN) de configuración de ingesta especificado.

```
aws ivs-realtime delete-ingest-configuration \
    --arn arn:aws:ivs:us-west-2:123456789012:ingest-configuration/AbCdEfGh1234
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Ingesta de transmisiones de IVS | Transmisión en tiempo real en la Guía del usuario de Servicio de vídeos interactivos de Amazon.

Ejemplo 2: forzar la eliminación de una configuración de ingesta activa

En el siguiente ejemplo de `delete-ingest-configuration`, se fuerza la eliminación de la configuración de ingesta activa para un nombre de recurso de Amazon (ARN) de configuración de ingesta especificado.

```
aws ivs-realtime delete-ingest-configuration \
    --arn arn:aws:ivs:us-west-2:123456789012:ingest-configuration/AbCdEfGh1234 \
    --force
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Ingesta de transmisiones de IVS | Transmisión en tiempo real en la Guía del usuario de Servicio de vídeos interactivos de Amazon.

- Para obtener información sobre la API, consulte DeleteIngestConfiguration en la Referencia de comandos de la AWS CLI.

`delete-public-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-public-key`.

AWS CLI

Para eliminar una clave pública

En el siguiente ejemplo de `delete-public-key`, se elimina la clave pública especificada.

```
aws ivs-realtime delete-public-key \
    --arn arn:aws:ivs:us-west-2:123456789012:public-key/abcdABC1efg2
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Distribuir los tokens de participantes en la Guía del usuario de Transmisión en tiempo real de Amazon IVS.

- Para obtener información sobre la API, consulte DeletePublicKey en la Referencia de comandos de la AWS CLI.

`delete-stage`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-stage`.

AWS CLI

Para eliminar un escenario

En el siguiente ejemplo de `delete-stage`, se elimina la fase especificada.

```
aws ivs-realtime delete-stage \
    --arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener información sobre la API, consulte DeleteStage en la Referencia de comandos de la AWS CLI.

`delete-storage-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-storage-configuration`.

AWS CLI

Para eliminar una configuración del almacenamiento de composición

En el siguiente ejemplo de `delete-storage-configuration`, se elimina la configuración del almacenamiento de composición especificada por el ARN (Nombre de recurso de Amazon) indicado.

```
aws ivs-realtime delete-storage-configuration \
    --arn "arn:aws:ivs:ap-northeast-1:123456789012:storage-configuration/
ABabCDcdEFef"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener información sobre la API, consulte DeleteStorageConfiguration en la Referencia de comandos de la AWS CLI.

`disconnect-participant`

En el siguiente ejemplo de código, se muestra cómo utilizar `disconnect-participant`.

AWS CLI

Para desconectar a un participante de la fase

En el siguiente ejemplo de `disconnect-participant`, se desconecta al participante especificado de la fase indicada.

```
aws ivs-realtime disconnect-participant \
    --stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --participant-id ABCDEfghij01234KLMN5678
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener información sobre la API, consulte DisconnectParticipant en la Referencia de comandos de la AWS CLI.

`get-composition`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-composition`.

AWS CLI

Ejemplo 1: obtener una composición con los ajustes de diseño predeterminados

En el siguiente ejemplo de `get-composition`, se obtiene la composición del ARN (Nombre de recurso de Amazon) especificado.

```
aws ivs-realtime get-composition \
    --arn "arn:aws:ivs:ap-northeast-1:123456789012:composition/abcdABCDefgh"
```

Salida:

```
{
    "composition": {
        "arn": "arn:aws:ivs:ap-northeast-1:123456789012:composition/abcdABCDefgh",
        "destinations": [
            {
                "configuration": {
                    "channel": {
                        "channelArn": "arn:aws:ivs:ap-
northeast-1:123456789012:channel/abcABCdefDEg",
                        "encoderConfigurationArn": "arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"
                    },
                    "name": ""
                },
                "id": "AabBCcdDEefF",
                "startTime": "2023-10-16T23:26:00+00:00",
                "state": "ACTIVE"
            },
            {
                "configuration": {
                    "name": "",
                    "s3": {
                        "encoderConfigurationArns": [
                            "arn:aws:ivs:arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"
                        ],
                        "recordingConfiguration": {
                            "format": "HLS",
                            "hlsConfiguration": {
                                "targetSegmentDurationSeconds": 2
                            }
```

```
                    },
                    "storageConfigurationArn": "arn:arn:aws:ivs:ap-
northeast-1:123456789012:storage-configuration/FefABabCDcdE",
                }
            },
            "detail": {
                "s3": {
                    "recordingPrefix": "aBcDeFgHhGfE/AbCdEfGhHgFe/GHFabcgefABC/
composite"
                }
            },
            "id": "GHFabcgefABC",
            "startTime": "2023-10-16T23:26:00+00:00",
            "state": "STARTING"
        }
    ],
    "layout": {
        "grid": {
            "featuredParticipantAttribute": "",
            "gridGap": 2,
            "omitStoppedVideo": false,
            "participantOrderAttribute": "",
            "videoAspectRatio": "VIDEO",
            "videoFillMode": ""
        }
    },
    "stageArn": "arn:aws:ivs:ap-northeast-1:123456789012:stage/defgABCDabcd",
    "startTime": "2023-10-16T23:24:00+00:00",
    "state": "ACTIVE",
    "tags": {}
  }
}
```

Para obtener más información, consulte Grabación compuesta de IVS | Transmisión en tiempo real en la Guía del usuario de Amazon Interactive Video Service.

Ejemplo 2: obtener una composición con los ajustes de diseño predeterminados

En el siguiente ejemplo de `get-composition`, se obtiene la composición del ARN (Nombre de recurso de Amazon) especificado que usa el diseño predeterminado.

```
aws ivs-realtime get-composition \
    --arn "arn:aws:ivs:ap-northeast-1:123456789012:composition/wxyzWXYZpqrs"
```

Salida:

```
{
    "composition": {
        "arn": "arn:aws:ivs:ap-northeast-1:123456789012:composition/wxyzWXYZpqrs",
        "destinations": [
            {
                "configuration": {
                    "channel": {
                        "channelArn": "arn:aws:ivs:ap-
northeast-1:123456789012:channel/abcABCdefDEg",
                        "encoderConfigurationArn": "arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"
                    },
                    "name": ""
                },
                "id": "AabBCcdDEefF",
                "startTime": "2023-10-16T23:26:00+00:00",
                "state": "ACTIVE"
            },
            {
                "configuration": {
                    "name": "",
                    "s3": {
                        "encoderConfigurationArns": [
                            "arn:aws:ivs:arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"
                        ],
                        "recordingConfiguration": {
                            "format": "HLS",
                            "hlsConfiguration": {
                                "targetSegmentDurationSeconds": 2
                            }
                        },
                        "storageConfigurationArn": "arn:arn:aws:ivs:ap-
northeast-1:123456789012:storage-configuration/FefABabCDcdE"
                    }
                },
                "detail": {
                    "s3": {
                        "recordingPrefix": "aBcDeFgHhGfE/AbCdEfGhHgFe/GHFabcgefABC/
composite"
                    }
                },
```

```
                "id": "GHFabcgefABC",
                "startTime": "2023-10-16T23:26:00+00:00",
                "state": "STARTING"
            }
        ],
        "layout": {
            "pip": {
                "featuredParticipantAttribute": "abcdefg",
                "gridGap": 0,
                "omitStoppedVideo": false,
                "participantOrderAttribute": "",
                "pipBehavior": "STATIC",
                "pipOffset": 0,
                "pipParticipantAttribute": "",
                "pipPosition": "BOTTOM_RIGHT",
                "videoFillMode": "COVER"
            }
        },
        "stageArn": "arn:aws:ivs:ap-northeast-1:123456789012:stage/defgABCDabcd",
        "startTime": "2023-10-16T23:24:00+00:00",
        "state": "ACTIVE",
        "tags": {}
    }
}
```

Para obtener más información, consulte Grabación compuesta de IVS | Transmisión en tiempo real en la Guía del usuario de Amazon Interactive Video Service.

Ejemplo 3: obtención de una composición con la grabación de miniaturas habilitada

En el siguiente ejemplo de `get-composition`, se obtiene la composición para el ARN (Nombre de recurso de Amazon) especificado, que tiene la grabación de miniaturas habilitada con la configuración predeterminada.

```
aws ivs-realtime get-composition \
    --arn "arn:aws:ivs:ap-northeast-1:123456789012:composition/abcdABCDefgh"
```

Salida:

```
{
    "composition": {
        "arn": "arn:aws:ivs:ap-northeast-1:123456789012:composition/abcdABCDefgh",
        "destinations": [
```

```
            {
                "configuration": {
                    "channel": {
                        "channelArn": "arn:aws:ivs:ap-
northeast-1:123456789012:channel/abcABCdefDEg",
                        "encoderConfigurationArn": "arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"
                    },
                    "name": ""
                },
                "id": "AabBCcdDEefF",
                "startTime": "2023-10-16T23:26:00+00:00",
                "state": "ACTIVE"
            },
            {
                "configuration": {
                    "name": "",
                    "s3": {
                        "encoderConfigurationArns": [
                            "arn:aws:ivs:arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"
                        ],
                        "recordingConfiguration": {
                            "format": "HLS",
                            "hlsConfiguration": {
                                "targetSegmentDurationSeconds": 2
                            }
                        },
                        "storageConfigurationArn": "arn:arn:aws:ivs:ap-
northeast-1:123456789012:storage-configuration/FefABabCDcdE",
                        "thumbnailConfigurations": [
                           {
                              "targetIntervalSeconds": 60,
                              "storage": [
                                  "SEQUENTIAL"
                              ],
                           }
                        ]
                    }
                },
                "detail": {
                    "s3": {
                        "recordingPrefix": "aBcDeFgHhGfE/AbCdEfGhHgFe/GHFabcgefABC/
composite"
```

```
                    }
                },
                "id": "GHFabcgefABC",
                "startTime": "2023-10-16T23:26:00+00:00",
                "state": "STARTING"
            }
        ],
        "layout": {
            "grid": {
                "featuredParticipantAttribute": ""
                "gridGap": 2,
                "omitStoppedVideo": false,
                "participantOrderAttribute": "",
                "videoAspectRatio": "VIDEO",
                "videoFillMode": ""                }
        },
        "stageArn": "arn:aws:ivs:ap-northeast-1:123456789012:stage/defgABCDabcd",
        "startTime": "2023-10-16T23:24:00+00:00",
        "state": "ACTIVE",
        "tags": {}
    }
}
```

Para obtener más información, consulte Grabación compuesta de IVS | Transmisión en tiempo real en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte GetComposition en la Referencia de comandos de la AWS CLI.

`get-encoder-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-encoder-configuration`.

AWS CLI

Para eliminar una configuración de codificador de composición

En el siguiente ejemplo de `get-encoder-configuration`, se obtiene la configuración del codificador de composición especificada por el ARN (Nombre de recurso de Amazon) indicado.

```
aws ivs-realtime get-encoder-configuration \
```

```
    --arn "arn:aws:ivs:ap-northeast-1:123456789012:encoder-configuration/
abcdABCDefgh"
```

Salida:

```
{
    "encoderConfiguration": {
        "arn": "arn:aws:ivs:ap-northeast-1:123456789012:encoder-configuration/
abcdABCDefgh",
        "name": "test-ec",
        "tags": {},
        "video": {
            "bitrate": 3500000,
            "framerate": 30,
            "height": 1080,
            "width": 1920
        }
    }
}
```

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener información sobre la API, consulte GetEncoderConfiguration en la Referencia de comandos de la AWS CLI.

`get-ingest-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ingest-configuration`.

AWS CLI

Obtención de información de configuración de ingesta

En el siguiente ejemplo de `get-ingest-configuration`, se obtiene la configuración de ingesta para un nombre de recurso de Amazon (ARN) de configuración de ingesta especificado.

```
aws ivs-realtime get-ingest-configuration \
    --arn arn:aws:ivs:us-west-2:123456789012:ingest-configuration/AbCdEfGh1234
```

Salida:

```
{
    "ingestConfiguration": {
        "name": "ingest1",
        "arn": "arn:aws:ivs:us-west-2:123456789012:ingest-configuration/
AbCdEfGh1234",
        "ingestProtocol": "RTMPS",
        "streamKey": "rt_123456789012_us-
west-2_AbCdEfGh1234_abcd1234efgh5678ijkl9012MNOP34",
        "stageArn": "",
        "participantId": "xyZ654abC321",
        "state": "INACTIVE",
        "userId": "",
        "tags": {}
    }
}
```

Para obtener más información, consulte Ingesta de transmisiones de IVS | Transmisión en tiempo real en la Guía del usuario de Servicio de vídeos interactivos de Amazon.

- Para obtener información sobre la API, consulte GetIngestConfiguration en la Referencia de comandos de la AWS CLI.

`get-participant`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-participant`.

AWS CLI

Ejemplo 1: Obtención de un participante de la etapa

En el siguiente ejemplo de `get-participant`, se obtiene al participante de la fase para un ID de participante y un ID de sesión específicos en el ARN (Nombre de recurso de Amazon) de la fase especificada.

```
aws ivs-realtime get-participant \
    --stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --session-id st-a1b2c3d4e5f6g \
    --participant-id abCDEf12GHIj
```

Salida:

```
{
```

```
    "participant": {
        "browserName": "Google Chrome",
        "browserVersion": "116",
        "firstJoinTime": "2023-04-26T20:30:34+00:00",
        "ispName": "Comcast",
        "osName": "Microsoft Windows 10 Pro",
        "osVersion": "10.0.19044",
        "participantId": "abCDEf12GHIj",
        "published": true,
        "recordingS3BucketName": "bucket-name",
        "recordingS3Prefix": "abcdABCDefgh/st-a1b2c3d4e5f6g/
abCDEf12GHIj/1234567890",
        "recordingState": "ACTIVE",
        "sdkVersion": "",
        "state": "CONNECTED",
        "userId": ""
    }
}
```

Para obtener más información, consulte Habilitación de varios hosts en un flujo de Amazon IVS en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

Ejemplo 2: Obtención de un participante de la etapa que se haya replicado en otra etapa

En el siguiente ejemplo de `get-participant`, se obtiene al participante de la fase para un ID de participante y un ID de sesión específicos en el ARN (Nombre de recurso de Amazon) de la fase especificada, cuando se ha replicado al participante en otra etapa.

```
aws ivs-realtime get-participant \
    --stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --session-id st-a1b2c3d4e5f6g \
    --participant-id abCDEf12GHIj
```

Salida:

```
{
    "participant": {
        "browserName": "Google Chrome",
        "browserVersion": "116",
        "firstJoinTime": "2023-04-26T20:30:34+00:00",
        "ispName": "Comcast",
        "osName": "Microsoft Windows 10 Pro",
```

```
        "osVersion": "10.0.19044",
        "participantId": "abCDEf12GHIj",
        "published": true,
        "recordingS3BucketName": "bucket-name",
        "recordingS3Prefix": "abcdABCDefgh/st-a1b2c3d4e5f6g/
abCDEf12GHIj/1234567890",
        "recordingState": "ACTIVE",
        "replicationState": "ACTIVE",
        "replicationType": "SOURCE",
        "sdkVersion": "",
        "state": "CONNECTED",
        "userId": ""
    }
}
```

Para obtener más información, consulte Habilitación de varios hosts en un flujo de Amazon IVS en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

Ejemplo 3: Obtención de un participante de la etapa que se haya replicado desde otra etapa

En el siguiente ejemplo de `get-participant`, se obtiene al participante de la etapa para un ID de participante y un ID de sesión específicos en el ARN (Nombre de recurso de Amazon) de la etapa especificada, cuando se ha replicado al participante en otra etapa.

```
aws ivs-realtime get-participant \
    --stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --session-id st-a1b2c3d4e5f6g \
    --participant-id abCDEf12GHIj
```

Salida:

```
{
    "participant": {
        "browserName": "Google Chrome",
        "browserVersion": "116",
        "firstJoinTime": "2023-04-26T20:30:34+00:00",
        "ispName": "Comcast",
        "osName": "Microsoft Windows 10 Pro",
        "osVersion": "10.0.19044",
        "participantId": "abCDEf12GHIj",
        "published": true,
        "recordingS3BucketName": "bucket-name",
```

```
        "recordingS3Prefix": "abcdABCDefgh/st-a1b2c3d4e5f6g/
abCDEf12GHIj/1234567890",
        "recordingState": "ACTIVE",
        "replicationState": "ACTIVE",
        "replicationType": "REPLICA",
        "sdkVersion": "",
        "state": "CONNECTED",
        "userId": ""
    }
}
```

Para obtener más información, consulte Habilitación de varios hosts en un flujo de Amazon IVS en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte GetParticipant en la Referencia de comandos de la AWS CLI.

`get-public-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-public-key`.

AWS CLI

Para obtener una clave pública existente que se utilice para firmar los tokens de los participantes de la fase

En el siguiente ejemplo de `get-public-key`, se obtiene una clave pública especificada por el ARN proporcionado para firmar los tokens de los participantes de la fase.

```
aws ivs-realtime get-public-key \
    --arn arn:aws:ivs:us-west-2:123456789012:public-key/abcdABC1efg2
```

Salida:

```
{
    "publicKey": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:public-key/abcdABC1efg2",
        "name": "",
        "publicKeyMaterial": "-----BEGIN PUBLIC KEY-----
\nMHYwEAYHKoZIzj0CAQYFK4EEACIDYgAEqVWUtqs6EktQMR1sCYmEzGvRwtaycI16\n9pmzcpiWu/
uhNStGlteJ5odRfRwVkoQUMnSZXTCcbn9bBTTmiWo4mJcFOOAzsthH
\n0UAb8NdD4tUE0At4a9hYP9IETEXAMPLE\n-----END PUBLIC KEY-----",
```

```
        "fingerprint": "12:a3:44:56:bc:7d:e8:9f:10:2g:34:hi:56:78:90:12",
        "tags": {}
    }
}
```

Para obtener más información, consulte Distribuir los tokens de participantes en la Guía del usuario de Transmisión en tiempo real de Amazon IVS.

- Para obtener información sobre la API, consulte GetPublicKey en la Referencia de comandos de la AWS CLI.

`get-stage-session`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-stage-session`.

AWS CLI

Para obtener una sesión de fase

En el siguiente ejemplo de `get-stage-session`, se obtiene la sesión de fase para un ID de sesión especificado de un ARN (Nombre de recurso de Amazon) de fase indicada.

```
aws ivs-realtime get-stage-session \
    --stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --session-id st-a1b2c3d4e5f6g
```

Salida:

```
{
    "stageSession": {
        "endTime": "2023-04-26T20:36:29+00:00",
        "sessionId": "st-a1b2c3d4e5f6g",
        "startTime": "2023-04-26T20:30:29.602000+00:00"
    }
}
```

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener información sobre la API, consulte GetStageSession en la Referencia de comandos de la AWS CLI.

get-stage

En el siguiente ejemplo de código, se muestra cómo utilizar `get-stage`.

AWS CLI

Para obtener la información de configuración de una fase

En el siguiente ejemplo de `get-stage`, se obtiene la sesión de fase para un ARN (Nombre de recurso de Amazon) de fase especificado.

```
aws ivs-realtime get-stage \
    --arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh
```

Salida:

```
{
    "stage": {
        "activeSessionId": "st-a1b2c3d4e5f6g",
        "arn": "arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh",
        "autoParticipantRecordingConfiguration": {
            "storageConfigurationArn": "",
            "mediaTypes": [
                "AUDIO_VIDEO"
            ],
            "thumbnailConfiguration": {
                "targetIntervalSeconds": 60,
                "storage": [
                    "SEQUENTIAL"
                ],
                "recordingMode": "DISABLED"
            },
            "recordingReconnectWindowSeconds": 0,
            "hlsConfiguration": {
                "targetSegmentDurationSeconds": 6
            },
            "recordParticipantReplicas": true
        },
        "endpoints": {
            "events": "wss://global.events.live-video.net",
            "rtmp": "rtmp://9x0y8z7s6t5u.global-contribute-staging.live-video.net/
app/",
```

```
            "rtmps": "rtmps://9x0y8z7s6t5u.global-contribute-staging.live-
video.net:443/app/",
            "whip": "https://9x0y8z7s6t5u.global-bm.whip.live-video.net"
        },
        "name": "test",
        "tags": {}
    }
}
```

Para obtener más información, consulte Habilitación de varios hosts en un flujo de Amazon IVS en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte GetStage en la Referencia de comandos de la AWS CLI.

`get-storage-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-storage-configuration`.

AWS CLI

Para obtener una configuración del almacenamiento de composición

En el siguiente ejemplo de `get-storage-configuration`, se obtiene la configuración del almacenamiento de composición especificada por el ARN (Nombre de recurso de Amazon) indicado.

```
aws ivs-realtime get-storage-configuration \
    --name arn "arn:aws:ivs:ap-northeast-1:123456789012:storage-configuration/
abcdABCDefgh"
```

Salida:

```
{
    "storageConfiguration": {
        "arn": "arn:aws:ivs:ap-northeast-1:123456789012:storage-configuration/
abcdABCDefgh",
        "name": "test-sc",
        "s3": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "tags": {}
```

```
    }
}
```

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener información sobre la API, consulte GetStorageConfiguration en la Referencia de comandos de la AWS CLI.

`import-public-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-public-key`.

AWS CLI

Para importar una clave pública existente que se utilice para firmar los tokens de los participantes de la fase

En el siguiente ejemplo de `import-public-key`, se importa una clave pública de un archivo de material para utilizarla para firmar los tokens de los participantes de la fase.

```
aws ivs-realtime import-public-key \
    --public-key-material="`cat public.pem`"
```

Salida:

```
{
    "publicKey": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:public-key/abcdABC1efg2",
        "name": "",
        "publicKeyMaterial": "-----BEGIN PUBLIC KEY-----
\nMHYwEAYHKoZIzj0CAQYFK4EEACIDYgAEqVWUtqs6EktQMR1sCYmEzGvRwtaycI16\n9pmzcpiWu/
uhNStGlteJ5odRfRwVkoQUMnSZXTCcbn9bBTTmiWo4mJcFOOAzsthH
\n0UAb8NdD4tUE0At4a9hYP9IETEXAMPLE\n-----END PUBLIC KEY-----",
        "fingerprint": "12:a3:44:56:bc:7d:e8:9f:10:2g:34:hi:56:78:90:12",
        "tags": {}
    }
}
```

Para obtener más información, consulte Distribuir los tokens de participantes en la Guía del usuario de Transmisión en tiempo real de Amazon IVS.

- Para obtener información sobre la API, consulte ImportPublicKey en la Referencia de comandos de la AWS CLI.

`list-compositions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-compositions`.

AWS CLI

Para obtener una lista de composiciones

En el siguiente ejemplo de `list-compositions`, se enumeran todas las composiciones de la cuenta de AWS en la región de AWS en la que se procesa la solicitud de la API.

```
aws ivs-realtime list-compositions
```

Salida:

```
{
    "compositions": [
        {
            "arn": "arn:aws:ivs:ap-northeast-1:123456789012:composition/
abcdABCDefgh",
            "destinations": [
                {
                    "id": "AabBCcdDEefF",
                    "startTime": "2023-10-16T23:25:23+00:00",
                    "state": "ACTIVE"
                }
            ],
            "stageArn": "arn:aws:ivs:ap-northeast-1:123456789012:stage/
defgABCDabcd",
            "startTime": "2023-10-16T23:25:21+00:00",
            "state": "ACTIVE",
            "tags": {}
        },
        {
            "arn": "arn:aws:ivs:ap-northeast-1:123456789012:composition/
ABcdabCDefgh",
            "destinations": [
                {
                    "endTime": "2023-10-16T23:25:00.786512+00:00",
```

```
                    "id": "aABbcCDdeEFf",
                    "startTime": "2023-10-16T23:24:01+00:00",
                    "state": "STOPPED"
                },
                {
                    "endTime": "2023-10-16T23:25:00.786512+00:00",
                    "id": "deEFfaABbcCD",
                    "startTime": "2023-10-16T23:24:01+00:00",
                    "state": "STOPPED"
                }
            ],
            "endTime": "2023-10-16T23:25:00+00:00",
            "stageArn": "arn:aws:ivs:ap-northeast-1:123456789012:stage/
efghabcdABCD",
            "startTime": "2023-10-16T23:24:00+00:00",
            "state": "STOPPED",
            "tags": {}
        }
    ]
}
```

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener información sobre la API, consulte ListCompositions en la Referencia de comandos de la AWS CLI.

`list-encoder-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-encoder-configurations`.

AWS CLI

Para enumerar las configuraciones de los codificadores de composición

En el siguiente ejemplo de `list-encoder-configurations`, se enumeran todas las composiciones del codificador de composición de AWS en la región de AWS en la que se procesa la solicitud de la API.

```
aws ivs-realtime list-encoder-configurations
```

Salida:

```
{
    "encoderConfigurations": [
        {
            "arn": "arn:aws:ivs:ap-northeast-1:123456789012:encoder-configuration/
abcdABCDefgh",
            "name": "test-ec-1",
            "tags": {}
        },
        {
            "arn": "arn:aws:ivs:ap-northeast-1:123456789012:encoder-configuration/
ABCefgEFGabc",
            "name": "test-ec-2",
            "tags": {}
        }
    ]
}
```

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener más información sobre la API, consulte ListEncoderConfigurations en la Referencia de comandos de la AWS CLI.

`list-ingest-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-ingest-configurations`.

AWS CLI

Obtención de información resumida sobre todas las configuraciones de ingesta

En el siguiente ejemplo de `list-ingest-configurations`, se muestran todas las configuraciones de ingesta para la cuenta de AWS, en la región de AWS en la que se procesa la solicitud de la API.

```
aws ivs-realtime list-ingest-configurations
```

Salida:

```
{
```

```
    "ingestConfigurations": [
        {
            "name": "",
            "arn": "arn:aws:ivs:us-west-2:123456789012:ingest-configuration/
XYZuvwSt4567",
            "ingestProtocol": "RTMPS",
            "stageArn": "arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh",
            "participnatId": "abC789Xyz456",
            "state": "INACTIVE"
            "userId": "",
        }
    ]
}
```

Para obtener más información, consulte Ingesta de transmisiones de IVS | Transmisión en tiempo real en la Guía del usuario de Servicio de vídeos interactivos de Amazon.

- Para obtener información sobre la API, consulte ListIngestConfigurations en la Referencia de comandos de la AWS CLI.

`list-participant-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-participant-events`.

AWS CLI

Ejemplo 1: Obtención de una lista de los eventos de los participantes de la etapa

En el siguiente ejemplo de `list-participant-events`, se enumeran todos los eventos de participantes de un ID de participante y un ID de sesión específicos de un ARN (Nombre de recurso de Amazon) de etapa especificado.

```
aws ivs-realtime list-participant-events \
    --stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --session-id st-a1b2c3d4e5f6g \
    --participant-id abCDEf12GHIj
```

Salida:

```
{
    "events": [
```

```
        {
            "eventTime": "2023-04-26T20:36:28+00:00",
            "name": "LEFT",
            "participantId": "abCDEf12GHIj"
        },
        {
            "eventTime": "2023-04-26T20:36:28+00:00",
            "name": "PUBLISH_STOPPED",
            "participantId": "abCDEf12GHIj"
        },
        {
            "eventTime": "2023-04-26T20:30:34+00:00",
            "name": "JOINED",
            "participantId": "abCDEf12GHIj"
        },
        {
            "eventTime": "2023-04-26T20:30:34+00:00",
            "name": "PUBLISH_STARTED",
            "participantId": "abCDEf12GHIj"
        }
    ]
}
```

Para obtener más información, consulte Habilitación de varios hosts en un flujo de Amazon IVS en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

Ejemplo 2: Obtención de una lista de los eventos de los participantes de la etapa, incluidos el inicio y la detención de la replicación de participantes

En el siguiente ejemplo de `list-participant-events`, se muestran todos los eventos de participantes de un ID de sesión específico de un ARN (Nombre de recurso de Amazon) de etapa especificado, donde un participante se ha replicado en otra etapa.

```
aws ivs-realtime list-participant-events \
    --stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --session-id st-a1b2c3d4e5f6g \
    --participant-id abCDEf12GHIj
```

Salida:

```
{
    "events": [
```

```
        {
            "eventTime": "2025-04-26T20:36:28+00:00",
            "name": "LEFT",
            "participantId": "abCDEf12GHIj"
        },
        {
            "eventTime": "2025-04-26T20:36:28+00:00",
            "name": "PUBLISH_STOPPED",
            "participantId": "abCDEf12GHIj"
        },
        {
            "eventTime": "2025-04-26T20:30:34+00:00",
            "name": "JOINED",
            "participantId": "abCDEf12GHIj"
        },
        {
            "eventTime": "2025-04-26T20:30:34+00:00",
            "name": "PUBLISH_STARTED",
            "participantId": "abCDEf12GHIj"
        },
        {
            "name": "REPLICATION_STARTED",
            "participantId": "abCDEf12GHIj",
            "eventTime": "2025-04-26T20:30:34+00:00",
            "destinationStageArn": "arn:aws:ivs:us-west-2:12345678901:stage/
ABCDabcdefgh",
            "destinationSessionId": "st-b1c2d3e4f5g6a"
        },
        {
            "name": "REPLICATION_STOPPED",
            "participantId": "abCDEf12GHIj",
            "eventTime": "2025-04-26T20:32:34+00:00",
            "destinationStageArn": "arn:aws:ivs:us-west-2:12345678901:stage/
ABCDabcdefgh",
            "destinationSessionId": "st-b1c2d3e4f5g6a"
        }
    ]
}
```

Para obtener más información, consulte Habilitación de varios hosts en un flujo de Amazon IVS en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte ListParticipantEvents en la Referencia de comandos de la AWS CLI.

`list-participant-replicas`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-participant-replicas`.

AWS CLI

Obtención de una lista de réplicas de los participantes de la etapa

En el siguiente ejemplo de `list-participant-replicas`, se muestran todos los participantes de la etapa replicados desde el ARN (Nombre de recurso de Amazon) de la etapa de origen especificado a otra etapa.

```
aws ivs-realtime list-participant-replicas \
    --source-stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --participant-id abCDEf12GHIj
```

Salida:

```
{
    "replicas": [
        {
            "sourceStageArn": "arn:aws:ivs:us-west-2:123456789012:stage/
abcdABCDefgh",
            "participantId": "abCDEf12GHIj",
            "sourceSessionId": "st-a1b2c3d4e5f6g",
            "destinationStageArn": "arn:aws:ivs:us-west-2:012345678901:stage/
ABCDabcdefgh",
            "destinationSessionId": "st-b1c2d3e4f5g6a",
            "replicationState": "ACTIVE"
        }
    ]
}
```

Para obtener más información, consulte Replicación de participantes de IVS en la Guía del usuario de Transmisión en tiempo real de Amazon IVS.

- Para obtener información sobre la API, consulte ListParticipantReplicas en la Referencia de comandos de la AWS CLI.

`list-participants`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-participants`.

AWS CLI

Ejemplo 1: Obtención de una lista de los participantes de la etapa

En el siguiente ejemplo de `list-participants`, se enumeran todos los participantes de un ID de sesión indicado de un ARN (Nombre de recurso de Amazon) de etapa especificado.

```
aws ivs-realtime list-participants \
    --stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --session-id st-a1b2c3d4e5f6g
```

Salida:

```
{
    "participants": [
        {
            "firstJoinTime": "2023-04-26T20:30:34+00:00",
            "participantId": "abCDEf12GHIj",
            "published": true,
            "recordingState": "STOPPED",
            "state": "DISCONNECTED",
            "userId": ""
        }
    ]
}
```

Para obtener más información, consulte Habilitación de varios hosts en un flujo de Amazon IVS en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

Ejemplo 2: Obtención de una lista de los participantes de la etapa, cuando un participante se ha replicado en otra etapa

En el siguiente ejemplo de `list-participants`, se muestran todos los participantes de un ID de sesión específico de un ARN (Nombre de recurso de Amazon) de etapa especificado, cuando un participante se ha replicado en otra etapa.

```
aws ivs-realtime list-participants \
    --stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --session-id st-a1b2c3d4e5f6g
```

Salida:

```
{
    "participants": [
        {
            "firstJoinTime": "2023-04-26T20:30:34+00:00",
            "participantId": "abCDEf12GHIj",
            "published": true,
            "recordingState": "STOPPED",
            "state": "DISCONNECTED",
            "userId": "",
            "replicationState": "ACTIVE",
            "replicationType": "SOURCE",
            "sourceStageArn": "",
            "sourceSessionId": ""
        }
    ]
}
```

Para obtener más información, consulte Habilitación de varios hosts en un flujo de Amazon IVS en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

Ejemplo 3: Obtención de una lista de los participantes de la etapa, cuando un participante se ha replicado desde otra etapa

En el siguiente ejemplo de `list-participants`, se muestran todos los participantes de un ID de sesión específico de un ARN (Nombre de recurso de Amazon) de etapa especificado, cuando un participante se ha replicado desde otra etapa.

```
aws ivs-realtime list-participants \
    --stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --session-id st-a1b2c3d4e5f6g
```

Salida:

```
{
    "participants": [
        {
            "firstJoinTime": "2023-04-26T20:30:34+00:00",
            "participantId": "abCDEf12GHIj",
            "published": true,
            "recordingState": "STOPPED",
            "state": "DISCONNECTED",
            "userId": "",
```

```
            "replicationState": "ACTIVE",
            "replicationType": "REPLICA",
            "sourceStageArn": "arn:aws:ivs:us-west-2:123456789012:stage/
abcdABCDefgh",
            "sourceSessionId": "st-a1b2c3d4e5f6g"
        }
    ]
}
```

Para obtener más información, consulte Habilitación de varios hosts en un flujo de Amazon IVS en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener información sobre la API, consulte ListParticipants en la Referencia de comandos de la AWS CLI.

`list-public-keys`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-public-keys`.

AWS CLI

Para enumerar las claves públicas existentes disponibles para firmar los tokens de los participantes de la fase

En el siguiente ejemplo de `list-public-keys`, se enumeran todas las claves públicas disponibles para firmar los tokens de los participantes en la fase en la región de AWS donde se procesa la solicitud de la API.

```
aws ivs-realtime list-public-keys
```

Salida:

```
{
    "publicKeys": [
        {
            "arn": "arn:aws:ivs:us-west-2:123456789012:public-key/abcdABC1efg2",
            "name": "",
            "tags": {}
        },
        {
            "arn": "arn:aws:ivs:us-west-2:123456789012:public-key/3bcdABCDefg4",
            "name": "",
```

```
            "tags": {}
        }
    ]
}
```

Para obtener más información, consulte Distribuir los tokens de participantes en la Guía del usuario de Transmisión en tiempo real de Amazon IVS.

- Para obtener detalles de la API, consulte ListPublicKeys en la Referencia de comandos de la AWS CLI.

`list-stage-sessions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-stage-sessions`.

AWS CLI

Para obtener una lista de las sesiones de la fase

En el siguiente ejemplo de `list-stage-sessions`, se enumeran todas las sesiones de un ARN (Nombre de recurso de Amazon) de etapa especificado.

```
aws ivs-realtime list-stage-sessions \
    --stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh
```

Salida:

```
{
    "stageSessions": [
        {
            "endTime": "2023-04-26T20:36:29+00:00",
            "sessionId": "st-a1b2c3d4e5f6g",
            "startTime": "2023-04-26T20:30:29.602000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener información sobre la API, consulte ListStageSessions en la Referencia de comandos de la AWS CLI.

`list-stages`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-stages`.

AWS CLI

Para obtener información resumida sobre todas las fases

En el siguiente ejemplo de `list-stages`, se enumeran todas las etapas de la cuenta de AWS en la región de AWS en la que se procesa la solicitud de la API.

```
aws ivs-realtime list-stages
```

Salida:

```
{
    "stages": [
        {
            "activeSessionId": "st-a1b2c3d4e5f6g",
            "arn": "arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh",
            "name": "stage1",
            "tags": {}
        },
        {
            "activeSessionId": "st-a123bcd456efg",
            "arn": "arn:aws:ivs:us-west-2:123456789012:stage/abcd1234ABCD",
            "name": "stage2",
            "tags": {}
        },
        {
            "activeSessionId": "st-abcDEF1234ghi",
            "arn": "arn:aws:ivs:us-west-2:123456789012:stage/ABCD1234efgh",
            "name": "stage3",
            "tags": {}
        }
    ]
}
```

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener información sobre la API, consulte ListStages en la Referencia de comandos de la AWS CLI.

`list-storage-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-storage-configurations`.

AWS CLI

Para enumerar las configuraciones de almacenamiento de composición

En el siguiente ejemplo de `list-storage-configurations`, se enumeran todas las configuraciones del almacenamiento de composición de la cuenta de AWS en la región de AWS en la que se procesa la solicitud de la API.

```
aws ivs-realtime list-storage-configurations
```

Salida:

```
{
    "storageConfigurations": [
        {
            "arn": "arn:aws:ivs:ap-northeast-1:123456789012:storage-configuration/
abcdABCDefgh",
            "name": "test-sc-1",
            "s3": {
                "bucketName": "amzn-s3-demo-bucket-1"
            },
            "tags": {}
        },
        {
            "arn": "arn:aws:ivs:ap-northeast-1:123456789012:storage-configuration/
ABCefgEFGabc",
            "name": "test-sc-2",
            "s3": {
                "bucketName": "amzn-s3-demo-bucket-2"
            },
            "tags": {}
        }
    ]
}
```

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener más información sobre la API, consulte ListStorageConfigurations en la Referencia de comandos de la AWS CLI.

`start-composition`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-composition`.

AWS CLI

Ejemplo 1: iniciar una composición con los ajustes de diseño predeterminados

En el siguiente ejemplo de `start-composition`, se inicia una composición para la etapa especificada que se va a transmitir a las ubicaciones indicadas.

```
aws ivs-realtime start-composition \
    --stage-arn arn:aws:ivs:ap-northeast-1:123456789012:stage/defgABCDabcd \
    --destinations '[{"channel": {"channelArn": "arn:aws:ivs:ap-
northeast-1:123456789012:channel/abcABCdefDEg", \
        "encoderConfigurationArn": "arn:aws:ivs:ap-northeast-1:123456789012:encoder-
configuration/ABabCDcdEFef"}}, \
        {"s3":{"encoderConfigurationArns":["arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"], \
        "recordingConfiguration": {"hlsConfiguration":
 {"targetSegmentDurationSeconds": 5}}, \
        "storageConfigurationArn":"arn:aws:ivs:ap-northeast-1:123456789012:storage-
configuration/FefABabCDcdE"}}]'
```

Salida:

```
{
    "composition": {
        "arn": "arn:aws:ivs:ap-northeast-1:123456789012:composition/abcdABCDefgh",
        "destinations": [
            {
                "configuration": {
                    "channel": {
                        "channelArn": "arn:aws:ivs:ap-
northeast-1:123456789012:channel/abcABCdefDEg",
                        "encoderConfigurationArn": "arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"
                    },
                    "name": ""
```

```
                },
                "id": "AabBCcdDEefF",
                "state": "STARTING"
            },
            {
                "configuration": {
                    "name": "",
                    "s3": {
                        "encoderConfigurationArns": [
                            "arn:aws:ivs:arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"
                        ],
                        "recordingConfiguration": {
                            "format": "HLS",
                            "hlsConfiguration": {
                                "targetSegmentDurationSeconds": 5
                            }
                        },
                        "storageConfigurationArn": "arn:arn:aws:ivs:ap-
northeast-1:123456789012:storage-configuration/FefABabCDcdE"
                    }
                },
                "detail": {
                    "s3": {
                        "recordingPrefix": "aBcDeFgHhGfE/AbCdEfGhHgFe/GHFabcgefABC/
composite"
                    }
                },
                "id": "GHFabcgefABC",
                "state": "STARTING"
            }
        ],
        "layout": {
            "grid": {
                "featuredParticipantAttribute": ""
                "gridGap": 2,
                "omitStoppedVideo": false,
                "participantOrderAttribute": "",
                "videoAspectRatio": "VIDEO",
                "videoFillMode": ""
            }
        },
        "stageArn": "arn:aws:ivs:ap-northeast-1:123456789012:stage/defgABCDabcd",
        "startTime": "2023-10-16T23:24:00+00:00",
```

```
        "state": "STARTING",
        "tags": {}
    }
}
```

Para obtener más información, consulte Grabación compuesta de IVS | Transmisión en tiempo real en la Guía del usuario de Amazon Interactive Video Service.

Ejemplo 2: iniciar una composición con los ajustes de diseño predeterminados

En el siguiente ejemplo de `start-composition`, se inicia una composición para la etapa especificada que se va a transmitir a las ubicaciones indicadas con el diseño predeterminado.

```
aws ivs-realtime start-composition \
    --stage-arn arn:aws:ivs:ap-northeast-1:123456789012:stage/defgABCDabcd \
    --destinations '[{"channel": {"channelArn": "arn:aws:ivs:ap-
northeast-1:123456789012:channel/abcABCdefDEg", \
        "encoderConfigurationArn": "arn:aws:ivs:ap-northeast-1:123456789012:encoder-
configuration/ABabCDcdEFef"}}, \
        {"s3":{"encoderConfigurationArns":["arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"], \
        "storageConfigurationArn":"arn:aws:ivs:ap-northeast-1:123456789012:storage-
configuration/FefABabCDcdE"}}]' \
    --layout pip='{featuredParticipantAttribute="abcdefg"}'
```

Salida:

```
{
    "composition": {
        "arn": "arn:aws:ivs:ap-northeast-1:123456789012:composition/wxyzWXYZpqrs",
        "destinations": [
            {
                "configuration": {
                    "channel": {
                        "channelArn": "arn:aws:ivs:ap-
northeast-1:123456789012:channel/abcABCdefDEg",
                        "encoderConfigurationArn": "arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"
                    },
                    "name": ""
                },
                "id": "AabBCcdDEefF",
                "state": "STARTING"
```

```
            },
            {
                "configuration": {
                    "name": "",
                    "s3": {
                        "encoderConfigurationArns": [
                            "arn:aws:ivs:arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"
                        ],
                        "recordingConfiguration": {
                            "format": "HLS",
                            "hlsConfiguration": {
                                "targetSegmentDurationSeconds": 2
                            }
                        },
                        "storageConfigurationArn": "arn:arn:aws:ivs:ap-
northeast-1:123456789012:storage-configuration/FefABabCDcdE"
                    }
                },
                "detail": {
                    "s3": {
                        "recordingPrefix": "aBcDeFgHhGfE/AbCdEfGhHgFe/GHFabcgefABC/
composite"
                    }
                },
                "id": "GHFabcgefABC",
                "state": "STARTING"
            }
        ],
        "layout": {
            "pip": {
                "featuredParticipantAttribute": "abcdefg",
                "gridGap": 0,
                "omitStoppedVideo": false,
                "participantOrderAttribute": "",
                "pipBehavior": "STATIC",
                "pipOffset": 0,
                "pipParticipantAttribute": "",
                "pipPosition": "BOTTOM_RIGHT",
                "videoFillMode": "COVER"
            }
        },
        "stageArn": "arn:aws:ivs:ap-northeast-1:123456789012:stage/defgABCDabcd",
        "startTime": "2023-10-16T23:24:00+00:00",
```

```
        "state": "STARTING",
        "tags": {}
    }
}
```

Para obtener más información, consulte Grabación compuesta de IVS | Transmisión en tiempo real en la Guía del usuario de Amazon Interactive Video Service.

Ejemplo 3: inicio de una composición con la grabación de miniaturas habilitada

En el siguiente ejemplo de `start-composition`, se inicia una composición para la etapa especificada que se va a transmitir a las ubicaciones indicadas con la grabación de miniaturas habilitada.

```
aws ivs-realtime start-composition \
    --stage-arn arn:aws:ivs:ap-northeast-1:123456789012:stage/defgABCDabcd \
    --destinations '[{"channel": {"channelArn": "arn:aws:ivs:ap-
northeast-1:123456789012:channel/abcABCdefDEg", \
        "encoderConfigurationArn": "arn:aws:ivs:ap-northeast-1:123456789012:encoder-
configuration/ABabCDcdEFef"}}, \
        {"s3": {"encoderConfigurationArns": ["arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"], \
        "storageConfigurationArn": "arn:aws:ivs:ap-northeast-1:123456789012:storage-
configuration/FefABabCDcdE", \
        "thumbnailConfigurations": [{"storage":
 ["SEQUENTIAL"],"targetIntervalSeconds": 60}]}}]'
```

Salida:

```
{
    "composition": {
        "arn": "arn:aws:ivs:ap-northeast-1:123456789012:composition/abcdABCDefgh",
        "destinations": [
            {
                "configuration": {
                    "channel": {
                        "channelArn": "arn:aws:ivs:ap-
northeast-1:123456789012:channel/abcABCdefDEg",
                        "encoderConfigurationArn": "arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"
                    },
                    "name": ""
                },
```

```
                "id": "AabBCcdDEefF",
                "state": "STARTING"
            },
            {
                "configuration": {
                    "name": "",
                    "s3": {
                        "encoderConfigurationArns": [
                            "arn:aws:ivs:arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"
                        ],
                        "recordingConfiguration": {
                            "format": "HLS",
                            "hlsConfiguration": {
                                "targetSegmentDurationSeconds": 2
                            }
                        },
                        "storageConfigurationArn": "arn:arn:aws:ivs:ap-
northeast-1:123456789012:storage-configuration/FefABabCDcdE",
                        "thumbnailConfigurations": [
                           {
                              "targetIntervalSeconds": 60,
                              "storage": [
                                  "SEQUENTIAL"
                              ]
                           }
                        ]
                    }
                },
                "detail": {
                    "s3": {
                        "recordingPrefix": "aBcDeFgHhGfE/AbCdEfGhHgFe/GHFabcgefABC/
composite"
                    }
                },
                "id": "GHFabcgefABC",
                "state": "STARTING"
            }
        ],
        "layout": {
            "grid": {
                "featuredParticipantAttribute": ""
                "gridGap": 2,
                "omitStoppedVideo": false,
```

```
                "participantOrderAttribute": "",
                "videoAspectRatio": "VIDEO",
                "videoFillMode": ""
            }
        },
        "stageArn": "arn:aws:ivs:ap-northeast-1:123456789012:stage/defgABCDabcd",
        "startTime": "2023-10-16T23:24:00+00:00",
        "state": "STARTING",
        "tags": {}
    }
}
```

Para obtener más información, consulte Grabación compuesta de IVS | Transmisión en tiempo real en la Guía del usuario de Amazon Interactive Video Service.

Ejemplo 4: Para iniciar una composición mediante un diseño de cuadrícula con un orden personalizado de los participantes

En el siguiente ejemplo de `start-composition`, se inicia una composición para la etapa especificada que se va a transmitir a las ubicaciones indicadas mediante el diseño de cuadrícula con el orden personalizado de los participantes.

```
aws ivs-realtime start-composition \
    --stage-arn arn:aws:ivs:ap-northeast-1:123456789012:stage/defgABCDabcd \
    --destinations '[{"channel": {"channelArn": "arn:aws:ivs:ap-
northeast-1:123456789012:channel/abcABCdefDEg", \
        "encoderConfigurationArn": "arn:aws:ivs:ap-northeast-1:123456789012:encoder-
configuration/ABabCDcdEFef"}}, \
        {"s3": {"encoderConfigurationArns": ["arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"], \
        "storageConfigurationArn": "arn:aws:ivs:ap-northeast-1:123456789012:storage-
configuration/FefABabCDcdE", \
        "thumbnailConfigurations": [{"storage":
 ["SEQUENTIAL"],"targetIntervalSeconds": 60}]}}]' \
    --layout grid='{participantOrderAttribute="abcdefg"}'
```

Salida:

```
{
    "composition": {
        "arn": "arn:aws:ivs:ap-northeast-1:123456789012:composition/abcdABCDefgh",
        "destinations": [
```

```
            {
                "configuration": {
                    "channel": {
                        "channelArn": "arn:aws:ivs:ap-
northeast-1:123456789012:channel/abcABCdefDEg",
                        "encoderConfigurationArn": "arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"
                    },
                    "name": ""
                },
                "id": "AabBCcdDEefF",
                "state": "STARTING"
            },
            {
                "configuration": {
                    "name": "",
                    "s3": {
                        "encoderConfigurationArns": [
                            "arn:aws:ivs:arn:aws:ivs:ap-
northeast-1:123456789012:encoder-configuration/ABabCDcdEFef"
                        ],
                        "recordingConfiguration": {
                            "format": "HLS",
                            "hlsConfiguration": {
                                "targetSegmentDurationSeconds": 2
                            }
                        },
                        "storageConfigurationArn": "arn:arn:aws:ivs:ap-
northeast-1:123456789012:storage-configuration/FefABabCDcdE",
                        "thumbnailConfigurations": [
                           {
                              "targetIntervalSeconds": 60,
                              "storage": [
                                  "SEQUENTIAL"
                              ]
                           }
                        ]
                    }
                },
                "detail": {
                    "s3": {
                        "recordingPrefix": "aBcDeFgHhGfE/AbCdEfGhHgFe/GHFabcgefABC/
composite"
                    }
```

```
                },
                "id": "GHFabcgefABC",
                "state": "STARTING"
            }
        ],
        "layout": {
            "grid": {
                "featuredParticipantAttribute": ""
                "gridGap": 2,
                "omitStoppedVideo": false,
                "participantOrderAttribute": "abcdefg",
                "videoAspectRatio": "VIDEO",
                "videoFillMode": ""
            }
        },
        "stageArn": "arn:aws:ivs:ap-northeast-1:123456789012:stage/defgABCDabcd",
        "startTime": "2023-10-16T23:24:00+00:00",
        "state": "STARTING",
        "tags": {}
    }
}
```

Para obtener más información, consulte Grabación compuesta de IVS | Transmisión en tiempo real en la Guía del usuario de Amazon Interactive Video Service.

- Para obtener información sobre la API, consulte StartComposition en la Referencia de comandos de la AWS CLI.

`start-participant-replication`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-participant-replication`.

AWS CLI

Inicio de la replicación de un participante de una etapa a otra

El siguiente ejemplo de `start-participant-replication`, replica un participante de una etapa de origen a una etapa de destino, donde cada etapa se especifica mediante su ARN (Nombre de recurso de Amazon).

```
aws ivs-realtime start-participant-replication \
    --source-stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --destination-stage-arn arn:aws:ivs:us-west-2:234567890123:stage/bcdABCDefghi \
```

```
    --participant-id abCDEf12GHIj
```

Salida:

```
{
    "accessControlAllowOrigin": "*",
    "accessControlExposeHeaders": "Access-Control-Allow-Origin,Access-Control-
Expose-Headers,Cache-Control,Content-Length, \
    Content-Security-Policy,Content-Type,date,Strict-Transport-Security,x-amz-apigw-
id,x-amzn-errormessage,x-amzn-errortype, \
    x-amzn-requestid,x-amzn-trace-id,X-Content-Type-Options,X-Frame-Options",
    "cacheControl": "no-store, no-cache",
    "contentSecurityPolicy": "default-src 'self'; upgrade-insecure-requests;",
    "strictTransportSecurity": "max-age:47304000; includeSubDomains",
    "xContentTypeOptions": "nosniff",
    "xFrameOptions": "DENY"
}
```

Para obtener más información, consulte Replicación de participantes de IVS en la Guía del usuario de Transmisión en tiempo real de Amazon IVS.

- Para obtener información sobre la API, consulte StartParticipantReplication en la Referencia de comandos de la AWS CLI.

`stop-composition`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-composition`.

AWS CLI

Para detener una composición

En el siguiente ejemplo de `stop-composition`, se detiene la composición especificada por el ARN (Nombre de recurso de Amazon) indicado.

```
aws ivs-realtime stop-composition \
    --arn "arn:aws:ivs:ap-northeast-1:123456789012:composition/abcdABCDefgh"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Habilitación de varios hosts en una transmisión de Amazon IVS en la Guía del usuario de Amazon IVS.

- Para obtener información sobre la API, consulte StopComposition en la Referencia de comandos de la AWS CLI.

`stop-participant-replication`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-participant-replication`.

AWS CLI

Detención de la replicación de un participante de una etapa a otra

En el siguiente ejemplo de `stop-participant-replication`, se detiene la replicación de un participante desde una etapa de origen a una etapa de destino, donde cada etapa se especifica mediante su ARN (Nombre de recurso de Amazon).

```
aws ivs-realtime stop-participant-replication \
    --source-stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --destination-stage-arn arn:aws:ivs:us-west-2:234567890123:stage/bcdABCDefghi \
    --participant-id abCDEf12GHIj
```

Salida:

```
{
    "accessControlAllowOrigin": "*",
    "accessControlExposeHeaders": "Access-Control-Allow-Origin,Access-Control-
Expose-Headers,Cache-Control,Content-Length, \
    Content-Security-Policy,Content-Type,date,Strict-Transport-Security,x-amz-apigw-
id,x-amzn-errormessage,x-amzn-errortype, \
    x-amzn-requestid,x-amzn-trace-id,X-Content-Type-Options,X-Frame-Options",
    "cacheControl": "no-store, no-cache",
    "contentSecurityPolicy": "default-src 'self'; upgrade-insecure-requests;",
    "strictTransportSecurity": "max-age:47304000; includeSubDomains",
    "xContentTypeOptions": "nosniff",
    "xFrameOptions": "DENY"
}
```

Para obtener más información, consulte Replicación de participantes de IVS en la Guía del usuario de Transmisión en tiempo real de Amazon IVS.

- Para obtener información sobre la API, consulte StopParticipantReplication en la Referencia de comandos de la AWS CLI.

`update-ingest-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-ingest-configuration`.

AWS CLI

Actualización de una configuración de ingesta

En el siguiente ejemplo de `update-inegst-configuration`, se actualiza una configuración de ingesta para adjuntarla a una etapa.

```
aws ivs-realtime update-ingest-configuration \
    --arn arn:aws:ivs:us-west-2:123456789012:ingest-configuration/AbCdEfGh1234 \
    --stage-arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh
```

Salida:

```
{
    "ingestConfiguration": {
        "name": "ingest1",
        "arn": "arn:aws:ivs:us-west-2:123456789012:ingest-configuration/
AbCdEfGh1234",
        "ingestProtocol": "RTMPS",
        "streamKey": "rt_123456789012_us-
west-2_AbCdEfGh1234_abcd1234efgh5678ijkl9012MNOP34",
        "stageArn": "arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh",
        "participantId": "xyZ654abC321",
        "state": "INACTIVE",
        "userId": "",
        "tags": {}
    }
}
```

Para obtener más información, consulte Ingesta de transmisiones de IVS | Transmisión en tiempo real en la Guía del usuario de Servicio de vídeos interactivos de Amazon.

- Para obtener información sobre la API, consulte UpdateIngestConfiguration en la Referencia de comandos de la AWS CLI.

`update-stage`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-stage`.

AWS CLI

Ejemplo 1: Actualización de la configuración de una etapa

En el siguiente ejemplo de `update-stage`, se actualiza una etapa para un ARN de etapa específico para actualizar el nombre de la etapa y configurar la grabación individual de los participantes con la grabación de miniaturas habilitada.

```
aws ivs-realtime update-stage \
    --arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --auto-participant-recording-configuration '{"mediaTypes":
 ["AUDIO_VIDEO"],"storageConfigurationArn": "arn:aws:ivs:us-
west-2:123456789012:storage-configuration/abcdABCDefgh",
 "recordingReconnectWindowSeconds": 100, \
        "thumbnailConfiguration": {"recordingMode": "INTERVAL","storage":
 ["SEQUENTIAL"],"targetIntervalSeconds": 60}} \
        "hlsConfiguration": {"targetSegmentDurationSeconds": 5}}' \
    --name stage1a
```

Salida:

```
{
    "stage": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh",
        "autoParticipantRecordingConfiguration": {
            "mediaTypes": [
                "AUDIO_VIDEO"
            ],
            "storageConfigurationArn": "arn:aws:ivs:us-west-2:123456789012:storage-
configuration/abcdABCDefgh",
            "thumbnailConfiguration": {
                "targetIntervalSeconds": 60,
                "storage": [
                    "SEQUENTIAL"
                ],
                "recordingMode": "INTERVAL"
            },
            "recordingReconnectWindowSeconds": 100,
            "hlsConfiguration": {
                "targetSegmentDurationSeconds": 5
            },
            "recordParticipantReplicas": true
        },
```

```
        "endpoints": {
            "events": "wss://global.events.live-video.net",
            "rtmp": "rtmp://9x0y8z7s6t5u.global-contribute-staging.live-video.net/
app/",
            "rtmps": "rtmps://9x0y8z7s6t5u.global-contribute-staging.live-
video.net:443/app/",
            "whip": "https://1a2b3c4d5e6f.global-bm.whip.live-video.net"
        },
        "name": "stage1a",
        "tags": {}
    }
}
```

Para obtener más información, consulte Habilitación de varios hosts en un flujo de Amazon IVS en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

Ejemplo 2: Actualización de la configuración de una etapa, incluida la desactivación de la grabación de réplicas de participantes

En el siguiente ejemplo de `update-stage`, se actualiza una etapa para un ARN de etapa específico para actualizar el nombre de la etapa y configurar la grabación individual de los participantes con la grabación de miniaturas habilitada y la grabación de réplicas de participantes desactivada.

```
aws ivs-realtime update-stage \
    --arn arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh \
    --auto-participant-recording-configuration '{"mediaTypes":
 ["AUDIO_VIDEO"],"storageConfigurationArn": "arn:aws:ivs:us-
west-2:123456789012:storage-configuration/abcdABCDefgh",
 "recordingReconnectWindowSeconds": 100, \
        "thumbnailConfiguration": {"recordingMode": "INTERVAL","storage":
 ["SEQUENTIAL"],"targetIntervalSeconds": 60}, "recordParticipantReplicas":false} \
        "hlsConfiguration": {"targetSegmentDurationSeconds": 5}}' \
    --name stage1a
```

Salida:

```
{
    "stage": {
        "arn": "arn:aws:ivs:us-west-2:123456789012:stage/abcdABCDefgh",
        "autoParticipantRecordingConfiguration": {
```

```
            "mediaTypes": [
                "AUDIO_VIDEO"
            ],
            "storageConfigurationArn": "arn:aws:ivs:us-west-2:123456789012:storage-
configuration/abcdABCDefgh",
            "thumbnailConfiguration": {
                "targetIntervalSeconds": 60,
                "storage": [
                    "SEQUENTIAL"
                ],
                "recordingMode": "INTERVAL"
            },
            "recordingReconnectWindowSeconds": 100,
            "hlsConfiguration": {
                "targetSegmentDurationSeconds": 5
            },
            "recordParticipantReplicas": false
        },
        "endpoints": {
            "events": "wss://global.events.live-video.net",
            "rtmp": "rtmp://9x0y8z7s6t5u.global-contribute-staging.live-video.net/
app/",
            "rtmps": "rtmps://9x0y8z7s6t5u.global-contribute-staging.live-
video.net:443/app/",
            "whip": "https://1a2b3c4d5e6f.global-bm.whip.live-video.net"
        },
        "name": "stage1a",
        "tags": {}
    }
}
```

Para obtener más información, consulte Habilitación de varios hosts en un flujo de Amazon IVS en la Guía del usuario de Transmisión de baja latencia de Amazon IVS.

- Para obtener más información sobre la API, consulte UpdateStage en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon Kendra que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon Kendra.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-data-source`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-data-source`.

AWS CLI

Para crear un conector de origen de datos de Amazon Kendra

En el siguiente ejemplo de `create-data-source`, se crea y configura un conector de origen de datos de Amazon Kendra. Puede utilizar `describe-data-source` para ver el estado de un conector de origen de datos y leer cualquier mensaje de error si el estado indica que un conector de origen de datos no se ha podido crear por completo (FAILED).

```
aws kendra create-data-source \
    --name "example data source 1" \
    --description "Example data source 1 for example index 1 contains the first set
 of example documents" \
    --tags '{"Key": "test resources", "Value": "kendra"}, {"Key": "test resources",
 "Value": "aws"}' \
    --role-arn "arn:aws:iam::my-account-id:role/
KendraRoleForS3TemplateConfigDataSource" \
    --index-id exampleindex1 \
    --language-code "es" \
    --schedule "0 0 18 ? * TUE,MON,WED,THU,FRI,SAT *" \
    --configuration '{"TemplateConfiguration": {"Template": file://
s3schemaconfig.json}}' \
    --type "TEMPLATE" \
    --custom-document-enrichment-configuration '{"PostExtractionHookConfiguration":
 {"LambdaArn": "arn:aws:iam::my-account-id:function/my-function-ocr-docs",
```

```
"S3Bucket": "s3://amzn-s3-demo-bucket/scanned-image-text-example-docs"}, "RoleArn":
"arn:aws:iam:my-account-id:role/KendraRoleForCDE"}' \
    --vpc-configuration '{"SecurityGroupIds": ["sg-1234567890abcdef0"], "SubnetIds":
["subnet-1c234","subnet-2b134"]}'
```

Salida:

```
{
    "Id": "exampledatasource1"
}
```

Para obtener más información, consulte Getting started with an Amazon Kendra index and data source connector en la Guía para desarrolladores de Amazon Kendra.

- Para obtener información sobre la API, consulte CreateDataSource en la Referencia de comandos de la AWS CLI.

`create-index`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-index`.

AWS CLI

Para crear un índice de Amazon Kendra

En el siguiente ejemplo de `create-index`, se crea y configura un índice de Amazon Kendra. Puede utilizar `describe-index` para ver el estado de un índice y leer cualquier mensaje de error si el estado muestra un índice que ha fallado (FAILED) al crearse completamente.

```
aws kendra create-index \
    --name "example index 1" \
    --description "Example index 1 contains the first set of example documents" \
    --tags '{"Key": "test resources", "Value": "kendra"}, {"Key": "test resources",
"Value": "aws"}' \
    --role-arn "arn:aws:iam::my-account-id:role/KendraRoleForExampleIndex" \
    --edition "DEVELOPER_EDITION" \
    --server-side-encryption-configuration '{"KmsKeyId": "my-kms-key-id"}' \
    --user-context-policy "USER_TOKEN" \
    --user-token-configurations '{"JsonTokenTypeConfiguration":
{"GroupAttributeField": "groupNameField", "UserNameAttributeField":
"userNameField"}}'
```

Salida:

```
{
   "Id": index1
}
```

Para obtener más información, consulte Getting started with an Amazon Kendra index and data source connector en la Guía para desarrolladores de Amazon Kendra.

- Para obtener información sobre la API, consulte CreateIndex en la Referencia de comandos de la AWS CLI.

`describe-data-source`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-data-source`.

AWS CLI

Para obtener información sobre un conector de origen de datos de Amazon Kendra

En el siguiente ejemplo de `describe-data-source`, se obtiene información sobre un conector de origen de datos de Amazon Kendra. Puede ver la configuración de un conector de origen de datos y leer cualquier mensaje de error si el estado indica que un conector de origen de datos no se ha podido crear por completo (FAILED).

```
aws kendra describe-data-source \
    --id exampledatasource1 \
    --index-id exampleindex1
```

Salida:

```
{
    "Configuration": {
        "TemplateConfiguration": {
            "Template": {
                "connectionConfiguration": {
                    "repositoryEndpointMetadata": {
                        "BucketName": "amzn-s3-demo-bucket"
                    }
                },
                "repositoryConfigurations": {
                    "document":{
```

```
                        "fieldMappings": [
                            {
                                "indexFieldName":"_document_title",
                                "indexFieldType":"STRING",
                                "dataSourceFieldName": "title"
                            },
                            {
                                "indexFieldName":"_last_updated_at",
                                "indexFieldType":"DATE",
                                "dataSourceFieldName": "modified_date"
                            }
                        ]
                    }
                },
                "additionalProperties": {
                    "inclusionPatterns": [
                        "*.txt",
                        "*.doc",
                        "*.docx"
                    ],
                    "exclusionPatterns": [
                        "*.json"
                    ],
                    "inclusionPrefixes": [
                        "PublicExampleDocsFolder"
                    ],
                    "exclusionPrefixes": [
                        "PrivateDocsFolder/private"
                    ],
                    "aclConfigurationFilePath": "ExampleDocsFolder/AclConfig.json",
                    "metadataFilesPrefix": "metadata"
                },
                "syncMode": "FULL_CRAWL",
                "type" : "S3",
                "version": "1.0.0"
            }
        }
    },
    "CreatedAt": 2024-02-25T13:30:10+00:00,
    "CustomDocumentEnrichmentConfiguration": {
        "PostExtractionHookConfiguration": {
            "LambdaArn": "arn:aws:iam::my-account-id:function/my-function-ocr-docs",
            "S3Bucket": "s3://amzn-s3-demo-bucket/scanned-image-text-example-docs/
function"
```

```
        },
        "RoleArn": "arn:aws:iam:my-account-id:role/KendraRoleForCDE"
    }
    "Description": "Example data source 1 for example index 1 contains the first set
 of example documents",
    "Id": exampledatasource1,
    "IndexId": exampleindex1,
    "LanguageCode": "en",
    "Name": "example data source 1",
    "RoleArn": "arn:aws:iam::my-account-id:role/
KendraRoleForS3TemplateConfigDataSource",
    "Schedule": "0 0 18 ? * TUE,MON,WED,THU,FRI,SAT *",
    "Status": "ACTIVE",
    "Type": "TEMPLATE",
    "UpdatedAt": 1709163615,
    "VpcConfiguration": {
        "SecurityGroupIds": ["sg-1234567890abcdef0"],
        "SubnetIds": ["subnet-1c234","subnet-2b134"]
    }
}
```

Para obtener más información, consulte Getting started with an Amazon Kendra index and data source connector en la Guía para desarrolladores de Amazon Kendra.

- Para obtener información sobre la API, consulte DescribeDataSource en la Referencia de comandos de la AWS CLI.

`describe-index`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-index`.

AWS CLI

Para obtener información sobre un índice de Amazon Kendra

En el siguiente ejemplo de `describe-index`, se obtiene información sobre un índice de Amazon Kendra. Puede ver la configuración de un índice y leer cualquier mensaje de error si el estado indica que el índice no se ha podido crear por completo (FAILED).

```
aws kendra describe-index \
    --id exampleindex1
```

Salida:

```
{
    "CapacityUnits": {
        "QueryCapacityUnits": 0,
        "StorageCapacityUnits": 0
    },
    "CreatedAt": 2024-02-25T12:30:10+00:00,
    "Description": "Example index 1 contains the first set of example documents",
    "DocumentMetadataConfigurations": [
        {
            "Name": "_document_title",
            "Relevance": {
                "Importance": 8
            },
            "Search": {
                "Displayable": true,
                "Facetable": false,
                "Searchable": true,
                "Sortable": false
            },
            "Type": "STRING_VALUE"
        },
        {
            "Name": "_document_body",
            "Relevance": {
                "Importance": 5
            },
            "Search": {
                "Displayable": true,
                "Facetable": false,
                "Searchable": true,
                "Sortable": false
            },
            "Type": "STRING_VALUE"
        },
        {
            "Name": "_last_updated_at",
            "Relevance": {
                "Importance": 6,
                "Duration": "2628000s",
                "Freshness": true
            },
            "Search": {
```

```
                "Displayable": true,
                "Facetable": false,
                "Searchable": true,
                "Sortable": true
            },
            "Type": "DATE_VALUE"
        },
        {
            "Name": "department_custom_field",
            "Relevance": {
                "Importance": 7,
                "ValueImportanceMap": {
                    "Human Resources" : 4,
                    "Marketing and Sales" : 2,
                    "Research and innvoation" : 3,
                    "Admin" : 1
                }
            },
            "Search": {
                "Displayable": true,
                "Facetable": true,
                "Searchable": true,
                "Sortable": true
            },
            "Type": "STRING_VALUE"
        }
    ],
    "Edition": "DEVELOPER_EDITION",
    "Id": "index1",
    "IndexStatistics": {
        "FaqStatistics": {
            "IndexedQuestionAnswersCount": 10
        },
        "TextDocumentStatistics": {
            "IndexedTextBytes": 1073741824,
            "IndexedTextDocumentsCount": 1200
        }
    },
    "Name": "example index 1",
    "RoleArn": "arn:aws:iam::my-account-id:role/KendraRoleForExampleIndex",
    "ServerSideEncryptionConfiguration": {
        "KmsKeyId": "my-kms-key-id"
    },
    "Status": "ACTIVE",
```

```
    "UpdatedAt": 1709163615,
    "UserContextPolicy": "USER_TOKEN",
    "UserTokenConfigurations": [
        {
            "JsonTokenTypeConfiguration": {
                "GroupAttributeField": "groupNameField",
                "UserNameAttributeField": "userNameField"
            }
        }
    ]
}
```

Para obtener más información, consulte Getting started with an Amazon Kendra index and data source connector en la Guía para desarrolladores de Amazon Kendra.

- Para obtener información sobre la API, consulte DescribeIndex en la Referencia de comandos de la AWS CLI.

`update-data-source`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-data-source`.

AWS CLI

Para actualizar un conector de origen de datos de Amazon Kendra

En el siguiente ejemplo de `update-data-source`, se actualiza la configuración de un conector de origen de datos de Amazon Kendra. Si la acción se realiza correctamente, el servicio no devuelve ningún resultado, el código de estado HTTP 200 o el código de retorno de AWS CLI 0. Se puede utilizar `describe-data-source` para ver la configuración y el estado de un conector de origen de datos.

```
aws kendra update-data-source \
    --id exampledatasource1 \
    --index-id exampleindex1 \
    --name "new name for example data source 1" \
    --description "new description for example data source 1" \
    --role-arn arn:aws:iam::my-account-id:role/KendraNewRoleForExampleDataSource \
    --configuration '{"TemplateConfiguration": {"Template": file://
s3schemanewconfig.json}}' \
    --custom-document-enrichment-configuration '{"PostExtractionHookConfiguration":
 {"LambdaArn": "arn:aws:iam::my-account-id:function/my-function-ocr-docs",
```

```
"S3Bucket": "s3://amzn-s3-demo-bucket/scanned-image-text-example-docs"}, "RoleArn":
"arn:aws:iam:my-account-id:role/KendraNewRoleForCDE"}' \
   --language-code "es" \
   --schedule "0 0 18 ? * MON,WED,FRI *" \
   --vpc-configuration '{"SecurityGroupIds": ["sg-1234567890abcdef0"], "SubnetIds":
["subnet-1c234","subnet-2b134"]}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Getting started with an Amazon Kendra index and data source connector en la Guía para desarrolladores de Amazon Kendra.

- Para obtener información sobre la API, consulte UpdateDataSource en la Referencia de comandos de la AWS CLI.

`update-index`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-index`.

AWS CLI

Para actualizar un índice de Amazon Kendra

En el siguiente ejemplo de `update-index`, se actualiza la configuración de un índice de Amazon Kendra. Si la acción se realiza correctamente, el servicio no devuelve ningún resultado, el código de estado HTTP 200 o el código de retorno de AWS CLI 0. Se puede utilizar `describe-index` para ver la configuración y el estado de un índice.

```
aws kendra update-index \
    --id enterpriseindex1 \
    --name "new name for Enterprise Edition index 1" \
    --description "new description for Enterprise Edition index 1" \
    --role-arn arn:aws:iam::my-account-id:role/KendraNewRoleForEnterpriseIndex \
    --capacity-units '{"QueryCapacityUnits": 2, "StorageCapacityUnits": 1}' \
    --document-metadata-configuration-updates '{"Name": "_document_title",
"Relevance": {"Importance": 6}}, {"Name": "_last_updated_at", "Relevance":
{"Importance": 8}}' \
   --user-context-policy "USER_TOKEN" \
   --user-token-configurations '{"JsonTokenTypeConfiguration":
{"GroupAttributeField": "groupNameField", "UserNameAttributeField":
"userNameField"}}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Getting started with an Amazon Kendra index and data source connector en la Guía para desarrolladores de Amazon Kendra.

- Para obtener información sobre la API, consulte UpdateIndex en la Referencia de comandos de la AWS CLI.

Ejemplos de Kinesis que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Kinesis.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-tags-to-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-tags-to-stream`.

AWS CLI

Para agregar etiquetas a un flujo de datos

El siguiente ejemplo de `add-tags-to-stream` asigna una etiqueta con la clave `samplekey` y el valor `example` al flujo especificado.

```
aws kinesis add-tags-to-stream \
    --stream-name samplestream \
    --tags samplekey=example
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetar sus flujos en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte AddTagsToStream en la Referencia de comandos de la AWS CLI.

`create-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-stream`.

AWS CLI

Creación de un flujo de datos

En el siguiente ejemplo de `create-stream` se crea un flujo de datos denominado samplestream con 3 particiones.

```
aws kinesis create-stream \
    --stream-name samplestream \
    --shard-count 3
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación de una secuencia en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte CreateStream en la Referencia de comandos de la AWS CLI.

`decrease-stream-retention-period`

En el siguiente ejemplo de código, se muestra cómo utilizar `decrease-stream-retention-period`.

AWS CLI

Para reducir el período de retención del flujo de datos

En el siguiente ejemplo de `decrease-stream-retention-period` se reduce el período de retención (el período de tiempo en el que se puede acceder a los registros de datos después de agregarlos al flujo) de un flujo llamado samplestream a 48 horas.

```
aws kinesis decrease-stream-retention-period \
    --stream-name samplestream \
    --retention-period-hours 48
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Changing the Data Retention Period en la Guía para desarrolladores de Amazon Kinesis.

- Para obtener información sobre la API, consulte DecreaseStreamRetentionPeriod en la Referencia de comandos de la AWS CLI.

`delete-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-stream`.

AWS CLI

Eliminación de un flujo de datos

En el siguiente ejemplo de `delete-stream` se elimina el flujo de datos especificado.

```
aws kinesis delete-stream \
    --stream-name samplestream
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de una secuencia en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte DeleteStream en la Referencia del comando de la AWS CLI.

`deregister-stream-consumer`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-stream-consumer`.

AWS CLI

Para anular el registro de un consumidor de flujos de datos

En el ejemplo de `deregister-stream-consumer` siguiente se anula el registro del consumidor especificado del flujo de datos también especificado.

```
aws kinesis deregister-stream-consumer \
    --stream-arn arn:aws:kinesis:us-west-2:123456789012:stream/samplestream \
    --consumer-name KinesisConsumerApplication
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Desarrollo de consumidores mediante la API de Kinesis Data Streams en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte DeregisterStreamConsumer en la Referencia de comandos de la AWS CLI.

`describe-limits`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-limits`.

AWS CLI

Para describir los límites de partición

En el siguiente ejemplo de `describe-limits` se muestran los límites de partición y el uso de la cuenta actual de AWS.

```
aws kinesis describe-limits
```

Salida:

```
{
    "ShardLimit": 500,
    "OpenShardCount": 29
}
```

Para obtener más información, consulte Resharding a Stream en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener detalles sobre la API, consulte DescribeLimits en la Referencia de comandos de la AWS CLI.

`describe-stream-consumer`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stream-consumer`.

AWS CLI

Para describir un consumidor de flujo de datos

En el siguiente ejemplo de `describe-stream-consumer` se devuelve la descripción del consumidor especificado, registrado en el flujo de datos especificado.

```
aws kinesis describe-stream-consumer \
    --stream-arn arn:aws:kinesis:us-west-2:012345678912:stream/samplestream \
    --consumer-name KinesisConsumerApplication
```

Salida:

```
{
    "ConsumerDescription": {
        "ConsumerName": "KinesisConsumerApplication",
        "ConsumerARN": "arn:aws:kinesis:us-west-2:123456789012:stream/samplestream/
consumer/KinesisConsumerApplication:1572383852",
        "ConsumerStatus": "ACTIVE",
        "ConsumerCreationTimestamp": 1572383852.0,
        "StreamARN": "arn:aws:kinesis:us-west-2:123456789012:stream/samplestream"
    }
}
```

Para obtener más información, consulte Reading Data from Amazon Kinesis Data Streams en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte DescribeStreamConsumer en la Referencia de comandos de la AWS CLI.

`describe-stream-summary`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stream-summary`.

AWS CLI

Para describir un resumen de flujo de datos

El siguiente ejemplo de `describe-stream-summary` proporciona una descripción resumida (sin la lista de particiones) del flujo de datos especificado.

```
aws kinesis describe-stream-summary \
    --stream-name samplestream
```

Salida:

```
{
    "StreamDescriptionSummary": {
        "StreamName": "samplestream",
        "StreamARN": "arn:aws:kinesis:us-west-2:123456789012:stream/samplestream",
        "StreamStatus": "ACTIVE",
        "RetentionPeriodHours": 48,
        "StreamCreationTimestamp": 1572297168.0,
        "EnhancedMonitoring": [
            {
                "ShardLevelMetrics": []
            }
        ],
        "EncryptionType": "NONE",
        "OpenShardCount": 3,
        "ConsumerCount": 0
    }
}
```

Para obtener más información, consulte Creación y administración de secuencias en la Guía para desarrolladores Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte DescribeStreamSummary en la Referencia de comandos de la AWS CLI.

`describe-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stream`.

AWS CLI

Descripción de un flujo de datos

En el siguiente ejemplo de `describe-stream` se devuelven los detalles del flujo de datos especificado.

```
aws kinesis describe-stream \
    --stream-name samplestream
```

Salida:

```
{
    "StreamDescription": {
        "Shards": [
            {
                "ShardId": "shardId-000000000000",
                "HashKeyRange": {
                    "StartingHashKey": "0",
                    "EndingHashKey": "113427455640312821154458202477256070484"
                },
                "SequenceNumberRange": {
                    "StartingSequenceNumber":
 "496008716829570364423650249261910734372510605801286533 14"
                }
            },
            {
                "ShardId": "shardId-000000000001",
                "HashKeyRange": {
                    "StartingHashKey": "113427455640312821154458202477256070485",
                    "EndingHashKey": "226854911280625642308916404954512140969"
                },
                "SequenceNumberRange": {
                    "StartingSequenceNumber":
 "496008716829793371875635555493326091555237089416346337 46"
                }
            },
            {
                "ShardId": "shardId-000000000002",
                "HashKeyRange": {
                    "StartingHashKey": "226854911280625642308916404954512140970",
                    "EndingHashKey": "340282366920938463463374607431768211455"
                },
                "SequenceNumberRange": {
                    "StartingSequenceNumber":
 "496008716830016379327620861724741448737963573031406141 78"
                }
            }
        ],
        "StreamARN": "arn:aws:kinesis:us-west-2:123456789012:stream/samplestream",
```

```
        "StreamName": "samplestream",
        "StreamStatus": "ACTIVE",
        "RetentionPeriodHours": 24,
        "EnhancedMonitoring": [
            {
                "ShardLevelMetrics": []
            }
        ],
        "EncryptionType": "NONE",
        "KeyId": null,
        "StreamCreationTimestamp": 1572297168.0
    }
}
```

Para obtener más información, consulte Creación y administración de secuencias en la Guía para desarrolladores Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte DescribeStream en la Referencia de comandos de la AWS CLI.

`disable-enhanced-monitoring`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-enhanced-monitoring`.

AWS CLI

Para deshabilitar la supervisión mejorada de métricas de nivel de partición

En el siguiente ejemplo de `disable-enhanced-monitoring` se deshabilita la supervisión mejorada de flujos de datos de Kinesis para métricas de nivel de partición.

```
aws kinesis disable-enhanced-monitoring \
    --stream-name samplestream --shard-level-metrics ALL
```

Salida:

```
{
    "StreamName": "samplestream",
    "CurrentShardLevelMetrics": [
        "IncomingBytes",
        "OutgoingRecords",
```

```
        "IteratorAgeMilliseconds",
        "IncomingRecords",
        "ReadProvisionedThroughputExceeded",
        "WriteProvisionedThroughputExceeded",
        "OutgoingBytes"
    ],
    "DesiredShardLevelMetrics": []
}
```

Para obtener más información, consulte Monitoring Streams in Amazon Kinesis Data Streams en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte DisableEnhancedMonitoring en la Referencia de la comandos de la AWS CLI.

`enable-enhanced-monitoring`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-enhanced-monitoring`.

AWS CLI

Para habilitar la supervisión mejorada de métricas de nivel de partición

En el siguiente ejemplo de `enable-enhanced-monitoring` se habilita la supervisión mejorada de flujos de datos de Kinesis para métricas de nivel de partición.

```
aws kinesis enable-enhanced-monitoring \
    --stream-name samplestream \
    --shard-level-metrics ALL
```

Salida:

```
{
    "StreamName": "samplestream",
    "CurrentShardLevelMetrics": [],
    "DesiredShardLevelMetrics": [
        "IncomingBytes",
        "OutgoingRecords",
        "IteratorAgeMilliseconds",
        "IncomingRecords",
        "ReadProvisionedThroughputExceeded",
```

```
        "WriteProvisionedThroughputExceeded",
        "OutgoingBytes"
    ]
}
```

Para obtener más información, consulte Monitoring Streams in Amazon Kinesis Data Streams en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte EnableEnhancedMonitoring en la Referencia de comandos de la AWS CLI.

`get-records`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-records`.

AWS CLI

Obtención de registros de una partición

En el siguiente ejemplo de `get-records` se obtienen registros de datos de la partición de un flujo de datos de Kinesis mediante el iterador de partición especificado.

```
aws kinesis get-records \
    --shard-iterator AAAAAAAAAAF7/0mWD7IuHj1yGv/
TKuNgx2ukD5xipCY4cy4gU96orWwZwcSXh3K9tAmGYeOZyLZrvzzeOFVf9iN99hUPw/w/
b0YWYeehfNvnf1DYt5XpDJghLKr3DzgznkTmMymDP3R+3wRKeuEw6/kdxY2yKJH0veaiekaVc4N2VwK/
GvaGP2Hh9Fg7N++q0Adg6fIDQPt4p8RpavDbk+A4sL9SWGE1
```

Salida:

```
{
    "Records": [],
    "MillisBehindLatest": 80742000
}
```

Para obtener más información, consulte Desarrollo de consumidores mediante la API de Kinesis Data Streams con el SDK de AWS para Java en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener detalles sobre la API, consulte GetRecords en la Referencia de comandos de la AWS CLI.

`get-shard-iterator`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-shard-iterator`.

AWS CLI

Para obtener un iterador de particiones

El siguiente ejemplo de `get-shard-iterator` utiliza el tipo de iterador de particiones `AT_SEQUENCE_NUMBER` y genera un iterador de particiones para empezar a leer los registros de datos exactamente desde la posición indicada por el número de secuencia especificado.

```
aws kinesis get-shard-iterator \
    --stream-name samplestream \
    --shard-id shardId-000000000001 \
    --shard-iterator-type LATEST
```

Salida:

```
{
    "ShardIterator": "AAAAAAAAAAFEvJjIYI+3jw/4aqgH9FifJ+n48XWTh/
IFIsbILP6o5eDueD39NXNBfpZ10WL5K6ADXk8w+5H+Qhd9cFA9k268CPXCz/kebq1TGYI7Vy
+lUkA9BuN3xvATxMBGxRY3zYK05gqgvaIRn94O8SqeEqwhigwZxNWxID3Ej7YYYcxQi8Q/fIrCjGAy/
n2r5Z9G864YpWDfN9upNNQAR/iiOWKs"
}
```

Para obtener más información, consulte Desarrollo de consumidores mediante la API de Kinesis Data Streams con el SDK de AWS para Java en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener detalles sobre la API, consulte GetShardIterator en la Referencia de comandos de la AWS CLI.

`increase-stream-retention-period`

En el siguiente ejemplo de código, se muestra cómo utilizar `increase-stream-retention-period`.

AWS CLI

Para aumentar el período de retención del flujo de datos

En el siguiente ejemplo de `increase-stream-retention-period` se aumenta el período de retención (el período de tiempo en el que se puede acceder a los registros de datos después de agregarlos al flujo) del flujo especificado a 168 horas.

```
aws kinesis increase-stream-retention-period \
    --stream-name samplestream \
    --retention-period-hours 168
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Changing the Data Retention Period en la Guía para desarrolladores de Amazon Kinesis.

- Para obtener información sobre la API, consulte IncreaseStreamRetentionPeriod en la Referencia de comandos de la AWS CLI.

`list-shards`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-shards`.

AWS CLI

Para enumerar las particiones de un flujo de datos

En el siguiente ejemplo de `list-shards` se enumeran todas las particiones del flujo especificado, empezando por el fragmento cuyo identificador sigue inmediatamente al `exclusive-start-shard-id` especificado de `shardId-000000000000`.

```
aws kinesis list-shards \
    --stream-name samplestream \
    --exclusive-start-shard-id shardId-000000000000
```

Salida:

```
{
    "Shards": [
        {
            "ShardId": "shardId-000000000001",
            "HashKeyRange": {
                "StartingHashKey": "113427455640312821154458202477256070485",
                "EndingHashKey": "226854911280625642308916404954512140969"
            },
```

```
            "SequenceNumberRange": {
                "StartingSequenceNumber":
 "496008716829793371875635555493326091555237089416346337 46"
            }
        },
        {
            "ShardId": "shardId-000000000002",
            "HashKeyRange": {
                "StartingHashKey": "226854911280625642308916404954512140970",
                "EndingHashKey": "340282366920938463463374607431768211455"
            },
            "SequenceNumberRange": {
                "StartingSequenceNumber":
 "496008716830016379327620861724741448737963573031406141 78"
            }
        }
    ]
}
```

Para obtener más información, consulte Listing Shards en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte ListShards en la Referencia de comandos de la AWS CLI.

`list-streams`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-streams`.

AWS CLI

Creación de una lista de flujos de datos

En el siguiente ejemplo de `list-streams` se enumeran todos los flujos de datos activos de la cuenta y la región actuales.

```
aws kinesis list-streams
```

Salida:

```
{
    "StreamNames": [
```

```
        "samplestream",
        "samplestream1"
    ]
}
```

Para obtener más información, consulte Visualización de secuencias en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte ListStreams en la Referencia de comandos de la AWS CLI.

`list-tags-for-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-stream`.

AWS CLI

Para enumerar las etiquetas de flujo de datos

En el siguiente ejemplo de `list-tags-for-stream` se enumeran las etiquetas adjuntas al flujo de datos especificado.

```
aws kinesis list-tags-for-stream \
    --stream-name samplestream
```

Salida:

```
{
    "Tags": [
        {
            "Key": "samplekey",
            "Value": "example"
        }
    ],
    "HasMoreTags": false
}
```

Para obtener más información, consulte Etiquetar sus flujos en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte ListTagsForStream en la Referencia de comandos de la AWS CLI.

`merge-shards`

En el siguiente ejemplo de código, se muestra cómo utilizar `merge-shards`.

AWS CLI

Para fusionar particiones

En el siguiente ejemplo de `merge-shards` se fusionan dos particiones adyacentes con los ID shardId-000000000000 y shardId-000000000001 en el flujo de datos especificado y los combina en una sola partición.

```
aws kinesis merge-shards \
    --stream-name samplestream \
    --shard-to-merge shardId-000000000000 \
    --adjacent-shard-to-merge shardId-000000000001
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Merging Two Shards en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte MergeShards en la Referencia de comandos de la AWS CLI.

`put-record`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-record`.

AWS CLI

Escritura de un registro en un flujo de datos

En el siguiente ejemplo de `put-record` se escribe un único registro de datos en el flujo de datos especificado mediante la clave de partición especificada.

```
aws kinesis put-record \
    --stream-name samplestream \
    --data sampledatarecord \
    --partition-key samplepartitionkey
```

Salida:

```
{
    "ShardId": "shardId-000000000009",
    "SequenceNumber": "49600902273357540915989931256901506243878407835297513618",
    "EncryptionType": "KMS"
}
```

Para obtener más información, consulte Desarrollo de productores mediante la API de Kinesis Data Streams con el SDK de AWS para Java en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte PutRecord en la Referencia de comandos de la AWS CLI.

`put-records`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-records`.

AWS CLI

Para escribir varios registros en un flujo de datos

En el siguiente ejemplo de `put-records`, se escribe un registro de datos con la clave de partición especificada y otro registro de datos con una clave de partición diferente en una sola llamada.

```
aws kinesis put-records \
    --stream-name samplestream \
    --
records Data=blob1,PartitionKey=partitionkey1 Data=blob2,PartitionKey=partitionkey2
```

Salida:

```
{
    "FailedRecordCount": 0,
    "Records": [
        {
            "SequenceNumber":
 "49600883331171471519674795588238531498465399900093808706",
            "ShardId": "shardId-000000000004"
```

```
        },
        {
            "SequenceNumber":
 "49600902273357540915989931256902715169698037101720764562",
            "ShardId": "shardId-000000000009"
        }
    ],
    "EncryptionType": "KMS"
}
```

Para obtener más información, consulte Desarrollo de productores mediante la API de Kinesis Data Streams con el SDK de AWS para Java en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte PutRecords en la Referencia de comandos de la AWS CLI.

`register-stream-consumer`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-stream-consumer`.

AWS CLI

Para registrar un consumidor de flujo de datos

En el siguiente ejemplo de `register-stream-consumer` se registra un consumidor llamado `KinesisConsumerApplication` con el flujo de datos especificado.

```
aws kinesis register-stream-consumer \
    --stream-arn arn:aws:kinesis:us-west-2:012345678912:stream/samplestream \
    --consumer-name KinesisConsumerApplication
```

Salida:

```
{
    "Consumer": {
        "ConsumerName": "KinesisConsumerApplication",
        "ConsumerARN": "arn:aws:kinesis:us-west-2: 123456789012:stream/samplestream/
consumer/KinesisConsumerApplication:1572383852",
        "ConsumerStatus": "CREATING",
        "ConsumerCreationTimestamp": 1572383852.0
    }
```

```
}
```

Para obtener más información, consulte Desarrollo de consumidores mediante la API de Kinesis Data Streams en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte RegisterStreamConsumer en la Referencia de comandos de la AWS CLI.

`remove-tags-from-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-tags-from-stream`.

AWS CLI

Para eliminar etiquetas de un flujo de datos

En el siguiente ejemplo de `remove-tags-from-stream` se elimina la etiqueta con la clave especificada del flujo de datos indicado.

```
aws kinesis remove-tags-from-stream \
    --stream-name samplestream \
    --tag-keys samplekey
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetar sus flujos en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte RemoveTagsFromStream en la Referencia de comandos de la AWS CLI.

`split-shard`

En el siguiente ejemplo de código, se muestra cómo utilizar `split-shard`.

AWS CLI

Para dividir particiones

En el siguiente ejemplo de `split-shard` se divide la partición especificada en dos nuevas particiones mediante una nueva clave hash inicial de 10.

```
aws kinesis split-shard \
    --stream-name samplestream \
    --shard-to-split shardId-000000000000 \
    --new-starting-hash-key 10
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Splitting a Shard en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte SplitShard en la Referencia de comandos de la AWS CLI.

`start-stream-encryption`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-stream-encryption`.

AWS CLI

Para habilitar el cifrado de flujos de datos

El siguiente ejemplo de `start-stream-encryption` habilita el cifrado del servidor para el flujo especificado mediante la clave de KMS de AWS indicada.

```
aws kinesis start-stream-encryption \
    --encryption-type KMS \
    --key-id arn:aws:kms:us-west-2:012345678912:key/a3c4a7cd-728b-45dd-
b334-4d3eb496e452 \
    --stream-name samplestream
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Data Protection in Amazon Kinesis Data Streams en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte StartStreamEncryption en la Referencia de comandos de la AWS CLI.

`stop-stream-encryption`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-stream-encryption`.

AWS CLI

Para deshabilitar el cifrado de flujos de datos

El siguiente ejemplo de `stop-stream-encryption` deshabilita el cifrado del servidor para el flujo especificado mediante la clave de KMS de AWS indicada.

```
aws kinesis start-stream-encryption \
    --encryption-type KMS \
    --key-id arn:aws:kms:us-west-2:012345678912:key/a3c4a7cd-728b-45dd-
b334-4d3eb496e452 \
    --stream-name samplestream
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Data Protection in Amazon Kinesis Data Streams en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte StopStreamEncryption en la Referencia de comandos de la AWS CLI.

`update-shard-count`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-shard-count`.

AWS CLI

Para actualizar el recuento de particiones en un flujo de datos

En el siguiente ejemplo de `update-shard-count` se actualiza el recuento de particiones del flujo de datos especificado a 6. En este ejemplo se utiliza escalado uniforme, que crea particiones del mismo tamaño.

```
aws kinesis update-shard-count \
    --stream-name samplestream \
    --scaling-type UNIFORM_SCALING \
    --target-shard-count 6
```

Salida:

```
{
```

```
    "StreamName": "samplestream",
    "CurrentShardCount": 3,
    "TargetShardCount": 6
}
```

Para obtener más información, consulte Resharding a Stream en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Para obtener información sobre la API, consulte UpdateShardCount en la Referencia de comandos de la AWS CLI.

AWS KMS Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS KMS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`cancel-key-deletion`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-key-deletion`.

AWS CLI

Para cancelar la eliminación programada de una clave de KMS administrada por el cliente

En el siguiente ejemplo de `cancel-key-deletion` se cancela la eliminación programada de una clave de KMS administrada por el cliente.

```
aws kms cancel-key-deletion \
```

```
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Salida:

```
{
    "KeyId": "arn:aws:kms:us-
west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

Cuando el comando `cancel-key-deletion` se ejecuta correctamente, se cancela la eliminación programada. Sin embargo, el estado de la clave de KMS es `Disabled`, por lo que no puede usar la clave de KMS en operaciones criptográficas. Para restaurar su funcionalidad, utilice el comando `enable-key`.

Para obtener más información, consulte Scheduling and canceling key deletion en la Guía para desarrolladores de AWS Key Management Service.

- Para ver detalles de la API, consulte CancelKeyDeletion en la Referencia de comandos de la AWS CLI.

`connect-custom-key-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `connect-custom-key-store`.

AWS CLI

Para conectar un almacén de claves personalizado

En el siguiente ejemplo de `connect-custom-key-store` se vuelve a conectar el almacén de claves personalizado especificado. Puede utilizar un comando como este para conectar un almacén de claves personalizado por primera vez o para volver a conectar un almacén de claves que estaba desconectado.

Puede usar este comando para conectar un almacén de claves de AWS CloudHSM o un almacén de claves externo.

```
aws kms connect-custom-key-store \
    --custom-key-store-id cks-1234567890abcdef0
```

El comando no devuelve ningún resultado. Para comprobar que se aplicó el comando, utilice el comando `describe-custom-key-stores`.

Para obtener información sobre cómo conectar un almacén de claves de AWS CloudHSM, consulte Connecting and disconnecting an AWS CloudHSM key store en la Guía para desarrolladores de AWS Key Management Service.

Para obtener información sobre cómo conectar un almacén de claves externo, consulte Connecting and disconnecting an external key store en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte ConnectCustomKeyStore en la Referencia de comandos de la AWS CLI.

`create-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-alias`.

AWS CLI

Creación de un alias de una clave de KMS

El siguiente comando `create-alias` crea un alias llamado `example-alias` de la clave de KMS identificada por el ID de clave `1234abcd-12ab-34cd-56ef-1234567890ab`.

Los nombres del alias no debe empezar por `alias/`. No utilice nombres de alias que comiencen por `alias/aws`; están reservados para que los use AWS.

```
aws kms create-alias \
    --alias-name alias/example-alias \
    --target-key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Este comando no devuelve ningún resultado. Para ver el nuevo alias, utilice el comando `list-aliases`.

Para obtener más información, consulte Uso de alias en la AWSGuía para desarrolladores de Key Management Service.

- Para ver los detalles de la API, consulte CreateAlias en la Referencia de comandos de la AWS CLI.

`create-custom-key-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-custom-key-store`.

AWS CLI

Ejemplo 1: crear un almacén de claves de AWS CloudHSM

En el siguiente ejemplo de `create-custom-key-store` se crea un almacén de claves de AWS CloudHSM respaldado por un clúster de AWS CloudHSM utilizando los parámetros necesarios. También puede añadir el `custom-key-store-type``parameter with the default value: ``AWS_CLOUDHSM`.

Para especificar la entrada de archivo para el comando `trust-anchor-certificate` en la CLI de AWS, se requiere el prefijo de `file://`.

```
aws kms create-custom-key-store \
    --custom-key-store-name ExampleCloudHSMKeyStore \
    --cloud-hsm-cluster-id cluster-1a23b4cdefg \
    --key-store-password kmsPswd \
    --trust-anchor-certificate file://customerCA.crt
```

Salida:

```
{
    "CustomKeyStoreId": cks-1234567890abcdef0
}
```

Para obtener más información, consulte Creating an AWS CloudHSM key store en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 2: crear un almacén de claves externo con conectividad a puntos de conexión públicos

El siguiente ejemplo de `create-custom-key-store` crea un almacén de claves externo (XKS) que se comunica con AWS KMS a través de Internet.

En este ejemplo, la `XksProxyUriPath` utiliza un prefijo opcional de `example-prefix`.

NOTA: Si usa la CLI de AWS versión 1.0, ejecute el siguiente comando antes de especificar un parámetro con un valor HTTP o HTTPS, como el parámetro XksProxyUriEndpoint.

```
aws configure set cli_follow_urlparam false
```

De lo contrario, la CLI de AWS versión 1.0 sustituye el valor del parámetro por el contenido que se encuentra en esa dirección URI.

```
aws kms create-custom-key-store \
    --custom-key-store-name ExamplePublicEndpointXKS \
    --custom-key-store-type EXTERNAL_KEY_STORE \
    --xks-proxy-connectivity PUBLIC_ENDPOINT \
    --xks-proxy-uri-endpoint "https://myproxy.xks.example.com" \
    --xks-proxy-uri-path "/example-prefix/kms/xks/v1" \
    --xks-proxy-authentication-credential "AccessKeyId=ABCDE12345670EXAMPLE,
 RawSecretAccessKey=DXjSUawnel2fr6SKC7G25CNxTyWKE5PF9XX6H/u9pSo="
```

Salida:

```
{
    "CustomKeyStoreId": cks-2234567890abcdef0
}
```

Para obtener más información, consulte Creating an external key store en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 3: crear un almacén de claves externo con conectividad a servicio de puntos de conexión de VPC

En el siguiente ejemplo de `create-custom-key-store` se crea un almacén de claves externo (XKS) que utiliza un servicio de punto de conexión de VPC de Amazon para comunicarse con KMS de AWS.

NOTA: Si usa la CLI de AWS versión 1.0, ejecute el siguiente comando antes de especificar un parámetro con un valor HTTP o HTTPS, como el parámetro XksProxyUriEndpoint.

```
aws configure set cli_follow_urlparam false
```

De lo contrario, la CLI de AWS versión 1.0 sustituye el valor del parámetro por el contenido que se encuentra en esa dirección URI.

```
aws kms create-custom-key-store \
    --custom-key-store-name ExampleVPCEndpointXKS \
    --custom-key-store-type EXTERNAL_KEY_STORE \
    --xks-proxy-connectivity VPC_ENDPOINT_SERVICE \
    --xks-proxy-uri-endpoint "https://myproxy-private.xks.example.com" \
    --xks-proxy-uri-path "/kms/xks/v1" \
    --xks-proxy-vpc-endpoint-service-name "com.amazonaws.vpce.us-east-1.vpce-svc-
example1" \
```

```
    --xks-proxy-authentication-credential "AccessKeyId=ABCDE12345670EXAMPLE,
 RawSecretAccessKey=DXjSUawnel2fr6SKC7G25CNxTyWKE5PF9XX6H/u9pSo="
```

Salida:

```
{
    "CustomKeyStoreId": cks-3234567890abcdef0
}
```

Para obtener más información, consulte Creating an external key store en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte CreateCustomKeyStore en la Referencia de comandos de la AWS CLI.

`create-grant`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-grant`.

AWS CLI

Creación de una concesión

En el siguiente ejemplo de `create-grant` se crea una concesión que permite al usuario `exampleUser` utilizar el comando `decrypt` de la clave de KMS del ejemplo `1234abcd-12ab-34cd-56ef-1234567890ab`. La entidad principal que se va a dar de baja es el rol `adminRole`. La concesión utiliza la limitación de concesión `EncryptionContextSubset` para permitir este permiso solo cuando el contexto de cifrado de la solicitud `decrypt` incluye un par clave-valor `"Department": "IT"`.

```
aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::123456789012:user/exampleUser \
    --operations Decrypt \
    --constraints EncryptionContextSubset={Department=IT} \
    --retiring-principal arn:aws:iam::123456789012:role/adminRole
```

Salida:

```
{
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2",
```

```
    "GrantToken": "<grant token here>"
}
```

Para ver información detallada sobre la concesión, utilice el comando `list-grants`.

Para obtener más información, consulte Concesiones en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte CreateGrant en la Referencia de comandos de la AWS CLI.

`create-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-key`.

AWS CLI

Ejemplo 1: Creación de una clave KMS administrada por el cliente en AWS KMS

En el siguiente ejemplo `create-key` se crea una clave de KMS de cifrado simétrico.

Para crear la clave de KMS básica, una clave de cifrado simétrica, no es necesario especificar ningún parámetro. Los valores predeterminados de esos parámetros crean una clave de cifrado simétrica.

Puesto que este comando no especifica una política de claves, la clave de KMS obtiene la política de claves predeterminada para las claves de KMS creadas mediante programación. Utilice el comando `get-key-policy` para ver la política de claves. Utilice el comando `put-key-policy` para cambiar la política de claves.

```
aws kms create-key
```

El comando `create-key` devuelve los metadatos de la clave, incluidos el ID de la clave y el ARN de la nueva clave de KMS. Puede usar estos valores para identificar la clave de KMS en otras operaciones de AWS KMS. La salida no incluye las etiquetas. Para ver las etiquetas de una clave de KMS, utilice `list-resource-tags command`.

Salida:

```
{
    "KeyMetadata": {
```

```
        "AWSAccountId": "111122223333",
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "CreationDate": "2017-07-05T14:04:55-07:00",
        "CurrentKeyMaterialId":
 "0b7fd7ddbac6eef27907413567cad8c810e2883dc8a7534067a82ee1142fc1e6",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "Description": "",
        "Enabled": true,
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "KeyManager": "CUSTOMER",
        "KeySpec": "SYMMETRIC_DEFAULT",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "MultiRegion": false,
        "Origin": "AWS_KMS"
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ]
    }
}
```

Nota: El comando `create-key` no permite especificar un alias. Para crear un alias para la nueva clave de KMS, utilice el comando `create-alias`.

Para obtener más información, consulte Creación de claves en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 2: Creación de una clave KMS de RSA asimétrica para el cifrado y el descifrado

El siguiente ejemplo de `create-key` se crea una clave de KMS que incluye un par de claves asimétricas RSA para el cifrado y el descifrado. No se puede cambiar la especificación de clave y el uso de la clave después de crear la clave:

```
aws kms create-key \
   --key-spec RSA_4096 \
   --key-usage ENCRYPT_DECRYPT
```

Salida:

```
{
    "KeyMetadata": {
```

```
        "Arn": "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333",
        "CreationDate": "2021-04-05T14:04:55-07:00",
        "CustomerMasterKeySpec": "RSA_4096",
        "Description": "",
        "Enabled": true,
        "EncryptionAlgorithms": [
            "RSAES_OAEP_SHA_1",
            "RSAES_OAEP_SHA_256"
        ],
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "KeyManager": "CUSTOMER",
        "KeySpec": "RSA_4096",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "MultiRegion": false,
        "Origin": "AWS_KMS"
    }
}
```

Para obtener más información, consulte Claves asimétricas en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 3: creación de una clave de KMS asimétrica de curva elíptica para la firma y la verificación

Creación de una clave de KMS asimétrica que contenga un par de claves asimétricas de curva elíptica (ECC) para la firma y la verificación. El parámetro `--key-usage` es obligatorio aunque `SIGN_VERIFY` sea el único valor válido para las claves KMS de ECC. No se puede cambiar la especificación de clave y el uso de la clave después de crear la clave:

```
aws kms create-key \
    --key-spec ECC_NIST_P521 \
    --key-usage SIGN_VERIFY
```

Salida:

```
{
    "KeyMetadata": {
        "Arn": "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
        "AWSAccountId": "111122223333",
        "CreationDate": "2019-12-02T07:48:55-07:00",
        "CustomerMasterKeySpec": "ECC_NIST_P521",
        "Description": "",
        "Enabled": true,
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "KeyManager": "CUSTOMER",
        "KeySpec": "ECC_NIST_P521",
        "KeyState": "Enabled",
        "KeyUsage": "SIGN_VERIFY",
        "MultiRegion": false,
        "Origin": "AWS_KMS",
        "SigningAlgorithms": [
            "ECDSA_SHA_512"
        ]
    }
}
```

Para obtener más información, consulte Claves asimétricas en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 4: Creación de una clave de KMS ML-DSA asimétrica para la firma y la verificación

En este ejemplo, se crea una clave de algoritmo de firma digital de module-lattice (ML-DSA) para la firma y la verificación. El parámetro de clave de uso es obligatorio aunque `SIGN_VERIFY` sea el único valor válido para las claves de ML-DSA.

```
aws kms create-key \
    --key-spec ML_DSA_65 \
    --key-usage SIGN_VERIFY
```

Salida:

```
{
    "KeyMetadata": {
        "Arn": "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333",
        "CreationDate": "2019-12-02T07:48:55-07:00",
        "Description": "",
        "Enabled": true,
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
        "KeyManager": "CUSTOMER",
        "KeySpec": "ML_DSA_65",
        "KeyState": "Enabled",
        "KeyUsage": "SIGN_VERIFY",
        "MultiRegion": false,
        "Origin": "AWS_KMS",
        "SigningAlgorithms": [
            "ML_DSA_SHAKE_256"
        ]
    }
}
```

Para obtener más información, consulte Claves asimétricas en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 5: Creación de una clave de KMS HMAC

En el siguiente ejemplo de `create-key` se crea una clave de KMS HMAC de 384 bits. El valor `GENERATE_VERIFY_MAC` del parámetro `--key-usage` es obligatorio aunque sea el único valor válido para las claves KMS HMAC.

```
aws kms create-key \
    --key-spec HMAC_384 \
    --key-usage GENERATE_VERIFY_MAC
```

Salida:

```
{
    "KeyMetadata": {
        "Arn": "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333",
        "CreationDate": "2022-04-05T14:04:55-07:00",
        "CustomerMasterKeySpec": "HMAC_384",
        "Description": "",
        "Enabled": true,
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "KeyManager": "CUSTOMER",
        "KeySpec": "HMAC_384",
        "KeyState": "Enabled",
        "KeyUsage": "GENERATE_VERIFY_MAC",
        "MacAlgorithms": [
```

```
            "HMAC_SHA_384"
        ],
        "MultiRegion": false,
        "Origin": "AWS_KMS"
    }
}
```

Para obtener más información, consulte Claves HMAC en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 6: Creación de una clave de KMS principal de varias regiones

En el siguiente ejemplo de `create-key` se crea una clave principal de cifrado simétrica de varias regiones. Puesto que los valores predeterminados de todos los parámetros crean una clave de cifrado simétrica, solo es necesario el parámetro `--multi-region` para esta clave de KMS. En la CLI de AWS, para indicar que un parámetro booleano es verdadero, simplemente especifique el nombre del parámetro.

```
aws kms create-key \
    --multi-region
```

Salida:

```
{
    "KeyMetadata": {
        "Arn": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef12345678990ab",
        "AWSAccountId": "111122223333",
        "CreationDate": "2021-09-02T016:15:21-09:00",
        "CurrentKeyMaterialId":
 "0b7fd7ddbac6eef27907413567cad8c810e2883dc8a7534067a82ee1142fc1e6",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "Description": "",
        "Enabled": true,
        "EncryptionAlgorithms": [
          "SYMMETRIC_DEFAULT"
        ],
        "KeyId": "mrk-1234abcd12ab34cd56ef12345678990ab",
        "KeyManager": "CUSTOMER",
        "KeySpec": "SYMMETRIC_DEFAULT",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
```

```
        "MultiRegion": true,
        "MultiRegionConfiguration": {
            "MultiRegionKeyType": "PRIMARY",
            "PrimaryKey": {
                "Arn": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef12345678990ab",
                "Region": "us-west-2"
            },
            "ReplicaKeys": []
        },
        "Origin": "AWS_KMS"
    }
}
```

Para obtener más información, consulte Claves asimétricas en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 7: Creación de una clave de KMS para material de claves importado

En el siguiente ejemplo de `create-key` se crea una clave de KMS sin material de claves. Cuando se complete la operación, puede importar su propio material de claves en la clave de KMS. Para crear esta clave de KMS, establezca el parámetro `--origin` en EXTERNAL.

```
aws kms create-key \
    --origin EXTERNAL
```

Salida:

```
{
     "KeyMetadata": {
         "Arn": "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
         "AWSAccountId": "111122223333",
         "CreationDate": "2019-12-02T07:48:55-07:00",
         "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
         "Description": "",
         "Enabled": false,
         "EncryptionAlgorithms": [
             "SYMMETRIC_DEFAULT"
         ],
         "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
         "KeyManager": "CUSTOMER",
```

```
        "KeySpec": "SYMMETRIC_DEFAULT",
        "KeyState": "PendingImport",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "MultiRegion": false,
        "Origin": "EXTERNAL"
    }
}
```

Para obtener más información, consulte Importar material de claves en claves de AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 6: creación de una clave de KMS en un almacén de claves de AWS CloudHSM

En el siguiente ejemplo de `create-key` se crea una clave de KMS en el almacén de claves de AWS CloudHSM especificado. La operación crea la clave de KMS y sus metadatos en AWS KMS y crea el material de claves en el clúster de AWS CloudHSM asociado al almacén de claves personalizado. Los parámetros `--custom-key-store-id` y `--origin` son obligatorios.

```
aws kms create-key \
    --origin AWS_CLOUDHSM \
    --custom-key-store-id cks-1234567890abcdef0
```

Salida:

```
{
    "KeyMetadata": {
        "Arn": "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333",
        "CloudHsmClusterId": "cluster-1a23b4cdefg",
        "CreationDate": "2019-12-02T07:48:55-07:00",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "CustomKeyStoreId": "cks-1234567890abcdef0",
        "Description": "",
        "Enabled": true,
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ],
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "KeyManager": "CUSTOMER",
        "KeySpec": "SYMMETRIC_DEFAULT",
        "KeyState": "Enabled",
```

```
        "KeyUsage": "ENCRYPT_DECRYPT",
        "MultiRegion": false,
        "Origin": "AWS_CLOUDHSM"
    }
}
```

Para obtener más información, consulte Almacenes de claves de AWS CloudHSM en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 8: Creación de una clave de KMS en un almacén de claves externo

En el siguiente ejemplo de `create-key` se crea una clave de KMS en el almacén de claves externo especificado. Los parámetros `--custom-key-store-id`, `--origin` y `--xks-key-id` son obligatorios en este comando.

El parámetro `--xks-key-id` especifica el ID de una clave de cifrado simétrica existente en el administrador de claves externo. Esta clave sirve como material de clave externa para la clave de KMS. El valor del parámetro `--origin` debe ser `EXTERNAL_KEY_STORE`. El parámetro `custom-key-store-id` debe identificar un almacén de claves externo que esté conectado a su proxy de almacén de claves externo.

```
aws kms create-key \
    --origin EXTERNAL_KEY_STORE \
    --custom-key-store-id cks-9876543210fedcba9 \
    --xks-key-id bb8562717f809024
```

Salida:

```
{
    "KeyMetadata": {
        "Arn": "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333",
        "CreationDate": "2022-12-02T07:48:55-07:00",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "CustomKeyStoreId": "cks-9876543210fedcba9",
        "Description": "",
        "Enabled": true,
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ],
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
        "KeyManager": "CUSTOMER",
        "KeySpec": "SYMMETRIC_DEFAULT",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "MultiRegion": false,
        "Origin": "EXTERNAL_KEY_STORE",
        "XksKeyConfiguration": {
            "Id": "bb8562717f809024"
        }
    }
}
```

Para obtener más información, consulte Almacenes de claves externos en la Guía para desarrolladores de AWS Key Management Service.

- Para ver los detalles de la API, consulte CreateKey en la Referencia de comandos de la AWS CLI.

`decrypt`

En el siguiente ejemplo de código, se muestra cómo utilizar `decrypt`.

AWS CLI

Ejemplo 1: Descifrado de un mensaje cifrado con una clave de KMS simétrica (Linux y macOS)

El siguiente ejemplo de comando `decrypt` muestra la forma recomendada de descifrar datos con la CLI de AWS. Esta versión muestra cómo descifrar los datos en una clave de KMS simétrica.

Proporcione el texto cifrado de un archivo. En el valor del parámetro `--ciphertext-blob`, utilice el prefijo `fileb://`, que indica a la CLI que lea los datos de un archivo binario. Si el archivo no se encuentra en el directorio actual, escriba la ruta completa al archivo. Para obtener más información sobre la lectura de los valores de los parámetros de la CLI de AWS desde un archivo, consulte Carga de parámetros de la CLI de AWS desde un archivo <https://docs.aws.amazon.com/cli/latest/userguide/cli-usage-parameters-file.html> en la Guía del usuario de la interfaz de línea de comandos de AWS y Prácticas recomendadas para los parámetros de archivos locales<https://aws.amazon.com/blogs/developer/best-practices-for-local-file-parameters/> en el Blog de herramientas de línea de comandos de AWS. Especifique la clave de KMS para descifrar el texto cifrado. El parámetro `--key-id` no es necesario al descifrar con una clave de KMS simétrica. AWS KMS puede obtener el ID de la clave de KMS que se utilizó para cifrar los datos de los metadatos en el texto cifrado. Pero siempre es una práctica recomendada

especificar la clave KMS que está utilizando. Esta práctica garantiza que utilice la clave de KMS pretendida y le impide descifrar inadvertidamente un texto cifrado mediante una clave de KMS en la que no confía. Solicite la salida de texto sin formato como valor de texto. El parámetro `--query` indica a la CLI que obtenga únicamente el valor del campo `Plaintext` de la salida. El parámetro `--output` devuelve la salida como texto. Decodifique en base64 el texto sin formato y guárdelo en un archivo. El siguiente ejemplo canaliza (|) el valor del parámetro `Plaintext` a la utilidad Base64, que lo decodifica. A continuación, redirige (>) la salida descodificada al archivo `ExamplePlaintext`.

Antes de ejecutar este comando, reemplace el ID de clave de ejemplo por uno válido de su cuenta de AWS.

```
aws kms decrypt \
    --ciphertext-blob fileb://ExampleEncryptedFile \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --output text \
    --query Plaintext | base64 \
    --decode > ExamplePlaintextFile
```

Este comando no genera ninguna salida. La salida del comando `decrypt` se descodifica en base64 y se guarda en un archivo.

Para obtener más información, consulte Decrypt en la Referencia de la API de AWS Key Management Service.

Ejemplo 2: Descifrado de un mensaje cifrado con una clave de KMS simétrica (símbolo del sistema de Windows)

El ejemplo siguiente es el mismo que el anterior, excepto que usa la utilidad `certutil` para descodificar en Base64 los datos de texto sin formato. Como se muestra en los siguientes ejemplos, este procedimiento requiere dos comandos.

Antes de ejecutar este comando, reemplace el ID de clave de ejemplo por uno válido de su cuenta de AWS.

```
aws kms decrypt ^
    --ciphertext-blob fileb://ExampleEncryptedFile ^
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab ^
    --output text ^
    --query Plaintext > ExamplePlaintextFile.base64
```

Ejecute el comando `certutil`.

```
certutil -decode ExamplePlaintextFile.base64 ExamplePlaintextFile
```

Salida:

```
Input Length = 18
Output Length = 12
CertUtil: -decode command completed successfully.
```

Para obtener más información, consulte Descifrado en la AWSReferencia de la API de Key Management Service.

Ejemplo 3: descifrado de un mensaje cifrado con una clave de KMS asimétrica (Linux y macOS)

El siguiente comando `decrypt` de ejemplo muestra cómo descifrar los datos cifrados con una clave KMS de RSA asimétrica.

Cuando se utiliza una clave de KMS asimétrica, es obligatorio el parámetro `encryption-algorithm`, que especifica el algoritmo que se utiliza para cifrar el texto sin formato.

Antes de ejecutar este comando, reemplace el ID de clave de ejemplo por uno válido de su cuenta de AWS.

```
aws kms decrypt \
    --ciphertext-blob fileb://ExampleEncryptedFile \
    --key-id 0987dcba-09fe-87dc-65ba-ab0987654321 \
    --encryption-algorithm RSAES_OAEP_SHA_256 \
    --output text \
    --query Plaintext | base64 \
    --decode > ExamplePlaintextFile
```

Este comando no genera ninguna salida. La salida del comando `decrypt` se descodifica en base64 y se guarda en un archivo.

Para obtener más información, consulte Claves asimétricas en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte Decrypt en la Referencia de comandos de la AWS CLI.

`delete-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-alias`.

AWS CLI

Eliminación de un alias de AWS KMS

En el siguiente ejemplo de `delete-alias` se elimina el alias `alias/example-alias`. El nombre de alias debe empezar por alias/.

```
aws kms delete-alias \
    --alias-name alias/example-alias
```

Este comando no genera ninguna salida. Utilice el comando `list-aliases` para encontrar el alias.

Para obtener más información, consulte Eliminación de un alias en la Guía para desarrolladores de AWS Key Management Service.

- Para ver los detalles de la API, consulte DeleteTopic en la Referencia de comandos de la AWS CLI.

`delete-custom-key-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-custom-key-store`.

AWS CLI

Para eliminar un almacén de claves personalizado

En el siguiente ejemplo de `delete-custom-key-store` se elimina el almacén de claves personalizado especificado.

La eliminación de un almacén de claves de AWS CloudHSM no afecta al clúster de CloudHSM asociado. La eliminación de un almacén de claves externo no afecta al proxy del almacén de claves externo asociado, al administrador de claves externo ni a las claves externas.

NOTA: Para poder eliminar un almacén de claves personalizado debe programar la eliminación de todas las claves de KMS del almacén de claves personalizado y, a continuación, esperar a que se eliminen esas claves de KMS. Seguidamente debe desconectar el almacén de

claves personalizado. Para obtener ayuda para buscar las claves de KMS en el almacén de claves personalizado, consulte Delete an AWS CloudHSM key store (API) en la Guía para desarrolladores de AWS Key Management Service.

```
delete-custom-key-store \
    --custom-key-store-id cks-1234567890abcdef0
```

El comando no devuelve ningún resultado. Para comprobar que el almacén de claves personalizado se ha eliminado, utilice el comando `describe-custom-key-stores`.

Para obtener información sobre cómo eliminar un almacén de claves de AWS CloudHSM, consulte Deleting an AWS CloudHSM key store en la Guía para desarrolladores de AWS Key Management Service.

Para obtener información sobre cómo eliminar almacenes de claves externos, consulte Deleting an external key store en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte DeleteCustomKeyStore en la Referencia de comandos de la AWS CLI.

`delete-imported-key-material`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-imported-key-material`.

AWS CLI

Para eliminar material de claves importado de una clave de KMS

En el siguiente ejemplo de `delete-imported-key-material` se elimina material de claves que se ha importado a una clave de KMS.

```
aws kms delete-imported-key-material \
   --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Salida:

```
{
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyMaterialId":
 "0b7fd7ddbac6eef27907413567cad8c810e2883dc8a7534067a82ee1142fc1e6"
```

```
}
```

Para obtener más información, consulte Eliminación de material de claves importado en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte DeleteImportedKeyMaterial en la Referencia de comandos de la AWS CLI.

`derive-shared-secret`

En el siguiente ejemplo de código, se muestra cómo utilizar `derive-shared-secret`.

AWS CLI

Para generar un secreto compartido

En el siguiente ejemplo de `derive-shared-secret` se genera un secreto compartido mediante un algoritmo de acuerdo de claves.

Debe utilizar una curva elíptica (ECC) asimétrica recomendada por NIST o un par de claves de KMS de SM2 (solo en las regiones de China) con un valor de `KeyUsage` de `KEY_AGREEMENT` para llamar a DeriveSharedSecret.

```
aws kms derive-shared-secret \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --key-agreement-algorithm ECDH \
    --public-
key "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvH3Yj0wbkLEpUl95Cv1cJVjsVNSjwGq3tCLnzXfhVwV
```

Salida:

```
{
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "SharedSecret": "MEYCIQCKZLWyTk5runarx6XiAkU9gv3lbwPO/pHa
+DXFehzdDwIhANwpsIV2g/9SPWLLsF6p/hiSskuIXMTRwqrMdVKWTMHG",
    "KeyAgreementAlgorithm": "ECDH",
    "KeyOrigin": "AWS_KMS"
}
```

Para obtener más información, consulte DeriveSharedSecret en la AWSReferencia de la API de Key Management Service.

- Para obtener información sobre la API, consulte DeriveSharedSecret en la Referencia de comandos de la AWS CLI.

`describe-custom-key-stores`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-custom-key-stores`.

AWS CLI

Ejemplo 1: obtener información sobre un almacén de claves de AWS CloudHSM

En el siguiente ejemplo de `describe-custom-key-store` se muestran los detalles sobre el almacén de claves de AWS CloudHSM especificado. El comando es el mismo para todos los tipos de almacenes de claves personalizados, pero el resultado difiere según el tipo de almacén de claves y, en el caso de un almacén de claves externo, su opción de conectividad.

De forma predeterminada, este comando muestra información acerca de todos los almacenes de claves personalizados de la cuenta y la región. Para mostrar información sobre un almacén de claves personalizado concreto, utilice el parámetro `custom-key-store-name` o `custom-key-store-id`.

```
aws kms describe-custom-key-stores \
    --custom-key-store-name ExampleCloudHSMKeyStore
```

El resultado de este comando incluye detalles útiles sobre el almacén de claves de AWS CloudHSM, incluido su estado de conexión (`ConnectionState`). Si el estado de conexión es `FAILED`, el resultado incluye un campo `ConnectionErrorCode` que describe el problema.

Salida:

```
{
    "CustomKeyStores": [
        {
            "CloudHsmClusterId": "cluster-1a23b4cdefg",
            "ConnectionState": "CONNECTED",
            "CreationDate": "2022-04-05T14:04:55-07:00",
            "CustomKeyStoreId": "cks-1234567890abcdef0",
            "CustomKeyStoreName": "ExampleExternalKeyStore",
            "TrustAnchorCertificate": "<certificate appears here>"
        }
```

```
    ]
}
```

Para obtener más información, consulte Viewing an AWS CloudHSM key store en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 2: obtener información sobre un almacén de claves externo con conectividad a puntos de conexión públicos

En el siguiente ejemplo de `describe-custom-key-store` se muestran los detalles sobre el almacén de claves externo especificado. El comando es el mismo para todos los tipos de almacenes de claves personalizados, pero el resultado difiere según el tipo de almacén de claves y, en el caso de un almacén de claves externo, su opción de conectividad.

De forma predeterminada, este comando muestra información acerca de todos los almacenes de claves personalizados de la cuenta y la región. Para mostrar información sobre un almacén de claves personalizado concreto, utilice el parámetro `custom-key-store-name` o `custom-key-store-id`.

```
aws kms describe-custom-key-stores \
    --custom-key-store-id cks-9876543210fedcba9
```

El resultado de este comando incluye detalles útiles sobre el almacén de claves externo, incluido su estado de conexión (`ConnectionState`). Si el estado de conexión es `FAILED`, el resultado incluye un campo `ConnectionErrorCode` que describe el problema.

Salida:

```
{
    "CustomKeyStores": [
        {
            "CustomKeyStoreId": "cks-9876543210fedcba9",
            "CustomKeyStoreName": "ExampleXKS",
            "ConnectionState": "CONNECTED",
            "CreationDate": "2022-12-02T07:48:55-07:00",
            "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
            "XksProxyConfiguration": {
                "AccessKeyId": "ABCDE12345670EXAMPLE",
                "Connectivity": "PUBLIC_ENDPOINT",
                "UriEndpoint": "https://myproxy.xks.example.com",
                "UriPath": "/example-prefix/kms/xks/v1"
```

```
            }
        }
    ]
}
```

Para obtener más información, consulte Viewing an external key store en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 3: obtener información acerca de un almacén de claves externo con conectividad al servicio de punto de conexión de VPC

En el siguiente ejemplo de `describe-custom-key-store` se muestran los detalles sobre el almacén de claves externo especificado. El comando es el mismo para todos los tipos de almacenes de claves personalizados, pero el resultado difiere según el tipo de almacén de claves y, en el caso de un almacén de claves externo, su opción de conectividad.

De forma predeterminada, este comando muestra información acerca de todos los almacenes de claves personalizados de la cuenta y la región. Para mostrar información sobre un almacén de claves personalizado concreto, utilice el parámetro `custom-key-store-name` o `custom-key-store-id`.

```
aws kms describe-custom-key-stores \
    --custom-key-store-id cks-2234567890abcdef0
```

El resultado de este comando incluye detalles útiles sobre el almacén de claves externo, incluido su estado de conexión (`ConnectionState`). Si el estado de conexión es `FAILED`, el resultado incluye un campo `ConnectionErrorCode` que describe el problema.

Salida:

```
{
    "CustomKeyStores": [
        {
            "CustomKeyStoreId": "cks-3234567890abcdef0",
            "CustomKeyStoreName": "ExampleVPCExternalKeyStore",
            "ConnectionState": "CONNECTED",
            "CreationDate": "2022-12-22T07:48:55-07:00",
            "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
            "XksProxyConfiguration": {
                "AccessKeyId": "ABCDE12345670EXAMPLE",
                "Connectivity": "VPC_ENDPOINT_SERVICE",
```

```
                "UriEndpoint": "https://myproxy-private.xks.example.com",
                "UriPath": "/kms/xks/v1",
                "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-
example1"
            }
        }
    ]
}
```

Para obtener más información, consulte Viewing an external key store en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte DescribeCustomKeyStores en la Referencia de comandos de la AWS CLI.

`describe-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-key`.

AWS CLI

Ejemplo 1: Búsqueda de información detallada sobre una clave de KMS

En el siguiente ejemplo de `describe-key` se obtiene información detallada sobre la clave administrada por AWS de Amazon S3 en la cuenta y la región de ejemplo. Puede usar este comando para obtener detalles sobre las claves administradas por AWS y las claves administradas por el cliente.

Para especificar la clave de KMS, utilice el parámetro `key-id`. En este ejemplo, se utiliza un valor de nombre de alias, pero puede utilizar un ID de clave, un ARN de clave, un nombre de alias o un ARN de alias en este comando.

```
aws kms describe-key \
    --key-id alias/aws/s3
```

Salida:

```
{
    "KeyMetadata": {
        "AWSAccountId": "846764612917",
        "KeyId": "b8a9477d-836c-491f-857e-07937918959b",
```

```
        "Arn": "arn:aws:kms:us-west-2:846764612917:key/
b8a9477d-836c-491f-857e-07937918959b",
        "CurrentKeyMaterialId":
 "0b7fd7ddbac6eef27907413567cad8c810e2883dc8a7534067a82ee1142fc1e6",
        "CreationDate": 2017-06-30T21:44:32.140000+00:00,
        "Enabled": true,
        "Description": "Default KMS key that protects my S3 objects when no other
 key is defined",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "Enabled",
        "Origin": "AWS_KMS",
        "KeyManager": "AWS",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ]
    }
}
```

Para obtener más información, consulte Visualización de claves en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 2: Obtención de detalles sobre una clave KMS de RSA asimétrica

En el siguiente ejemplo de `describe-key` se obtiene información detallada acerca de una clave KMS de RSA asimétrica que se utiliza para la firma y la verificación.

```
aws kms describe-key \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Salida:

```
{
    "KeyMetadata": {
        "AWSAccountId": "111122223333",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "CreationDate": "2019-12-02T19:47:14.861000+00:00",
        "CustomerMasterKeySpec": "RSA_2048",
        "Enabled": false,
        "Description": "",
```

```
        "KeyState": "Disabled",
        "Origin": "AWS_KMS",
        "MultiRegion": false,
        "KeyManager": "CUSTOMER",
        "KeySpec": "RSA_2048",
        "KeyUsage": "SIGN_VERIFY",
        "SigningAlgorithms": [
            "RSASSA_PKCS1_V1_5_SHA_256",
            "RSASSA_PKCS1_V1_5_SHA_384",
            "RSASSA_PKCS1_V1_5_SHA_512",
            "RSASSA_PSS_SHA_256",
            "RSASSA_PSS_SHA_384",
            "RSASSA_PSS_SHA_512"
        ]
    }
}
```

Ejemplo 3: obtención de detalles sobre una clave de réplica de varias regiones

En el siguiente ejemplo de `describe-key` se obtienen los metadatos de una clave de réplica de varias regiones. Esta clave de varias regiones es una clave de cifrado simétrica. La salida de un comando `describe-key` para cualquier clave de varias regiones devuelve información sobre la clave principal y todas sus réplicas.

```
aws kms describe-key \
    --key-id arn:aws:kms:ap-northeast-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab
```

Salida:

```
{
    "KeyMetadata": {
        "MultiRegion": true,
        "AWSAccountId": "111122223333",
        "Arn": "arn:aws:kms:ap-northeast-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "CreationDate": "2021-06-28T21:09:16.114000+00:00",
        "CurrentKeyMaterialId":
 "0b7fd7ddbac6eef27907413567cad8c810e2883dc8a7534067a82ee1142fc1e6",
        "Description": "",
        "Enabled": true,
        "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
```

```
        "KeyManager": "CUSTOMER",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "Origin": "AWS_KMS",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ],
        "MultiRegionConfiguration": {
            "MultiRegionKeyType": "PRIMARY",
            "PrimaryKey": {
                "Arn": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                "Region": "us-west-2"
            },
            "ReplicaKeys": [
                {
                    "Arn": "arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "eu-west-1"
                },
                {
                    "Arn": "arn:aws:kms:ap-northeast-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "ap-northeast-1"
                },
                {
                    "Arn": "arn:aws:kms:sa-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "sa-east-1"
                }
            ]
        }
    }
}
```

Ejemplo 4: obtención de detalles sobre una clave HMAC KMS

En el siguiente ejemplo de `describe-key` se obtiene información detallada acerca de una clave KMS de HMAC.

```
aws kms describe-key \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Salida:

```
{
    "KeyMetadata": {
        "AWSAccountId": "123456789012",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "Arn": "arn:aws:kms:us-
west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "CreationDate": "2022-04-03T22:23:10.194000+00:00",
        "Enabled": true,
        "Description": "Test key",
        "KeyUsage": "GENERATE_VERIFY_MAC",
        "KeyState": "Enabled",
        "Origin": "AWS_KMS",
        "KeyManager": "CUSTOMER",
        "CustomerMasterKeySpec": "HMAC_256",
        "MacAlgorithms": [
            "HMAC_SHA_256"
        ],
        "MultiRegion": false
    }
}
```

- Para obtener información sobre la API, consulte DescribeKey en la Referencia de comandos de la AWS CLI.

`disable-key-rotation`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-key-rotation`.

AWS CLI

Para deshabilitar la rotación automática de una clave de KMS

En el siguiente ejemplo de `disable-key-rotation`, se deshabilita la rotación automática de una clave de KMS administrada. Para volver a habilitar la rotación automática, utilice el comando `enable-key-rotation`.

```
aws kms disable-key-rotation \
    --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Este comando no genera ninguna salida. Para comprobar que la rotación automática está deshabilitada para la clave de KMS, utilice el comando `get-key-rotation-status`.

Para obtener más información, consulte Rotación de claves en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte DisableKeyRotation en la Referencia de comandos de la AWS CLI.

`disable-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-key`.

AWS CLI

Desactivación temporal de una clave de KMS

El siguiente comando `disable-key` desactiva una clave de KMS administrada por el cliente. Para volver a habilitar la clave de KMS, utilice el comando `enable-key`.

```
aws kms disable-key \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Habilitar y deshabilitar claves en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte DisableKey en la Referencia de comandos de la AWS CLI.

`disconnect-custom-key-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `disconnect-custom-key-store`.

AWS CLI

Para desconectar un almacén de claves personalizado

En el siguiente ejemplo de `disconnect-custom-key-store` se desconecta un almacén de claves personalizado de su clúster de AWS CloudHSM. Puede desconectar un almacén de claves

para solucionar un problema, actualizar su configuración o impedir que las claves de KMS del almacén de claves se utilicen en operaciones criptográficas.

Este comando es igual para todos los almacenes de claves personalizados, incluidos los almacenes de claves de AWS CloudHSM y los almacenes de claves externos.

Antes de ejecutar este comando, reemplace el ID del almacén de claves personalizado de ejemplo por uno válido.

```
$ aws kms disconnect-custom-key-store \
    --custom-key-store-id cks-1234567890abcdef0
```

Este comando no produce ningún resultado. Compruebe que el comando ha sido efectivo, utilice el comando `describe-custom-key-stores`.

Para obtener más información sobre cómo desconectar un almacén de claves de AWS CloudHSM, consulte Connecting and disconnecting an AWS CloudHSM key store en la Guía para desarrolladores de AWS Key Management Service.

Para obtener más información sobre cómo desconectar un almacén de claves externo, consulte Connecting and disconnecting an external key store en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte DisconnectCustomKeyStore en la Referencia de la comandos de la AWS CLI.

`enable-key-rotation`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-key-rotation`.

AWS CLI

Para habilitar la rotación automática de una clave de KMS

El siguiente ejemplo de `enable-key-rotation` permite la rotación automática de una clave de KMS administrada por el cliente con un período de rotación de 180 días. La clave de KMS se rotará un año (aproximadamente 365 días) a partir de la fecha en que se complete este comando y cada año a partir de entonces.

El parámetro `--key-id` identifica las claves KMS. En este ejemplo, se utiliza un valor de ARN clave, pero puede utilizar el ID de clave o el ARN de la clave de KMS. El parámetro `--`

`rotation-period-in-days` especifica el número de días entre cada fecha de rotación. Especifique un valor comprendido entre 90 y 2560 días. El valor predeterminado es 365 días si no se especifica ningún valor.

```
aws kms enable-key-rotation \
    --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --rotation-period-in-days 180
```

Este comando no genera ninguna salida. Utilice el comando `get-key-rotation-status` para comprobar que la clave de KMS está habilitada.

Para obtener más información, consulte Rotación de claves en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre las API, consulte EnableKeyRotation en la Referencia de comandos de la AWS CLI.

`enable-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-key`.

AWS CLI

Activación de una clave de KMS

En el siguiente ejemplo de `enable-key` se habilita una clave administrada por el cliente. Puede utilizar un comando como este para habilitar una clave de KMS que deshabilitó temporalmente mediante el comando `disable-key`. También puede usarlo para habilitar una clave de KMS que esté deshabilitada porque la eliminación estaba programada y esta se canceló.

Para especificar la clave de KMS, utilice el parámetro `key-id`. En este ejemplo, se utiliza un valor de ID de clave, pero puede utilizar un ID de clave o un valor de ARN de clave en este comando.

Antes de ejecutar este comando, reemplace el ID de claves de ejemplo por uno válido.

```
aws kms enable-key \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Este comando no genera ninguna salida. Utilice el comando `describe-key` para comprobar que la clave de KMS está habilitada. Consulte los valores de los campos `KeyState` y `Enabled` en la salida `describe-key`.

Para obtener más información, consulte Habilitar y deshabilitar claves en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte EnableKey en la Referencia de comandos de la AWS CLI.

`encrypt`

En el siguiente ejemplo de código, se muestra cómo utilizar `encrypt`.

AWS CLI

Ejemplo 1: Cifrado del contenido de un archivo en Linux o MacOS

El siguiente comando `encrypt` muestra la forma recomendada de cifrar datos con la CLI de AWS.

```
aws kms encrypt \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --plaintext fileb://ExamplePlaintextFile \
    --output text \
    --query CiphertextBlob | base64 \
    --decode > ExampleEncryptedFile
```

El comando hace varias cosas:

Utiliza el parámetro `--plaintext` para indicar los datos que se van a cifrar. El valor de este parámetro debe estar codificado en base64. El valor del parámetro `plaintext` debe estar codificado en base64 o debe usar el prefijo `fileb://`, que indica a la CLI de AWS que lea los datos binarios del archivo. Si el archivo no está en el directorio actual, escriba la ruta completa al archivo. Por ejemplo: `fileb:///var/tmp/ExamplePlaintextFile` o `fileb://C:\Temp\ExamplePlaintextFile`. Para obtener más información sobre la lectura de los valores de los parámetros de la CLI de AWS de un archivo, consulte Carga de parámetros desde un archivo en la Guía del usuario de la interfaz de línea de comandos de AWS y Prácticas recomendadas para los parámetros de archivos locales en el Blog de herramientas de línea de comandos de AWS. Utiliza los parámetros `--output` y `--query` para controlar la salida del comando. Estos parámetros extraen los datos cifrados, denominados texto cifrado, de la salida del comando. Para

obtener más información sobre el control de la salida, consulte Control de salida de comandos en la Guía del usuario de la interfaz de línea de comandos de AWS. Utiliza la utilidad `base64` para decodificar la salida extraída en datos binarios. El texto cifrado que devuelve un comando `encrypt` correcto es texto codificado en base64. Debe decodificar este texto antes de poder utilizar la CLI de AWS para descifrarlo. Guarda el texto cifrado binario en un archivo. La parte final del comando (`> ExampleEncryptedFile`) guarda el texto cifrado binario en un archivo para facilitar el descifrado. Para ver un comando de ejemplo que usa la CLI de AWS para descifrar datos, consulte los ejemplos de descifrado.

Ejemplo 2: Uso de la CLI de AWS para cifrar datos en Windows

Este ejemplo es igual al anterior, excepto que utiliza la herramienta `certutil` en lugar de `base64`. Como se muestra en el siguiente ejemplo, este procedimiento requiere dos comandos.

```
aws kms encrypt \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --plaintext fileb://ExamplePlaintextFile \
    --output text \
    --query CiphertextBlob > C:\Temp\ExampleEncryptedFile.base64

certutil -decode C:\Temp\ExampleEncryptedFile.base64 C:\Temp\ExampleEncryptedFile
```

Ejemplo 3: cifrado con una clave de KMS asimétrica

El siguiente comando `encrypt` muestra cómo cifrar texto sin formato con una clave de KMS asimétrica. El parámetro `--encryption-algorithm` es obligatorio. Como en todos los comandos de la CLI de `encrypt`, el parámetro `plaintext` debe estar codificado en base64 o debe usar el prefijo `fileb://`, que indica a la CLI de AWS que lea los datos binarios del archivo.

```
aws kms encrypt \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --encryption-algorithm RSAES_OAEP_SHA_256 \
    --plaintext fileb://ExamplePlaintextFile \
    --output text \
    --query CiphertextBlob | base64 \
    --decode > ExampleEncryptedFile
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte Encrypt en la Referencia de comandos de la AWS CLI.

`generate-data-key-pair-without-plaintext`

En el siguiente ejemplo de código, se muestra cómo utilizar `generate-data-key-pair-without-plaintext`.

AWS CLI

Para generar un par de claves de datos asimétricas ECC NIST P

El siguiente ejemplo de `generate-data-key-pair-without-plaintext` solicita un par de claves ECC NIST P384 para su uso fuera de AWS.

El comando devuelve una clave pública en texto no cifrado y una copia de la clave privada cifrada con la clave de KMS especificada. No devuelve una clave privada en texto no cifrado. Puede almacenar de forma segura la clave privada cifrada con los datos cifrados y llamar a KMS de AWS para que descifre la clave privada cuando necesite usarla.

Para solicitar un par de claves de datos asimétricas ECC NIST P384, utilice el parámetro `key-pair-spec` con un valor de `ECC_NIST_P384`.

La clave de KMS que especifique debe ser una clave de KMS de cifrado simétrica, es decir, una clave de KMS con un valor `KeySpec` de `SYMMETRIC_DEFAULT`.

NOTA: Los valores de la salida de este ejemplo se han truncado para su visualización.

```
aws kms generate-data-key-pair-without-plaintext \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --key-pair-spec ECC_NIST_P384
```

Salida:

```
{
    "PrivateKeyCiphertextBlob": "AQIDAHi6LtupRpdKl2aJTzkK6FbhOtQkMlQJJH3PdtHvS/y
+hAFFxmiD134doUDzMGmfCEtcAAAHaTCCB2UGCSqGSIb3DQEHBqCCB1...",
    "PublicKey":
 "MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEA3A3eGMyPrvSn7+LdlJE1oUoQV5HpEuHAVbdOyND
+NmYDH/mL1OSIEuLrcdZ5hrMH4pk83r40l...",
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyMaterialId":
 "0b7fd7ddbac6eef27907413567cad8c810e2883dc8a7534067a82ee1142fc1e6",
    "KeyPairSpec": "ECC_NIST_P384"
```

```
}
```

Las `PublicKey` y `PrivateKeyCiphertextBlob` se devuelven en formato codificado en Base64.

Para obtener más información, consulte Data key pairs en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte GenerateDataKeyPairWithoutPlaintext en la Referencia de comandos de la AWS CLI.

`generate-data-key-pair`

En el siguiente ejemplo de código, se muestra cómo utilizar `generate-data-key-pair`.

AWS CLI

Para generar un par de claves de datos asimétricas RSA de 2048 bits

En el siguiente ejemplo de `generate-data-key-pair` se solicita una clave de datos simétrica RSA de 2048 bits para su uso fuera de AWS. El comando devuelve una clave pública en texto no cifrado y una clave privada en texto no cifrado para su uso y eliminación inmediatos, y una copia de esa clave de datos cifrada con la clave de KMS especificada. Puede almacenar de forma segura la clave privada cifrada con los datos cifrados.

Para solicitar un par de claves de datos asimétricas RSA de 2048 bits, utilice el parámetro `key-pair-spec` con un valor de `RSA_2048`.

La clave de KMS que especifique debe ser una clave de KMS de cifrado simétrica, es decir, una clave de KMS con un valor `KeySpec` de `SYMMETRIC_DEFAULT`.

NOTA: Los valores de la salida de este ejemplo se han truncado para su visualización.

```
aws kms generate-data-key-pair \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --key-pair-spec RSA_2048
```

Salida:

```
{
```

```
    "PrivateKeyCiphertextBlob": "AQIDAHi6LtupRpdKl2aJTzkK6FbhOtQkMlQJJH3PdtHvS/y
+hAFFxmiD134doUDzMGmfCEtcAAAHaTCCB2UGCSqGSIb3DQEHBqCCB1...",
    "PrivateKeyPlaintext": "MIIG/
QIBADANBgkqhkiG9w0BAQEFAASCBucwggbjAgEAAoIBgQDcDd4YzI
+u9Kfv4t2UkTWhShBXkekS4cBVt07I0P42ZgMf+YvU5IgS4ut...",
    "PublicKey":
 "MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEA3A3eGMyPrvSn7+LdlJE1oUoQV5HpEuHAVbdOyND
+NmYDH/mL1OSIEuLrcdZ5hrMH4pk83r40l...",
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyMaterialId":
 "0b7fd7ddbac6eef27907413567cad8c810e2883dc8a7534067a82ee1142fc1e6"
    "KeyPairSpec": "RSA_2048"
}
```

Las `PublicKey`, `PrivateKeyPlaintext` y `PrivateKeyCiphertextBlob` se devuelven en formato codificado en Base64.

Para obtener más información, consulte Data key pairs en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte GenerateDataKeyPair en la Referencia de comandos de AWS CLI.

`generate-data-key-without-plaintext`

En el siguiente ejemplo de código, se muestra cómo utilizar `generate-data-key-without-plaintext`.

AWS CLI

Generación de una clave de datos simétrica de 256 bits sin una clave de texto no cifrado

En el siguiente ejemplo de `generate-data-key-without-plaintext` se solicita una copia cifrada de una clave de datos simétrica de 256 bits para usarla fuera de AWS. Puede llamar a AWS KMS para descifrar la clave de datos cuando esté listo para usarla.

Para solicitar una clave de datos de 256 bits, utilice el parámetro `key-spec` con un valor de `AES_256`. Para solicitar una clave de datos de 128 bits, utilice el parámetro `key-spec` con un valor de `AES_128`. Para el resto longitudes de clave de datos, utilice el parámetro `number-of-bytes`.

La clave de KMS que especifique debe ser una clave de KMS de cifrado simétrica, es decir, una clave de KMS con un valor de especificación de clave SYMMETRIC_DEFAULT.

```
aws kms generate-data-key-without-plaintext \
    --key-id "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab" \
    --key-spec AES_256
```

Salida:

```
{
    "CiphertextBlob":
 "AQEDAHjRYf5WytIc0C857tFSnBaPn2F8DgfmThbJlGfR8P3WlwAAAH4wfAYJKoZIhvcNAQcGoG8wbQIBADBoBgkqhk
    "KeyId": "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyMaterialId":
 "0b7fd7ddbac6eef27907413567cad8c810e2883dc8a7534067a82ee1142fc1e6"
}
```

`CiphertextBlob` (clave de datos cifrada) se devuelve en formato codificado en base64.

Para obtener más información, consulte Claves de datos en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte GenerateDataKeyWithoutPlaintext en la Referencia de comandos de la AWS CLI.

`generate-data-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `generate-data-key`.

AWS CLI

Ejemplo 1: Generación de una clave de datos simétrica de 256 bits

En el siguiente ejemplo de `generate-data-key` se solicita una clave de datos simétrica de 256 bits para usarla fuera de AWS. El comando devuelve una clave de datos en texto sin formato para su uso y eliminación inmediatos, y una copia de esa clave de datos cifrada bajo la clave de KMS especificada. Puede almacenar de forma segura la clave de datos cifrada con los datos cifrados.

Para solicitar una clave de datos de 256 bits, utilice el parámetro `key-spec` con un valor de `AES_256`. Para solicitar una clave de datos de 128 bits, utilice el parámetro `key-spec` con un valor de `AES_128`. Para el resto longitudes de clave de datos, utilice el parámetro `number-of-bytes`.

La clave de KMS que especifique debe ser una clave de KMS de cifrado simétrica, es decir, una clave de KMS con un valor de especificación de clave SYMMETRIC_DEFAULT.

```
aws kms generate-data-key \
    --key-id alias/ExampleAlias \
    --key-spec AES_256
```

Salida:

```
{
    "Plaintext": "VdzKNHGzUAzJeRBVY+uUmofUGGiDzyB3+i9fVkh3piw=",
    "KeyId": "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyMaterialId":
 "0b7fd7ddbac6eef27907413567cad8c810e2883dc8a7534067a82ee1142fc1e6",
    "CiphertextBlob":
 "AQEDAHjRYf5WytIc0C857tFSnBaPn2F8DgfmThbJlGfR8P3WlwAAAH4wfAYJKoZIhvcNAQcGoG8wbQIBADBoBgkqhk
+YdhV8MrkBQPeac0ReRVNDt9qleAt+SHgIRF8P0H+7U="
}
```

`Plaintext` (clave de datos de texto sin formato) y `CiphertextBlob` (clave de datos cifrada) se devuelven en formato codificado en base64.

Para obtener más información, consulte Claves de datos en la Guía para desarrolladores de AWS Key Management Service. Ejemplo 2: Generación de una clave de datos simétrica de 512 bits

En el siguiente ejemplo de `generate-data-key` se solicita una clave de datos simétrica de 512 bits para cifrado y descifrado. El comando devuelve una clave de datos en texto sin formato para su uso y eliminación inmediatos, y una copia de esa clave de datos cifrada bajo la clave de KMS especificada. Puede almacenar de forma segura la clave de datos cifrada con los datos cifrados.

Para solicitar una longitud de clave distinta de 128 o 256 bits, utilice el parámetro `number-of-bytes`. Para solicitar una clave de datos de 512 bits, en el siguiente ejemplo se utiliza el parámetro `number-of-bytes` con un valor de 64 (bytes).

La clave KMS que especifique debe ser una clave de KMS de cifrado simétrica, es decir, una clave de KMS con un valor de especificación de clave de SYMMETRIC_DEFAULT.

NOTA: Los valores de la salida de este ejemplo se han truncado para su visualización.

```
aws kms generate-data-key \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --number-of-bytes 64
```

Salida:

```
{
    "CiphertextBlob": "AQIBAHi6LtupRpdKl2aJTzkK6FbhOtQkMlQJJH3PdtHvS/y+hAEnX/
QQNmMwDfg2korNMEc8AAACaDCCAmQGCSqGSIb3DQEHBqCCAlUwggJRAgEAMIICSgYJKoZ...",
    "Plaintext": "ty8Lr0Bk6OF07M2BWt6qbFdNB
+G00ZLtf5MSEb4al3R2UKWGOp06njAwy2n72VRm2m7z/
Pm9Wpbvttz6a4lSo9hgPvKhZ5y6RTm4OovEXiVfBveyX3DQxDzRSwbKDPk/...",
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyMaterialId":
 "0b7fd7ddbac6eef27907413567cad8c810e2883dc8a7534067a82ee1142fc1e6"
}
```

`Plaintext` (clave de datos de texto sin formato) y `CiphertextBlob` (clave de datos cifrada) se devuelven en formato codificado en base64.

Para obtener más información, consulte Claves de datos en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte GenerateDataKey en la Referencia de comandos de la AWS CLI.

`generate-mac`

En el siguiente ejemplo de código, se muestra cómo utilizar `generate-mac`.

AWS CLI

Ejemplo 1: Generación de un HMAC para un mensaje

El siguiente comando `generate-mac` genera un HMAC para un mensaje, una clave KMS HMAC y un algoritmo MAC. El algoritmo debe ser compatible con la clave KMS HMAC especificada.

En la CLI v2 de AWS, el valor del parámetro `message` debe estar codificado en Base64. O bien, puede guardar el mensaje en un archivo y usar el prefijo `fileb://`, que indica a la CLI de AWS que lea los datos binarios del archivo.

Antes de ejecutar este comando, reemplace el ID de clave de ejemplo por uno válido de su cuenta de AWS. El ID de clave debe representar una clave KMS HMAC con un uso de clave de `GENERATE_VERIFY_MAC`.

```
msg=(echo 'Hello World' | base64)

aws kms generate-mac \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --message fileb://Message \
    --mac-algorithm HMAC_SHA_384
```

Salida:

```
{
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Mac": "<HMAC_TAG>",
    "MacAlgorithm": "HMAC_SHA_384"
}
```

Para obtener más información acerca del uso de claves KMS HMAC en AWS KMS, consulte Claves HMAC en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 2: Guardado de un HMAC en un archivo (Linux y macOS)

En el siguiente ejemplo de `generate-mac`, se genera un HMAC para un mensaje corto almacenado en un archivo local. El comando también obtiene la propiedad `Mac` de la respuesta, la decodifica en Base64 y la guarda en el archivo ExampleMac. Puede usar el archivo de MAC en un comando `verify-mac` que verifique el MAC.

El comando `generate-mac` requiere un mensaje codificado en Base64 y un algoritmo de MAC que admita la clave KMS HMAC. Para obtener los algoritmos de MAC que admite la clave KMS, utilice el comando `describe-key`.

Antes de ejecutar este comando, reemplace el ID de clave de ejemplo por uno válido de su cuenta de AWS. El ID de clave debe representar una clave KMS asimétrica con un uso de clave de GENERATE_VERIFY_MAC.

```
echo 'hello world' | base64 > EncodedMessage

aws kms generate-mac \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --message fileb://EncodedMessage \
    --mac-algorithm HMAC_SHA_384 \
    --output text \
    --query Mac | base64 --decode > ExampleMac
```

Este comando no genera ninguna salida. En este ejemplo, se extrae la propiedad `Mac` del resultado y se guarda en un archivo.

Para obtener más información acerca del uso de claves KMS HMAC en AWS KMS, consulte Claves HMAC en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

- Para ver los detalles de la API, consulte GenerateMac en la Referencia de comandos de la AWS CLI.

`generate-random`

En el siguiente ejemplo de código, se muestra cómo utilizar `generate-random`.

AWS CLI

Ejemplo 1: Generación de una cadena de bytes aleatoria de 256 bits (Linux o macOS)

En el siguiente ejemplo de `generate-random` se genera una cadena de bytes aleatoria de 256 bits (32 bytes) codificada en base64. El ejemplo decodifica la cadena de bytes y la guarda en el archivo aleatorio.

Al ejecutar este comando, debe usar el parámetro `number-of-bytes` para especificar la longitud del valor aleatorio en bytes.

No se especifica una clave de KMS cuando se ejecuta este comando. La cadena de bytes aleatoria no está relacionada con ninguna clave de KMS.

De forma predeterminada, AWS KMS genera el número aleatorio. Sin embargo, si especifica un almacén de claves personalizado, la cadena de bytes aleatoria se genera en el clúster de AWS CloudHSM asociado al almacén de claves personalizado.

Este ejemplo utiliza los parámetros y valores siguientes:

Utiliza el parámetro `--number-of-bytes` obligatorio con un valor de `32` para solicitar una cadena de 32 bytes (256 bits). Utiliza el parámetro `--output` con un valor de `text` para indicar a la CLI de AWS que devuelva la salida como texto, en lugar de JSON. Utiliza `--query parameter` para extraer el valor de la propiedad `Plaintext` de la respuesta. Canaliza (|) la salida del comando a la utilidad `base64`, que decodifica la salida extraída. Utiliza el operador de redireccionamiento (>) para guardar la cadena de bytes decodificada al archivo `ExampleRandom`. Utiliza el operador de redireccionamiento (>) para guardar el texto cifrado binario en un archivo.

```
aws kms generate-random \
    --number-of-bytes 32 \
    --output text \
    --query Plaintext | base64 --decode > ExampleRandom
```

Este comando no genera ninguna salida.

Para obtener más información, consulte GenerateRandom en la Referencia de la API de AWS Key Management Service.

Ejemplo 2: Generación de un número aleatorio de 256 bits (símbolo del sistema de Windows)

En el siguiente ejemplo se utiliza el comando `generate-random` para generar una cadena de bytes aleatoria codificada en base64 de 256 bits (32 bytes). El ejemplo decodifica la cadena de bytes y la guarda en el archivo aleatorio. Este ejemplo es igual al anterior, excepto que usa la utilidad `certutil` de Windows para decodificar en base64 la cadena de bytes aleatoria antes de guardarla en un archivo.

En primer lugar, genere una cadena de bytes aleatoria codificada en base64 y guárdela en un archivo temporal, `ExampleRandom.base64`.

```
aws kms generate-random \
    --number-of-bytes 32 \
    --output text \
    --query Plaintext > ExampleRandom.base64
```

Puesto que el resultado del comando `generate-random` se guarda en un archivo, este ejemplo no produce ningún resultado.

Ahora utilice el comando `certutil -decode` para decodificar la cadena de bytes codificada en base64 del archivo `ExampleRandom.base64`. A continuación, guarda la cadena de bytes decodificada en el archivo `ExampleRandom`.

```
certutil -decode ExampleRandom.base64 ExampleRandom
```

Salida:

```
Input Length = 18
Output Length = 12
CertUtil: -decode command completed successfully.
```

Para obtener más información, consulte GenerateRandom en la Referencia de la API de AWS Key Management Service.

- Para obtener información sobre la API, consulte GenerateRandom en la Referencia de comandos de la AWS CLI.

`get-key-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-key-policy`.

AWS CLI

Copia de una política de claves de una clave de KMS a otra

En el siguiente ejemplo de `get-key-policy` se obtiene la política de claves de una clave de KMS y se guarda en un archivo de texto. A continuación, reemplaza la política de una clave de KMS diferente utilizando el archivo de texto como entrada de la política.

Puesto que el parámetro `--policy` de `put-key-policy` requiere una cadena, debe usar la opción `--output text` para devolver la salida como una cadena de texto en lugar de JSON.

```
aws kms get-key-policy \
    --policy-name default \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --query Policy \
    --output text > policy.txt

aws kms put-key-policy \
    --policy-name default \
    --key-id 0987dcba-09fe-87dc-65ba-ab0987654321 \
    --policy file://policy.txt
```

Este comando no genera ninguna salida.

Para obtener más información, consulte PutKeyPolicy en la Referencia de la API de AWS KMS.

- Para obtener información sobre la API, consulte GetKeyPolicy en la Referencia de comandos de la AWS CLI.

`get-key-rotation-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-key-rotation-status`.

AWS CLI

Para recuperar el estado de rotación de una clave de KMS.

El siguiente ejemplo de `get-key-rotation-status` devuelve información sobre el estado de rotación de la clave de KMS especificada, que incluye si la rotación automática está habilitada, el período de rotación y la próxima fecha de rotación programada. Puede usar este comando en claves de KMS administradas por el cliente y claves administradas por AWS. Sin embargo, todas las claves de KMS administradas por AWS se rotan cada año de forma automática.

```
aws kms get-key-rotation-status \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Salida:

```
{
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyRotationEnabled": true,
    "NextRotationDate": "2024-02-14T18:14:33.587000+00:00",
    "RotationPeriodInDays": 365
}
```

Para obtener más información, consulte Rotación de claves en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte GetKeyRotationStatus en la Referencia de comandos de la AWS CLI.

`get-parameters-for-import`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-parameters-for-import`.

AWS CLI

Para obtener los elementos necesarios para importar material de claves en una clave de KMS

En el siguiente ejemplo de `get-parameters-for-import` se obtiene la clave pública y el token de importación que necesita para importar material de claves en una clave de KMS. Cuando utilice el comando `import-key-material`, asegúrese de utilizar el token de importación y el material de claves cifrados con la clave pública que se devolvieron en el mismo comando `get-parameters-for-import`. Además, el algoritmo de encapsulado que especifique en este comando debe ser el que utilice para cifrar el material de claves con la clave pública.

Para especificar la clave de KMS, utilice el parámetro `key-id`. En este ejemplo, se utiliza un ID de clave, pero puede utilizar un ID de clave o un ARN de clave en este comando.

```
aws kms get-parameters-for-import \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --wrapping-algorithm RSAES_OAEP_SHA_256 \
    --wrapping-key-spec RSA_2048
```

Salida:

```
{
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "PublicKey": "<public key base64 encoded data>",
    "ImportToken": "<import token base64 encoded data>",
    "ParametersValidTo": 1593893322.32
}
```

Para obtener más información, consulte Download the public key and import token en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte GetParametersForImport en la Referencia de comandos de la AWS CLI.

`get-public-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-public-key`.

AWS CLI

Ejemplo 1: descargar la clave pública de una clave de KMS asimétrica

El siguiente ejemplo de `get-public-key` descarga la clave pública de una clave de KMS asimétrica.

Además de devolver la clave pública, el resultado incluye la información necesaria para utilizarla de forma segura fuera de KMS de AWS, incluidos el uso de la clave y los algoritmos de cifrado compatibles.

```
aws kms get-public-key \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Salida:

```
{
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "PublicKey": "jANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAl5epvg1/
QtJhxSi2g9SDEVg8QV/...",
    "CustomerMasterKeySpec": "RSA_4096",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "EncryptionAlgorithms": [
        "RSAES_OAEP_SHA_1",
        "RSAES_OAEP_SHA_256"
    ]
}
```

Para obtener más información acerca del uso de claves KMS asimétricas en AWS, consulte Uso de claves en AWS KMS en la AWS Guía para desarrolladores de Key Management Service.
Ejemplo 2: convertir una clave pública a formato DER (Linux y macOS)

El siguiente ejemplo de `get-public-key` descarga la clave pública de una clave de KMS asimétrica y la guarda en un archivo DER.

Cuando utiliza el comando `get-public-key` en la AWS CLI, devuelve una clave pública X.509 codificada en DER que está codificada en Base64. En este ejemplo se obtiene el valor de la propiedad `PublicKey` en forma de texto. Descodifica la `PublicKey` en Base64 y la guarda en el archivo `public_key.der`. El parámetro `output` devuelve el resultado como texto, en lugar de

como JSON. El parámetro `--query` obtiene solo la propiedad `PublicKey`, no las propiedades que necesita para usar la clave pública de forma segura fuera de AWS KMS.

Antes de ejecutar este comando, reemplace el ID de clave de ejemplo por uno válido de su cuenta de AWS.

```
aws kms get-public-key \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --output text \
    --query PublicKey | base64 --decode > public_key.der
```

Este comando no genera ninguna salida.

Para obtener más información acerca del uso de claves KMS asimétricas en AWS KMS, consulte Uso de claves asimétricas en AWS KMS en la AWS Guía para desarrolladores de Key Management Service.

- Para obtener información sobre la API, consulte GetPublicKey en la Referencia de comandos de la AWS CLI.

`import-key-material`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-key-material`.

AWS CLI

Para importar material de claves en una clave de KMS

En el siguiente ejemplo de `import-key-material` se carga el material de claves en una clave de KMS que se ha creado sin material de claves. El estado de clave de la clave de KMS debe ser `PendingImport`.

Este comando utiliza material de claves que usted ha cifrado con la clave pública que ha devuelto el comando `get-parameters-for-import`. También usa el token de importación del mismo comando `get-parameters-for-import`.

El parámetro `expiration-model` indica que el material de claves caduca automáticamente en la fecha y la hora especificadas por el parámetro `valid-to`. Cuando vence el material de claves, AWS KMS lo elimina, el estado de la clave de KMS cambia a `Pending import` y la clave de KMS no se puede utilizar. Para restaurar la clave de KMS debe volver a importar el

mismo material de claves. Para usar material de claves diferente debe crear una clave de KMS nueva.

Antes de ejecutar este comando, reemplace el ID de clave de ejemplo por un ID de clave o un ARN de clave válido de su cuenta de AWS.

```
aws kms import-key-material \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --encrypted-key-material fileb://EncryptedKeyMaterial.bin \
    --import-token fileb://ImportToken.bin \
    --expiration-model KEY_MATERIAL_EXPIRES \
    --valid-to 2021-09-21T19:00:00Z
```

Salida:

```
{
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyMaterialId":
 "0b7fd7ddbac6eef27907413567cad8c810e2883dc8a7534067a82ee1142fc1e6"
}
```

Para obtener más información sobre la importación de material de claves, consulte Importing Key Material en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte ImportKeyMaterial en la Referencia de comandos de la AWS CLI.

`list-aliases`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-aliases`.

AWS CLI

Ejemplo 1: Creación de una lista de todos los alias de una cuenta y una región de AWS

En el siguiente ejemplo se utiliza el comando `list-aliases` para enumerar todos los alias de la región predeterminada de la cuenta de AWS. La salida incluye los alias asociados a las claves KMS administradas por AWS y por el cliente.

```
aws kms list-aliases
```

Salida:

```
{
    "Aliases": [
        {
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/testKey",
            "AliasName": "alias/testKey",
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
        },
        {
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/FinanceDept",
            "AliasName": "alias/FinanceDept",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321"
        },
        {
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/dynamodb",
            "AliasName": "alias/aws/dynamodb",
            "TargetKeyId": "1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
        },
        {
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/ebs",
            "AliasName": "alias/aws/ebs",
            "TargetKeyId": "0987ab65-43cd-21ef-09ab-87654321cdef"
        },
        ...
    ]
}
```

Ejemplo 2: Creación de una lista de todos los alias de una clave de KMS concreta

En el siguiente ejemplo se utiliza el comando `list-aliases` y su parámetro `key-id` para mostrar todos los alias que están asociados con una determinada clave de KMS.

Cada alias está asociado a una sola clave de KMS, pero una clave de KMS puede tener varios alias. Este comando resulta muy útil porque la consola de AWS KMS solo muestra un alias para cada clave de KMS. Debe utilizar el comando `list-aliases` para encontrar todos los alias de una clave de KMS.

En este ejemplo, se utiliza el ID de la clave de KMS del parámetro `--key-id`, pero puede utilizar un ID de clave, un ARN de clave, un nombre de alias o un ARN de alias en este comando.

```
aws kms list-aliases --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Salida:

```
{
    "Aliases": [
        {
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/oregon-test-key",
            "AliasName": "alias/oregon-test-key"
        },
        {
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/project121-test",
            "AliasName": "alias/project121-test"
        }
    ]
}
```

Para obtener más información, consulte Uso de alias en la Guía para desarrolladores de AWS Key Management Service.

- Para ver los detalles de la API, consulte ListAliases en la Referencia de comandos de la AWS CLI.

`list-grants`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-grants`.

AWS CLI

Visualización de las concesiones de una clave de AWS KMS

En el siguiente ejemplo de `list-grants` se muestran todas las concesiones de la clave de KMS administrada por AWS especificada para Amazon DynamoDB en su cuenta. Esta concesión permite a DynamoDB utilizar la clave de KMS en su nombre para cifrar una tabla de DynamoDB antes de escribirla en el disco. Puede usar un comando como este para ver las concesiones de las claves de KMS administradas por AWS y administradas por el cliente en la cuenta y la región de AWS.

Este comando usa el parámetro `key-id` con un ID de la clave para identificar la clave de KMS. Puede utilizar un ID o ARN de clave para identificar la clave de KMS. Para obtener el ID de la clave o el ARN de la clave de una clave de KMS administrada por AWS, utilice el comando `list-keys` o `list-aliases`.

```
aws kms list-grants \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

La salida muestra que la concesión otorga a Amazon DynamoDB permiso para usar la clave de KMS para operaciones criptográficas y le da permiso para ver detalles sobre la clave de KMS (`DescribeKey`) y para retirar concesiones (`RetireGrant`). La restricción `EncryptionContextSubset` limita estos permisos a las solicitudes que incluyen los pares de contexto de cifrado especificados. Como resultado, los permisos de la concesión solo son efectivos en la cuenta y la tabla de DynamoDB especificadas.

```
{
    "Grants": [
        {
            "Constraints": {
                "EncryptionContextSubset": {
                    "aws:dynamodb:subscriberId": "123456789012",
                    "aws:dynamodb:tableName": "Services"
                }
            },
            "IssuingAccount": "arn:aws:iam::123456789012:root",
            "Name": "8276b9a6-6cf0-46f1-b2f0-7993a7f8c89a",
            "Operations": [
                "Decrypt",
                "Encrypt",
                "GenerateDataKey",
                "ReEncryptFrom",
                "ReEncryptTo",
                "RetireGrant",
                "DescribeKey"
            ],
            "GrantId":
 "1667b97d27cf748cf05b487217dd4179526c949d14fb3903858e25193253fe59",
            "KeyId": "arn:aws:kms:us-
west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "RetiringPrincipal": "dynamodb.us-west-2.amazonaws.com",
            "GranteePrincipal": "dynamodb.us-west-2.amazonaws.com",
            "CreationDate": "2021-05-13T18:32:45.144000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Concesiones en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte ListGrants en la Referencia de comandos de la AWS CLI.

`list-key-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-key-policies`.

AWS CLI

Obtención de los nombres de las políticas de claves de una clave de KMS

En el siguiente ejemplo de `list-key-policies` se obtienen los nombres de las políticas de clave de una clave administrada por el cliente en la cuenta y la región del ejemplo. Puede usar este comando para encontrar los nombres de las políticas de claves para las claves administradas por AWS y por el cliente.

Este comando no resulta útil, ya que el único nombre de la política de claves válido es `default`.

Para especificar la clave de KMS, utilice el parámetro `key-id`. En este ejemplo, se utiliza un valor de ID de clave, pero puede utilizar un ID de clave o un ARN de clave en este comando.

```
aws kms list-key-policies \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Salida:

```
{
    "PolicyNames": [
    "default"
    ]
}
```

Para obtener más información acerca de las políticas de claves de AWS KMS, consulte Uso de políticas de claves en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte ListKeyPolicies en la Referencia de comandos de la AWS CLI.

`list-key-rotations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-key-rotations`.

AWS CLI

Para recuperar información sobre todas las rotaciones de material de claves completadas

En el siguiente ejemplo de `list-key-rotations` se muestra información sobre todas las rotaciones de material de claves completadas para la clave de KMS especificada.

```
aws kms list-key-rotations \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Salida:

```
{
    "Rotations": [
        {
            "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "RotationDate": "2024-03-02T10:11:36.564000+00:00",
            "RotationType": "AUTOMATIC"
        },
        {
            "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "RotationDate": "2024-04-05T15:14:47.757000+00:00",
            "RotationType": "ON_DEMAND"
        }
    ],
    "Truncated": false
}
```

Para obtener más información, consulte Rotación de claves en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte ListKeyRotations en la Referencia de comandos de la AWS CLI.

`list-keys`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-keys`.

AWS CLI

Obtención de las claves KMS de una cuenta y una región

En el siguiente ejemplo de `list-keys` se obtienen las claves de KMS de una cuenta y una región. Este comando devuelve las claves administradas por AWS y por el cliente.

```
aws kms list-keys
```

Salida:

```
{
    "Keys": [
        {
            "KeyArn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
        },
        {
            "KeyArn": "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321",
            "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321"
        },
        {
            "KeyArn": "arn:aws:kms:us-
east-2:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "KeyId": "1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
        }
    ]
}
```

Para obtener más información, consulte Visualización de claves en la Guía para desarrolladores de AWS Key Management Service.

- Para ver los detalles de la API, consulte ListKeys en la Referencia de comandos de la AWS CLI.

`list-resource-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-tags`.

AWS CLI

Para obtener las etiquetas de una clave de KMS

En el siguiente ejemplo de `list-resource-tags` se obtienen las etiquetas para una clave de KMS. Para añadir una o más etiquetas de recurso en claves de KMS, utilice el comando `tag-resource`. El resultado muestra que esta clave de KMS tiene dos etiquetas de recursos, cada una de las cuales tiene una clave y un valor.

Para especificar la clave de KMS, utilice el parámetro `key-id`. En este ejemplo, se utiliza un valor de ID de clave, pero puede utilizar un ID de clave o un ARN de clave en este comando.

```
aws kms list-resource-tags \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Salida:

```
{
    "Tags": [
    {
        "TagKey": "Dept",
        "TagValue": "IT"
    },
    {
        "TagKey": "Purpose",
        "TagValue": "Test"
    }
    ],
    "Truncated": false
}
```

Para obtener información sobre el uso de etiquetas en AWS KMS, consulte Etiquetar claves en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte ListResourceTags en la Referencia de comandos de la AWS CLI.

`list-retirable-grants`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-retirable-grants`.

AWS CLI

Para ver las concesiones que una entidad principal puede retirar

En el siguiente ejemplo de `list-retirable-grants` se muestran todas las concesiones que el usuario `ExampleAdmin` puede retirar en las claves de KMS en una cuenta y una región de AWS. Puede usar un comando como este para ver las concesiones que cualquier entidad principal de cuenta puede retirar en claves de KMS en la cuenta y la región de AWS.

El valor del parámetro `retiring-principal` obligatorio debe ser el nombre de recurso de Amazon (ARN) de una cuenta, usuario o rol.

No puede especificar un servicio con el valor de `retiring-principal` en este comando, aunque un servicio pueda ser la entidad principal que se retira. Para buscar las concesiones en las que un servicio concreto es la entidad principal que se retira, utilice el comando `list-grants`.

El resultado muestra que el usuario `ExampleAdmin` tiene permiso para retirar concesiones en dos claves de KMS diferentes de la cuenta y la región. Además de la entidad principal que se retira, la cuenta tiene permiso para retirar cualquier concesión de la cuenta.

```
aws kms list-retirable-grants \
    --retiring-principal arn:aws:iam::111122223333:user/ExampleAdmin
```

Salida:

```
{
    "Grants": [
        {
            "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "GrantId":
 "156b69c63cb154aa21f59929ff19760717be8d9d82b99df53e18b94a15a5e88e",
            "Name": "",
            "CreationDate": 2021-01-14T20:17:36.419000+00:00,
            "GranteePrincipal": "arn:aws:iam::111122223333:user/ExampleUser",
            "RetiringPrincipal": "arn:aws:iam::111122223333:user/ExampleAdmin",
            "IssuingAccount": "arn:aws:iam::111122223333:root",
            "Operations": [
                "Encrypt"
            ],
```

```
            "Constraints": {
                "EncryptionContextSubset": {
                    "Department": "IT"
                }
            }
        },
        {
            "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321",
            "GrantId":
 "8c94d1f12f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2",
            "Name": "",
            "CreationDate": "2021-02-02T19:49:49.638000+00:00",
            "GranteePrincipal": "arn:aws:iam::111122223333:role/ExampleRole",
            "RetiringPrincipal": "arn:aws:iam::111122223333:user/ExampleAdmin",
            "IssuingAccount": "arn:aws:iam::111122223333:root",
            "Operations": [
                "Decrypt"
            ],
            "Constraints": {
                "EncryptionContextSubset": {
                    "Department": "IT"
                }
            }
        }
    ],
    "Truncated": false
}
```

Para obtener más información, consulte Concesiones en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte ListRetirableGrants en la Referencia de comandos de la AWS CLI.

`put-key-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-key-policy`.

AWS CLI

Cambio de la política de claves de una clave de KMS

En el siguiente ejemplo de `put-key-policy` se cambia la política de claves para una clave administrada por el cliente.

Para empezar, cree una política de clave y guárdela en un archivo JSON local. En este ejemplo, el archivo es `key_policy.json`. También puede especificar la política de claves como un valor de cadena del parámetro `policy`.

La primera instrucción de esta política de claves da permiso a la cuenta de AWS para utilizar políticas de IAM para controlar el acceso a la clave de KMS. La segunda instrucción otorga permiso al usuario `test-user` para ejecutar los comandos `describe-key` y `list-keys` de la clave de KMS.

Contenido de `key_policy.json`:

```
{
    "Version":"2012-10-17",
    "Id" : "key-default-1",
    "Statement" : [
        {
            "Sid" : "Enable IAM User Permissions",
            "Effect" : "Allow",
            "Principal" : {
                "AWS" : "arn:aws:iam::111122223333:root"
            },
            "Action" : "kms:*",
            "Resource" : "*"
        },
        {
            "Sid" : "Allow Use of Key",
            "Effect" : "Allow",
            "Principal" : {
                "AWS" : "arn:aws:iam::111122223333:user/test-user"
            },
            "Action" : [
                "kms:DescribeKey",
                "kms:ListKeys"
            ],
            "Resource" : "*"
        }
    ]
}
```

Para identificar la clave de KMS, en este ejemplo se utiliza el ID de clave, pero también se puede utilizar un ARN de la clave. El comando utiliza el parámetro `policy` para especificar las políticas de claves. Para indicar que la política se encuentra en un archivo, utiliza el prefijo `file://` necesario. Este prefijo es necesario para identificar los archivos de todos los sistemas operativos compatibles. Por último, el comando usa el parámetro `policy-name` con un valor de `default`. Si no se especifica ningún nombre de política, el valor predeterminado es `default`. El único valor válido es `default`.

```
aws kms put-key-policy \
    --policy-name default \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --policy file://key_policy.json
```

Este comando no produce ninguna salida. Para comprobar que se aplicó el comando, utilice el comando `get-key-policy`. El siguiente comando de ejemplo obtiene la política de claves para la misma clave de KMS. El parámetro `output` con un valor de `text` devuelve un formato de texto que es fácil de leer.

```
aws kms get-key-policy \
    --policy-name default \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --output text
```

Salida:

```
{
    "Version":"2012-10-17",
    "Id" : "key-default-1",
    "Statement" : [
        {
            "Sid" : "Enable IAM User Permissions",
            "Effect" : "Allow",
            "Principal" : {
                "AWS" : "arn:aws:iam::111122223333:root"
            },
            "Action" : "kms:*",
            "Resource" : "*"
            },
            {
            "Sid" : "Allow Use of Key",
            "Effect" : "Allow",
```

```
            "Principal" : {
                "AWS" : "arn:aws:iam::111122223333:user/test-user"
            },
            "Action" : [ "kms:Describe", "kms:List" ],
            "Resource" : "*"
        }
    ]
}
```

Para obtener más información, consulte Cambio de una política de claves en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte PutKeyPolicy en la Referencia de comandos de la AWS CLI.

`re-encrypt`

En el siguiente ejemplo de código, se muestra cómo utilizar `re-encrypt`.

AWS CLI

Ejemplo 1: Cómo volver a cifrar un mensaje cifrado con una clave de KMS simétrica diferente (Linux y macOS).

El siguiente comando `re-encrypt` de ejemplo muestra la forma recomendada de volver a cifrar los datos con la CLI de AWS.

Proporcione el texto cifrado de un archivo. En el valor del parámetro `--ciphertext-blob`, utilice el prefijo `fileb://`, que indica a la CLI que lea los datos de un archivo binario. Si el archivo no se encuentra en el directorio actual, escriba la ruta completa al archivo. Para obtener más información sobre la lectura de los valores de los parámetros de la CLI de AWS de un archivo, consulte Carga de los parámetros de la CLI de AWS de un archivo en la Guía del usuario de la interfaz de línea de comandos de AWS y las Prácticas recomendadas para los parámetros de archivos locales en el Blog de herramientas de línea de comandos de AWS. Especifique la clave KMS de origen, que descifra el texto cifrado. No se requiere el parámetro `--source-key-id` al descifrar con claves de KMS de cifrado simétrico. AWS KMS puede obtener la clave de KMS que se utilizó para cifrar los datos de los metadatos en el blob de texto cifrado. Pero siempre es una práctica recomendada especificar la clave KMS que está utilizando. Esta práctica garantiza que utilice la clave de KMS pretendida y le impide descifrar inadvertidamente un texto cifrado mediante una clave de KMS en la que no confía. Especifique la clave de KMS de destino,

que vuelve a cifrar los datos. El parámetro `--destination-key-id` siempre es obligatorio. En este ejemplo, se utiliza un ARN de clave, pero se puede utilizar cualquier identificador de clave válido. Solicite la salida de texto sin formato como un valor de texto. El parámetro `--query` indica a la CLI que obtenga únicamente el valor del campo `Plaintext` de la salida. El parámetro `--output` devuelve la salida como texto. Decodifique en base64 el texto sin formato y guárdelo en un archivo. El siguiente ejemplo canaliza (|) el valor del parámetro `Plaintext` a la utilidad Base64, que lo decodifica. A continuación, redirige (>) la salida descodificada al archivo `ExamplePlaintext`.

Antes de ejecutar este comando, reemplace los ID de clave de ejemplo por identificadores de clave válidos de su cuenta de AWS.

```
aws kms re-encrypt \
    --ciphertext-blob fileb://ExampleEncryptedFile \
    --source-key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --destination-key-id 0987dcba-09fe-87dc-65ba-ab0987654321 \
    --query CiphertextBlob \
    --output text | base64 --decode > ExampleReEncryptedFile
```

Este comando no genera ninguna salida. La salida del comando `re-encrypt` se descodifica en base64 y se guarda en un archivo.

Para obtener más información, consulte ReEncrypt en la Referencia de la API de AWS Key Management Service.

Ejemplo 2: Cómo volver a cifrar un mensaje cifrado con una clave de KMS simétrica diferente (Linux y macOS).

El siguiente comando `re-encrypt` de ejemplo es el mismo que el anterior, excepto que usa la utilidad `certutil` para descodificar en Base64 los datos de texto sin formato. Como se muestra en los siguientes ejemplos, este procedimiento requiere dos comandos.

Antes de ejecutar este comando, reemplace el ID de clave de ejemplo por uno válido de su cuenta de AWS.

```
aws kms re-encrypt ^
    --ciphertext-blob fileb://ExampleEncryptedFile ^
    --source-key-id 1234abcd-12ab-34cd-56ef-1234567890ab ^
    --destination-key-id 0987dcba-09fe-87dc-65ba-ab0987654321 ^
    --query CiphertextBlob ^
```

```
    --output text > ExampleReEncryptedFile.base64
```

A continuación, use la utilidad `certutil`

```
certutil -decode ExamplePlaintextFile.base64 ExamplePlaintextFile
```

Salida:

```
Input Length = 18
Output Length = 12
CertUtil: -decode command completed successfully.
```

Para obtener más información, consulte ReEncrypt en la Referencia de la API de AWS Key Management Service.

- Para obtener información sobre la API, consulte ReEncrypt en la Referencia de comandos de la AWS CLI.

`retire-grant`

En el siguiente ejemplo de código, se muestra cómo utilizar `retire-grant`.

AWS CLI

Retirada de una concesión en una clave maestra de cliente

En el siguiente ejemplo de `retire-grant` se elimina una concesión de una clave de KMS.

El siguiente comando de ejemplo especifica los parámetros `grant-id` y `key-id`. El valor del parámetro `key-id` debe ser el ARN de la clave de KMS.

```
aws kms retire-grant \
    --grant-id 1234a2345b8a4e350500d432bccf8ecd6506710e1391880c4f7f7140160c9af3 \
    --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Este comando no genera ninguna salida. Utilice el comando `list-grants` para confirmar que la concesión se ha retirado.

Para obtener más información, consulte Retiro y revocación de concesiones en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte RetireGrant en la Referencia de comandos de la AWS CLI.

`revoke-grant`

En el siguiente ejemplo de código, se muestra cómo utilizar `revoke-grant`.

AWS CLI

Revocación de una concesión en una clave maestra de cliente

En el siguiente ejemplo de `revoke-grant` se elimina una concesión de una clave de KMS. El siguiente comando de ejemplo especifica los parámetros `grant-id` y `key-id`. El valor del parámetro `key-id` puede ser el ID de clave o el ARN de la clave de KMS.

```
aws kms revoke-grant \
    --grant-id 1234a2345b8a4e350500d432bccf8ecd6506710e1391880c4f7f7140160c9af3 \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Este comando no genera ninguna salida. Utilice el comando `list-grants` para confirmar que la concesión se ha revocado.

Para obtener más información, consulte Retiro y revocación de concesiones en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte RevokeGrant en la Referencia de comandos de la AWS CLI.

`rotate-key-on-demand`

En el siguiente ejemplo de código, se muestra cómo utilizar `rotate-key-on-demand`.

AWS CLI

Para realizar rotación bajo demanda de una clave de KMS

El siguiente ejemplo de `rotate-key-on-demand` inicia inmediatamente la rotación del material de claves para la clave de KMS especificada.

```
aws kms rotate-key-on-demand \
```

```
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Salida:

```
{
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

Para obtener más información, consulte How to perform on-demand key rotation en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre las API, consulte RotateKeyOnDemand en la Referencia de comandos de la AWS CLI.

`schedule-key-deletion`

En el siguiente ejemplo de código, se muestra cómo utilizar `schedule-key-deletion`.

AWS CLI

Programación de la eliminación de una clave de KMS administrada por el cliente.

En el siguiente ejemplo de `schedule-key-deletion` se programa la eliminación de la clave de KMS administrada por el cliente especificada en 15 días.

El parámetro `--key-id` identifica las claves KMS. En este ejemplo, se utiliza un valor de ARN clave, pero puede utilizar el ID de clave o el ARN de la clave de KMS. El parámetro `--pending-window-in-days` especifica la duración del período de espera de 7 a 30 días. De forma predeterminada, el periodo de espera es de 30 días. En este ejemplo, se especifica un valor de 15, que indica a AWS que elimina permanentemente la clave de KMS 15 días después de que se complete el comando.

```
aws kms schedule-key-deletion \
    --key-id arn:aws:kms:us-
west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --pending-window-in-days 15
```

La respuesta incluye el ARN de la clave, el estado de la clave, el período de espera (`PendingWindowInDays`) y la fecha de eliminación en tiempo Unix. Para ver la fecha de

eliminación en hora local, utilice la consola de AWS KMS. Las claves KMS en el estado de clave `PendingDeletion` no se pueden utilizar en operaciones criptográficas.

```
{
    "KeyId": "arn:aws:kms:us-
west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "DeletionDate": "2022-06-18T23:43:51.272000+00:00",
    "KeyState": "PendingDeletion",
    "PendingWindowInDays": 15
}
```

Para obtener más información, consulte Eliminación de claves en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte ScheduleKeyDeletion en la Referencia de comandos de la AWS CLI.

`sign`

En el siguiente ejemplo de código, se muestra cómo utilizar `sign`.

AWS CLI

Ejemplo 1: generar una firma digital para un mensaje

El siguiente ejemplo de `sign` genera una firma criptográfica para un mensaje corto. El resultado del comando incluye un campo de `Signature` codificado en Base64 que puede comprobar mediante el comando `verify`.

Debe especificar un mensaje para firmar y un algoritmo de firma que admita su clave KMS asimétrica. Para obtener los algoritmos de firma de su clave KMS, utilice el comando `describe-key`.

En la CLI v2 de AWS, el valor del parámetro `message` debe estar codificado en Base64. O bien, puede guardar el mensaje en un archivo y usar el prefijo `fileb://`, que indica a la CLI de AWS que lea los datos binarios del archivo.

Antes de ejecutar este comando, reemplace el ID de clave de ejemplo por uno válido de su cuenta de AWS. El ID de clave debe representar una clave KMS asimétrica con un uso de clave de SIGN_VERIFY.

```
msg=(echo 'Hello World' | base64)

aws kms sign \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --message fileb://UnsignedMessage \
    --message-type RAW \
    --signing-algorithm RSASSA_PKCS1_V1_5_SHA_256
```

Salida:

```
{
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Signature": "ABCDEFhpyVYyTxbafE74ccSvEJLJr3zuoV1Hfymz4qv+/
fxmxNLA7SE1SiF8lHw80fKZZ3bJ...",
    "SigningAlgorithm": "RSASSA_PKCS1_V1_5_SHA_256"
}
```

Para obtener más información acerca del uso de claves KMS asimétricas en AWS, consulte Uso de claves en AWS KMS en la AWS Guía para desarrolladores de Key Management Service.

Ejemplo 2: guardar una firma digital en un archivo (Linux y macOS)

El siguiente ejemplo de `sign` genera una firma criptográfica para un mensaje corto almacenado en un archivo local. El comando también obtiene la propiedad `Signature` de la respuesta, la decodifica en Base64 y la guarda en el archivo ExampleSignature. Puede usar el archivo de firmas en un comando `verify` que verifique la firma.

El comando `sign` requiere un mensaje codificado en Base64 y un algoritmo de firma que admita su clave KMS asimétrica. Para obtener los algoritmos de firma que admite su clave KMS, utilice el comando `describe-key`.

Antes de ejecutar este comando, reemplace el ID de clave de ejemplo por uno válido de su cuenta de AWS. El ID de clave debe representar una clave KMS asimétrica con un uso de clave de SIGN_VERIFY.

```
echo 'hello world' | base64 > EncodedMessage

aws kms sign \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
```

```
    --message fileb://EncodedMessage \
    --message-type RAW \
    --signing-algorithm RSASSA_PKCS1_V1_5_SHA_256 \
    --output text \
    --query Signature | base64 --decode > ExampleSignature
```

Este comando no genera ninguna salida. En este ejemplo, se extrae la propiedad `Signature` del resultado y se guarda en un archivo.

Para obtener más información acerca del uso de claves KMS asimétricas en AWS KMS, consulte Uso de claves asimétricas en AWS KMS en la AWS Guía para desarrolladores de Key Management Service.

- Para obtener información de la API, consulte Sign en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para agregar una etiqueta a una clave de KMS

En el siguiente ejemplo de `tag-resource`, se agregan las etiquetas `"Purpose":"Test"` y `"Dept":"IT"` a una clave KMS administrada por el cliente. Puede usar etiquetas como estas para etiquetar las claves KMS y crear categorías de claves KMS para permisos y auditoría.

Para especificar la clave de KMS, utilice el parámetro `key-id`. En este ejemplo, se utiliza un valor de ID de clave, pero puede utilizar un ID de clave o un ARN de clave en este comando.

```
aws kms tag-resource \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --tags TagKey='Purpose',TagValue='Test' TagKey='Dept',TagValue='IT'
```

Este comando no genera ninguna salida. Para ver las etiquetas de una clave KMS de AWS KMS, utilice el comando `list-resource-tags`.

Para obtener información sobre el uso de etiquetas en AWS KMS, consulte Etiquetar claves en la Guía para desarrolladores de AWS Key Management Service.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar una etiqueta de una clave de KMS

En el siguiente ejemplo de `untag-resource` se elimina la etiqueta con la clave `"Purpose"` de una clave de KMS administrada por el cliente.

Para especificar la clave de KMS, utilice el parámetro `key-id`. En este ejemplo, se utiliza un valor de ID de clave, pero puede utilizar un ID de clave o un ARN de clave en este comando. Antes de ejecutar este comando, reemplace el ID de clave de ejemplo por uno válido de su cuenta de AWS.

```
aws kms untag-resource \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --tag-key 'Purpose'
```

Este comando no genera ninguna salida. Para ver las etiquetas de una clave KMS de AWS KMS, utilice el comando `list-resource-tags`.

Para obtener información sobre el uso de etiquetas en AWS KMS, consulte Etiquetar claves en la Guía para desarrolladores de AWS Key Management Service.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-alias`.

AWS CLI

Asociación de un alias a una clave de KMS diferente

En el siguiente ejemplo de `update-alias` se asocia el alias `alias/test-key` a una clave de KMS diferente.

El parámetro `--alias-name` especifica el alias. El valor del nombre del alias debe empezar por `alias/`. El parámetro `--target-key-id` especifica la clave de KMS que se va a asociar al alias. No es necesario especificar la clave de KMS actual para el alias.

```
aws kms update-alias \
    --alias-name alias/test-key \
    --target-key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Este comando no genera ninguna salida. Utilice el comando `list-aliases` para encontrar el alias.

Para obtener más información, consulte Actualización de alias en la AWSGuía para desarrolladores de Key Management Service.

- Para obtener información sobre la API, consulte UpdateAlias en la Referencia de comandos de la AWS CLI.

`update-custom-key-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-custom-key-store`.

AWS CLI

Ejemplo 1: editar el nombre descriptivo de un almacén de claves personalizado

En el siguiente ejemplo de `update-custom-key-store` se cambia el nombre del almacén de claves personalizado. Este ejemplo funciona para un almacén de claves de AWS CloudHSM o para un almacén de claves externo.

Utilice el `custom-key-store-id` para identificar el almacén de claves. Utilice el parámetro `new-custom-key-store-name` para especificar el nuevo nombre descriptivo.

Para actualizar el nombre descriptivo de un almacén de claves de AWS CloudHSM, primero debe desconectar el almacén de claves, por ejemplo, mediante el comando `disconnect-custom-key-store`. Puede actualizar el nombre descriptivo de un almacén de claves externo mientras esté conectado o desconectado. Para buscar el estado de conexión del almacén de claves personalizado, utilice el comando `describe-custom-key-store`.

```
aws kms update-custom-key-store \
```

```
    --custom-key-store-id cks-1234567890abcdef0 \
    --new-custom-key-store-name ExampleKeyStore
```

Este comando no devuelve ningún dato. Para comprobar si el comando ha funcionado, utilice un comando `describe-custom-key-stores`.

Para obtener información sobre cómo actualizar un almacén de claves de AWS CloudHSM, consulte Editing AWS CloudHSM key store settings en la Guía para desarrolladores de AWS Key Management Service.

Para obtener más información sobre cómo actualizar un almacén de claves externo, consulte Editing external key store properties en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 2: editar la contraseña kmsuser de un almacén de claves de AWS CloudHSM

En el siguiente ejemplo de `update-custom-key-store` se actualiza el valor de la contraseña `kmsuser` a la contraseña actual del `kmsuser` en el clúster de CloudHSM asociado al almacén de claves especificado. Este comando no cambia la contraseña `kmsuser` del clúster. Simplemente indica a AWS KMS la contraseña actual. Si KMS no tiene la contraseña `kmsuser` actual, no podrá conectarse al almacén de claves de AWS CloudHSM.

NOTA: Antes de actualizar un almacén de claves de AWS CloudHSM debe desconectarlo. Utilice el comando `disconnect-custom-key-store`. Cuando se completa el comando, puede volver a conectar el almacén de claves de AWS CloudHSM. Utilice el comando `connect-custom-key-store`.

```
aws kms update-custom-key-store \
    --custom-key-store-id cks-1234567890abcdef0 \
    --key-store-password ExamplePassword
```

El comando no devuelve ningún resultado. Para comprobar que el comando ha sido efectivo, utilice el comando `describe-custom-key-stores`.

Para obtener información sobre cómo actualizar un almacén de claves de AWS CloudHSM, consulte Editing AWS CloudHSM key store settings en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 3: editar el clúster de AWS CloudHSM de un almacén de claves de AWS CloudHSM

En el siguiente ejemplo se cambia el clúster de AWS CloudHSM asociado a un almacén de claves de AWS CloudHSM por un clúster relacionado, por ejemplo, una copia de seguridad diferente del mismo clúster.

NOTA: Antes de actualizar un almacén de claves de AWS CloudHSM debe desconectarlo. Utilice el comando `disconnect-custom-key-store`. Cuando se completa el comando, puede volver a conectar el almacén de claves de AWS CloudHSM. Utilice el comando `connect-custom-key-store`.

```
aws kms update-custom-key-store \
    --custom-key-store-id cks-1234567890abcdef0 \
    --cloud-hsm-cluster-id cluster-1a23b4cdefg
```

El comando no devuelve ningún resultado. Para comprobar que el comando ha sido efectivo, utilice el comando `describe-custom-key-stores`.

Para obtener información sobre cómo actualizar un almacén de claves de AWS CloudHSM, consulte Editing AWS CloudHSM key store settings en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 4: editar la credencial de autenticación proxy de un almacén de claves externo

En el siguiente ejemplo se actualiza la credencial de autenticación del proxy para el almacén de claves externo. Debe especificar el `raw-secret-access-key` y el `access-key-id`, incluso si cambia solo uno de los valores. Puede utilizar esta característica para corregir una credencial no válida o cambiarla cuando la rota el proxy del almacén de claves externo.

Establezca la credencial de autenticación del proxy para AWS KMS en el almacén de claves externo. A continuación, utilice este comando para proporcionar la credencial a AWS KMS. AWS KMS utiliza esta credencial para firmar sus solicitudes en el proxy del almacén de claves externo.

Puede actualizar la credencial de autenticación del proxy mientras el almacén de claves externo esté conectado o desconectado. Para buscar el estado de conexión del almacén de claves personalizado, utilice el comando `describe-custom-key-store`.

```
aws kms update-custom-key-store \
    --custom-key-store-id cks-1234567890abcdef0 \
    --xks-proxy-authentication-credential "AccessKeyId=ABCDE12345670EXAMPLE,
 RawSecretAccessKey=DXjSUawnel2fr6SKC7G25CNxTyWKE5PF9XX6H/u9pSo="
```

El comando no devuelve ningún resultado. Para comprobar que el comando ha sido efectivo, utilice el comando `describe-custom-key-stores`.

Para obtener más información sobre cómo actualizar un almacén de claves externo, consulte Editing external key store properties en la Guía para desarrolladores de AWS Key Management Service.

Ejemplo 5: editar la conectividad del proxy de un almacén de claves externo

En el siguiente ejemplo se cambia la opción de conectividad del proxy del almacén de claves externo de conectividad de punto de conexión público a punto de conexión de servicio de punto de conexión de VPC. Además de cambiar el valor de `xks-proxy-connectivity`, debe cambiar el valor de `xks-proxy-uri-endpoint` para que refleje el nombre de DNS privado asociado al servicio de punto de conexión de VPC. También debe añadir un valor de `xks-proxy-vpc-endpoint-service-name`.

NOTA: Antes de actualizar la conectividad del proxy de un almacén externo debe desconectarlo. Utilice el comando `disconnect-custom-key-store`. Una vez completado el comando, puede volver a conectar el almacén de claves externo mediante el comando `connect-custom-key-store`.

```
aws kms update-custom-key-store \
    --custom-key-store-id cks-1234567890abcdef0 \
    --xks-proxy-connectivity VPC_ENDPOINT_SERVICE \
    --xks-proxy-uri-endpoint "https://myproxy-private.xks.example.com" \
    --xks-proxy-vpc-endpoint-service-name "com.amazonaws.vpce.us-east-1.vpce-svc-example"
```

El comando no devuelve ningún resultado. Para comprobar que el comando ha sido efectivo, utilice el comando `describe-custom-key-stores`.

Para obtener más información sobre cómo actualizar un almacén de claves externo, consulte Editing external key store properties en la Guía para desarrolladores de AWS Key Management Service.

- Para obtener información sobre la API, consulte UpdateCustomKeyStore en la Referencia de comandos de AWS CLI.

update-key-description

En el siguiente ejemplo de código, se muestra cómo utilizar `update-key-description`.

AWS CLI

Ejemplo 1: agregar o cambiar una descripción de una clave de KMS administrada por el cliente

En el siguiente ejemplo de `update-key-description` se agrega una descripción a una clave de KMS administrada por el cliente. Puede utilizar el mismo comando para cambiar una descripción existente.

El parámetro `--key-id` identifica la clave de KMS en el comando. En este ejemplo se utiliza un valor de ARN de clave, pero puede utilizar el ID de clave o el ARN de la clave de KMS. El parámetro `--description` especifica la nueva descripción. El valor de este parámetro reemplaza a la descripción actual de la clave de KMS, si la hay.

```
aws kms update-key-description \
    --key-id arn:aws:kms:us-
west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --description "IT Department test key"
```

Este comando no genera ninguna salida. Para ver la descripción de una clave de KMS, utilice el comando `describe-key`.

Para obtener más información, consulte UpdateKeyDescription en la AWSReferencia de la API Key Management Service.

Ejemplo 2: eliminar la descripción de una clave de KMS administrada por el cliente

El siguiente ejemplo de `update-key-description` elimina la descripción de una clave de KMS administrada por el cliente

El parámetro `--key-id` identifica la clave de KMS en el comando. En este ejemplo se utiliza un valor de ID de clave, pero puede utilizar el ID de clave o el ARN de clave de la clave de KMS. El parámetro `--description` con un valor de cadena vacío ('') elimina la descripción existente.

```
aws kms update-key-description \
    --key-id 0987dcba-09fe-87dc-65ba-ab0987654321 \
    --description ''
```

Este comando no genera ninguna salida. Para ver la descripción de una clave de KMS, utilice el comando describe-key.

Para obtener más información, consulte UpdateKeyDescription en la AWSReferencia de la API Key Management Service.

- Para obtener información sobre la API, consulte UpdateKeyDescription en la Referencia de comandos de la AWS CLI.

`verify-mac`

En el siguiente ejemplo de código, se muestra cómo utilizar `verify-mac`.

AWS CLI

Ejemplo 1: Verificación de un HMAC

El siguiente comando `verify-mac` verifica un HMAC para un mensaje específico, claves KMS HMAC y un algoritmo MAC. Un valor de “true” en el campo MacValid de la respuesta indica que el HMAC es válido.

En la CLI v2 de AWS, el valor del parámetro `message` debe estar codificado en Base64. O bien, puede guardar el mensaje en un archivo y usar el prefijo `fileb://`, que indica a la CLI de AWS que lea los datos binarios del archivo.

El MAC que especifique no puede estar codificado en base64. Para obtener ayuda para decodificar el MAC que devuelve el comando `generate-mac`, consulte los ejemplos de comandos `generate-mac`.

Antes de ejecutar este comando, reemplace el ID de clave de ejemplo por uno válido de su cuenta de AWS. El ID de clave debe representar una clave KMS HMAC con un uso de clave de `GENERATE_VERIFY_MAC`.

```
msg=(echo 'Hello World' | base64)

aws kms verify-mac \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --message fileb://Message \
    --mac-algorithm HMAC_SHA_384 \
    --mac fileb://ExampleMac
```

Salida:

```
{
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "MacValid": true,
```

```
    "MacAlgorithm": "HMAC_SHA_384"
}
```

Para obtener más información acerca del uso de claves KMS HMAC en AWS KMS, consulte Claves HMAC en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

- Para ver los detalles de la API, consulte VerifyMac en la Referencia de comandos de la AWS CLI.

`verify`

En el siguiente ejemplo de código, se muestra cómo utilizar `verify`.

AWS CLI

Para verificar una firma digital

En el siguiente ejemplo de `verify`, se verifica una firma criptográfica para un mensaje corto codificado en Base64. El identificador de clave, el mensaje, el tipo de mensaje y el algoritmo de firma deben ser los mismos que se usaron para firmar el mensaje.

En la CLI v2 de AWS, el valor del parámetro `message` debe estar codificado en Base64. O bien, puede guardar el mensaje en un archivo y usar el prefijo `fileb://`, que indica a la CLI de AWS que lea los datos binarios del archivo.

La firma que especifique no puede estar codificada en base64. Para obtener ayuda para decodificar la firma que devuelve el comando `sign`, consulte los ejemplos de comandos `sign`.

El resultado del comando incluye un campo `SignatureValid` booleano que indica que se verificó la firma. Si se produce un error en la validación de la firma, también se produce un error en el comando `verify`.

Antes de ejecutar este comando, reemplace el ID de clave de ejemplo por uno válido de su cuenta de AWS.

```
aws kms verify \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --message fileb://EncodedMessage \
    --message-type RAW \
    --signing-algorithm RSASSA_PKCS1_V1_5_SHA_256 \
    --signature fileb://ExampleSignature
```

Salida:

```
{
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "SignatureValid": true,
    "SigningAlgorithm": "RSASSA_PKCS1_V1_5_SHA_256"
}
```

Para obtener más información sobre el uso de claves KMS asimétricas en AWS KMS, consulte Uso de claves simétricas y asimétricas en la AWSGuía para desarrolladores de Key Management Service.

- Para obtener información sobre la API, consulte Verify en la Referencia de comandos de la AWS CLI.

Ejemplos de Lake Formation que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios comunes utilizando la AWS Command Line Interface con Lake Formation.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-lf-tags-to-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-lf-tags-to-resource`.

AWS CLI

Para asociar una o más etiquetas LF a un recurso existente

En el siguiente ejemplo de `add-lf-tags-to-resource` se asocia una etiqueta LF determinada al recurso de tabla.

```
aws lakeformation add-lf-tags-to-resource \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "123456789111",
    "Resource": {
        "Table": {
            "CatalogId": "123456789111",
            "DatabaseName": "tpc",
            "Name": "dl_tpc_promotion"
        }
    },
    "LFTags": [{
        "CatalogId": "123456789111",
        "TagKey": "usergroup",
        "TagValues": [
            "analyst"
        ]
    }]
}
```

Salida:

```
{
    "Failures": []
}
```

Para obtener más información, consulte Assigning LF-Tags to Data Catalog resources en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener detalles sobre la API, consulte AddLfTagsToResource en la Referencia de comandos de la AWS CLI.

`batch-grant-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-grant-permissions`.

AWS CLI

Para conceder permisos masivos sobre recursos a las entidades principales

En el siguiente ejemplo de `batch-grant-permissions` se concede acceso masivo a recursos específicos a entidades principales.

```
aws lakeformation batch-grant-permissions \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "123456789111",
    "Entries": [{
            "Id": "1",
            "Principal": {
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-
developer"
            },
            "Resource": {
                "Table": {
                    "CatalogId": "123456789111",
                    "DatabaseName": "tpc",
                    "Name": "dl_tpc_promotion"
                }
            },
            "Permissions": [
                "ALL"
            ],
            "PermissionsWithGrantOption": [
                "ALL"
            ]
        },
        {
            "Id": "2",
            "Principal": {
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-
developer"
            },
            "Resource": {
                "Table": {
                    "CatalogId": "123456789111",
```

```
                    "DatabaseName": "tpc",
                    "Name": "dl_tpc_customer"
                }
            },
            "Permissions": [
                "ALL"
            ],
            "PermissionsWithGrantOption": [
                "ALL"
            ]
        },
        {
            "Id": "3",
            "Principal": {
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-
business-analyst"
            },
            "Resource": {
                "Table": {
                    "CatalogId": "123456789111",
                    "DatabaseName": "tpc",
                    "Name": "dl_tpc_promotion"
                }
            },
            "Permissions": [
                "ALL"
            ],
            "PermissionsWithGrantOption": [
                "ALL"
            ]
        },
        {
            "Id": "4",
            "Principal": {
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-
developer"
            },
            "Resource": {
                "DataCellsFilter": {
                    "TableCatalogId": "123456789111",
                    "DatabaseName": "tpc",
                    "TableName": "dl_tpc_item",
                    "Name": "developer_item"
                }
```

```
            },
            "Permissions": [
                "SELECT"
            ],
            "PermissionsWithGrantOption": []
        }
    ]
}
```

Salida:

```
{
    "Failures": []
}
```

Para obtener más información, consulte Granting and revoking permissions on Data Catalog resources en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener detalles sobre la API, consulte BatchGrantPermissions en la Referencia de comandos de AWS CLI.

`batch-revoke-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-revoke-permissions`.

AWS CLI

Para revocar permisos masivos sobre recursos de las entidades principales

En el siguiente ejemplo de `batch-revoke-permissions` se revoca acceso masivo a recursos específicos de entidades principales.

```
aws lakeformation batch-revoke-permissions \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "123456789111",
    "Entries": [{
            "Id": "1",
            "Principal": {
```

```
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-
developer"
            },
            "Resource": {
                "Table": {
                    "CatalogId": "123456789111",
                    "DatabaseName": "tpc",
                    "Name": "dl_tpc_promotion"
                }
            },
            "Permissions": [
                "ALL"
            ],
            "PermissionsWithGrantOption": [
                "ALL"
            ]
        },
        {
            "Id": "2",
            "Principal": {
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-
business-analyst"
            },
            "Resource": {
                "Table": {
                    "CatalogId": "123456789111",
                    "DatabaseName": "tpc",
                    "Name": "dl_tpc_promotion"
                }
            },
            "Permissions": [
                "ALL"
            ],
            "PermissionsWithGrantOption": [
                "ALL"
            ]
        }
    ]
}
```

Salida:

```
{
```

```
    "Failures": []
}
```

Para obtener más información, consulte Granting and revoking permissions on Data Catalog resources en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte BatchRevokePermissions en la Referencia de comandos de la AWS CLI.

`cancel-transaction`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-transaction`.

AWS CLI

Para cancelar una transacción

El siguiente ejemplo de `cancel-transaction` cancela la transacción.

```
aws lakeformation cancel-transaction \
    --transaction-id='b014d972ca8347b89825e33c5774aec4'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Reading from and writing to the data lake within transactions en la Guía para desarrolladores de AWS Lake Formation.

- Para ver detalles de la API, consulte CancelTransaction en la Referencia de comandos de la AWS CLI.

`commit-transaction`

En el siguiente ejemplo de código, se muestra cómo utilizar `commit-transaction`.

AWS CLI

Para confirmar una transacción

El siguiente ejemplo de `commit-transaction` cancela la transacción.

```
aws lakeformation commit-transaction \
    --transaction-id='b014d972ca8347b89825e33c5774aec4'
```

Salida:

```
{
    "TransactionStatus": "committed"
}
```

Para obtener más información, consulte Reading from and writing to the data lake within transactions en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte CommitTransaction en la Referencia de comandos de la AWS CLI.

`create-data-cells-filter`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-data-cells-filter`.

AWS CLI

Ejemplo 1: crear un filtro de celdas de datos

El siguiente ejemplo de `create-data-cells-filter` crea un filtro de celdas de datos para conceder acceso a determinadas columnas en función de la condición de la fila.

```
aws lakeformation create-data-cells-filter \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "TableData": {
        "ColumnNames": ["p_channel_details", "p_start_date_sk", "p_promo_name"],
        "DatabaseName": "tpc",
        "Name": "developer_promotion",
        "RowFilter": {
            "FilterExpression": "p_promo_name='ese'"
        },
        "TableCatalogId": "123456789111",
        "TableName": "dl_tpc_promotion"
    }
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Data filtering and cell-level security in Lake Formation en la Guía para desarrolladores de AWS Lake Formation.

Ejemplo 2: crear un filtro de columnas

El siguiente ejemplo de `create-data-cells-filter` crea un filtro de datos para conceder acceso a determinadas columnas.

```
aws lakeformation create-data-cells-filter \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "TableData": {
        "ColumnNames": ["p_channel_details", "p_start_date_sk", "p_promo_name"],
        "DatabaseName": "tpc",
        "Name": "developer_promotion_allrows",
        "RowFilter": {
            "AllRowsWildcard": {}
        },
        "TableCatalogId": "123456789111",
        "TableName": "dl_tpc_promotion"
    }
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Data filtering and cell-level security in Lake Formation en la Guía para desarrolladores de AWS Lake Formation.

Ejemplo 3: crear un filtro de datos con columnas excluidas

El siguiente ejemplo de `create-data-cells-filter` crea un filtro de datos para permitir conceder acceso a todas las columnas salvo las mencionadas.

```
aws lakeformation create-data-cells-filter \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
```

```
    "TableData": {
        "ColumnWildcard": {
            "ExcludedColumnNames": ["p_channel_details", "p_start_date_sk"]
        },
        "DatabaseName": "tpc",
        "Name": "developer_promotion_excludecolumn",
        "RowFilter": {
            "AllRowsWildcard": {}
        },
        "TableCatalogId": "123456789111",
        "TableName": "dl_tpc_promotion"
    }
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Data filtering and cell-level security in Lake Formation en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte CreateDataCellsFilter en la Referencia de comandos de la AWS CLI.

`create-lf-tag`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-lf-tag`.

AWS CLI

Para crear una etiqueta LF

En el siguiente ejemplo de `create-lf-tag` se crea una etiqueta LF con el nombre y los valores especificados.

```
aws lakeformation create-lf-tag \
    --catalog-id '123456789111' \
    --tag-key 'usergroup' \
    --tag-values '["developer","analyst","campaign"]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing LF-Tags for metadata access control en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte CreateLfTag en la Referencia de comandos de la AWS CLI.

`delete-data-cells-filter`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-data-cells-filter`.

AWS CLI

Para eliminar un filtro de celdas de datos

En el siguiente ejemplo de `delete-data-cells-filter` se elimina un filtro de celdas de datos específico.

```
aws lakeformation delete-data-cells-filter \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "TableCatalogId": "123456789111",
    "DatabaseName": "tpc",
    "TableName": "dl_tpc_promotion",
    "Name": "developer_promotion"
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Data filtering and cell-level security in Lake Formation en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte DeleteDataCellsFilter en la Referencia de comandos de la AWS CLI.

`delete-lf-tag`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-lf-tag`.

AWS CLI

Para eliminar una definición de etiqueta LF

En el siguiente ejemplo de `delete-lf-tag` se elimina la definición de etiqueta LF.

```
aws lakeformation delete-lf-tag \
    --catalog-id '123456789111' \
    --tag-key 'usergroup'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing LF-Tags for metadata access control en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte DeleteLfTag en la Referencia de comandos de la AWS CLI.

`delete-objects-on-cancel`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-objects-on-cancel`.

AWS CLI

Para eliminar un objeto cuando se cancela la transacción

El siguiente ejemplo de `delete-objects-on-cancel` elimina el objeto s3 indicado cuando se cancela la transacción.

```
aws lakeformation delete-objects-on-cancel \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "012345678901",
    "DatabaseName": "tpc",
    "TableName": "dl_tpc_household_demographics_gov",
    "TransactionId": "1234d972ca8347b89825e33c5774aec4",
    "Objects": [{
        "Uri": "s3://lf-data-lake-012345678901/target/
dl_tpc_household_demographics_gov/run-unnamed-1-part-block-0-r-00000-snappy-
ff26b17504414fe88b302cd795eabd00.parquet",
        "ETag": "1234ab1fc50a316b149b4e1f21a73800"
    }]
```

```
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Reading from and writing to the data lake within transactions en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte DeleteObjectsOnCancel en la Referencia de comandos de la AWS CLI.

`deregister-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-resource`.

AWS CLI

Para anular el registro del almacenamiento de un lago de datos

En el siguiente ejemplo de `deregister-resource` se anula el registro del recurso administrado por Lake Formation.

```
aws lakeformation deregister-resource \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ResourceArn": "arn:aws:s3:::lf-emr-athena-result-123"
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adding an Amazon S3 location to your data lake en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información acerca de la API, consulte DeregisterResource en la Referencia de comandos de la AWS CLI.

`describe-transaction`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-transaction`.

AWS CLI

Para recuperar los detalles de una transacción

El siguiente ejemplo de `describe-transaction` devuelve los detalles de una sola transacción.

```
aws lakeformation describe-transaction \
    --transaction-id='8cb4b1a7cc8d486fbaca9a64e7d9f5ce'
```

Salida:

```
{
    "TransactionDescription": {
        "TransactionId": "12345972ca8347b89825e33c5774aec4",
        "TransactionStatus": "committed",
        "TransactionStartTime": "2022-08-10T14:29:04.046000+00:00",
        "TransactionEndTime": "2022-08-10T14:29:09.681000+00:00"
    }
}
```

Para obtener más información, consulte Reading from and writing to the data lake within transactions en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte DescribeTransaction en la Referencia de comandos de la AWS CLI.

`extend-transaction`

En el siguiente ejemplo de código, se muestra cómo utilizar `extend-transaction`.

AWS CLI

Para ampliar una transacción

El siguiente ejemplo de `extend-transaction` amplía la transacción.

```
aws lakeformation extend-transaction \
    --transaction-id='8cb4b1a7cc8d486fbaca9a64e7d9f5ce'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Reading from and writing to the data lake within transactions en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener más información sobre la API, consulte ExtendTransaction en la Referencia de comandos de la AWS CLI.

`get-data-lake-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-data-lake-settings`.

AWS CLI

Para recuperar la configuración de un lago de datos administrado por AWS Lake Formation

El siguiente ejemplo de `get-data-lake-settings` recupera la lista de administradores del lago de datos y otros ajustes del lago de datos.

```
aws lakeformation get-data-lake-settings \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "123456789111"
}
```

Salida:

```
{
    "DataLakeSettings": {
        "DataLakeAdmins": [{
            "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-admin"
        }],
        "CreateDatabaseDefaultPermissions": [],
        "CreateTableDefaultPermissions": [
                {
                        "Principal": {
                            "DataLakePrincipalIdentifier": "IAM_ALLOWED_PRINCIPALS"
                        },
                        "Permissions": [
                            "ALL"
                        ]
```

```
                }
        ],
        "TrustedResourceOwners": [],
        "AllowExternalDataFiltering": true,
        "ExternalDataFilteringAllowList": [{
            "DataLakePrincipalIdentifier": "123456789111"
        }],
        "AuthorizedSessionTagValueList": [
            "Amazon EMR"
        ]
    }
}
```

Para obtener más información, consulte Changing the default security settings for your data lake en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte GetDataLakeSettings en la Referencia de comandos de la AWS CLI.

`get-effective-permissions-for-path`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-effective-permissions-for-path`.

AWS CLI

Para recuperar permisos de recursos ubicados en una ruta específica

En el siguiente ejemplo de `get-effective-permissions-for-path` se devuelven los permisos de Lake Formation para un recurso de tabla o base de datos especificado ubicado en una ruta de Amazon S3.

```
aws lakeformation get-effective-permissions-for-path \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "123456789111",
    "ResourceArn": "arn:aws:s3:::lf-data-lake-123456789111"
}
```

Salida:

```
{
    "Permissions": [{
            "Principal": {
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-
campaign-manager"
            },
            "Resource": {
                "Database": {
                    "Name": "tpc"
                }
            },
            "Permissions": [
                "DESCRIBE"
            ],
            "PermissionsWithGrantOption": []
        },
        {
            "Principal": {
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:role/EMR-
RuntimeRole"
            },
            "Resource": {
                "Database": {
                    "Name": "tpc"
                }
            },
            "Permissions": [
                "ALL"
            ],
            "PermissionsWithGrantOption": []
        },
        {
            "Principal": {
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:saml-
provider/oktaSAMLProvider:user/emr-developer"
            },
            "Resource": {
                "Database": {
                    "Name": "tpc"
                }
            },
            "Permissions": [
```

```
                "ALL",
                "DESCRIBE"
            ],
            "PermissionsWithGrantOption": []
        },
        {
            "Principal": {
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-
admin"
            },
            "Resource": {
                "Database": {
                    "Name": "tpc"
                }
            },
            "Permissions": [
                "ALL",
                "ALTER",
                "CREATE_TABLE",
                "DESCRIBE",
                "DROP"
            ],
            "PermissionsWithGrantOption": [
                "ALL",
                "ALTER",
                "CREATE_TABLE",
                "DESCRIBE",
                "DROP"
            ]
        },
        {
            "Principal": {
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:role/LF-
GlueServiceRole"
            },
            "Resource": {
                "Database": {
                    "Name": "tpc"
                }
            },
            "Permissions": [
                "CREATE_TABLE"
            ],
            "PermissionsWithGrantOption": []
```

```
        }
    ],
    "NextToken":
 "E5SlJDSTZleUp6SWpvaU9UQTNORE0zTXpFeE5Ua3pJbjE5TENKbGVIQnBjbUYwYVc5dUlqcDdJbk5sWTI5dVpITWlP
}
```

Para obtener más información, consulte Managing Lake Formation permissions en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte GetEffectivePermissionsForPath en la Referencia de comandos de la AWS CLI.

`get-lf-tag`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-lf-tag`.

AWS CLI

Para recuperar una definición de etiqueta LF

En el siguiente ejemplo de `get-lf-tag` se recupera la definición de una etiqueta LF.

```
aws lakeformation get-lf-tag \
    --catalog-id '123456789111' \
    --tag-key 'usergroup'
```

Salida:

```
{
    "CatalogId": "123456789111",
    "TagKey": "usergroup",
    "TagValues": [
        "analyst",
        "campaign",
        "developer"
    ]
}
```

Para obtener más información, consulte Managing LF-Tags for metadata access control en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte GetLfTag en la Referencia de comandos de la AWS CLI.

`get-query-state`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-query-state`.

AWS CLI

Para recuperar el estado de una consulta enviada

En el siguiente ejemplo de `get-query-state` se devuelve el estado de una consulta enviada anteriormente.

```
aws lakeformation get-query-state \
    --query-id='1234273f-4a62-4cda-8d98-69615ee8be9b'
```

Salida:

```
{
    "State": "FINISHED"
}
```

Para obtener más información, consulte Transactional data operations en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte GetQueryState en la Referencia de comandos de la AWS CLI.

`get-query-statistics`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-query-statistics`.

AWS CLI

Para recuperar estadísticas de consultas

En el siguiente ejemplo de `get-query-statistics` se recuperan las estadísticas sobre la planificación y la ejecución de una consulta.

```
aws lakeformation get-query-statistics \
```

```
    --query-id='1234273f-4a62-4cda-8d98-69615ee8be9b'
```

Salida:

```
{
    "ExecutionStatistics": {
        "AverageExecutionTimeMillis": 0,
        "DataScannedBytes": 0,
        "WorkUnitsExecutedCount": 0
    },
    "PlanningStatistics": {
        "EstimatedDataToScanBytes": 43235,
        "PlanningTimeMillis": 2377,
        "QueueTimeMillis": 440,
        "WorkUnitsGeneratedCount": 1
    },
    "QuerySubmissionTime": "2022-08-11T02:14:38.641870+00:00"
}
```

Para obtener más información, consulte Transactional data operations en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte GetQueryStatistics en la Referencia de comandos de la AWS CLI.

`get-resource-lf-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource-lf-tags`.

AWS CLI

Para mostrar etiquetas LF

En el siguiente ejemplo de `list-lf-tags` se devuelve la lista de etiquetas LF que el solicitante tiene permiso para ver.

```
aws lakeformation list-lf-tags \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
```

```
    "CatalogId": "123456789111",
    "ResourceShareType": "ALL",
    "MaxResults": 2
}
```

Salida:

```
{
"LFTags": [{
        "CatalogId": "123456789111",
        "TagKey": "category",
        "TagValues": [
            "private",
            "public"
        ]
    },
    {
        "CatalogId": "123456789111",
        "TagKey": "group",
        "TagValues": [
            "analyst",
            "campaign",
            "developer"
        ]
    }],
    "NextToken": "kIiwiZXhwaXJhdGlvbiI6eyJzZWNvbmRzIjoxNjYwMDY4dCI6ZmFsc2V9"
}
```

Para obtener más información, consulte Managing LF-Tags for metadata access control en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte GetResourceLfTags en la Referencia de comandos de la AWS CLI.

`get-table-objects`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-table-objects`.

AWS CLI

Para mostrar objetos de una tabla gobernada

En el siguiente ejemplo de `get-table-objects` se devuelve el conjunto de objetos de Amazon S3 que componen la tabla gobernada especificada.

```
aws lakeformation get-table-objects \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "012345678901",
    "DatabaseName": "tpc",
    "TableName": "dl_tpc_household_demographics_gov",
    "QueryAsOfTime": "2022-08-10T15:00:00"
}
```

Salida:

```
{
    "Objects": [{
        "PartitionValues": [],
        "Objects": [{
            "Uri": "s3://lf-data-lake-012345678901/target/
dl_tpc_household_demographics_gov/run-unnamed-1-part-block-0-r-00000-snappy-
ff26b17504414fe88b302cd795eabd00.parquet",
            "ETag": "12345b1fc50a316b149b4e1f21a73800",
            "Size": 43235
        }]
    }]
}
```

Para obtener más información, consulte Reading from and writing to the data lake within transactions en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte GetTableObjects en la Referencia de comandos de la AWS CLI.

`get-work-unit-results`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-work-unit-results`.

AWS CLI

Para recuperar unidades de trabajo de una consulta determinada

En el siguiente ejemplo de `get-work-unit-results` se devuelven las unidades de trabajo resultantes de la consulta.

```
aws lakeformation get-work-units \
    --query-id='1234273f-4a62-4cda-8d98-69615ee8be9b' \
    --work-unit-id '0' \
    --work-unit-token 'B2fMSdmQXe9umX8Ux8XCo4=' outfile
```

Salida:

```
outfile with Blob content.
```

Para obtener más información, consulte Transactional data operations en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte GetWorkUnitResults en la Referencia de comandos de la AWS CLI.

`get-work-units`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-work-units`.

AWS CLI

Para recuperar unidades de trabajo

En el siguiente ejemplo de `get-work-units` se recuperan las unidades de trabajo generadas por la operación StartQueryPlanning.

```
aws lakeformation get-work-units \
    --query-id='1234273f-4a62-4cda-8d98-69615ee8be9b'
```

Salida:

```
{
    "WorkUnitRanges": [{
        "WorkUnitIdMax": 0,
```

```
        "WorkUnitIdMin": 0,
        "WorkUnitToken":
 "1234eMAk4kLO4umqEL4Z5WuxL04AXwABABVhd3MtY3J5cHRvLXB1YmxpYy1rZXkAREEwYm9QbkhINmFYTWphbmMxZW
+f88jzGrYq22gE6jkQlpOB
+Oet2eqNUmFudAAAAfjB8BgkqhkiG9w0BBwagbzBtAgEAMGgGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMCOEWRda
wAAAAEAAAAAAAAAAAAAAAEAAACX3/w5h75QAPomfKH+cyEKYU1yccUmBl
+VSojiGOtdsUk7vcjYXUUboYm3dvqRqX2s4gROMOn
+Ij8R0/8jYmnHkpvyAFNVRPyETyIKg7k5Z9+5I1c2d3446Jw/moWGGxjH8AEG9h27ytmOhozxDOEi/
F2ZoXz6wlGDfGUo/2WxCkYOhTyNaw6TM
+7drTM7yrW4iNVLUM0LX0xnFjIAhLhooWJek6vjQZUAZzBlAjBH8okRtYP8R7AY2Wls/
hqFBhG0V4l42AC0LxsuZbMQrE2SzWZUZ0E9Uew7/n0cyX4CMQDR79INyv4ysMByW9kKGGKyba+cCNklExMR
+btBQBmMuB2fMSdmQXe9umX8Ux8XCo4="
    }],
    "QueryId": "1234273f-4a62-4cda-8d98-69615ee8be9b"
}
```

Para obtener más información, consulte Transactional data operations en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte GetWorkUnits en la Referencia de comandos de la AWS CLI.

`grant-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `grant-permissions`.

AWS CLI

Ejemplo 1: conceder permisos a la entidad principal sobre los recursos mediante etiquetas LF

En el siguiente ejemplo de `grant-permissions` se conceden TODOS los permisos a la entidad principal en el recurso de base de datos que coincida con la política de etiquetas LF.

```
aws lakeformation grant-permissions \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "123456789111",
    "Principal": {
        "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-admin"
```

```
    },
    "Resource": {
        "LFTagPolicy": {
            "CatalogId": "123456789111",
            "ResourceType": "DATABASE",
            "Expression": [{
                "TagKey": "usergroup",
                "TagValues": [
                    "analyst",
                    "developer"
                ]
            }]
        }
    },
    "Permissions": [
        "ALL"
    ],
    "PermissionsWithGrantOption": [
        "ALL"
    ]
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Granting and revoking permissions on Data Catalog resources en la Guía para desarrolladores de AWS Lake Formation.

Ejemplo 2: conceder permisos de nivel de columna a la entidad principal

En el siguiente ejemplo de `grant-permissions` se concede permiso a la entidad principal para seleccionar una columna específica.

```
aws lakeformation grant-permissions \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "123456789111",
    "Principal": {
        "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-developer"
    },
```

```
    "Resource": {
        "TableWithColumns": {
            "CatalogId": "123456789111",
            "ColumnNames": ["p_end_date_sk"],
            "DatabaseName": "tpc",
            "Name": "dl_tpc_promotion"
        }
    },
    "Permissions": [
        "SELECT"
    ],
    "PermissionsWithGrantOption": []
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Granting and revoking permissions on Data Catalog resources en la Guía para desarrolladores de AWS Lake Formation.

Ejemplo 3: conceder permisos de tabla a la entidad principal

En el siguiente ejemplo de `grant-permissions` se concede a la entidad principal permiso de selección en todas las tablas de una base de datos determinada.

```
aws lakeformation grant-permissions \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "123456789111",
    "Principal": {
        "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-developer"
    },
    "Resource": {
        "Table": {
            "CatalogId": "123456789111",
            "DatabaseName": "tpc",
            "TableWildcard": {}
        }
    },
    "Permissions": [
```

```
        "SELECT"
    ],
    "PermissionsWithGrantOption": []
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Granting and revoking permissions on Data Catalog resources en la Guía para desarrolladores de AWS Lake Formation.

Ejemplo 4: conceder permisos sobre etiquetas LF a la entidad principal

En el siguiente ejemplo de `grant-permissions` se concede permiso de asociación sobre etiquetas LF a la entidad principal.

```
aws lakeformation grant-permissions \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "123456789111",
    "Principal": {
        "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-developer"
    },
    "Resource": {
        "LFTag": {
            "CatalogId": "123456789111",
            "TagKey": "category",
            "TagValues": [
                "private", "public"
            ]
        }

    },
    "Permissions": [
        "ASSOCIATE"
    ],
    "PermissionsWithGrantOption": []
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Granting and revoking permissions on Data Catalog resources en la Guía para desarrolladores de AWS Lake Formation.

Ejemplo 5: conceder permisos sobre ubicaciones de datos a la entidad principal

En el siguiente ejemplo de `grant-permissions` se conceden permisos de ubicación de datos a la entidad principal.

```
aws lakeformation grant-permissions \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "123456789111",
    "Principal": {
        "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-developer"
    },
    "Resource": {
        "DataLocation": {
            "CatalogId": "123456789111",
            "ResourceArn": "arn:aws:s3:::lf-data-lake-123456789111"
        }
    },
    "Permissions": [
        "DATA_LOCATION_ACCESS"
    ],
    "PermissionsWithGrantOption": []
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Granting and revoking permissions on Data Catalog resources en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte GrantPermissions en la Referencia de comandos de la AWS CLI.

`list-data-cells-filter`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-data-cells-filter`.

AWS CLI

Para mostrar filtros de celdas de datos

En el siguiente ejemplo de `list-data-cells-filter` se muestra un filtro de celdas de datos para una tabla determinada.

```
aws lakeformation list-data-cells-filter \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "MaxResults": 2,
    "Table": {
        "CatalogId": "123456789111",
        "DatabaseName": "tpc",
        "Name": "dl_tpc_promotion"
    }
}
```

Salida:

```
{
    "DataCellsFilters": [{
            "TableCatalogId": "123456789111",
            "DatabaseName": "tpc",
            "TableName": "dl_tpc_promotion",
            "Name": "developer_promotion",
            "RowFilter": {
                "FilterExpression": "p_promo_name='ese'"
            },
            "ColumnNames": [
                "p_channel_details",
                "p_start_date_sk",
                "p_purpose",
                "p_promo_id",
                "p_promo_name",
                "p_end_date_sk",
                "p_discount_active"
            ]
        },
```

```
        {
            "TableCatalogId": "123456789111",
            "DatabaseName": "tpc",
            "TableName": "dl_tpc_promotion",
            "Name": "developer_promotion_allrows",
            "RowFilter": {
                "FilterExpression": "TRUE",
                "AllRowsWildcard": {}
            },
            "ColumnNames": [
                "p_channel_details",
                "p_start_date_sk",
                "p_promo_name"
            ]
        }
    ],
    "NextToken": "2MDA2MTgwNiwibmFub3MiOjE0MDAwMDAwMH19"
}
```

Para obtener más información, consulte Data filtering and cell-level security in Lake Formation en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte ListDataCellsFilter en la Referencia de comandos de la AWS CLI.

`list-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-permissions`.

AWS CLI

Ejemplo 1: recuperar una lista de permisos de la entidad principal sobre un recurso

En el siguiente ejemplo de `list-permissions` se devuelve una lista de permisos de la entidad principal sobre recursos de la base de datos.

```
aws lakeformation list-permissions \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
```

```
    "CatalogId": "123456789111",
    "ResourceType": "DATABASE",
    "MaxResults": 2
}
```

Salida:

```
{
    "PrincipalResourcePermissions": [{
        "Principal": {
            "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-
campaign-manager"
        },
        "Resource": {
            "Database": {
                "CatalogId": "123456789111",
                "Name": "tpc"
            }
        },
        "Permissions": [
            "DESCRIBE"
        ],
        "PermissionsWithGrantOption": []
    }],
    "NextToken":
 "E5SlJDSTZleUp6SWpvaU9UQTNORE0zTXpFeE5Ua3pJbjE5TENKbGVIQnBjbUYwYVc5dUlqcDdJbk5sWTI5dVpITWlP
}
```

Para obtener más información, consulte Managing Lake Formation permissions en la Guía para desarrolladores de AWS Lake Formation.

Ejemplo 2: recuperar una lista de permisos de la entidad principal sobre la tabla con filtros de datos

En el siguiente ejemplo de `list-permissions` se enumeran los permisos de tabla con filtros de datos relacionados concedidos a la entidad principal.

```
aws lakeformation list-permissions \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "123456789111",
    "Resource": {
        "Table": {
            "CatalogId": "123456789111",
            "DatabaseName": "tpc",
            "Name": "dl_tpc_customer"
        }
    },
    "IncludeRelated": "TRUE",
    "MaxResults": 10
}
```

Salida:

```
{
    "PrincipalResourcePermissions": [{
            "Principal": {
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:role/
Admin"
            },
            "Resource": {
                "Table": {
                    "CatalogId": "123456789111",
                    "DatabaseName": "customer",
                    "Name": "customer_invoice"
                }
            },
            "Permissions": [
                "ALL",
                "ALTER",
                "DELETE",
                "DESCRIBE",
                "DROP",
                "INSERT"
            ],
            "PermissionsWithGrantOption": [
                "ALL",
                "ALTER",
                "DELETE",
                "DESCRIBE",
                "DROP",
                "INSERT"
```

```
            ]
        },
        {
            "Principal": {
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:role/
Admin"
            },
            "Resource": {
                "TableWithColumns": {
                    "CatalogId": "123456789111",
                    "DatabaseName": "customer",
                    "Name": "customer_invoice",
                    "ColumnWildcard": {}
                }
            },
            "Permissions": [
                "SELECT"
            ],
            "PermissionsWithGrantOption": [
                "SELECT"
            ]
        },
        {
            "Principal": {
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:role/
Admin"
            },
            "Resource": {
                "DataCellsFilter": {
                    "TableCatalogId": "123456789111",
                    "DatabaseName": "customer",
                    "TableName": "customer_invoice",
                    "Name": "dl_us_customer"
                }
            },
            "Permissions": [
                "DESCRIBE",
                "SELECT",
                "DROP"
            ],
            "PermissionsWithGrantOption": []
        }
    ],
    "NextToken": "VyeUFjY291bnRQZXJtaXNzaW9ucyI6ZmFsc2V9"
```

```
}
```

Para obtener más información, consulte Managing Lake Formation permissions en la Guía para desarrolladores de AWS Lake Formation.

Ejemplo 3: recuperar una lista de permisos de la entidad principal sobre las etiquetas LF

En el siguiente ejemplo de `list-permissions` se enumeran los permisos sobre etiquetas LF concedidos a la entidad principal.

```
aws lakeformation list-permissions \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "123456789111",
    "Resource": {
        "LFTag": {
            "CatalogId": "123456789111",
            "TagKey": "category",
            "TagValues": [
                "private"
            ]
        }
    },
    "MaxResults": 10
}
```

Salida:

```
{
    "PrincipalResourcePermissions": [{
            "Principal": {
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-
admin"
            },
            "Resource": {
                "LFTag": {
                    "CatalogId": "123456789111",
                    "TagKey": "category",
```

```
                    "TagValues": [
                        "*"
                    ]
                }
            },
            "Permissions": [
                "DESCRIBE"
            ],
            "PermissionsWithGrantOption": [
                "DESCRIBE"
            ]
        },
        {
            "Principal": {
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-
admin"
            },
            "Resource": {
                "LFTag": {
                    "CatalogId": "123456789111",
                    "TagKey": "category",
                    "TagValues": [
                        "*"
                    ]
                }
            },
            "Permissions": [
                "ASSOCIATE"
            ],
            "PermissionsWithGrantOption": [
                "ASSOCIATE"
            ]
        }
    ],
    "NextToken": "EJwY21GMGFXOXVJanA3SW5Ocm1pc3Npb25zIjpmYWxzZX0="
}
```

Para obtener más información, consulte Managing Lake Formation permissions en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte ListPermissions en la Referencia de comandos de la AWS CLI.

`list-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resources`.

AWS CLI

Para enumerar los recursos administrados por Lake Formation

En el siguiente ejemplo de `list-resources` se enumeran los recursos que coinciden con la condición que administra Lake Formation.

```
aws lakeformation list-resources \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "FilterConditionList": [{
        "Field": "ROLE_ARN",
        "ComparisonOperator": "CONTAINS",
        "StringValueList": [
            "123456789111"
        ]
    }],
    "MaxResults": 10
}
```

Salida:

```
{
    "ResourceInfoList": [{
            "ResourceArn": "arn:aws:s3:::lf-data-lake-123456789111",
            "RoleArn": "arn:aws:iam::123456789111:role/LF-GlueServiceRole",
            "LastModified": "2022-07-21T02:12:46.669000+00:00"
        },
        {
            "ResourceArn": "arn:aws:s3:::lf-emr-test-123456789111",
            "RoleArn": "arn:aws:iam::123456789111:role/EMRLFS3Role",
            "LastModified": "2022-07-29T16:22:03.211000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Managing Lake Formation permissions en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener más información sobre la API, consulte ListResources en la Referencia de comandos de la AWS CLI.

`list-transactions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-transactions`.

AWS CLI

Para enumerar todos los detalles de las transacciones

En el siguiente ejemplo de `list-transactions` se devuelven metadatos sobre transacciones y su estado.

```
aws lakeformation list-transactions \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "123456789111",
    "StatusFilter": "ALL",
    "MaxResults": 3
}
```

Salida:

```
{
    "Transactions": [{
            "TransactionId": "1234569f08804cb790d950d4d0fe485e",
            "TransactionStatus": "committed",
            "TransactionStartTime": "2022-08-10T14:32:29.220000+00:00",
            "TransactionEndTime": "2022-08-10T14:32:33.751000+00:00"
        },
        {
            "TransactionId": "12345972ca8347b89825e33c5774aec4",
            "TransactionStatus": "committed",
            "TransactionStartTime": "2022-08-10T14:29:04.046000+00:00",
```

```
            "TransactionEndTime": "2022-08-10T14:29:09.681000+00:00"
        },
        {
            "TransactionId": "12345daf6cb047dbba8ad9b0414613b2",
            "TransactionStatus": "committed",
            "TransactionStartTime": "2022-08-10T13:56:51.261000+00:00",
            "TransactionEndTime": "2022-08-10T13:56:51.547000+00:00"
        }
    ],
    "NextToken": "77X1ebypsI7os+X2lhHsZLGNCDK3nNGpwRdFpicSOHgcX1/
QMoniUAKcpR3kj3ts3PVdMA=="
}
```

Para obtener más información, consulte Reading from and writing to the data lake within transactions en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte ListTransactions en la Referencia de comandos de la AWS CLI.

`put-data-lake-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-data-lake-settings`.

AWS CLI

Para establecer la configuración de un lago de datos administrado por AWS Lake Formation

En el siguiente ejemplo de `put-data-lake-settings`, se establece la lista de administradores del lago de datos y otros ajustes del lago de datos.

```
aws lakeformation put-data-lake-settings \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "DataLakeSettings": {
        "DataLakeAdmins": [{
                "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-
admin"
            }
        ],
```

```
        "CreateDatabaseDefaultPermissions": [],
        "CreateTableDefaultPermissions": [],
        "TrustedResourceOwners": [],
        "AllowExternalDataFiltering": true,
        "ExternalDataFilteringAllowList": [{
            "DataLakePrincipalIdentifier ": "123456789111"
        }],
        "AuthorizedSessionTagValueList": ["Amazon EMR"]
    }
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Changing the default security settings for your data lake en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte PutDataLakeSettings en la Referencia de comandos de la AWS CLI.

`register-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-resource`.

AWS CLI

Ejemplo 1: registrar almacenamiento de lago de datos mediante un rol vinculado al servicio

En el siguiente ejemplo de `register-resource` se registra el recurso administrado por Lake Formation utilizando un rol vinculado al servicio.

```
aws lakeformation register-resource \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ResourceArn": "arn:aws:s3:::lf-emr-athena-result-123",
    "UseServiceLinkedRole": true
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adding an Amazon S3 location to your data lake en la Guía para desarrolladores de AWS Lake Formation.

Ejemplo 2: registrar almacenamiento de lago de datos mediante un rol personalizado

En el siguiente ejemplo de `register-resource` se registra el recurso administrado por Lake Formation utilizando un rol personalizado.

```
aws lakeformation register-resource \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "ResourceArn": "arn:aws:s3:::lf-emr-athena-result-123",
    "UseServiceLinkedRole": false,
    "RoleArn": "arn:aws:iam::123456789111:role/LF-GlueServiceRole"
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adding an Amazon S3 location to your data lake en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte RegisterResource en la Referencia de comandos de la AWS CLI.

`remove-lf-tags-from-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-lf-tags-from-resource`.

AWS CLI

Para eliminar una etiqueta LF de un recurso

En el siguiente ejemplo de `remove-lf-tags-from-resource` se elimina la asociación de etiqueta LF con el recurso de tabla.

```
aws lakeformation remove-lf-tags-from-resource \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "123456789111",
    "Resource": {
        "Table": {
            "CatalogId": "123456789111",
            "DatabaseName": "tpc",
            "Name": "dl_tpc_promotion"
        }
    },
    "LFTags": [{
        "CatalogId": "123456789111",
        "TagKey": "usergroup",
        "TagValues": [
            "developer"
        ]
    }]
}
```

Salida:

```
{
    "Failures": []
}
```

Para obtener más información, consulte Assigning LF-Tags to Data Catalog resources en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte RemoveLfTagsFromResource en la Referencia de comandos de la AWS CLI.

`revoke-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `revoke-permissions`.

AWS CLI

Para revocar permisos sobre recursos de la entidad principal

En el siguiente ejemplo de `revoke-permissions` se revoca el acceso de la entidad principal a una tabla específica de una base de datos determinada.

```
aws lakeformation revoke-permissions \
```

```
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "123456789111",
    "Principal": {
        "DataLakePrincipalIdentifier": "arn:aws:iam::123456789111:user/lf-developer"
    },
    "Resource": {
        "Table": {
            "CatalogId": "123456789111",
            "DatabaseName": "tpc",
            "Name": "dl_tpc_promotion"
        }
    },
    "Permissions": [
        "ALL"
    ],
    "PermissionsWithGrantOption": []
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Granting and revoking permissions on Data Catalog resources en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte RevokePermissions en la Referencia de comandos de la AWS CLI.

`search-databases-by-lf-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-databases-by-lf-tags`.

AWS CLI

Para buscar recursos de base de datos por LFTags

En el siguiente ejemplo de `search-databases-by-lf-tags` se buscan recursos de base de datos que coincidan con la expresión de LFTag.

```
aws lakeformation search-databases-by-lf-tags \
```

```
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "MaxResults": 1,
    "CatalogId": "123456789111",
    "Expression": [{
        "TagKey": "usergroup",
        "TagValues": [
            "developer"
        ]
    }]
}
```

Salida:

```
{
    "DatabaseList": [{
        "Database": {
            "CatalogId": "123456789111",
            "Name": "tpc"
        },
        "LFTags": [{
            "CatalogId": "123456789111",
            "TagKey": "usergroup",
            "TagValues": [
                "developer"
            ]
        }]
    }]
}
```

Para obtener más información, consulte Viewing the resources that a LF-Tag is assigned to en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener más información sobre la API, consulte SearchDatabasesByLfTags en la Referencia de comandos de la AWS CLI.

`search-tables-by-lf-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-tables-by-lf-tags`.

AWS CLI

Para buscar recursos de tabla por LFTags

En el siguiente ejemplo de `search-tables-by-lf-tags` se buscan recursos de tabla que coincidan con la expresión de LFTag.

```
aws lakeformation search-tables-by-lf-tags \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "MaxResults": 2,
    "CatalogId": "123456789111",
    "Expression": [{
        "TagKey": "usergroup",
        "TagValues": [
            "developer"
        ]
    }]
}
```

Salida:

```
{
    "NextToken": "c2VhcmNoQWxsVGFnc0luVGFibGVzIjpmYWxzZX0=",
    "TableList": [{
        "Table": {
            "CatalogId": "123456789111",
            "DatabaseName": "tpc",
            "Name": "dl_tpc_item"
        },
        "LFTagOnDatabase": [{
            "CatalogId": "123456789111",
            "TagKey": "usergroup",
            "TagValues": [
                "developer"
            ]
        }],
        "LFTagsOnTable": [{
            "CatalogId": "123456789111",
            "TagKey": "usergroup",
```

```
            "TagValues": [
                "developer"
            ]
        }],
        "LFTagsOnColumns": [{
                "Name": "i_item_desc",
                "LFTags": [{
                    "CatalogId": "123456789111",
                    "TagKey": "usergroup",
                    "TagValues": [
                        "developer"
                    ]
                }]
            },
            {
                "Name": "i_container",
                "LFTags": [{
                    "CatalogId": "123456789111",
                    "TagKey": "usergroup",
                    "TagValues": [
                        "developer"
                    ]
                }]
            },
            {
                "Name": "i_wholesale_cost",
                "LFTags": [{
                    "CatalogId": "123456789111",
                    "TagKey": "usergroup",
                    "TagValues": [
                        "developer"
                    ]
                }]
            },
            {
                "Name": "i_manufact_id",
                "LFTags": [{
                    "CatalogId": "123456789111",
                    "TagKey": "usergroup",
                    "TagValues": [
                        "developer"
                    ]
                }]
            },
```

```
            {
                "Name": "i_brand_id",
                "LFTags": [{
                    "CatalogId": "123456789111",
                    "TagKey": "usergroup",
                    "TagValues": [
                        "developer"
                    ]
                }]
            },
            {
                "Name": "i_formulation",
                "LFTags": [{
                    "CatalogId": "123456789111",
                    "TagKey": "usergroup",
                    "TagValues": [
                        "developer"
                    ]
                }]
            },
            {
                "Name": "i_current_price",
                "LFTags": [{
                    "CatalogId": "123456789111",
                    "TagKey": "usergroup",
                    "TagValues": [
                        "developer"
                    ]
                }]
            },
            {
                "Name": "i_size",
                "LFTags": [{
                    "CatalogId": "123456789111",
                    "TagKey": "usergroup",
                    "TagValues": [
                        "developer"
                    ]
                }]
            },
            {
                "Name": "i_rec_start_date",
                "LFTags": [{
                    "CatalogId": "123456789111",
```

```
                "TagKey": "usergroup",
                "TagValues": [
                    "developer"
                ]
            }]
        },
        {
            "Name": "i_manufact",
            "LFTags": [{
                "CatalogId": "123456789111",
                "TagKey": "usergroup",
                "TagValues": [
                    "developer"
                ]
            }]
        },
        {
            "Name": "i_item_sk",
            "LFTags": [{
                "CatalogId": "123456789111",
                "TagKey": "usergroup",
                "TagValues": [
                    "developer"
                ]
            }]
        },
        {
            "Name": "i_manager_id",
            "LFTags": [{
                "CatalogId": "123456789111",
                "TagKey": "usergroup",
                "TagValues": [
                    "developer"
                ]
            }]
        },
        {
            "Name": "i_item_id",
            "LFTags": [{
                "CatalogId": "123456789111",
                "TagKey": "usergroup",
                "TagValues": [
                    "developer"
                ]
```

```
            }]
        },
        {
            "Name": "i_class_id",
            "LFTags": [{
                "CatalogId": "123456789111",
                "TagKey": "usergroup",
                "TagValues": [
                    "developer"
                ]
            }]
        },
        {
            "Name": "i_class",
            "LFTags": [{
                "CatalogId": "123456789111",
                "TagKey": "usergroup",
                "TagValues": [
                    "developer"
                ]
            }]
        },
        {
            "Name": "i_category",
            "LFTags": [{
                "CatalogId": "123456789111",
                "TagKey": "usergroup",
                "TagValues": [
                    "developer"
                ]
            }]
        },
        {
            "Name": "i_category_id",
            "LFTags": [{
                "CatalogId": "123456789111",
                "TagKey": "usergroup",
                "TagValues": [
                    "developer"
                ]
            }]
        },
        {
            "Name": "i_brand",
```

```
                "LFTags": [{
                    "CatalogId": "123456789111",
                    "TagKey": "usergroup",
                    "TagValues": [
                        "developer"
                    ]
                }]
            },
            {
                "Name": "i_units",
                "LFTags": [{
                    "CatalogId": "123456789111",
                    "TagKey": "usergroup",
                    "TagValues": [
                        "developer"
                    ]
                }]
            },
            {
                "Name": "i_rec_end_date",
                "LFTags": [{
                    "CatalogId": "123456789111",
                    "TagKey": "usergroup",
                    "TagValues": [
                        "developer"
                    ]
                }]
            },
            {
                "Name": "i_color",
                "LFTags": [{
                    "CatalogId": "123456789111",
                    "TagKey": "usergroup",
                    "TagValues": [
                        "developer"
                    ]
                }]
            },
            {
                "Name": "i_product_name",
                "LFTags": [{
                    "CatalogId": "123456789111",
                    "TagKey": "usergroup",
                    "TagValues": [
```

```
                        "developer"
                    ]
                }]
            }
        ]
    }]
}
```

Para obtener más información, consulte Viewing the resources that a LF-Tag is assigned to en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener más información sobre la API, consulte SearchTablesByLfTags en la Referencia de comandos de la AWS CLI.

`start-query-planning`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-query-planning`.

AWS CLI

Para procesar una instrucción de consulta

En el siguiente ejemplo de `start-query-planning` se envía una solicitud para procesar una instrucción de consulta.

```
aws lakeformation start-query-planning \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "QueryPlanningContext": {
        "CatalogId": "012345678901",
        "DatabaseName": "tpc"
    },
    "QueryString": "select * from dl_tpc_household_demographics_gov where
 hd_income_band_sk=9"
}
```

Salida:

```
{
```

```
    "QueryId": "772a273f-4a62-4cda-8d98-69615ee8be9b"
}
```

Para obtener más información, consulte Reading from and writing to the data lake within transactions en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte StartQueryPlanning en la Referencia de comandos de la AWS CLI.

`start-transaction`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-transaction`.

AWS CLI

Para iniciar una nueva transacción

En el siguiente ejemplo de `start-transaction` se inicia una nueva transacción y se devuelve su ID de transacción.

```
aws lakeformation start-transaction \
    --transaction-type = 'READ_AND_WRITE'
```

Salida:

```
{
    "TransactionId": "b014d972ca8347b89825e33c5774aec4"
}
```

Para obtener más información, consulte Reading from and writing to the data lake within transactions en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte StartTransaction en la Referencia de comandos de la AWS CLI.

`update-lf-tag`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-lf-tag`.

AWS CLI

Para actualizar una definición de etiqueta LF

En el siguiente ejemplo de `update-lf-tag` se actualiza la definición de etiqueta LF.

```
aws lakeformation update-lf-tag \
    --catalog-id '123456789111' \
    --tag-key 'usergroup' \
    --tag-values-to-add '["admin"]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing LF-Tags for metadata access control en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información sobre la API, consulte UpdateLfTag en la Referencia de comandos de la AWS CLI.

`update-table-objects`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-table-objects`.

AWS CLI

Para modificar objetos de una tabla gobernada

En el siguiente ejemplo de `update-table-objects` se agregan objetos S3 proporcionados a la tabla gobernada especificada.

```
aws lakeformation update-table-objects \
    --cli-input-json file://input.json
```

Contenido de `input.json`:

```
{
    "CatalogId": "012345678901",
    "DatabaseName": "tpc",
    "TableName": "dl_tpc_household_demographics_gov",
    "TransactionId": "12347a9f75424b9b915f6ff201d2a190",
    "WriteOperations": [{
        "AddObject": {
            "Uri": "s3://lf-data-lake-012345678901/target/
dl_tpc_household_demographics_gov/run-unnamed-1-part-block-0-r-00000-snappy-
ff26b17504414fe88b302cd795eabd00.parquet",
            "ETag": "1234ab1fc50a316b149b4e1f21a73800",
```

```
            "Size": 42200
        }
    }]
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Reading from and writing to the data lake within transactions en la Guía para desarrolladores de AWS Lake Formation.

- Para obtener información acerca de la API, consulte UpdateTableObjects en la Referencia de comandos de la AWS CLI.

Ejemplos de Lambda que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Lambda.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-layer-version-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-layer-version-permission`.

AWS CLI

Para añadir permisos a una versión de capa

En el siguiente ejemplo de `add-layer-version-permission`, se concede permiso a la cuenta especificada para utilizar la versión 1 de la capa `my-layer`.

```
aws lambda add-layer-version-permission \
    --layer-name my-layer \
    --statement-id xaccount \
    --action lambda:GetLayerVersion  \
    --principal 123456789012 \
    --version-number 1
```

Salida:

```
{
    "RevisionId": "35d87451-f796-4a3f-a618-95a3671b0a0c",
    "Statement":
    {
        "Sid":"xaccount",
        "Effect":"Allow",
        "Principal":{
            "AWS":"arn:aws:iam::210987654321:root"
        },
        "Action":"lambda:GetLayerVersion",
        "Resource":"arn:aws:lambda:us-east-2:123456789012:layer:my-layer:1"
    }
}
```

Para obtener más información, consulte Capas de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte AddLayerVersionPermission en la Referencia de comandos de la AWS CLI.

`add-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-permission`.

AWS CLI

Para añadir permisos a una función de Lambda existente

El siguiente ejemplo de `add-permission` concede permiso al servicio de Amazon SNS para invocar una función llamada `my-function`.

```
aws lambda add-permission \
```

```
    --function-name my-function \
    --action lambda:InvokeFunction \
    --statement-id sns \
    --principal sns.amazonaws.com
```

Salida:

```
{
    "Statement":
    {
        "Sid":"sns",
        "Effect":"Allow",
        "Principal":{
            "Service":"sns.amazonaws.com"
        },
        "Action":"lambda:InvokeFunction",
        "Resource":"arn:aws:lambda:us-east-2:123456789012:function:my-function"
    }
}
```

Para obtener más información, consulte Uso de políticas basadas en recursos para AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener más información sobre la API, consulte AddPermission en la Referencia de comandos de la AWS CLI.

`create-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-alias`.

AWS CLI

Creación de un alias para una función de Lambda

En el siguiente ejemplo de `create-alias`, se crea un alias llamado `LIVE` que apunta a la versión 1 de la función de Lambda `my-function`.

```
aws lambda create-alias \
    --function-name my-function \
    --description "alias for live version of function" \
    --function-version 1 \
    --name LIVE
```

Salida:

```
{
    "FunctionVersion": "1",
    "Name": "LIVE",
    "AliasArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function:LIVE",
    "RevisionId": "873282ed-4cd3-4dc8-a069-d0c647e470c6",
    "Description": "alias for live version of function"
}
```

Para obtener más información, consulte Configuración de los alias de las funciones de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para ver los detalles de la API, consulte CreateAlias en la Referencia de comandos de la AWS CLI.

`create-event-source-mapping`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-event-source-mapping`.

AWS CLI

Para crear una asignación entre un origen de eventos y una función de AWS Lambda

En el siguiente ejemplo de `create-event-source-mapping` se crea una asignación entre una cola de SQS y la función de Lambda `my-function`.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --batch-size 5 \
    --event-source-arn arn:aws:sqs:us-west-2:123456789012:mySQSqueue
```

Salida:

```
{
    "UUID": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
    "StateTransitionReason": "USER_INITIATED",
    "LastModified": 1569284520.333,
    "BatchSize": 5,
    "State": "Creating",
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
```

```
    "EventSourceArn": "arn:aws:sqs:us-west-2:123456789012:mySQSqueue"
}
```

Para obtener más información sobre los eventos en Lambda, consulte Mapeos de origen de eventos AWS en la Guía para desarrolladores de AWS.

- Para obtener información sobre la API, consulte CreateEventSourceMapping en la Referencia de comandos de la AWS CLI.

`create-function`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-function`.

AWS CLI

Para crear una función de Lambda

El siguiente ejemplo de `create-function` crea una función de Lambda con el nombre `my-function`.

```
aws lambda create-function \
    --function-name my-function \
    --runtime nodejs22.x \
    --zip-file fileb://my-function.zip \
    --handler my-function.handler \
    --role arn:aws:iam::123456789012:role/service-role/MyTestFunction-role-tges6bf4
```

Contenido de `my-function.zip`:

```
This file is a deployment package that contains your function code and any
 dependencies.
```

Salida:

```
{
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "CodeSha256": "PFn4S+er27qk+UuZSTKEQfNKG/XNn7QJs90mJgq6oH8=",
    "FunctionName": "my-function",
```

```
    "CodeSize": 308,
    "RevisionId": "873282ed-4cd3-4dc8-a069-d0c647e470c6",
    "MemorySize": 128,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "Version": "$LATEST",
    "Role": "arn:aws:iam::123456789012:role/service-role/MyTestFunction-role-
zgur6bf4",
    "Timeout": 3,
    "LastModified": "2025-10-14T22:26:11.234+0000",
    "Handler": "my-function.handler",
    "Runtime": "nodejs22.x",
    "Description": ""
}
```

Para obtener más información, consulte Configuración de la memoria de funciones de Lambda en la Guía para desarrolladores de Lambda de AWS.

- Para obtener información de la API, consulte CreateFunction en la Referencia de comandos de la AWS CLI.

`delete-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-alias`.

AWS CLI

Eliminación de un alias de función de Lambda

En el siguiente ejemplo de `delete-alias`, se elimina el alias nombrado `LIVE` de la función de Lambda `my-function`.

```
aws lambda delete-alias \
    --function-name my-function \
    --name LIVE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de los alias de las funciones de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para ver los detalles de la API, consulte DeleteTopic en la Referencia de comandos de la AWS CLI.

`delete-event-source-mapping`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-event-source-mapping`.

AWS CLI

Para eliminar una asignación entre un origen de eventos y una función de AWS Lambda

En el siguiente ejemplo de `delete-event-source-mapping` se elimina una asignación entre una cola de SQS y la función de `my-function` Lambda.

```
aws lambda delete-event-source-mapping \
    --uuid  a1b2c3d4-5678-90ab-cdef-11111EXAMPLE
```

Salida:

```
{
    "UUID": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
    "StateTransitionReason": "USER_INITIATED",
    "LastModified": 1569285870.271,
    "BatchSize": 5,
    "State": "Deleting",
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "EventSourceArn": "arn:aws:sqs:us-west-2:123456789012:mySQSqueue"
}
```

Para obtener más información sobre los eventos en Lambda, consulte Mapeos de origen de eventos AWS en la Guía para desarrolladores de AWS.

- Para obtener información sobre la API, consulte DeleteEventSourceMapping en la Referencia de comandos de la AWS CLI.

`delete-function-concurrency`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-function-concurrency`.

AWS CLI

Eliminación del límite de ejecución simultánea reservado de una función

En el siguiente ejemplo de `delete-function-concurrency`, se elimina el límite de ejecución simultánea reservado de la función `my-function`.

```
aws lambda delete-function-concurrency \
    --function-name  my-function
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Reserva de simultaneidad para una función de Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte DeleteFunctionConcurrency en la Referencia de comandos de la AWS CLI.

`delete-function-event-invoke-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-function-event-invoke-config`.

AWS CLI

Para eliminar la configuración de una invocación asíncrona

En el siguiente ejemplo de `delete-function-event-invoke-config` se elimina la configuración de invocación asíncrona para el alias `GREEN` de la función especificada.

```
aws lambda delete-function-event-invoke-config --function-name my-function:GREEN
```

- Para obtener información sobre la API, consulte DeleteFunctionEventInvokeConfig en la Referencia de comandos de la AWS CLI.

`delete-function`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-function`.

AWS CLI

Ejemplo 1: eliminar una función de Lambda con el nombre de la función

En el siguiente ejemplo de `delete-function`, se elimina la función de Lambda denominada `my-function` especificando el nombre de la función.

```
aws lambda delete-function \
    --function-name my-function
```

Este comando no genera ninguna salida.

Ejemplo 2: eliminar una función de Lambda con el ARN de la función

En el siguiente ejemplo de `delete-function`, se elimina la función de Lambda denominada `my-function` especificando el ARN de la función.

```
aws lambda delete-function \
    --function-name arn:aws:lambda:us-west-2:123456789012:function:my-function
```

Este comando no genera ninguna salida.

Ejemplo 3: eliminar una función de Lambda con el ARN parcial de la función

En el siguiente ejemplo de `delete-function`, se elimina la función de Lambda denominada `my-function` especificando el ARN parcial de la función.

```
aws lambda delete-function \
    --function-name 123456789012:function:my-function
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración las funciones de Lambda de AWS en la Guía para desarrolladores de Lambda de AWS.

- Para obtener información de la API, consulte DeleteFunction en la Referencia de comandos de la AWS CLI.

`delete-layer-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-layer-version`.

AWS CLI

Para eliminar una versión de una capa de Lambda

En el siguiente ejemplo de `delete-layer-version`, se elimina la versión 2 de la capa llamada `my-layer`.

```
aws lambda delete-layer-version \
    --layer-name my-layer \
```

```
    --version-number 2
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Capas de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte DeleteLayerVersion en la Referencia de comandos de la AWS CLI.

`delete-provisioned-concurrency-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-provisioned-concurrency-config`.

AWS CLI

Eliminación de la configuración de simultaneidad aprovisionada

En el siguiente ejemplo de `delete-provisioned-concurrency-config`, se elimina la configuración de simultaneidad aprovisionada para el alias `GREEN` de la función especificada.

```
aws lambda delete-provisioned-concurrency-config \
    --function-name my-function \
    --qualifier GREEN
```

- Para obtener información sobre la API, consulte DeleteProvisionedConcurrencyConfig en la Referencia de comandos de la AWS CLI.

`get-account-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-account-settings`.

AWS CLI

Recuperación de detalles de su cuenta en una región de AWS

En el siguiente ejemplo de `get-account-settings`, se muestran los límites de Lambda y la información de uso de su cuenta.

```
aws lambda get-account-settings
```

Salida:

```
{
    "AccountLimit": {
       "CodeSizeUnzipped": 262144000,
       "UnreservedConcurrentExecutions": 1000,
       "ConcurrentExecutions": 1000,
       "CodeSizeZipped": 52428800,
       "TotalCodeSize": 80530636800
    },
    "AccountUsage": {
       "FunctionCount": 4,
       "TotalCodeSize": 9426
    }
}
```

Para obtener más información, consulte Límites de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte GetAccountSettings en la Referencia de comandos de la AWS CLI.

`get-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-alias`.

AWS CLI

Recuperación de detalles sobre el alias de una función

En el siguiente ejemplo de `get-alias`, se muestran detalles del alias nombrado `LIVE` de la función de Lambda `my-function`.

```
aws lambda get-alias \
    --function-name my-function \
    --name LIVE
```

Salida:

```
{
    "FunctionVersion": "3",
```

```
    "Name": "LIVE",
    "AliasArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function:LIVE",
    "RevisionId": "594f41fb-b85f-4c20-95c7-6ca5f2a92c93",
    "Description": "alias for live version of function"
}
```

Para obtener más información, consulte Configuración de los alias de las funciones de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para ver los detalles de la API, consulte GetAlias en la Referencia de comandos de AWS CLI.

`get-event-source-mapping`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-event-source-mapping`.

AWS CLI

Para recuperar detalles sobre una asignación de orígenes de eventos

En el siguiente ejemplo de `get-event-source-mapping` se muestran los detalles de la asignación entre una cola de SQS y la función de `my-function` Lambda.

```
aws lambda get-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
```

Salida:

```
{
    "UUID": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
    "StateTransitionReason": "USER_INITIATED",
    "LastModified": 1569284520.333,
    "BatchSize": 5,
    "State": "Enabled",
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "EventSourceArn": "arn:aws:sqs:us-west-2:123456789012:mySQSqueue"
}
```

Para obtener más información sobre los eventos en Lambda, consulte Mapeos de origen de eventos AWS en la Guía para desarrolladores de AWS.

- Para obtener información sobre la API, consulte GetEventSourceMapping en la Referencia de comandos de la AWS CLI.

`get-function-concurrency`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-function-concurrency`.

AWS CLI

Visualización de la configuración de simultaneidad reservada para una función

En el siguiente ejemplo de `get-function-concurrency`, se recupera la configuración de simultaneidad reservada para la función especificada.

```
aws lambda get-function-concurrency \
    --function-name my-function
```

Salida:

```
{
    "ReservedConcurrentExecutions": 250
}
```

- Para obtener información sobre la API, consulte GetFunctionConcurrency en la Referencia de comandos de la AWS CLI.

`get-function-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-function-configuration`.

AWS CLI

Recuperación de la configuración específica de la versión de una función de Lambda

En el siguiente ejemplo de `get-function-configuration`, se muestran los ajustes de la versión 2 de la función `my-function`.

```
aws lambda get-function-configuration \
    --function-name  my-function:2
```

Salida:

```
{
```

```
    "FunctionName": "my-function",
    "LastModified": "2019-09-26T20:28:40.438+0000",
    "RevisionId": "e52502d4-9320-4688-9cd6-152a6ab7490d",
    "MemorySize": 256,
    "Version": "2",
    "Role": "arn:aws:iam::123456789012:role/service-role/my-function-role-uy3l9qyq",
    "Timeout": 3,
    "Runtime": "nodejs10.x",
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "CodeSha256": "5tT2qgzYUHaqwR716pZ2dpkn/0J1FrzJmlKidWoaCgk=",
    "Description": "",
    "VpcConfig": {
        "SubnetIds": [],
        "VpcId": "",
        "SecurityGroupIds": []
    },
    "CodeSize": 304,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function:2",
    "Handler": "index.handler"
}
```

Para obtener más información, consulte Configuración las funciones de Lambda de AWS en la Guía para desarrolladores de Lambda de AWS.

- Para obtener información sobre la API, consulte GetFunctionConfiguration en la Referencia de comandos de la AWS CLI.

`get-function-event-invoke-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-function-event-invoke-config`.

AWS CLI

Para ver la configuración de una invocación asíncrona

En el siguiente ejemplo de `get-function-event-invoke-config` se recupera la configuración de invocación asíncrona para el alias `BLUE` de la función especificada.

```
aws lambda get-function-event-invoke-config \
```

```
    --function-name my-function:BLUE
```

Salida:

```
{
    "LastModified": 1577824396.653,
    "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-
function:BLUE",
    "MaximumRetryAttempts": 0,
    "MaximumEventAgeInSeconds": 3600,
    "DestinationConfig": {
        "OnSuccess": {},
        "OnFailure": {
            "Destination": "arn:aws:sqs:us-east-2:123456789012:failed-invocations"
        }
    }
}
```

- Para obtener información sobre la API, consulte GetFunctionEventInvokeConfig en la Referencia de comandos de la AWS CLI.

`get-function`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-function`.

AWS CLI

Cómo recuperar información sobre una función

En el siguiente ejemplo de `get-function` se muestra información sobre la función `my-function`.

```
aws lambda get-function \
    --function-name  my-function
```

Salida:

```
{
    "Concurrency": {
        "ReservedConcurrentExecutions": 100
    },
    "Code": {
```

```
        "RepositoryType": "S3",
        "Location": "https://awslambda-us-west-2-tasks.s3.us-west-2.amazonaws.com/
snapshots/123456789012/my-function..."
    },
    "Configuration": {
        "TracingConfig": {
            "Mode": "PassThrough"
        },
        "Version": "$LATEST",
        "CodeSha256": "5tT2qgzYUHoqwR616pZ2dpkn/0J1FrzJmlKidWaaCgk=",
        "FunctionName": "my-function",
        "VpcConfig": {
            "SubnetIds": [],
            "VpcId": "",
            "SecurityGroupIds": []
        },
        "MemorySize": 128,
        "RevisionId": "28f0fb31-5c5c-43d3-8955-03e76c5c1075",
        "CodeSize": 304,
        "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
        "Handler": "index.handler",
        "Role": "arn:aws:iam::123456789012:role/service-role/helloWorldPython-role-
uy3l9qyq",
        "Timeout": 3,
        "LastModified": "2025-09-24T18:20:35.054+0000",
        "Runtime": "nodejs22.x",
        "Description": ""
    }
}
```

Para obtener más información, consulte Configuración de la memoria de funciones de Lambda en la Guía para desarrolladores de Lambda de AWS.

- Para obtener información sobre la API, consulte GetFunction en la Referencia de comandos de la AWS CLI.

`get-layer-version-by-arn`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-layer-version-by-arn`.

AWS CLI

Para recuperar información sobre una versión de capa de Lambda

En el siguiente ejemplo de `get-layer-version-by-arn` se muestra información sobre la versión de capa con el nombre de recurso de Amazon (ARN) especificado.

```
aws lambda get-layer-version-by-arn \
    --arn "arn:aws:lambda:us-west-2:123456789012:layer:AWSLambda-Python311-SciPy1x:2"
```

Salida:

```
{
    "LayerVersionArn": "arn:aws:lambda:us-west-2:123456789012:layer:AWSLambda-Python311-SciPy1x:2",
    "Description": "AWS Lambda SciPy layer for Python 3.11 (scipy-1.1.0, numpy-1.15.4) https://github.com/scipy/scipy/releases/tag/v1.1.0 https://github.com/numpy/numpy/releases/tag/v1.15.4",
    "CreatedDate": "2023-10-12T10:09:38.398+0000",
    "LayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:AWSLambda-Python311-SciPy1x",
    "Content": {
        "CodeSize": 41784542,
        "CodeSha256": "GGmv8ocUw4cly0T8HL0Vx/f5V4RmSCGNjDIslY4VskM=",
        "Location": "https://awslambda-us-west-2-layers.s3.us-west-2.amazonaws.com/snapshots/123456789012/..."
    },
    "Version": 2,
    "CompatibleRuntimes": [
        "python3.11"
    ],
    "LicenseInfo": "SciPy: https://github.com/scipy/scipy/blob/main/LICENSE.txt, NumPy: https://github.com/numpy/numpy/blob/main/LICENSE.txt"
}
```

Para obtener más información, consulte Capas de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte GetLayerVersionByArn en la Referencia de comandos de la AWS CLI.

`get-layer-version-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-layer-version-policy`.

AWS CLI

Para recuperar la política de permisos de una versión de capa de Lambda

En el siguiente ejemplo de `get-layer-version-policy`, se muestra información sobre la política de la versión 1 de la capa llamada `my-layer`.

```
aws lambda get-layer-version-policy \
    --layer-name my-layer \
    --version-number 1
```

Salida:

```
{
    "Policy": {
        "Version":"2012-10-17",
        "Id":"default",
        "Statement":
        [
            {
                "Sid":"xaccount",
                "Effect":"Allow",
                "Principal": {"AWS":"arn:aws:iam::123456789012:root"},
                "Action":"lambda:GetLayerVersion",
                "Resource":"arn:aws:lambda:us-west-2:123456789012:layer:my-layer:1"
            }
        ]
    },
    "RevisionId": "c68f21d2-cbf0-4026-90f6-1375ee465cd0"
}
```

Para obtener más información, consulte Capas de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte GetLayerVersionPolicy en la Referencia de comandos de la AWS CLI.

`get-layer-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-layer-version`.

AWS CLI

Para recuperar información sobre una versión de capa de Lambda

En el siguiente ejemplo de `get-layer-version`, se muestra información sobre la versión 1 de la capa llamada `my-layer`.

```
aws lambda get-layer-version \
    --layer-name my-layer \
    --version-number 1
```

Salida:

```
{
    "Content": {
        "Location": "https://awslambda-us-east-2-layers.s3.us-east-2.amazonaws.com/
snapshots/123456789012/my-layer-4aaa2fbb-ff77-4b0a-ad92-5b78a716a96a?
versionId=27iWyA73cCAYqyH...",
        "CodeSha256": "tv9jJO+rPbXUUXuRKi7CwHzKtLDkDRJLB3cC3Z/ouXo=",
        "CodeSize": 169
    },
    "LayerArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer",
    "LayerVersionArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:1",
    "Description": "My Python layer",
    "CreatedDate": "2018-11-14T23:03:52.894+0000",
    "Version": 1,
    "LicenseInfo": "MIT",
    "CompatibleRuntimes": [
        "python3.10",
        "python3.11"
    ]
}
```

Para obtener más información, consulte Capas de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte GetLayerVersion en la Referencia de comandos de la AWS CLI.

`get-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-policy`.

AWS CLI

Recuperación de la política de IAM basada en recursos para una función, una versión o un alias

En el siguiente ejemplo de `get-policy` se muestra información de la política sobre la función de Lambda `my-function`.

```
aws lambda get-policy \
    --function-name my-function
```

Salida:

```
{
    "Policy": {
        "Version":"2012-10-17",
        "Id":"default",
        "Statement":
        [
            {
                "Sid":"iot-events",
                "Effect":"Allow",
                "Principal": {"Service":"iotevents.amazonaws.com"},
                "Action":"lambda:InvokeFunction",
                "Resource":"arn:aws:lambda:us-west-2:123456789012:function:my-
function"
            }
        ]
    },
    "RevisionId": "93017fc9-59cb-41dc-901b-4845ce4bf668"
}
```

Para obtener más información, consulte Uso de políticas basadas en recursos para AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte GetPolicy en la Referencia de comandos de la AWS CLI.

`get-provisioned-concurrency-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-provisioned-concurrency-config`.

AWS CLI

Visualización de una configuración de simultaneidad aprovisionada

En el siguiente ejemplo de `get-provisioned-concurrency-config` se muestran detalles de la configuración de simultaneidad aprovisionada para el alias BLUE de la función especificada.

```
aws lambda get-provisioned-concurrency-config \
    --function-name my-function \
    --qualifier BLUE
```

Salida:

```
{
    "RequestedProvisionedConcurrentExecutions": 100,
    "AvailableProvisionedConcurrentExecutions": 100,
    "AllocatedProvisionedConcurrentExecutions": 100,
    "Status": "READY",
    "LastModified": "2019-12-31T20:28:49+0000"
}
```

- Para obtener información sobre la API, consulte GetProvisionedConcurrencyConfig en la Referencia de comandos de la AWS CLI.

`invoke`

En el siguiente ejemplo de código, se muestra cómo utilizar `invoke`.

AWS CLI

Ejemplo 1: invocar una función de Lambda de forma sincrónica

En el siguiente ejemplo de `invoke`, se invoca la función `my-function` de forma sincrónica. La opción `cli-binary-format` es obligatoria si va a utilizar la versión 2 de la CLI de AWS. Para obtener más información, consulte las opciones globales de la línea de comandos admitidas en la CLI de AWS en la Guía del usuario de la interfaz de línea de comandos de AWS.

```
aws lambda invoke \
    --function-name my-function \
    --cli-binary-format raw-in-base64-out \
    --payload '{ "name": "Bob" }' \
```

```
    response.json
```

Salida:

```
{
    "ExecutedVersion": "$LATEST",
    "StatusCode": 200
}
```

Para obtener más información, consulte Invocar una función de Lambda de forma sincrónica en la Guía para desarrolladores de AWS Lambda.

Ejemplo 2: invocar una función de Lambda de forma asíncrona

En el siguiente ejemplo de `invoke`, se invoca la función `my-function` de forma asíncrona. La opción `cli-binary-format` es obligatoria si va a utilizar la versión 2 de la CLI de AWS. Para obtener más información, consulte las opciones globales de la línea de comandos admitidas en la CLI de AWS en la Guía del usuario de la interfaz de línea de comandos de AWS.

```
aws lambda invoke \
    --function-name my-function \
    --invocation-type Event \
    --cli-binary-format raw-in-base64-out \
    --payload '{ "name": "Bob" }' \
    response.json
```

Salida:

```
{
    "StatusCode": 202
}
```

Para obtener más información, consulte Invocar una función de Lambda de forma asincrónica en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte Invocar en la Referencia de comandos de la AWS CLI.

`list-aliases`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-aliases`.

AWS CLI

Para recuperar la lista de alias para una función de Lambda

En el siguiente ejemplo de `list-aliases` se muestra una lista de alias de la función de Lambda `my-function`.

```
aws lambda list-aliases \
    --function-name my-function
```

Salida:

```
{
    "Aliases": [
        {
            "AliasArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:BETA",
            "RevisionId": "a410117f-ab16-494e-8035-7e204bb7933b",
            "FunctionVersion": "2",
            "Name": "BETA",
            "Description": "alias for beta version of function"
        },
        {
            "AliasArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:LIVE",
            "RevisionId": "21d40116-f8b1-40ba-9360-3ea284da1bb5",
            "FunctionVersion": "1",
            "Name": "LIVE",
            "Description": "alias for live version of function"
        }
    ]
}
```

Para obtener más información, consulte Configuración de los alias de las funciones de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para ver los detalles de la API, consulte ListAliases en la Referencia de comandos de la AWS CLI.

`list-event-source-mappings`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-event-source-mappings`.

AWS CLI

Para mostrar las asignaciones de orígenes de eventos de una función

En el siguiente ejemplo de `list-event-source-mappings` se muestra una lista de asignaciones de orígenes de eventos de la función de Lambda `my-function`.

```
aws lambda list-event-source-mappings \
    --function-name my-function
```

Salida:

```
{
    "EventSourceMappings": [
        {
            "UUID": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
            "StateTransitionReason": "USER_INITIATED",
            "LastModified": 1569284520.333,
            "BatchSize": 5,
            "State": "Enabled",
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function",
            "EventSourceArn": "arn:aws:sqs:us-west-2:123456789012:mySQSqueue"
        }
    ]
}
```

Para obtener más información sobre los eventos en Lambda, consulte Mapeos de origen de eventos AWS en la Guía para desarrolladores de AWS.

- Para obtener información sobre la API, consulte ListEventSourceMappings en la Referencia de comandos de la AWS CLI.

`list-function-event-invoke-configs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-function-event-invoke-configs`.

AWS CLI

Para ver una lista de configuraciones de invocación asíncrona

En el siguiente ejemplo de `list-function-event-invoke-configs` se enumeran las configuraciones de invocación asíncrona para la función especificada.

```
aws lambda list-function-event-invoke-configs \
    --function-name my-function
```

Salida:

```
{
    "FunctionEventInvokeConfigs": [
        {
            "LastModified": 1577824406.719,
            "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-
function:GREEN",
            "MaximumRetryAttempts": 2,
            "MaximumEventAgeInSeconds": 1800
        },
        {
            "LastModified": 1577824396.653,
            "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-
function:BLUE",
            "MaximumRetryAttempts": 0,
            "MaximumEventAgeInSeconds": 3600
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListFunctionEventInvokeConfigs en la Referencia de comandos de la AWS CLI.

`list-functions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-functions`.

AWS CLI

Cómo recuperar una lista de funciones de Lambda

En el siguiente ejemplo de `list-functions`, se muestra una lista de todas las funciones para el usuario actual:

```
aws lambda list-functions
```

Salida:

```
{
    "Functions": [
        {
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "$LATEST",
            "CodeSha256": "dBG9m8SGdmlEjw/JYXlhhvCrAv5TxvXsbL/RMr0fT/I=",
            "FunctionName": "helloworld",
            "MemorySize": 128,
            "RevisionId": "1718e831-badf-4253-9518-d0644210af7b",
            "CodeSize": 294,
            "FunctionArn": "arn:aws:lambda:us-
west-2:123456789012:function:helloworld",
            "Handler": "helloworld.handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/MyTestFunction-
role-zgur6bf4",
            "Timeout": 3,
            "LastModified": "2025-09-23T18:32:33.857+0000",
            "Runtime": "nodejs22.x",
            "Description": ""
        },
        {
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "$LATEST",
            "CodeSha256": "sU0cJ2/hOZevwV/lTxCuQqK3gDZP3i8gUoqUUVRmY6E=",
            "FunctionName": "my-function",
            "VpcConfig": {
                "SubnetIds": [],
                "VpcId": "",
                "SecurityGroupIds": []
            },
            "MemorySize": 256,
            "RevisionId": "93017fc9-59cb-41dc-901b-4845ce4bf668",
            "CodeSize": 266,
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function",
```

```
            "Handler": "index.handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/helloWorldPython-
role-uy3l9qyq",
            "Timeout": 3,
            "LastModified": "2025-10-01T16:47:28.490+0000",
            "Runtime": "nodejs22.x",
            "Description": ""
        },
        {
            "Layers": [
                {
                    "CodeSize": 41784542,
                    "Arn": "arn:aws:lambda:us-west-2:420165488524:layer:AWSLambda-
Python37-SciPy1x:2"
                },
                {
                    "CodeSize": 4121,
                    "Arn": "arn:aws:lambda:us-
west-2:123456789012:layer:pythonLayer:1"
                }
            ],
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "$LATEST",
            "CodeSha256": "ZQukCqxtkqFgyF2cU41Avj99TKQ/hNihPtDtRcc08mI=",
            "FunctionName": "my-python-function",
            "VpcConfig": {
                "SubnetIds": [],
                "VpcId": "",
                "SecurityGroupIds": []
            },
            "MemorySize": 128,
            "RevisionId": "80b4eabc-acf7-4ea8-919a-e874c213707d",
            "CodeSize": 299,
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
python-function",
            "Handler": "lambda_function.lambda_handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/my-python-function-
role-z5g7dr6n",
            "Timeout": 3,
            "LastModified": "2025-10-01T19:40:41.643+0000",
            "Runtime": "python3.11",
            "Description": ""
```

```
        }
    ]
}
```

Para obtener más información, consulte Configuración de la memoria de funciones de Lambda en la Guía para desarrolladores de Lambda de AWS.

- Para obtener información sobre la API, consulte ListFunctions en la Referencia de comandos de la AWS CLI.

`list-layer-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-layer-versions`.

AWS CLI

Para mostrar las versiones de una capa de AWS Lambda

En el siguiente ejemplo de `list-layers-versions` se muestra información sobre las versiones de la capa llamada `my-layer`.

```
aws lambda list-layer-versions \
    --layer-name my-layer
```

Salida:

```
{
    "Layers": [
        {
            "LayerVersionArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-
layer:2",
            "Version": 2,
            "Description": "My layer",
            "CreatedDate": "2023-11-15T00:37:46.592+0000",
            "CompatibleRuntimes": [
                "python3.10",
                "python3.11"
            ]
        }
    ]
}
```

Para obtener más información, consulte Capas de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte ListLayerVersions en la Referencia de comandos de la AWS CLI.

`list-layers`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-layers`.

AWS CLI

Para mostrar capas que sean compatibles con el tiempo de ejecución de una función

En el siguiente ejemplo de `list-layers` se muestra información sobre las capas que son compatibles con el tiempo de ejecución de Python 3.11.

```
aws lambda list-layers \
    --compatible-runtime python3.11
```

Salida:

```
{
    "Layers": [
        {
            "LayerName": "my-layer",
            "LayerArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer",
            "LatestMatchingVersion": {
                "LayerVersionArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-
layer:2",
                "Version": 2,
                "Description": "My layer",
                "CreatedDate": "2023-11-15T00:37:46.592+0000",
                "CompatibleRuntimes": [
                    "python3.10",
                    "python3.11"
                ]
            }
        }
    ]
}
```

Para obtener más información, consulte Capas de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte ListLayers en la Referencia de comandos de la AWS CLI.

`list-provisioned-concurrency-configs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-provisioned-concurrency-configs`.

AWS CLI

Obtención de una lista de configuraciones de simultaneidad aprovisionada

En el siguiente ejemplo `list-provisioned-concurrency-configs`, se enumeran las configuraciones de simultaneidad aprovisionadas para la función especificada.

```
aws lambda list-provisioned-concurrency-configs \
    --function-name my-function
```

Salida:

```
{
    "ProvisionedConcurrencyConfigs": [
        {
            "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-
function:GREEN",
            "RequestedProvisionedConcurrentExecutions": 100,
            "AvailableProvisionedConcurrentExecutions": 100,
            "AllocatedProvisionedConcurrentExecutions": 100,
            "Status": "READY",
            "LastModified": "2019-12-31T20:29:00+0000"
        },
        {
            "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-
function:BLUE",
            "RequestedProvisionedConcurrentExecutions": 100,
            "AvailableProvisionedConcurrentExecutions": 100,
            "AllocatedProvisionedConcurrentExecutions": 100,
            "Status": "READY",
            "LastModified": "2019-12-31T20:28:49+0000"
        }
```

```
    ]
}
```

- Para obtener información sobre la API, consulte ListProvisionedConcurrencyConfigs en la Referencia del comando de la AWS CLI.

`list-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags`.

AWS CLI

Recuperación de la lista de etiquetas para una función de Lambda

En el siguiente ejemplo de `list-tags`, se muestran las etiquetas asociadas a la función de Lambda `my-function`.

```
aws lambda list-tags \
    --resource arn:aws:lambda:us-west-2:123456789012:function:my-function
```

Salida:

```
{
    "Tags": {
        "Category": "Web Tools",
        "Department": "Sales"
    }
}
```

Para obtener más información, consulte Etiquetas de funciones de Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener más información sobre la API, consulte ListTags en la Referencia de comandos de la AWS CLI.

`list-versions-by-function`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-versions-by-function`.

AWS CLI

Recuperación de la lista de versiones de una función

En el siguiente ejemplo de `list-versions-by-function`, se muestra la lista de versiones de la función de Lambda `my-function`.

```
aws lambda list-versions-by-function \
    --function-name my-function
```

Salida:

```
{
    "Versions": [
        {
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "$LATEST",
            "CodeSha256": "sU0cJ2/hOZevwV/lTxCuQqK3gDZP3i8gUoqUUVRmY6E=",
            "FunctionName": "my-function",
            "VpcConfig": {
                "SubnetIds": [],
                "VpcId": "",
                "SecurityGroupIds": []
            },
            "MemorySize": 256,
            "RevisionId": "93017fc9-59cb-41dc-901b-4845ce4bf668",
            "CodeSize": 266,
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:$LATEST",
            "Handler": "index.handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/helloWorldPython-
role-uy3l9qyq",
            "Timeout": 3,
            "LastModified": "2019-10-01T16:47:28.490+0000",
            "Runtime": "nodejs10.x",
            "Description": ""
        },
        {
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "1",
            "CodeSha256": "5tT2qgzYUHoqwR616pZ2dpkn/0J1FrzJmlKidWaaCgk=",
            "FunctionName": "my-function",
            "VpcConfig": {
```

```
                "SubnetIds": [],
                "VpcId": "",
                "SecurityGroupIds": []
            },
            "MemorySize": 256,
            "RevisionId": "949c8914-012e-4795-998c-e467121951b1",
            "CodeSize": 304,
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:1",
            "Handler": "index.handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/helloWorldPython-
role-uy3l9qyq",
            "Timeout": 3,
            "LastModified": "2019-09-26T20:28:40.438+0000",
            "Runtime": "nodejs10.x",
            "Description": "new version"
        },
        {
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "2",
            "CodeSha256": "sU0cJ2/hOZevwV/lTxCuQqK3gDZP3i8gUoqUUVRmY6E=",
            "FunctionName": "my-function",
            "VpcConfig": {
                "SubnetIds": [],
                "VpcId": "",
                "SecurityGroupIds": []
            },
            "MemorySize": 256,
            "RevisionId": "cd669f21-0f3d-4e1c-9566-948837f2e2ea",
            "CodeSize": 266,
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:2",
            "Handler": "index.handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/helloWorldPython-
role-uy3l9qyq",
            "Timeout": 3,
            "LastModified": "2019-10-01T16:47:28.490+0000",
            "Runtime": "nodejs10.x",
            "Description": "newer version"
        }
    ]
```

```
}
```

Para obtener más información, consulte Configuración de los alias de las funciones de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte ListVersionsByFunction en la Referencia de comandos de la AWS CLI.

`publish-layer-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `publish-layer-version`.

AWS CLI

Para crear una versión de capa de Lambda

En el siguiente ejemplo de `publish-layer-version` se crea una nueva versión de capa de biblioteca de Python. El comando recupera el contenido de la capa, un archivo llamado `layer.zip` en el bucket de S3 especificado.

```
aws lambda publish-layer-version \
    --layer-name my-layer \
    --description "My Python layer" \
    --license-info "MIT" \
    --content S3Bucket=lambda-layers-us-west-2-123456789012,S3Key=layer.zip \
    --compatible-runtimes python3.10 python3.11
```

Salida:

```
{
    "Content": {
        "Location": "https://awslambda-us-west-2-layers.s3.us-west-2.amazonaws.com/
snapshots/123456789012/my-layer-4aaa2fbb-ff77-4b0a-ad92-5b78a716a96a?
versionId=27iWyA73cCAYqyH...",
        "CodeSha256": "tv9jJO+rPbXUUXuRKi7CwHzKtLDkDRJLB3cC3Z/ouXo=",
        "CodeSize": 169
    },
    "LayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:my-layer",
    "LayerVersionArn": "arn:aws:lambda:us-west-2:123456789012:layer:my-layer:1",
    "Description": "My Python layer",
    "CreatedDate": "2023-11-14T23:03:52.894+0000",
```

```
    "Version": 1,
    "LicenseInfo": "MIT",
    "CompatibleRuntimes": [
        "python3.10",
        "python3.11"
    ]
}
```

Para obtener más información, consulte Capas de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte PublishLayerVersion en la Referencia de comandos de la AWS CLI.

`publish-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `publish-version`.

AWS CLI

Publicación de una nueva versión de la función de Lambda

En el siguiente ejemplo de `publish-version`, se publica una nueva versión de la función de Lambda `my-function`.

```
aws lambda publish-version \
    --function-name my-function
```

Salida:

```
{
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "CodeSha256": "dBG9m8SGdmlEjw/JYXlhhvCrAv5TxvXsbL/RMr0fT/I=",
    "FunctionName": "my-function",
    "CodeSize": 294,
    "RevisionId": "f31d3d39-cc63-4520-97d4-43cd44c94c20",
    "MemorySize": 128,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function:3",
    "Version": "2",
```

```
    "Role": "arn:aws:iam::123456789012:role/service-role/MyTestFunction-role-
zgur6bf4",
    "Timeout": 3,
    "LastModified": "2019-09-23T18:32:33.857+0000",
    "Handler": "my-function.handler",
    "Runtime": "nodejs10.x",
    "Description": ""
}
```

Para obtener más información, consulte Configuración de los alias de las funciones de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener detalles de la API, consulte PublishVersion en la Referencia de comandos de la AWS CLI.

`put-function-concurrency`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-function-concurrency`.

AWS CLI

Configuración de un límite de simultaneidad reservado para una función

En el siguiente ejemplo de `put-function-concurrency`, se configuran 100 ejecuciones simultáneas reservadas para la función `my-function`.

```
aws lambda put-function-concurrency \
    --function-name  my-function  \
    --reserved-concurrent-executions 100
```

Salida:

```
{
    "ReservedConcurrentExecutions": 100
}
```

Para obtener más información, consulte Reserva de simultaneidad para una función de Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte PutFunctionConcurrency en la Referencia de comandos de la AWS CLI.

put-function-event-invoke-config

En el siguiente ejemplo de código, se muestra cómo utilizar put-function-event-invoke-config.

AWS CLI

Para configurar la gestión de errores para invocación asíncrona.

En el siguiente ejemplo de put-function-event-invoke-config se establece una duración máxima de eventos de una hora y se deshabilitan los reintentos para la función especificada.

```
aws lambda put-function-event-invoke-config \
    --function-name my-function \
    --maximum-event-age-in-seconds 3600 \
    --maximum-retry-attempts 0
```

Salida:

```
{
    "LastModified": 1573686021.479,
    "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-function:
$LATEST",
    "MaximumRetryAttempts": 0,
    "MaximumEventAgeInSeconds": 3600,
    "DestinationConfig": {
        "OnSuccess": {},
        "OnFailure": {}
    }
}
```

- Para obtener información sobre la API, consulte PutFunctionEventInvokeConfig en la Referencia de comandos de la AWS CLI.

put-provisioned-concurrency-config

En el siguiente ejemplo de código, se muestra cómo utilizar put-provisioned-concurrency-config.

AWS CLI

Asignación de simultaneidad aprovisionada

En el siguiente ejemplo de `put-provisioned-concurrency-config`, se asignan 100 simultaneidades aprovisionadas para el alias BLUE de la función especificada.

```
aws lambda put-provisioned-concurrency-config \
    --function-name my-function \
    --qualifier BLUE \
    --provisioned-concurrent-executions 100
```

Salida:

```
{
    "Requested ProvisionedConcurrentExecutions": 100,
    "Allocated ProvisionedConcurrentExecutions": 0,
    "Status": "IN_PROGRESS",
    "LastModified": "2019-11-21T19:32:12+0000"
}
```

- Para obtener información sobre la API, consulte PutProvisionedConcurrencyConfig en la Referencia de comandos de la AWS CLI.

`remove-layer-version-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-layer-version-permission`.

AWS CLI

Para eliminar permisos de versiones de capa

En el siguiente ejemplo de `remove-layer-version-permission` se elimina el permiso de una cuenta para configurar una versión de capa.

```
aws lambda remove-layer-version-permission \
    --layer-name my-layer \
    --statement-id xaccount \
    --version-number 1
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Capas de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte RemoveLayerVersionPermission en la Referencia de comandos de la AWS CLI.

`remove-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-permission`.

AWS CLI

Eliminación de permisos de una función de Lambda existente

En el siguiente ejemplo de `remove-permission`, se elimina el permiso para invocar una función denominada `my-function`.

```
aws lambda remove-permission \
    --function-name my-function \
    --statement-id sns
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de políticas basadas en recursos para AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para obtener información sobre la API, consulte RemovePermission en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Adición de etiquetas a una función de Lambda existente

En el siguiente ejemplo de `tag-resource`, se agrega una etiqueta con el nombre de clave `DEPARTMENT` y un valor de `Department A` a la función de Lambda especificada.

```
aws lambda tag-resource \
    --resource arn:aws:lambda:us-west-2:123456789012:function:my-function \
    --tags "DEPARTMENT=Department A"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetas de funciones de Lambda en la Guía para desarrolladores de AWS Lambda.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de etiquetas de una función de Lambda existente

En el siguiente ejemplo de `untag-resource`, se elimina la etiqueta con el nombre de clave `DEPARTMENT` de la función de Lambda `my-function`.

```
aws lambda untag-resource \
    --resource arn:aws:lambda:us-west-2:123456789012:function:my-function \
    --tag-keys DEPARTMENT
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetas de funciones de Lambda en la Guía para desarrolladores de AWS Lambda.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-alias`.

AWS CLI

Actualización del alias de una función

En el siguiente ejemplo de `update-alias`, se actualiza el alias nombrado `LIVE` para que apunte a la versión 3 de la función de Lambda `my-function`.

```
aws lambda update-alias \
    --function-name my-function \
```

```
    --function-version 3 \
    --name LIVE
```

Salida:

```
{
    "FunctionVersion": "3",
    "Name": "LIVE",
    "AliasArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function:LIVE",
    "RevisionId": "594f41fb-b85f-4c20-95c7-6ca5f2a92c93",
    "Description": "alias for live version of function"
}
```

Para obtener más información, consulte Configuración de los alias de las funciones de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

- Para ver los detalles de la API, consulte UpdateAlias en la Referencia de comandos de la AWS CLI.

`update-event-source-mapping`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-event-source-mapping`.

AWS CLI

Para actualizar la asignación entre un origen de eventos y una función de AWS Lambda

En el siguiente ejemplo de `update-event-source-mapping` se actualiza el tamaño de lote a ocho en la asignación especificada.

```
aws lambda update-event-source-mapping \
    --uuid  "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --batch-size 8
```

Salida:

```
{
    "UUID": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
    "StateTransitionReason": "USER_INITIATED",
    "LastModified": 1569284520.333,
    "BatchSize": 8,
```

```
    "State": "Updating",
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "EventSourceArn": "arn:aws:sqs:us-west-2:123456789012:mySQSqueue"
}
```

Para obtener más información sobre los eventos en Lambda, consulte Mapeos de origen de eventos AWS en la Guía para desarrolladores de AWS.

- Para obtener información sobre la API, consulte UpdateEventSourceMapping en la Referencia de comandos de la AWS CLI.

`update-function-code`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-function-code`.

AWS CLI

Cómo actualizar el código de una función de Lambda

En el siguiente ejemplo de `update-function-code`, se reemplaza el código de la versión no publicada ($LATEST) de la función `my-function` por el contenido del archivo zip especificado.

```
aws lambda update-function-code \
    --function-name  my-function \
    --zip-file fileb://my-function.zip
```

Salida:

```
{
    "FunctionName": "my-function",
    "LastModified": "2019-09-26T20:28:40.438+0000",
    "RevisionId": "e52502d4-9320-4688-9cd6-152a6ab7490d",
    "MemorySize": 256,
    "Version": "$LATEST",
    "Role": "arn:aws:iam::123456789012:role/service-role/my-function-role-uy3l9qyq",
    "Timeout": 3,
    "Runtime": "nodejs10.x",
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "CodeSha256": "5tT2qgzYUHaqwR716pZ2dpkn/0J1FrzJmlKidWoaCgk=",
    "Description": "",
```

```
    "VpcConfig": {
        "SubnetIds": [],
        "VpcId": "",
        "SecurityGroupIds": []
    },
    "CodeSize": 304,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "Handler": "index.handler"
}
```

Para obtener más información, consulte Configuración las funciones de Lambda de AWS en la Guía para desarrolladores de Lambda de AWS.

- Para obtener información acerca de la API, consulte UpdateFunctionCode en la Referencia de comandos de la AWS CLI.

`update-function-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-function-configuration`.

AWS CLI

Para modificar la configuración de una función

En el siguiente ejemplo de `update-function-configuration`, se modifica el tamaño de la memoria para que sea de 256 MB para la versión no publicada ($LATEST) de la función `my-function`.

```
aws lambda update-function-configuration \
    --function-name  my-function \
    --memory-size 256
```

Salida:

```
{
    "FunctionName": "my-function",
    "LastModified": "2019-09-26T20:28:40.438+0000",
    "RevisionId": "e52502d4-9320-4688-9cd6-152a6ab7490d",
    "MemorySize": 256,
    "Version": "$LATEST",
    "Role": "arn:aws:iam::123456789012:role/service-role/my-function-role-uy3l9qyq",
    "Timeout": 3,
```

```
    "Runtime": "nodejs10.x",
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "CodeSha256": "5tT2qgzYUHaqwR716pZ2dpkn/0J1FrzJmlKidWoaCgk=",
    "Description": "",
    "VpcConfig": {
        "SubnetIds": [],
        "VpcId": "",
        "SecurityGroupIds": []
    },
    "CodeSize": 304,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "Handler": "index.handler"
}
```

Para obtener más información, consulte Configuración las funciones de Lambda de AWS en la Guía para desarrolladores de Lambda de AWS.

- Para obtener información acerca de la API, consulte UpdateFunctionConfiguration en la Referencia de comandos de la AWS CLI.

`update-function-event-invoke-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-function-event-invoke-config`.

AWS CLI

Para actualizar una configuración de invocación asíncrona

En el siguiente ejemplo de `update-function-event-invoke-config` se agrega un destino en caso de fallo a la configuración de invocación asíncrona existente para la función especificada.

```
aws lambda update-function-event-invoke-config \
    --function-name my-function \
    --destination-config '{"OnFailure":{"Destination": "arn:aws:sqs:us-
east-2:123456789012:destination"}}'
```

Salida:

```
{
```

```
    "LastModified": 1573687896.493,
    "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-function:
$LATEST",
    "MaximumRetryAttempts": 0,
    "MaximumEventAgeInSeconds": 3600,
    "DestinationConfig": {
        "OnSuccess": {},
        "OnFailure": {
            "Destination": "arn:aws:sqs:us-east-2:123456789012:destination"
        }
    }
}
```

- Para obtener información sobre la API, consulte UpdateFunctionEventInvokeConfig en la Referencia de comandos de la AWS CLI.

Ejemplos de License Manager que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con License Manager.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-license-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-license-configuration`.

AWS CLI

Ejemplo 1: crear una configuración de licencias

El siguiente ejemplo de `create-license-configuration` crea una configuración de licencia con un límite máximo de 10 núcleos.

```
aws license-manager create-license-configuration --name my-license-configuration \
    --license-counting-type Core \
    --license-count 10 \
    --license-count-hard-limit
```

Salida:

```
{
  "LicenseConfigurationArn": "arn:aws:license-manager:us-
west-2:123456789012:license-configuration:lic-6eb6586f508a786a2ba41EXAMPLE1111"
}
```

Ejemplo 2: crear una configuración de licencias

En el siguiente ejemplo de `create-license-configuration`, se crea una configuración de licencia con un límite flexible de 100 vCPU. Utiliza una regla para habilitar la optimización de vCPU.

```
aws license-manager create-license-configuration --name my-license-configuration
    --license-counting-type vCPU \
    --license-count 100 \
    --license-rules "#honorVcpuOptimization=true"
```

Salida:

```
{
  "LicenseConfigurationArn": "arn:aws:license-manager:us-
west-2:123456789012:license-configuration:lic-6eb6586f508a786a2ba41EXAMPLE2222"
}
```

- Para obtener información sobre la API, consulte CreateLicenseConfiguration en la Referencia de comandos de la AWS CLI.

`delete-license-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-license-configuration`.

AWS CLI

Eliminación de una configuración de licencias

En el siguiente ejemplo de `delete-license-configuration`, se elimina la configuración de licencia especificada.

```
aws license-manager delete-license-configuration \
    --license-configuration-arn arn:aws:license-manager:us-
west-2:123456789012:license-configuration:lic-6eb6586f508a786a2ba4f56c1EXAMPLE
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteLicenseConfiguration en la Referencia de comandos de la AWS CLI.

`get-license-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-license-configuration`.

AWS CLI

Para obtener información sobre la configuración de licencias

En el siguiente ejemplo de `get-license-configuration`, se muestran los detalles de la configuración de licencias especificada.

```
aws license-manager get-license-configuration \
    --license-configuration-arn arn:aws:license-manager:us-
west-2:123456789012:license-configuration:lic-38b658717b87478aaa7c00883EXAMPLE
```

Salida:

```
{
    "LicenseConfigurationId": "lic-38b658717b87478aaa7c00883EXAMPLE",
    "LicenseConfigurationArn": "arn:aws:license-manager:us-
west-2:123456789012:license-configuration:lic-38b658717b87478aaa7c00883EXAMPLE",
    "Name": "my-license-configuration",
    "LicenseCountingType": "vCPU",
    "LicenseRules": [],
    "LicenseCountHardLimit": false,
```

```
    "ConsumedLicenses": 0,
    "Status": "AVAILABLE",
    "OwnerAccountId": "123456789012",
    "ConsumedLicenseSummaryList": [
        {
            "ResourceType": "EC2_INSTANCE",
            "ConsumedLicenses": 0
        },
        {
            "ResourceType": "EC2_HOST",
            "ConsumedLicenses": 0
        },
        {
            "ResourceType": "SYSTEMS_MANAGER_MANAGED_INSTANCE",
            "ConsumedLicenses": 0
        }
    ],
    "ManagedResourceSummaryList": [
        {
            "ResourceType": "EC2_INSTANCE",
            "AssociationCount": 0
        },
        {
            "ResourceType": "EC2_HOST",
            "AssociationCount": 0
        },
        {
            "ResourceType": "EC2_AMI",
            "AssociationCount": 2
        },
        {
            "ResourceType": "SYSTEMS_MANAGER_MANAGED_INSTANCE",
            "AssociationCount": 0
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetLicenseConfiguration en la Referencia de comandos de la AWS CLI.

`get-service-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-settings`.

AWS CLI

Para obtener la configuración de License Manager

El siguiente ejemplo de `get-service-settings` muestra la configuración del servicio de License Manager en la región actual.

```
aws license-manager get-service-settings
```

A continuación, se muestra un ejemplo de salida si la detección de recursos entre cuentas está deshabilitada.

```
{
    "OrganizationConfiguration": {
        "EnableIntegration": false
    },
    "EnableCrossAccountsDiscovery": false
}
```

A continuación, se muestra un ejemplo de salida si la detección de recursos entre cuentas está habilitada.

```
{
    "S3BucketArn": "arn:aws:s3:::aws-license-manager-service-c22d6279-35c4-47c4-bb",
    "OrganizationConfiguration": {
        "EnableIntegration": true
    },
    "EnableCrossAccountsDiscovery": true
}
```

- Para obtener información sobre la API, consulte GetServiceSettings en la Referencia de comandos de la AWS CLI.

`list-associations-for-license-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-associations-for-license-configuration`.

AWS CLI

Para obtener asociaciones para una configuración de licencias

El siguiente ejemplo de `list-associations-for-license-configuration` muestra información detallada sobre las asociaciones de la configuración de licencias especificada.

```
aws license-manager list-associations-for-license-configuration \
    --license-configuration-arn arn:aws:license-manager:us-
west-2:123456789012:license-configuration:lic-38b658717b87478aaa7c00883EXAMPLE
```

Salida:

```
{
    "LicenseConfigurationAssociations": [
        {
            "ResourceArn": "arn:aws:ec2:us-west-2::image/ami-1234567890abcdef0",
            "ResourceType": "EC2_AMI",
            "ResourceOwnerId": "123456789012",
            "AssociationTime": 1568825118.617
        },
        {
            "ResourceArn": "arn:aws:ec2:us-west-2::image/ami-0abcdef1234567890",
            "ResourceType": "EC2_AMI",
            "ResourceOwnerId": "123456789012",
            "AssociationTime": 1568825118.946
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListAssociationsForLicenseConfiguration en la Referencia de comandos de la AWS CLI.

`list-license-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-license-configurations`.

AWS CLI

Ejemplo 1: enumeración de todas las configuraciones de licencia

El siguiente ejemplo de `list-license-configurations` muestra todas las configuraciones de licencias.

```
aws license-manager list-license-configurations
```

Salida:

```
{
    "LicenseConfigurations": [
        {
            "LicenseConfigurationId": "lic-6eb6586f508a786a2ba4f56c1EXAMPLE",
            "LicenseConfigurationArn": "arn:aws:license-manager:us-
west-2:123456789012:license-configuration:lic-6eb6586f508a786a2ba4f56c1EXAMPLE",
            "Name": "my-license-configuration",
            "LicenseCountingType": "Core",
            "LicenseRules": [],
            "LicenseCount": 10,
            "LicenseCountHardLimit": true,
            "ConsumedLicenses": 0,
            "Status": "AVAILABLE",
            "OwnerAccountId": "123456789012",
            "ConsumedLicenseSummaryList": [
                {
                    "ResourceType": "EC2_INSTANCE",
                    "ConsumedLicenses": 0
                },
                {
                    "ResourceType": "EC2_HOST",
                    "ConsumedLicenses": 0
                },
                {
                    "ResourceType": "SYSTEMS_MANAGER_MANAGED_INSTANCE",
                    "ConsumedLicenses": 0
                }
            ],
            "ManagedResourceSummaryList": [
                {
                    "ResourceType": "EC2_INSTANCE",
                    "AssociationCount": 0
                },
                {
                    "ResourceType": "EC2_HOST",
                    "AssociationCount": 0
                },
                {
                    "ResourceType": "EC2_AMI",
                    "AssociationCount": 0
                },
                {
```

```
                    "ResourceType": "SYSTEMS_MANAGER_MANAGED_INSTANCE",
                    "AssociationCount": 0
                }
            ]
        },
        {
            ...
        }
    ]
}
```

Ejemplo 2: enumeración de configuraciones de licencias específicas

El siguiente ejemplo de `list-license-configurations` muestra solo la configuración de licencias especificada.

```
aws license-manager list-license-configurations \
    --license-configuration-arns arn:aws:license-manager:us-
west-2:123456789012:license-configuration:lic-38b658717b87478aaa7c00883EXAMPLE
```

- Para obtener información sobre la API, consulte ListLicenseConfigurations en la Referencia de comandos de la AWS CLI.

`list-license-specifications-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-license-specifications-for-resource`.

AWS CLI

Para enumerar las configuraciones de licencias para un recurso

El siguiente ejemplo de `list-license-specifications-for-resource` muestra las configuraciones de licencias asociadas a la Imagen de máquina de Amazon (AMI) especificada.

```
aws license-manager list-license-specifications-for-resource \
    --resource-arn arn:aws:ec2:us-west-2::image/ami-1234567890abcdef0
```

Salida:

```
{
```

```
    "LicenseConfigurationArn": "arn:aws:license-manager:us-
west-2:123456789012:license-configuration:lic-38b658717b87478aaa7c00883EXAMPLE"
}
```

- Para obtener información sobre la API, consulte ListLicenseSpecificationsForResource en la Referencia de comandos de la AWS CLI.

`list-resource-inventory`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-inventory`.

AWS CLI

Para enumerar los recursos del inventario de recursos

En el ejemplo de `list-resource-inventory`, se enumeran los recursos administrados mediante el inventario de Systems Manager.

```
aws license-manager list-resource-inventory
```

Salida:

```
{
    "ResourceInventoryList": [
        {
            "Platform": "Red Hat Enterprise Linux Server",
            "ResourceType": "EC2Instance",
            "PlatformVersion": "7.4",
            "ResourceArn": "arn:aws:ec2:us-west-2:1234567890129:instance/
i-05d3cdfb05bd36376",
            "ResourceId": "i-05d3cdfb05bd36376",
            "ResourceOwningAccountId": "1234567890129"
        },
        {
            "Platform": "Amazon Linux",
            "ResourceType": "EC2Instance",
            "PlatformVersion": "2",
            "ResourceArn": "arn:aws:ec2:us-west-2:1234567890129:instance/
i-0b1d036cfd4594808",
            "ResourceId": "i-0b1d036cfd4594808",
            "ResourceOwningAccountId": "1234567890129"
```

```
        },
        {
            "Platform": "Microsoft Windows Server 2019 Datacenter",
            "ResourceType": "EC2Instance",
            "PlatformVersion": "10.0.17763",
            "ResourceArn": "arn:aws:ec2:us-west-2:1234567890129:instance/
i-0cdb3b54a2a8246ad",
            "ResourceId": "i-0cdb3b54a2a8246ad",
            "ResourceOwningAccountId": "1234567890129"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListResourceInventory en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de una configuración de licencias

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran las etiquetas para la configuración de licencias especificada.

```
aws license-manager list-tags-for-resource \
    --resource-arn arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-6eb6586f508a786a2ba4f56c1EXAMPLE
```

Salida:

```
{
    "Tags": [
        {
            "Key": "project",
            "Value": "lima"
        }
    ]
}
```

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-usage-for-license-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-usage-for-license-configuration`.

AWS CLI

Para enumerar las licencias en uso para una configuración de licencias

En el siguiente ejemplo de `list-usage-for-license-configuration`, se muestra información sobre los recursos que utilizan licencias para la configuración de licencias especificada. Por ejemplo, si el tipo de licencia es vCPU, todas las instancias consumen una licencia por vCPU.

```
aws license-manager list-usage-for-license-configuration \
    --license-configuration-arn arn:aws:license-manager:us-
west-2:123456789012:license-configuration:lic-38b658717b87478aaa7c00883EXAMPLE
```

Salida:

```
{
    "LicenseConfigurationUsageList": [
        {
            "ResourceArn": "arn:aws:ec2:us-west-2:123456789012:instance/
i-04a636d18e83cfacb",
            "ResourceType": "EC2_INSTANCE",
            "ResourceStatus": "running",
            "ResourceOwnerId": "123456789012",
            "AssociationTime": 1570892850.519,
            "ConsumedLicenses": 2
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListUsageForLicenseConfiguration en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para agregar una etiqueta a una configuración de licencias

El siguiente ejemplo de `tag-resource` agrega la etiqueta especificada (nombre y valor de la clave) a la configuración de licencias especificada.

```
aws license-manager tag-resource \
    --tags Key=project,Value=lima \
    --resource-arn arn:aws:license-manager:us-west-2:123456789012:license-configuration:lic-6eb6586f508a786a2ba4f56c1EXAMPLE
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar etiquetas de una configuración de licencias

El siguiente ejemplo de `untag-resource` elimina la etiqueta especificada (nombre de clave y recurso) de la configuración de licencias especificada.

```
aws license-manager untag-resource \
    --tag-keys project \
    --resource-arn arn:aws:license-manager:us-west-2:123456789012:license-configuration:lic-6eb6586f508a786a2ba4f56c1EXAMPLE
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-license-configuration

En el siguiente ejemplo de código, se muestra cómo utilizar `update-license-configuration`.

AWS CLI

Actualización de una configuración de licencias

El siguiente ejemplo de `update-license-configuration` actualiza la configuración de licencias especificada para eliminar el límite estricto.

```
aws license-manager update-license-configuration \
    --no-license-count-hard-limit \
    --license-configuration-arn arn:aws:license-manager:us-
west-2:880185128111:license-configuration:lic-6eb6586f508a786a2ba4f56c1EXAMPLE
```

Este comando no genera ninguna salida.

El siguiente ejemplo de `update-license-configuration` actualiza la configuración de licencias especificada para cambiar su estado a `DISABLED`.

```
aws license-manager update-license-configuration \
    --license-configuration-status DISABLED
    --license-configuration-arn arn:aws:license-manager:us-
west-2:880185128111:license-configuration:lic-6eb6586f508a786a2ba4f56c1EXAMPLE
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte UpdateLicenseConfiguration en la Referencia de comandos de la AWS CLI.

update-license-specifications-for-resource

En el siguiente ejemplo de código, se muestra cómo utilizar `update-license-specifications-for-resource`.

AWS CLI

Para actualizar las configuraciones de licencias de un recurso

El siguiente ejemplo de `update-license-specifications-for-resource` reemplaza la configuración de licencias asociada a la Imagen de máquina de Amazon (AMI) especificada al eliminar una configuración de licencias y agregar otra.

```
aws license-manager update-license-specifications-for-resource \
    --resource-arn arn:aws:ec2:us-west-2::image/ami-1234567890abcdef0 \
    --remove-license-specifications LicenseConfigurationArn=arn:aws:license-
manager:us-west-2:123456789012:license-
configuration:lic-38b658717b87478aaa7c00883EXAMPLE \
    --add-license-specifications LicenseConfigurationArn=arn:aws:license-manager:us-
west-2:123456789012:license-configuration:lic-42b6deb06e5399a980d555927EXAMPLE
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte UpdateLicenseSpecificationsForResource en la Referencia de comandos de la AWS CLI.

`update-service-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-service-settings`.

AWS CLI

Para actualizar la configuración de License Manager

El siguiente ejemplo de `update-service-settings` permite la detección de recursos entre cuentas para License Manager en la región de AWS actual. El bucket de Amazon S3 es la sincronización de datos de recursos necesaria para el inventario de Systems Manager.

```
aws license-manager update-service-settings \
    --organization-configuration EnableIntegration=true \
    --enable-cross-accounts-discovery \
    --s3-bucket-arn arn:aws:s3:::aws-license-manager-service-abcd1234EXAMPLE
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte UpdateServiceSettings en la Referencia de comandos de la AWS CLI.

Lightsail Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Lightsail.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`allocate-static-ip`

En el siguiente ejemplo de código, se muestra cómo utilizar `allocate-static-ip`.

AWS CLI

Creación de IP estáticas

En el siguiente ejemplo de `allocate-static-ip`, se crea la IP estática especificada, que se puede asociar a una instancia.

```
aws lightsail allocate-static-ip \
    --static-ip-name StaticIp-1
```

Salida:

```
{
    "operations": [
        {
            "id": "b5d06d13-2f19-4683-889f-dEXAMPLEed79",
            "resourceName": "StaticIp-1",
            "resourceType": "StaticIp",
```

```
            "createdAt": 1571071325.076,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationType": "AllocateStaticIp",
            "status": "Succeeded",
            "statusChangedAt": 1571071325.274
        }
    ]
}
```

- Para obtener información sobre la API, consulte AllocateStaticIp en la Referencia de comandos de la AWS CLI.

`attach-disk`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-disk`.

AWS CLI

Para asociar un disco de almacenamiento en bloque a una instancia

En el siguiente ejemplo de `attach-disk`, se asocia un disco `Disk-1` a una instancia `WordPress_Multisite-1` con la ruta de disco de `/dev/xvdf`.

```
aws lightsail attach-disk \
    --disk-name Disk-1 \
    --disk-path /dev/xvdf \
    --instance-name WordPress_Multisite-1
```

Salida:

```
{
    "operations": [
        {
            "id": "10a08267-19ce-43be-b913-6EXAMPLE7e80",
            "resourceName": "Disk-1",
            "resourceType": "Disk",
            "createdAt": 1571071465.472,
```

```
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "WordPress_Multisite-1",
            "operationType": "AttachDisk",
            "status": "Started",
            "statusChangedAt": 1571071465.472
        },
        {
            "id": "2912c477-5295-4539-88c9-bEXAMPLEd1f0",
            "resourceName": "WordPress_Multisite-1",
            "resourceType": "Instance",
            "createdAt": 1571071465.474,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "Disk-1",
            "operationType": "AttachDisk",
            "status": "Started",
            "statusChangedAt": 1571071465.474
        }
    ]
}
```

- Para obtener información sobre la API, consulte AttachDisk en la Referencia de comandos de la AWS CLI.

`attach-instances-to-load-balancer`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-instances-to-load-balancer`.

AWS CLI

Asociación de instancias a un equilibrador de carga

En el siguiente ejemplo de `attach-instances-to-load-balancer`, se asocian las instancia `MEAN-1`, `MEAN-2` y `MEAN-3` al equilibrador de carga `LoadBalancer-1`.

```
aws lightsail attach-instances-to-load-balancer \
    --instance-names {"MEAN-1","MEAN-2","MEAN-3"} \
    --load-balancer-name LoadBalancer-1
```

Salida:


```
{
    "operations": [
        {
            "id": "8055d19d-abb2-40b9-b527-1EXAMPLE3c7b",
            "resourceName": "LoadBalancer-1",
            "resourceType": "LoadBalancer",
            "createdAt": 1571071699.892,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "MEAN-2",
            "operationType": "AttachInstancesToLoadBalancer",
            "status": "Started",
            "statusChangedAt": 1571071699.892
        },
        {
            "id": "c35048eb-8538-456a-a118-0EXAMPLEfb73",
            "resourceName": "MEAN-2",
            "resourceType": "Instance",
            "createdAt": 1571071699.887,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "LoadBalancer-1",
            "operationType": "AttachInstancesToLoadBalancer",
            "status": "Started",
            "statusChangedAt": 1571071699.887
        },
        {
            "id": "910d09e0-adc5-4372-bc2e-0EXAMPLEd891",
            "resourceName": "LoadBalancer-1",
            "resourceType": "LoadBalancer",
            "createdAt": 1571071699.882,
```

```
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "MEAN-3",
            "operationType": "AttachInstancesToLoadBalancer",
            "status": "Started",
            "statusChangedAt": 1571071699.882
        },
        {
            "id": "178b18ac-43e8-478c-9bed-1EXAMPLE4755",
            "resourceName": "MEAN-3",
            "resourceType": "Instance",
            "createdAt": 1571071699.901,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "LoadBalancer-1",
            "operationType": "AttachInstancesToLoadBalancer",
            "status": "Started",
            "statusChangedAt": 1571071699.901
        },
        {
            "id": "fb62536d-2a98-4190-a6fc-4EXAMPLE7470",
            "resourceName": "LoadBalancer-1",
            "resourceType": "LoadBalancer",
            "createdAt": 1571071699.885,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "MEAN-1",
            "operationType": "AttachInstancesToLoadBalancer",
            "status": "Started",
            "statusChangedAt": 1571071699.885
        },
        {
            "id": "787dac0d-f98d-46c3-8571-3EXAMPLE5a85",
            "resourceName": "MEAN-1",
            "resourceType": "Instance",
```

```
            "createdAt": 1571071699.901,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "LoadBalancer-1",
            "operationType": "AttachInstancesToLoadBalancer",
            "status": "Started",
            "statusChangedAt": 1571071699.901
        }
    ]
}
```

- Para obtener información sobre la API, consulte AttachInstancesToLoadBalancer en la Referencia de comandos de la AWS CLI.

`attach-load-balancer-tls-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-load-balancer-tls-certificate`.

AWS CLI

Para asociar certificados TLS a un equilibrador de carga

En el siguiente ejemplo de `attach-load-balancer-tls-certificate`, se asocia el certificado TLS del equilibrador de carga `Certificate2` al equilibrador de carga `LoadBalancer-1`.

```
aws lightsail attach-load-balancer-tls-certificate \
    --certificate-name Certificate2 \
    --load-balancer-name LoadBalancer-1
```

Salida:

```
{
    "operations": [
        {
            "id": "cf1ad6e3-3cbb-4b8a-a7f2-3EXAMPLEa118",
            "resourceName": "LoadBalancer-1",
            "resourceType": "LoadBalancer",
```

```
            "createdAt": 1571072255.416,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "Certificate2",
            "operationType": "AttachLoadBalancerTlsCertificate",
            "status": "Succeeded",
            "statusChangedAt": 1571072255.416
        },
        {
            "id": "dae1bcfb-d531-4c06-b4ea-bEXAMPLEc04e",
            "resourceName": "Certificate2",
            "resourceType": "LoadBalancerTlsCertificate",
            "createdAt": 1571072255.416,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "LoadBalancer-1",
            "operationType": "AttachLoadBalancerTlsCertificate",
            "status": "Succeeded",
            "statusChangedAt": 1571072255.416
        }
    ]
}
```

- Para obtener información sobre la API, consulte AttachLoadBalancerTlsCertificate en la Referencia de comandos de la AWS CLI.

`attach-static-ip`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-static-ip`.

AWS CLI

Para asociar una IP estática a una instancia

En el siguiente ejemplo de `attach-static-ip`, se asocia una IP estática `StaticIp-1` a la instancia `MEAN-1`.

```
aws lightsail attach-static-ip \
    --static-ip-name StaticIp-1 \
    --instance-name MEAN-1
```

Salida:

```
{
    "operations": [
        {
            "id": "45e6fa13-4808-4b8d-9292-bEXAMPLE20b2",
            "resourceName": "StaticIp-1",
            "resourceType": "StaticIp",
            "createdAt": 1571072569.375,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "MEAN-1",
            "operationType": "AttachStaticIp",
            "status": "Succeeded",
            "statusChangedAt": 1571072569.375
        },
        {
            "id": "9ee09a17-863c-4e51-8a6d-3EXAMPLE5475",
            "resourceName": "MEAN-1",
            "resourceType": "Instance",
            "createdAt": 1571072569.376,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "StaticIp-1",
            "operationType": "AttachStaticIp",
            "status": "Succeeded",
            "statusChangedAt": 1571072569.376
        }
    ]
}
```

- Para obtener información sobre la API, consulte AttachStaticIp en la Referencia de comandos de la AWS CLI.

`close-instance-public-ports`

En el siguiente ejemplo de código, se muestra cómo utilizar `close-instance-public-ports`.

AWS CLI

Para cerrar los puertos de firewall para una instancia

En el siguiente ejemplo de `close-instance-public-ports`, se cierra el puerto TCP 22 de una instancia `MEAN-2`.

```
aws lightsail close-instance-public-ports \
    --instance-name MEAN-2 \
    --port-info fromPort=22,protocol=TCP,toPort=22
```

Salida:

```
{
    "operation": {
        "id": "4f328636-1c96-4649-ae6d-1EXAMPLEf446",
        "resourceName": "MEAN-2",
        "resourceType": "Instance",
        "createdAt": 1571072845.737,
        "location": {
            "availabilityZone": "us-west-2a",
            "regionName": "us-west-2"
        },
        "isTerminal": true,
        "operationDetails": "22/tcp",
        "operationType": "CloseInstancePublicPorts",
        "status": "Succeeded",
        "statusChangedAt": 1571072845.737
    }
}
```

- Para obtener información sobre la API, consulte CloseInstancePublicPorts en la Referencia de comandos de la AWS CLI.

`copy-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-snapshot`.

AWS CLI

Ejemplo 1: copiar una instantánea en la misma región de AWS

El siguiente ejemplo de `copy-snapshot` copia la instantánea de la instancia `MEAN-1-1571075291` como una instantánea de instancia `MEAN-1-Copy` dentro de la misma región de AWS `us-west-2`.

```
aws lightsail copy-snapshot \
    --source-snapshot-name MEAN-1-1571075291 \
    --target-snapshot-name MEAN-1-Copy \
    --source-region us-west-2
```

Salida:

```
{
    "operations": [
        {
            "id": "ced16fc1-f401-4556-8d82-1EXAMPLEb982",
            "resourceName": "MEAN-1-Copy",
            "resourceType": "InstanceSnapshot",
            "createdAt": 1571075581.498,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "us-west-2:MEAN-1-1571075291",
            "operationType": "CopySnapshot",
            "status": "Started",
            "statusChangedAt": 1571075581.498
        }
    ]
}
```

Para obtener más información, consulte Copia de instantáneas de una región de AWS a otra en Amazon Lightsail en la Guía para desarrolladores de Lightsail.

Ejemplo 2: copiar una instantánea de una región de AWS a otra

En el siguiente ejemplo de `copy-snapshot`, se copia la instantánea de instancia `MEAN-1-1571075291` como instantánea de instancia `MEAN-1-1571075291-Copy` de la región de AWS `us-west-2` a `us-east-1`.

```
aws lightsail copy-snapshot \
    --source-snapshot-name MEAN-1-1571075291 \
    --target-snapshot-name MEAN-1-1571075291-Copy \
    --source-region us-west-2 \
    --region us-east-1
```

Salida:

```
{
    "operations": [
        {
            "id": "91116b79-119c-4451-b44a-dEXAMPLEd97b",
            "resourceName": "MEAN-1-1571075291-Copy",
            "resourceType": "InstanceSnapshot",
            "createdAt": 1571075695.069,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-east-1"
            },
            "isTerminal": false,
            "operationDetails": "us-west-2:MEAN-1-1571075291",
            "operationType": "CopySnapshot",
            "status": "Started",
            "statusChangedAt": 1571075695.069
        }
    ]
}
```

Para obtener más información, consulte Copia de instantáneas de una región de AWS a otra en Amazon Lightsail en la Guía para desarrolladores de Lightsail.

Ejemplo 3: copiar una instantánea automática dentro de la misma región de AWS

El siguiente ejemplo de `copy-snapshot` copia la instantánea automática `2019-10-14` de la instancia `WordPress-1` como una instantánea manual `WordPress-1-10142019` en la región de AWS `us-west-2`.

```
aws lightsail copy-snapshot \
```

```
    --source-resource-name WordPress-1 \
    --restore-date 2019-10-14 \
    --target-snapshot-name WordPress-1-10142019 \
    --source-region us-west-2
```

Salida:

```
{
    "operations": [
        {
            "id": "be3e6754-cd1d-48e6-ad9f-2EXAMPLE1805",
            "resourceName": "WordPress-1-10142019",
            "resourceType": "InstanceSnapshot",
            "createdAt": 1571082412.311,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "us-west-2:WordPress-1",
            "operationType": "CopySnapshot",
            "status": "Started",
            "statusChangedAt": 1571082412.311
        }
    ]
}
```

Para obtener más información, consulte Keeping automatic snapshots of instances or disks in Amazon Lightsail en la Guía para desarrolladores de Lightsail.

Ejemplo 4: copiar una instantánea automática de una región de AWS a otra

El siguiente ejemplo de `copy-snapshot` copia la instantánea automática `2019-10-14` de la instancia `WordPress-1` como una instantánea manual `WordPress-1-10142019` de la región de AWS `us-west-2` en `us-east-1`.

```
aws lightsail copy-snapshot \
    --source-resource-name WordPress-1 \
    --restore-date 2019-10-14 \
    --target-snapshot-name WordPress-1-10142019 \
    --source-region us-west-2 \
    --region us-east-1
```

Salida:

```
{
    "operations": [
        {
            "id": "dffa128b-0b07-476e-b390-bEXAMPLE3775",
            "resourceName": "WordPress-1-10142019",
            "resourceType": "InstanceSnapshot",
            "createdAt": 1571082493.422,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-east-1"
            },
            "isTerminal": false,
            "operationDetails": "us-west-2:WordPress-1",
            "operationType": "CopySnapshot",
            "status": "Started",
            "statusChangedAt": 1571082493.422
        }
    ]
}
```

Para obtener más información, consulte Keeping automatic snapshots of instances or disks in Amazon Lightsail en la Guía para desarrolladores de Lightsail.

- Para obtener información sobre la API, consulte CopySnapshot en la Referencia de comandos de la AWS CLI.

`create-disk-from-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-disk-from-snapshot`.

AWS CLI

Para crear un disco a partir de una instantánea de disco

En el siguiente ejemplo de `create-disk-from-snapshot`, se crea un disco de almacenamiento en bloques denominado `Disk-2` a partir de la instantánea del disco de almacenamiento en bloques especificada. El disco se crea en la zona de disponibilidad y región de AWS especificadas, con 32 GB de espacio de almacenamiento.

```
aws lightsail create-disk-from-snapshot \
```

```
    --disk-name Disk-2 \
    --disk-snapshot-name Disk-1-1566839161 \
    --availability-zone us-west-2a \
    --size-in-gb 32
```

Salida:

```
{
    "operations": [
        {
            "id": "d42b605d-5ef1-4b4a-8791-7a3e8b66b5e7",
            "resourceName": "Disk-2",
            "resourceType": "Disk",
            "createdAt": 1569624941.471,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "CreateDiskFromSnapshot",
            "status": "Started",
            "statusChangedAt": 1569624941.791
        }
    ]
}
```

Para más obtener más información, consulte Creating a block storage disk from a snapshot in Amazon Lightsail en la Guía para desarrolladores de Lightsail.

- Para obtener información sobre la API, consulte CreateDiskFromSnapshot en la Referencia de comandos de la AWS CLI.

`create-disk-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-disk-snapshot`.

AWS CLI

Ejemplo 1: crear una instantánea de un disco

En el siguiente ejemplo de `create-disk-snapshot`, se crea una instantánea llamada `DiskSnapshot-1` del disco de almacenamiento en bloques especificado.

```
aws lightsail create-disk-snapshot \
    --disk-name Disk-1 \
    --disk-snapshot-name DiskSnapshot-1
```

Salida:

```
{
    "operations": [
        {
            "id": "fa74c6d2-03a3-4f42-a7c7-792f124d534b",
            "resourceName": "DiskSnapshot-1",
            "resourceType": "DiskSnapshot",
            "createdAt": 1569625129.739,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "Disk-1",
            "operationType": "CreateDiskSnapshot",
            "status": "Started",
            "statusChangedAt": 1569625129.739
        },
        {
            "id": "920a25df-185c-4528-87cd-7b85f5488c06",
            "resourceName": "Disk-1",
            "resourceType": "Disk",
            "createdAt": 1569625129.739,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "DiskSnapshot-1",
            "operationType": "CreateDiskSnapshot",
            "status": "Started",
            "statusChangedAt": 1569625129.739
        }
    ]
}
```

Ejemplo 2: crear una instantánea del disco del sistema de una instancia

En el siguiente ejemplo de `create-disk-snapshot`, se crea una instantánea del disco del sistema de la instancia especificada.

```
aws lightsail create-disk-snapshot \
    --instance-name WordPress-1 \
    --disk-snapshot-name SystemDiskSnapshot-1
```

Salida:

```
{
    "operations": [
        {
            "id": "f508cf1c-6597-42a6-a4c3-4aebd75af0d9",
            "resourceName": "SystemDiskSnapshot-1",
            "resourceType": "DiskSnapshot",
            "createdAt": 1569625294.685,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "WordPress-1",
            "operationType": "CreateDiskSnapshot",
            "status": "Started",
            "statusChangedAt": 1569625294.685
        },
        {
            "id": "0bb9f712-da3b-4d99-b508-3bf871d989e5",
            "resourceName": "WordPress-1",
            "resourceType": "Instance",
            "createdAt": 1569625294.685,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "SystemDiskSnapshot-1",
            "operationType": "CreateDiskSnapshot",
            "status": "Started",
            "statusChangedAt": 1569625294.685
        }
    ]
```

```
}
```

Para obtener más información, consulte Snapshots in Amazon Lightsail y Creating a snapshot of an instance root volume in Amazon Lightsail en la Guía para desarrolladores de Lightsail.

- Para obtener información sobre la API, consulte CreateDiskSnapshot en la Referencia de comandos de la AWS CLI.

`create-disk`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-disk`.

AWS CLI

Para crear un disco de almacenamiento en bloques

En el siguiente ejemplo de `create-disk`, se crea un disco de almacenamiento en bloques `Disk-1` en la zona de disponibilidad y la región de AWS especificadas, con 32 GB de espacio de almacenamiento.

```
aws lightsail create-disk \
    --disk-name Disk-1 \
    --availability-zone us-west-2a \
    --size-in-gb 32
```

Salida:

```
{
    "operations": [
        {
            "id": "1c85e2ec-86ba-4697-b936-77f4d3dc013a",
            "resourceName": "Disk-1",
            "resourceType": "Disk",
            "createdAt": 1569449220.36,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "CreateDisk",
            "status": "Started",
            "statusChangedAt": 1569449220.588
```

```
        }
    ]
}
```

- Para obtener información sobre la API, consulte CreateDisk en la Referencia de comandos de la AWS CLI.

`create-domain-entry`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-domain-entry`.

AWS CLI

Para crear una entrada de dominio (registro DNS)

En el siguiente ejemplo de `create-domain-entry`, se crea un registro DNS (A) para el ápex del dominio especificado que apunta a la dirección IP de una instancia.

Nota: Las operaciones de API relacionadas con el dominio de Lightsail solo están disponibles en la región `us-east-1`. Si su perfil de CLI está configurado para usar una región diferente, debe incluir el parámetro `--region us-east-1` o el comando generará error.

```
aws lightsail create-domain-entry \
    --region us-east-1 \
    --domain-name example.com \
    --domain-entry name=example.com,type=A,target=192.0.2.0
```

Salida:

```
{
    "operation": {
        "id": "5be4494d-56f4-41fc-8730-693dcd0ef9e2",
        "resourceName": "example.com",
        "resourceType": "Domain",
        "createdAt": 1569865296.519,
        "location": {
            "availabilityZone": "all",
            "regionName": "global"
        },
        "isTerminal": true,
        "operationType": "CreateDomainEntry",
        "status": "Succeeded",
```

```
        "statusChangedAt": 1569865296.519
    }
}
```

Para obtener más información, consulte DNS in Amazon Lightsail y Creating a DNS zone to manage your domain's DNS records in Amazon Lightsail en la documentación de Guía para desarrolladores de Lightsail.

- Para obtener información sobre la API, consulte CreateDomainEntry en la Referencia de comandos de la AWS CLI.

`create-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-domain`.

AWS CLI

Para crear un dominio (zona DNS)

En el siguiente ejemplo de `create-domain`, se crea una zona DNS para el dominio especificado.

Nota: Las operaciones de API relacionadas con el dominio de Lightsail solo están disponibles en la región `us-east-1`. Si su perfil de CLI está configurado para usar una región diferente, debe incluir el parámetro `--region us-east-1` o el comando generará error.

```
aws lightsail create-domain \
    --region us-east-1 \
    --domain-name example.com
```

Salida:

```
{
    "operation": {
        "id": "64e522c8-9ae1-4c05-9b65-3f237324dc34",
        "resourceName": "example.com",
        "resourceType": "Domain",
        "createdAt": 1569864291.92,
        "location": {
            "availabilityZone": "all",
            "regionName": "global"
        },
```

```
        "isTerminal": true,
        "operationType": "CreateDomain",
        "status": "Succeeded",
        "statusChangedAt": 1569864292.109
    }
}
```

Para obtener más información, consulte DNS in Amazon Lightsail y Creating a DNS zone to manage your domain's DNS records in Amazon Lightsail en la documentación de Guía para desarrolladores de Lightsail.

- Para obtener información sobre la API, consulte CreateDomain en la Referencia de comandos de la AWS CLI.

`create-instance-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-instance-snapshot`.

AWS CLI

Para crear una instantánea de una instancia

En el siguiente ejemplo de `create-instance-snapshot`, se crea una instantánea del disco del sistema de la instancia especificada.

```
aws lightsail create-instance-snapshot \
    --instance-name WordPress-1 \
    --instance-snapshot-name WordPress-Snapshot-1
```

Salida:

```
{
    "operations": [
        {
            "id": "4c3db559-9dd0-41e7-89c0-2cb88c19786f",
            "resourceName": "WordPress-Snapshot-1",
            "resourceType": "InstanceSnapshot",
            "createdAt": 1569866438.48,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
```

```
            "isTerminal": false,
            "operationDetails": "WordPress-1",
            "operationType": "CreateInstanceSnapshot",
            "status": "Started",
            "statusChangedAt": 1569866438.48
        },
        {
            "id": "c04fdc45-2981-488c-88b5-d6d2fd759a6a",
            "resourceName": "WordPress-1",
            "resourceType": "Instance",
            "createdAt": 1569866438.48,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "WordPress-Snapshot-1",
            "operationType": "CreateInstanceSnapshot",
            "status": "Started",
            "statusChangedAt": 1569866438.48
        }
    ]
}
```

- Para obtener información sobre la API, consulte CreateInstanceSnapshot en la Referencia de comandos de la AWS CLI.

`create-instances-from-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-instances-from-snapshot`.

AWS CLI

Para crear una instancia a partir de una instantánea

En el siguiente ejemplo de `create-instances-from-snapshot`, se crea una instancia a partir de la instantánea de la instancia especificada, en la zona de disponibilidad y región AWS especificadas, mediante el paquete de 12 USD.

Nota: La agrupación que especifique debe tener especificaciones iguales o superiores a la agrupación de la instancia de origen original utilizada para crear la instantánea.

```
aws lightsail create-instances-from-snapshot \
```

```
    --instance-snapshot-name WordPress-1-1569866208 \
    --instance-names WordPress-2 \
    --availability-zone us-west-2a \
    --bundle-id small_3_0
```

Salida:

```
{
    "operations": [
        {
            "id": "003f8271-b711-464d-b9b8-7f3806cb496e",
            "resourceName": "WordPress-2",
            "resourceType": "Instance",
            "createdAt": 1569865914.908,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "CreateInstancesFromSnapshot",
            "status": "Started",
            "statusChangedAt": 1569865914.908
        }
    ]
}
```

- Para obtener información sobre la API, consulte CreateInstancesFromSnapshot en la Referencia de comandos de la AWS CLI.

`create-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-instances`.

AWS CLI

Ejemplo 1: crear una instancia única

En el siguiente ejemplo de `create-instances`, se crea una instancia en la región y la zona de disponibilidad de AWS especificadas utilizando el esquema WordPress y una agrupación de 5 USD.

```
aws lightsail create-instances \
```

```
    --instance-names Instance-1 \
    --availability-zone us-west-2a \
    --blueprint-id wordpress \
    --bundle-id nano_3_0
```

Salida:

```
{
    "operations": [
        {
            "id": "9a77158f-7be3-4d6d-8054-cf5ae2b720cc",
            "resourceName": "Instance-1",
            "resourceType": "Instance",
            "createdAt": 1569447986.061,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "CreateInstance",
            "status": "Started",
            "statusChangedAt": 1569447986.061
        }
    ]
}
```

Ejemplo 2: crear varias instancias a la vez

En el siguiente ejemplo de `create-instances`, se crean tres instancias en la región y la zona de disponibilidad de AWS especificadas utilizando el esquema WordPress y una agrupación de 5 USD.

```
aws lightsail create-instances \
    --instance-names {"Instance1","Instance2","Instance3"} \
    --availability-zone us-west-2a \
    --blueprint-id wordpress \
    --bundle-id nano_3_0
```

Salida:

```
{
    "operations": [
```

```
        {
            "id": "5492f015-9d2e-48c6-8eea-b516840e6903",
            "resourceName": "Instance1",
            "resourceType": "Instance",
            "createdAt": 1569448780.054,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "CreateInstance",
            "status": "Started",
            "statusChangedAt": 1569448780.054
        },
        {
            "id": "c58b5f46-2676-44c8-b95c-3ad375898515",
            "resourceName": "Instance2",
            "resourceType": "Instance",
            "createdAt": 1569448780.054,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "CreateInstance",
            "status": "Started",
            "statusChangedAt": 1569448780.054
        },
        {
            "id": "a5ad8006-9bee-4499-9eb7-75e42e6f5882",
            "resourceName": "Instance3",
            "resourceType": "Instance",
            "createdAt": 1569448780.054,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "CreateInstance",
            "status": "Started",
            "statusChangedAt": 1569448780.054
        }
    ]
```

```
}
```

- Para obtener información sobre la API, consulte CreateInstances en la Referencia de comandos de la AWS CLI.

`create-key-pair`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-key-pair`.

AWS CLI

Creación de un par de claves

En el siguiente ejemplo de `create-key-pair`, se crea un par de claves que se puede utilizar para autenticarse y conectarse a una instancia.

```
aws lightsail create-key-pair \
    --key-pair-name MyPersonalKeyPair
```

El resultado proporciona el valor de base64 de clave privada que puede usar para autenticarse en instancias que usan el par de claves creado. Nota: Copie y pegue el valor de base64 de clave privada en una ubicación segura, ya que no podrá recuperarlo más adelante.

```
{
    "keyPair": {
        "name": "MyPersonalKeyPair",
        "arn": "arn:aws:lightsail:us-west-2:111122223333:KeyPair/55025c71-198f-403b-
b42f-a69433e724fb",
        "supportCode": "621291663362/MyPersonalKeyPair",
        "createdAt": 1569866556.567,
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "resourceType": "KeyPair"
    },
    "publicKeyBase64": "ssh-rsa ssh-rsa
 AAAAB3NzaC1yc2EAAAADAQABAAABAQCV0xUEwx96amPERH7K1bVT1tTFl9OmNk6o7m5YVHk9xlOdMbDRbFvhtXvw4jz
+BHUgedGUXno6uF7agqxZNO1kPLJBIVTW26SSYBJ0tE
+y804UyVsjrbUqCaMXDhmfXpWulMPwuXhwcKh7e8hwoTfkiX0E6Ql
+KqF/MiA3w6DCjEqvvdIO7SiEZJFsuGNfYDDN3w60Rel5MUhmn3OJdn4y/
A7NWb3IxL4pPfVE4rgFRKU8n1jp9kwRnlVMVBOWuGXk6n+H6M2f1 ",
```

```
    "privateKeyBase64": "-----BEGIN RSA PRIVATE KEY-----
EXAMPLETCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
\nVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6\nb24xFDASBgNVBAsTC0lBTSBD
\nBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
\nMTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
\nVQQHEwdTZWF0dGxlMQ8wDQEXAMPLEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
\nb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
\nYXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMEXAMPLE4GmWIWJ
\n21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
\nrDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
\nIbb3OhjZnzcvQAaREXAMPLEMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4\nnUhVVxYUntneD9+h8Mg9q6q
+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
\nFFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OEXAMPLELvjx79LjSTb
\nNYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=\n-----END RSA PRIVATE KEY-----",
    "operation": {
        "id": "67f984db-9994-45fe-ad38-59bafcaf82ef",
        "resourceName": "MyPersonalKeyPair",
        "resourceType": "KeyPair",
        "createdAt": 1569866556.567,
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "isTerminal": true,
        "operationType": "CreateKeyPair",
        "status": "Succeeded",
        "statusChangedAt": 1569866556.704
    }
}
```

- Para obtener información sobre la API, consulte CreateKeyPair en la Referencia de comandos de la AWS CLI.

`create-load-balancer-tls-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-load-balancer-tls-certificate`.

AWS CLI

Para crear el certificado TLS de un equilibrador de carga

En el siguiente ejemplo de `create-load-balancer-tls-certificate` se crea un certificado TLS que se asocia al equilibrador de carga especificado. El certificado creado se aplica a los dominios especificados. Nota: Solo se pueden crear dos certificados para un equilibrador de carga.

```
aws lightsail create-load-balancer-tls-certificate \
    --certificate-alternative-names abc.example.com \
    --certificate-domain-name example.com \
    --certificate-name MySecondCertificate \
    --load-balancer-name MyFirstLoadBalancer
```

Salida:

```
{
    "operations": [
        {
            "id": "be663aed-cb46-41e2-9b23-e2f747245bd4",
            "resourceName": "MySecondCertificate",
            "resourceType": "LoadBalancerTlsCertificate",
            "createdAt": 1569867364.971,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "MyFirstLoadBalancer",
            "operationType": "CreateLoadBalancerTlsCertificate",
            "status": "Succeeded",
            "statusChangedAt": 1569867365.219
        },
        {
            "id": "f3dfa930-969e-41cc-ac7d-337178716f6d",
            "resourceName": "MyFirstLoadBalancer",
            "resourceType": "LoadBalancer",
            "createdAt": 1569867364.971,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "MySecondCertificate",
            "operationType": "CreateLoadBalancerTlsCertificate",
```

```
            "status": "Succeeded",
            "statusChangedAt": 1569867365.219
        }
    ]
}
```

- Para obtener información sobre la API, consulte CreateLoadBalancerTlsCertificate en la Referencia de comandos de la AWS CLI.

`create-load-balancer`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-load-balancer`.

AWS CLI

Para crear un equilibrador de carga

En el siguiente ejemplo de `create-load-balancer` se crea un equilibrador de carga con un certificado TLS. El certificado TLS se aplica a los dominios especificados y enruta el tráfico a las instancias del puerto 80.

```
aws lightsail create-load-balancer \
    --certificate-alternative-names www.example.com test.example.com \
    --certificate-domain-name example.com \
    --certificate-name Certificate-1 \
    --instance-port 80 \
    --load-balancer-name LoadBalancer-1
```

Salida:

```
{
    "operations": [
        {
            "id": "cc7b920a-83d8-4762-a74e-9174fe1540be",
            "resourceName": "LoadBalancer-1",
            "resourceType": "LoadBalancer",
            "createdAt": 1569867169.406,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
```

```
            "isTerminal": false,
            "operationType": "CreateLoadBalancer",
            "status": "Started",
            "statusChangedAt": 1569867169.406
        },
        {
            "id": "658ed43b-f729-42f3-a8e4-3f8024d3c98d",
            "resourceName": "LoadBalancer-1",
            "resourceType": "LoadBalancerTlsCertificate",
            "createdAt": 1569867170.193,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "LoadBalancer-1",
            "operationType": "CreateLoadBalancerTlsCertificate",
            "status": "Succeeded",
            "statusChangedAt": 1569867170.54
        },
        {
            "id": "4757a342-5181-4870-b1e0-227eebc35ab5",
            "resourceName": "LoadBalancer-1",
            "resourceType": "LoadBalancer",
            "createdAt": 1569867170.193,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "Certificate-1",
            "operationType": "CreateLoadBalancerTlsCertificate",
            "status": "Succeeded",
            "statusChangedAt": 1569867170.54
        }
    ]
}
```


Para obtener más información, consulte Equilibradores de carga de Lightsail en la Guía para desarrolladores de Lightsail.

- Para obtener información sobre la API, consulte CreateLoadBalancer en la Referencia de comandos de la AWS CLI.

`create-relational-database-from-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-relational-database-from-snapshot`.

AWS CLI

Para crear una base de datos administrada a partir de una instantánea

En el siguiente ejemplo de `create-relational-database-from-snapshot` se crea una instancia administrada a partir de la instantánea especificada en la zona de disponibilidad y la región AWS especificadas utilizando una agrupación de base de datos estándar de 15 USD. Nota: La agrupación que especifique debe tener especificaciones iguales o superiores a la agrupación de la base de datos de origen original utilizada para crear la instantánea.

```
aws lightsail create-relational-database-from-snapshot \
    --relational-database-snapshot-name Database-Oregon-1-1566839359 \
    --relational-database-name Database-1 \
    --availability-zone us-west-2a \
    --relational-database-bundle-id micro_1_0 \
    --no-publicly-accessible
```

Salida:

```
{
    "operations": [
        {
            "id": "ad6d9193-9d5c-4ea1-97ae-8fe6de600b4c",
            "resourceName": "Database-1",
            "resourceType": "RelationalDatabase",
            "createdAt": 1569867916.938,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "CreateRelationalDatabaseFromSnapshot",
            "status": "Started",
            "statusChangedAt": 1569867918.643
        }
    ]
}
```

- Para obtener información sobre la API, consulte CreateRelationalDatabaseFromSnapshot en la Referencia de comandos de la AWS CLI.

`create-relational-database-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-relational-database-snapshot`.

AWS CLI

Para crear una instantánea de la base de datos administrada

En el siguiente ejemplo de `create-relational-database-snapshot` se crea una instantánea de la base de datos administrada especificada.

```
aws lightsail create-relational-database-snapshot \
    --relational-database-name Database1 \
    --relational-database-snapshot-name RelationalDatabaseSnapshot1
```

Salida:

```
{
    "operations": [
        {
            "id": "853667fb-ea91-4c02-8d20-8fc5fd43b9eb",
            "resourceName": "RelationalDatabaseSnapshot1",
            "resourceType": "RelationalDatabaseSnapshot",
            "createdAt": 1569868074.645,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "Database1",
            "operationType": "CreateRelationalDatabaseSnapshot",
            "status": "Started",
            "statusChangedAt": 1569868074.645
        },
        {
            "id": "fbafa521-3cac-4be8-9773-1c143780b239",
            "resourceName": "Database1",
            "resourceType": "RelationalDatabase",
```

```
            "createdAt": 1569868074.645,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "RelationalDatabaseSnapshot1",
            "operationType": "CreateRelationalDatabaseSnapshot",
            "status": "Started",
            "statusChangedAt": 1569868074.645
        }
    ]
}
```

- Para obtener información sobre la API, consulte CreateRelationalDatabaseSnapshot en la Referencia de comandos de la AWS CLI.

`create-relational-database`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-relational-database`.

AWS CLI

Para crear una base de datos administrada

El siguiente ejemplo de `create-relational-database` crea una base de datos administrada en la región y zona de disponibilidad de AWS especificadas utilizando el motor de base de datos MySQL 5.6 (mysql_5_6) y una agrupación de base de datos estándar de 15 USD (micro_1_0). La base de datos administrada se rellena previamente con un nombre de usuario maestro y no es de acceso público.

```
aws lightsail create-relational-database \
    --relational-database-name Database-1 \
    --availability-zone us-west-2a \
    --relational-database-blueprint-id mysql_5_6 \
    --relational-database-bundle-id micro_1_0 \
    --master-database-name dbmaster \
    --master-username user \
    --no-publicly-accessible
```

Salida:

```
{
    "operations": [
        {
            "id": "b52bedee-73ed-4798-8d2a-9c12df89adcd",
            "resourceName": "Database-1",
            "resourceType": "RelationalDatabase",
            "createdAt": 1569450017.244,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "CreateRelationalDatabase",
            "status": "Started",
            "statusChangedAt": 1569450018.637
        }
    ]
}
```

- Para obtener información sobre la API, consulte CreateRelationalDatabase en la Referencia de comandos de la AWS CLI.

`delete-auto-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-auto-snapshot`.

AWS CLI

Para eliminar una instantánea automática

En el siguiente ejemplo de `delete-auto-snapshot`, se elimina la instantánea automática `2019-10-10` de la instancia `WordPress-1`.

```
aws lightsail delete-auto-snapshot \
    --resource-name WordPress-1 \
    --date 2019-10-10
```

Salida:

```
{
    "operations": [
        {
```

```
            "id": "31c36e09-3d52-46d5-b6d8-7EXAMPLE534a",
            "resourceName": "WordPress-1",
            "resourceType": "Instance",
            "createdAt": 1571088141.501,
            "location": {
                "availabilityZone": "us-west-2",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "DeleteAutoSnapshot-2019-10-10",
            "operationType": "DeleteAutoSnapshot",
            "status": "Succeeded"
        }
    ]
}
```

Para obtener más información, consulte Eliminación de instantáneas automáticas en Amazon Lightsail en la Guía para desarrolladores de Lightsail.

- Para obtener información sobre la API, consulte DeleteAutoSnapshot en la Referencia de comandos de la AWS CLI.

`delete-disk-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-disk-snapshot`.

AWS CLI

Para eliminar una instantánea de un disco de almacenamiento en bloques

En el siguiente ejemplo de `delete-disk-snapshot`, se elimina la instantánea especificada de un disco de almacenamiento en bloques.

```
aws lightsail delete-disk-snapshot \
    --disk-snapshot-name DiskSnapshot-1
```

Salida:

```
{
    "operations": [
        {
            "id": "d1e5766d-b81e-4595-ad5d-02afbccfcd5d",
```

```
            "resourceName": "DiskSnapshot-1",
            "resourceType": "DiskSnapshot",
            "createdAt": 1569873552.79,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationType": "DeleteDiskSnapshot",
            "status": "Succeeded",
            "statusChangedAt": 1569873552.79
        }
    ]
}
```

- Para obtener información sobre la API, consulte DeleteDiskSnapshot en la Referencia de comandos de la AWS CLI.

`delete-disk`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-disk`.

AWS CLI

Para eliminar un disco de almacenamiento en bloques

En el siguiente ejemplo de `delete-disk`, se elimina el disco de almacenamiento en bloques especificado.

```
aws lightsail delete-disk \
    --disk-name Disk-1
```

Salida:

```
{
    "operations": [
        {
            "id": "6378c70f-4d75-4f7a-ab66-730fca0bb2fc",
            "resourceName": "Disk-1",
            "resourceType": "Disk",
            "createdAt": 1569872887.864,
            "location": {
```

```
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationType": "DeleteDisk",
            "status": "Succeeded",
            "statusChangedAt": 1569872887.864
        }
    ]
}
```

- Para obtener información sobre la API, consulte DeleteDisk en la Referencia de comandos de la AWS CLI.

`delete-domain-entry`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-domain-entry`.

AWS CLI

Para eliminar una entrada de dominio (registro DNS)

En el siguiente ejemplo de `delete-domain-entry`, se elimina la entrada de dominio especificada de un dominio existente.

Nota: Las operaciones de API relacionadas con el dominio de Lightsail solo están disponibles en la región `us-east-1`. Si su perfil de CLI está configurado para usar una región diferente, debe incluir el parámetro `--region us-east-1` o el comando generará error.

```
aws lightsail delete-domain-entry \
    --region us-east-1 \
    --domain-name example.com \
    --domain-entry name=123.example.com,target=192.0.2.0,type=A
```

Salida:

```
{
    "operation": {
        "id": "06eacd01-d785-420e-8daa-823150c7dca1",
        "resourceName": "example.com ",
        "resourceType": "Domain",
        "createdAt": 1569874157.005,
```

```
        "location": {
            "availabilityZone": "all",
            "regionName": "global"
        },
        "isTerminal": true,
        "operationType": "DeleteDomainEntry",
        "status": "Succeeded",
        "statusChangedAt": 1569874157.005
    }
}
```

- Para obtener información sobre la API, consulte DeleteDomainEntry en la Referencia de comandos de la AWS CLI.

`delete-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-domain`.

AWS CLI

Para eliminar un dominio (zona DNS)

En el siguiente ejemplo de `delete-domain`, se elimina el dominio especificado y todas las entradas del dominio (registros DNS).

Nota: Las operaciones de API relacionadas con el dominio de Lightsail solo están disponibles en la región `us-east-1`. Si su perfil de CLI está configurado para usar una región diferente, debe incluir el parámetro `--region us-east-1` o el comando generará error.

```
aws lightsail delete-domain \
    --region us-east-1 \
    --domain-name example.com
```

Salida:

```
{
    "operation": {
        "id": "fcef5265-5af1-4a46-a3d7-90b5e18b9b32",
        "resourceName": "example.com",
        "resourceType": "Domain",
        "createdAt": 1569873788.13,
        "location": {
```

```
            "availabilityZone": "all",
            "regionName": "global"
        },
        "isTerminal": true,
        "operationType": "DeleteDomain",
        "status": "Succeeded",
        "statusChangedAt": 1569873788.13
    }
}
```

- Para obtener información sobre la API, consulte DeleteDomain en la Referencia de comandos de la AWS CLI.

`delete-instance-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-instance-snapshot`.

AWS CLI

título

En el siguiente ejemplo de `delete-instance-snapshot`, se elimina la instantánea especificada de una instancia.,

```
aws lightsail delete-instance-snapshot \
    --instance-snapshot-name WordPress-1-Snapshot-1
```

Salida:

```
{
    "operations": [
        {
            "id": "14dad182-976a-46c6-bfd4-9480482bf0ea",
            "resourceName": "WordPress-1-Snapshot-1",
            "resourceType": "InstanceSnapshot",
            "createdAt": 1569874524.562,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationType": "DeleteInstanceSnapshot",
```

```
            "status": "Succeeded",
            "statusChangedAt": 1569874524.562
        }
    ]
}
```

- Para obtener información sobre la API, consulte DeleteInstanceSnapshot en la Referencia de comandos de la AWS CLI.

`delete-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-instance`.

AWS CLI

Para eliminar una instancia

En el siguiente ejemplo de `delete-instance`, se elimina la instancia especificada.

```
aws lightsail delete-instance \
    --instance-name WordPress-1
```

Salida:

```
{
    "operations": [
        {
            "id": "d77345a3-8f80-4d2e-b47d-aaa622718df2",
            "resourceName": "Disk-1",
            "resourceType": "Disk",
            "createdAt": 1569874357.469,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "WordPress-1",
            "operationType": "DetachDisk",
            "status": "Started",
            "statusChangedAt": 1569874357.469
        },
        {
```

```
            "id": "708fa606-2bfd-4e48-a2c1-0b856585b5b1",
            "resourceName": "WordPress-1",
            "resourceType": "Instance",
            "createdAt": 1569874357.465,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "Disk-1",
            "operationType": "DetachDisk",
            "status": "Started",
            "statusChangedAt": 1569874357.465
        },
        {
            "id": "3187e823-8acb-405d-b098-fad5ceb17bec",
            "resourceName": "WordPress-1",
            "resourceType": "Instance",
            "createdAt": 1569874357.829,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationType": "DeleteInstance",
            "status": "Succeeded",
            "statusChangedAt": 1569874357.829
        }
    ]
}
```

- Para obtener información sobre la API, consulte DeleteInstance en la Referencia de comandos de la AWS CLI.

`delete-key-pair`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-key-pair`.

AWS CLI

Eliminar un par de claves

En el siguiente ejemplo de `delete-key-pair`, se elimina el par de claves especificado.

```
aws lightsail delete-key-pair \
    --key-pair-name MyPersonalKeyPair
```

Salida:

```
{
    "operation": {
        "id": "81621463-df38-4810-b866-6e801a15abbf",
        "resourceName": "MyPersonalKeyPair",
        "resourceType": "KeyPair",
        "createdAt": 1569874626.466,
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "isTerminal": true,
        "operationType": "DeleteKeyPair",
        "status": "Succeeded",
        "statusChangedAt": 1569874626.685
    }
}
```

- Para obtener información sobre la API, consulte DeleteKeyPair en la Referencia de comandos de la AWS CLI.

`delete-known-host-keys`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-known-host-keys`.

AWS CLI

Para eliminar claves de host conocidas de una instancia

En el siguiente ejemplo de `delete-known-host-keys`, se elimina la clave de host conocida de la instancia especificada.

```
aws lightsail delete-known-host-keys \
    --instance-name Instance-1
```

Salida:

```
{
    "operations": [
        {
            "id": "c61afe9c-45a4-41e6-a97e-d212364da3f5",
            "resourceName": "Instance-1",
            "resourceType": "Instance",
            "createdAt": 1569874760.201,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationType": "DeleteKnownHostKeys",
            "status": "Succeeded",
            "statusChangedAt": 1569874760.201
        }
    ]
}
```

Para obtener más información, consulte la sección Resolución de los errores de conexión con clientes SSH y RDP basados en navegador de Amazon Lightsail en la Guía para desarrolladores de Lightsail.

- Para obtener información sobre la API, consulte DeleteKnownHostKeys en la Referencia de comandos de la AWS CLI.

`delete-load-balancer-tls-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-load-balancer-tls-certificate`.

AWS CLI

Para eliminar un certificado TLS de un equilibrador de carga

En el siguiente ejemplo de `delete-load-balancer-tls-certificate`, se elimina el certificado TLS especificado del equilibrador de carga indicado.

```
aws lightsail delete-load-balancer-tls-certificate \
    --load-balancer-name MyFirstLoadBalancer \
    --certificate-name MyFirstCertificate
```

Salida:

```
{
    "operations": [
        {
            "id": "50bec274-e45e-4caa-8a69-b763ef636583",
            "resourceName": "MyFirstCertificate",
            "resourceType": "LoadBalancerTlsCertificate",
            "createdAt": 1569874989.48,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "DeleteLoadBalancerTlsCertificate",
            "status": "Started",
            "statusChangedAt": 1569874989.48
        },
        {
            "id": "78c58cdc-a59a-4b27-8213-500638634a8f",
            "resourceName": "MyFirstLoadBalancer",
            "resourceType": "LoadBalancer",
            "createdAt": 1569874989.48,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "DeleteLoadBalancerTlsCertificate",
            "status": "Started",
            "statusChangedAt": 1569874989.48
        }
    ]
}
```

- Para obtener información sobre la API, consulte DeleteLoadBalancerTlsCertificate en la Referencia de comandos de la AWS CLI.

`delete-load-balancer`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-load-balancer`.

AWS CLI

Eliminación de un equilibrador de carga

En el siguiente ejemplo de `delete-load-balancer`, se elimina el equilibrador de carga especificado y los certificados TLS asociados.

```
aws lightsail delete-load-balancer \
    --load-balancer-name MyFirstLoadBalancer
```

Salida:

```
{
    "operations": [
        {
            "id": "a8c968c7-72a3-4680-a714-af8f03eea535",
            "resourceName": "MyFirstLoadBalancer",
            "resourceType": "LoadBalancer",
            "createdAt": 1569875092.125,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationType": "DeleteLoadBalancer",
            "status": "Succeeded",
            "statusChangedAt": 1569875092.125
        },
        {
            "id": "f91a29fc-8ce3-4e69-a227-ea70ca890bf5",
            "resourceName": "MySecondCertificate",
            "resourceType": "LoadBalancerTlsCertificate",
            "createdAt": 1569875091.938,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "DeleteLoadBalancerTlsCertificate",
            "status": "Started",
            "statusChangedAt": 1569875091.938
        },
        {
```

```
            "id": "cf64c060-154b-4eb4-ba57-84e2e41563d6",
            "resourceName": "MyFirstLoadBalancer",
            "resourceType": "LoadBalancer",
            "createdAt": 1569875091.94,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "DeleteLoadBalancerTlsCertificate",
            "status": "Started",
            "statusChangedAt": 1569875091.94
        }
    ]
}
```

Para obtener más información, consulte el título en la guía.

- Para obtener información sobre la API, consulte DeleteLoadBalancer en la Referencia de comandos de la AWS CLI.

`delete-relational-database-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-relational-database-snapshot`.

AWS CLI

Para eliminar una instantánea de una base de datos administrada

En el siguiente ejemplo de `delete-relational-database-snapshot`, se elimina una instantánea especificada de una base de datos administrada.

```
aws lightsail delete-relational-database-snapshot \
    --relational-database-snapshot-name Database-Oregon-1-1566839359
```

Salida:

```
{
    "operations": [
        {
            "id": "b99acae8-735b-4823-922f-30af580e3729",
```

```
            "resourceName": "Database-Oregon-1-1566839359",
            "resourceType": "RelationalDatabaseSnapshot",
            "createdAt": 1569875293.58,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationType": "DeleteRelationalDatabaseSnapshot",
            "status": "Succeeded",
            "statusChangedAt": 1569875293.58
        }
    ]
}
```

- Para obtener información sobre la API, consulte DeleteRelationalDatabaseSnapshot en la Referencia de comandos de la AWS CLI.

`delete-relational-database`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-relational-database`.

AWS CLI

Para eliminar una base de datos administrada

En el siguiente ejemplo de `delete-relational-database`, se elimina la base de datos administrada especificada.

```
aws lightsail delete-relational-database \
    --relational-database-name Database-1
```

Salida:

```
{
    "operations": [
        {
            "id": "3b0c41c1-053d-46f0-92a3-14f76141dc86",
            "resourceName": "Database-1",
            "resourceType": "RelationalDatabase",
            "createdAt": 1569875210.999,
            "location": {
```

```
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "DeleteRelationalDatabase",
            "status": "Started",
            "statusChangedAt": 1569875210.999
        },
        {
            "id": "01ddeae8-a87a-4a4b-a1f3-092c71bf9180",
            "resourceName": "Database-1",
            "resourceType": "RelationalDatabase",
            "createdAt": 1569875211.029,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "Database-1-FinalSnapshot-1569875210793",
            "operationType": "CreateRelationalDatabaseSnapshot",
            "status": "Started",
            "statusChangedAt": 1569875211.029
        },
        {
            "id": "74d73681-30e8-4532-974e-1f23cd3f9f73",
            "resourceName": "Database-1-FinalSnapshot-1569875210793",
            "resourceType": "RelationalDatabaseSnapshot",
            "createdAt": 1569875211.029,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "Database-1",
            "operationType": "CreateRelationalDatabaseSnapshot",
            "status": "Started",
            "statusChangedAt": 1569875211.029
        }
    ]
}
```

- Para obtener información sobre la API, consulte DeleteRelationalDatabase en la Referencia de comandos de la AWS CLI.

`detach-static-ip`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-static-ip`.

AWS CLI

Para desasociar una IP estática de una instancia

En el siguiente ejemplo de `detach-static-ip`, se desasocia una IP estática `StaticIp-1` de cualquier instancia asociada.

```
aws lightsail detach-static-ip \
    --static-ip-name StaticIp-1
```

Salida:

```
{
    "operations": [
        {
            "id": "2a43d8a3-9f2d-4fe7-bdd0-eEXAMPLE3cf3",
            "resourceName": "StaticIp-1",
            "resourceType": "StaticIp",
            "createdAt": 1571088261.999,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "MEAN-1",
            "operationType": "DetachStaticIp",
            "status": "Succeeded",
            "statusChangedAt": 1571088261.999
        },
        {
            "id": "41a7d40c-74e8-4d2e-a837-cEXAMPLEf747",
            "resourceName": "MEAN-1",
            "resourceType": "Instance",
            "createdAt": 1571088262.022,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
```

```
            "operationDetails": "StaticIp-1",
            "operationType": "DetachStaticIp",
            "status": "Succeeded",
            "statusChangedAt": 1571088262.022
        }
    ]
}
```

- Para obtener información sobre la API, consulte DetachStaticIp en la Referencia de comandos de la AWS CLI.

`get-active-names`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-active-names`.

AWS CLI

Para obtener nombres de recursos activos

El siguiente ejemplo de `get-active-names` devuelve los nombres de recursos activos de la región de AWS configurada.

```
aws lightsail get-active-names
```

Salida:

```
{
    "activeNames": [
        "WordPress-1",
        "StaticIp-1",
        "MEAN-1",
        "Plesk_Hosting_Stack_on_Ubuntu-1"
    ]
}
```

- Para obtener información sobre la API, consulte GetActiveNames en la Referencia de comandos de la AWS CLI.

`get-auto-snapshots`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-auto-snapshots`.

AWS CLI

Para obtener las instantáneas automáticas disponibles para una instancia

En el siguiente ejemplo de `get-auto-snapshots`, se devuelven las instantáneas automáticas disponibles para la instancia `WordPress-1`

```
aws lightsail get-auto-snapshots \
    --resource-name WordPress-1
```

Salida:

```
{
    "resourceName": "WordPress-1",
    "resourceType": "Instance",
    "autoSnapshots": [
        {
            "date": "2019-10-14",
            "createdAt": 1571033872.0,
            "status": "Success",
            "fromAttachedDisks": []
        },
        {
            "date": "2019-10-13",
            "createdAt": 1570947473.0,
            "status": "Success",
            "fromAttachedDisks": []
        },
        {
            "date": "2019-10-12",
            "createdAt": 1570861072.0,
            "status": "Success",
            "fromAttachedDisks": []
        },
        {
            "date": "2019-10-11",
            "createdAt": 1570774672.0,
            "status": "Success",
            "fromAttachedDisks": []
        }
    ]
}
```

Para obtener más información, consulte Keeping automatic snapshots of instances or disks in Amazon Lightsail en la Guía para desarrolladores de Lightsail.

- Para obtener información sobre la API, consulte GetAutoSnapshots en la Referencia de comandos de la AWS CLI.

`get-blueprints`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-blueprints`.

AWS CLI

Para obtener los esquemas para nuevas instancias

En el siguiente ejemplo de `get-blueprints`, se muestran detalles sobre todos los esquemas disponibles que se pueden utilizar para crear nuevas instancias en Amazon Lightsail.

```
aws lightsail get-blueprints
```

Salida:

```
{
    "blueprints": [
        {
            "blueprintId": "wordpress",
            "name": "WordPress",
            "group": "wordpress",
            "type": "app",
            "description": "Bitnami, the leaders in application packaging, and
 Automattic, the experts behind WordPress, have teamed up to offer this official
 WordPress image. This image is a pre-configured, ready-to-run image for running
 WordPress on Amazon Lightsail. WordPress is the world's most popular content
 management platform. Whether it's for an enterprise or small business website, or
 a personal or corporate blog, content authors can easily create content using its
 new Gutenberg editor, and developers can extend the base platform with additional
 features. Popular plugins like Jetpack, Akismet, All in One SEO Pack, WP Mail,
 Google Analytics for WordPress, and Amazon Polly are all pre-installed in this
 image. Let's Encrypt SSL certificates are supported through an auto-configuration
 script.",
            "isActive": true,
            "minPower": 0,
            "version": "6.5.3-0",
            "versionCode": "1",
```

```
            "productUrl": "https://aws.amazon.com/marketplace/pp/B00NN8Y43U",
            "licenseUrl": "https://aws.amazon.com/marketplace/pp/B00NN8Y43U#pdp-
usage",
            "platform": "LINUX_UNIX"
        },
        {
            "blueprintId": "lamp_8_bitnami",
            "name": "LAMP (PHP 8)",
            "group": "lamp_8",
            "type": "app",
            "description": "LAMP with PHP 8.X packaged by Bitnami enables you
 to quickly start building your websites and applications by providing a coding
 framework. As a developer, it provides standalone project directories to store your
 applications. This blueprint is configured for production environments. It includes
 SSL auto-configuration with Let's Encrypt certificates, and the latest releases of
 PHP, Apache, and MariaDB on Linux. This application also includes phpMyAdmin, PHP
 main modules and Composer.",
            "isActive": true,
            "minPower": 0,
            "version": "8.2.18-4",
            "versionCode": "1",
            "productUrl": "https://aws.amazon.com/marketplace/pp/
prodview-6g3gzfcih6dvu",
            "licenseUrl": "https://aws.amazon.com/marketplace/pp/
prodview-6g3gzfcih6dvu#pdp-usage",
            "platform": "LINUX_UNIX"
        },
        {
            "blueprintId": "nodejs",
            "name": "Node.js",
            "group": "node",
            "type": "app",
            "description": "Node.js packaged by Bitnami is a pre-configured, ready
 to run image for Node.js on Amazon EC2. It includes the latest version of Node.js,
 Apache, Python and Redis. The image supports multiple Node.js applications, each
 with its own virtual host and project directory. It is configured for production
 use and is secure by default, as all ports except HTTP, HTTPS and SSH ports are
 closed. Let's Encrypt SSL certificates are supported through an auto-configuration
 script. Developers benefit from instant access to a secure, update and consistent
 Node.js environment without having to manually install and configure multiple
 components and libraries.",
            "isActive": true,
            "minPower": 0,
            "version": "18.20.2-0",
```

```
            "versionCode": "1",
            "productUrl": "https://aws.amazon.com/marketplace/pp/B00NNZUAKO",
            "licenseUrl": "https://aws.amazon.com/marketplace/pp/B00NNZUAKO#pdp-
usage",
            "platform": "LINUX_UNIX"
        },
        ...
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetBlueprints en la Referencia de comandos de la AWS CLI.

`get-bundles`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bundles`.

AWS CLI

Para obtener las agrupaciones de nuevas instancias

En el siguiente ejemplo de `get-bundles`, se muestran detalles sobre todas las agrupaciones disponibles que se pueden utilizar para crear nuevas instancias en Amazon Lightsail.

```
aws lightsail get-bundles
```

Salida:

```
{
    "bundles": [
        {
            "price": 5.0,
            "cpuCount": 2,
            "diskSizeInGb": 20,
            "bundleId": "nano_3_0",
            "instanceType": "nano",
            "isActive": true,
            "name": "Nano",
            "power": 298,
            "ramSizeInGb": 0.5,
```

```
            "transferPerMonthInGb": 1024,
            "supportedPlatforms": [
                "LINUX_UNIX"
            ]
        },
        {
            "price": 7.0,
            "cpuCount": 2,
            "diskSizeInGb": 40,
            "bundleId": "micro_3_0",
            "instanceType": "micro",
            "isActive": true,
            "name": "Micro",
            "power": 500,
            "ramSizeInGb": 1.0,
            "transferPerMonthInGb": 2048,
            "supportedPlatforms": [
                "LINUX_UNIX"
            ]
        },
        {
            "price": 12.0,
            "cpuCount": 2,
            "diskSizeInGb": 60,
            "bundleId": "small_3_0",
            "instanceType": "small",
            "isActive": true,
            "name": "Small",
            "power": 1000,
            "ramSizeInGb": 2.0,
            "transferPerMonthInGb": 3072,
            "supportedPlatforms": [
                "LINUX_UNIX"
            ]
        },
        ...
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetBundles en la Referencia de comandos de la AWS CLI.

get-cloud-formation-stack-records

En el siguiente ejemplo de código, se muestra cómo utilizar `get-cloud-formation-stack-records`.

AWS CLI

Para obtener los registros de la pila de CloudFormation y sus pilas asociadas

En el siguiente ejemplo de `get-cloud-formation-stack-records`, se muestran detalles sobre los registros de la pila de CloudFormation y sus pilas asociadas que se utilizan para crear recursos de Amazon EC2 a partir de instantáneas exportadas de Amazon Lightsail.

```
aws lightsail get-cloud-formation-stack-records
```

Salida:

```
{
    "cloudFormationStackRecords": [
        {
            "name": "CloudFormationStackRecord-588a4243-
e2d1-490d-8200-3a7513ecebdf",
            "arn": "arn:aws:lightsail:us-
west-2:111122223333:CloudFormationStackRecord/28d646ab-27bc-48d9-a422-1EXAMPLE6d37",
            "createdAt": 1565301666.586,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "resourceType": "CloudFormationStackRecord",
            "state": "Succeeded",
            "sourceInfo": [
                {
                    "resourceType": "ExportSnapshotRecord",
                    "name": "ExportSnapshotRecord-
e02f23d7-0453-4aa9-9c95-91aa01a141dd",
                    "arn": "arn:aws:lightsail:us-
west-2:111122223333:ExportSnapshotRecord/f12b8792-f3ea-4d6f-b547-2EXAMPLE8796"
                }
            ],
            "destinationInfo": {
```

```
                "id": "arn:aws:cloudformation:us-west-2:111122223333:stack/
Lightsail-Stack-588a4243-e2d1-490d-8200-3EXAMPLEebdf/063203b0-
ba28-11e9-838b-0EXAMPLE8b00",
                "service": "Aws::CloudFormation::Stack"
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetCloudFormationStackRecords en la Referencia de comandos de la AWS CLI.

`get-disk-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-disk-snapshot`.

AWS CLI

Para obtener información sobre una instantánea de disco

En el siguiente ejemplo de `get-disk-snapshot`, se muestran detalles sobre la instantánea de disco `Disk-1-1566839161`.

```
aws lightsail get-disk-snapshot \
    --disk-snapshot-name Disk-1-1566839161
```

Salida:

```
{
    "diskSnapshot": {
        "name": "Disk-1-1566839161",
        "arn": "arn:aws:lightsail:us-west-2:111122223333:DiskSnapshot/
e2d0fa53-8ee0-41a0-8e56-0EXAMPLE1051",
        "supportCode": "6EXAMPLE3362/snap-0EXAMPLE06100d09",
        "createdAt": 1566839163.749,
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "resourceType": "DiskSnapshot",
        "tags": [],
```

```
        "sizeInGb": 8,
        "state": "completed",
        "progress": "100%",
        "fromDiskName": "Disk-1",
        "fromDiskArn": "arn:aws:lightsail:us-west-2:111122223333:Disk/
c21cfb0a-07f2-44ae-9a23-bEXAMPLE8096",
        "isFromAutoSnapshot": false
    }
}
```

Para obtener más información, consulte el título en la guía.

- Para obtener información sobre la API, consulte GetDiskSnapshot en la Referencia de comandos de la AWS CLI.

`get-disk-snapshots`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-disk-snapshots`.

AWS CLI

Para obtener información sobre todas las instantáneas de disco

En el siguiente ejemplo de `get-disk-snapshots`, se muestran detalles sobre todas las instantáneas de disco en la región de AWS configurada.

```
aws lightsail get-disk-snapshots
```

Salida:

```
{
    "diskSnapshots": [
        {
            "name": "Disk-2-1571090588",
            "arn": "arn:aws:lightsail:us-
west-2:111122223333:DiskSnapshot/32e889a9-38d4-4687-9f21-eEXAMPLE7839",
            "supportCode": "6EXAMPLE3362/snap-0EXAMPLE1ca192a4",
            "createdAt": 1571090591.226,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
```

```
            "resourceType": "DiskSnapshot",
            "tags": [],
            "sizeInGb": 8,
            "state": "completed",
            "progress": "100%",
            "fromDiskName": "Disk-2",
            "fromDiskArn": "arn:aws:lightsail:us-
west-2:111122223333:Disk/6a343ff8-6341-422d-86e2-bEXAMPLE16c2",
            "isFromAutoSnapshot": false
        },
        {
            "name": "Disk-1-1566839161",
            "arn": "arn:aws:lightsail:us-west-2:111122223333:DiskSnapshot/
e2d0fa53-8ee0-41a0-8e56-0EXAMPLE1051",
            "supportCode": "6EXAMPLE3362/snap-0EXAMPLEe06100d09",
            "createdAt": 1566839163.749,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "resourceType": "DiskSnapshot",
            "tags": [],
            "sizeInGb": 8,
            "state": "completed",
            "progress": "100%",
            "fromDiskName": "Disk-1",
            "fromDiskArn": "arn:aws:lightsail:us-west-2:111122223333:Disk/
c21cfb0a-07f2-44ae-9a23-bEXAMPLE8096",
            "isFromAutoSnapshot": false
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetDiskSnapshots en la Referencia de comandos de la AWS CLI.

`get-disk`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-disk`.

AWS CLI

Para obtener información sobre un disco de almacenamiento en bloques

En el siguiente ejemplo de `get-disk`, se muestran detalles sobre el disco `Disk-1`.

```
aws lightsail get-disk \
    --disk-name Disk-1
```

Salida:

```
{
    "disk": {
        "name": "Disk-1",
        "arn": "arn:aws:lightsail:us-west-2:111122223333:Disk/
c21cfb0a-07f2-44ae-9a23-bEXAMPLE8096",
        "supportCode": "6EXAMPLE3362/vol-0EXAMPLEf2f88b32f",
        "createdAt": 1566585439.587,
        "location": {
            "availabilityZone": "us-west-2a",
            "regionName": "us-west-2"
        },
        "resourceType": "Disk",
        "tags": [],
        "sizeInGb": 8,
        "isSystemDisk": false,
        "iops": 100,
        "path": "/dev/xvdf",
        "state": "in-use",
        "attachedTo": "WordPress_Multisite-1",
        "isAttached": true,
        "attachmentState": "attached"
    }
}
```

Para obtener más información, consulte el título en la guía.

- Para obtener información sobre la API, consulte GetDisk en la Referencia de comandos de la AWS CLI.

`get-disks`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-disks`.

AWS CLI

Para obtener información sobre todos los discos de almacenamiento en bloques

En el siguiente ejemplo de `get-disks`, se muestran detalles sobre todos los discos en la región de AWS configurada.

```
aws lightsail get-disks
```

Salida:

```
{
    "disks": [
        {
            "name": "Disk-2",
            "arn": "arn:aws:lightsail:us-
west-2:111122223333:Disk/6a343ff8-6341-422d-86e2-bEXAMPLE16c2",
            "supportCode": "6EXAMPLE3362/vol-0EXAMPLE929602087",
            "createdAt": 1571090461.634,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "resourceType": "Disk",
            "tags": [],
            "sizeInGb": 8,
            "isSystemDisk": false,
            "iops": 100,
            "state": "available",
            "isAttached": false,
            "attachmentState": "detached"
        },
        {
            "name": "Disk-1",
            "arn": "arn:aws:lightsail:us-west-2:111122223333:Disk/
c21cfb0a-07f2-44ae-9a23-bEXAMPLE8096",
            "supportCode": "6EXAMPLE3362/vol-0EXAMPLEf2f88b32f",
            "createdAt": 1566585439.587,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "resourceType": "Disk",
            "tags": [],
            "sizeInGb": 8,
            "isSystemDisk": false,
            "iops": 100,
```

```
            "path": "/dev/xvdf",
            "state": "in-use",
            "attachedTo": "WordPress_Multisite-1",
            "isAttached": true,
            "attachmentState": "attached"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetDisks en la Referencia de comandos de la AWS CLI.

`get-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-domain`.

AWS CLI

Para obtener información acerca de un dominio

En el siguiente ejemplo de `get-domain`, se muestran detalles sobre el dominio `example.com`.

Nota: Las operaciones de API relacionadas con el dominio de Lightsail solo están disponibles en la región `us-east-1` de AWS. Si su perfil de CLI está configurado para usar una región diferente, debe incluir el parámetro `` --region us-east-1`` o el comando generará error.

```
aws lightsail get-domain \
    --domain-name example.com \
    --region us-east-1
```

Salida:

```
{
    "domain": {
        "name": "example.com",
        "arn":
 "arn:aws:lightsail:global:111122223333:Domain/28cda903-3f15-44b2-9baf-3EXAMPLEb304",
        "supportCode": "6EXAMPLE3362//hostedzone/ZEXAMPLEONGSC1",
        "createdAt": 1570728588.6,
        "location": {
            "availabilityZone": "all",
            "regionName": "global"
```

```
        },
        "resourceType": "Domain",
        "tags": [],
        "domainEntries": [
            {
                "id": "-1682899164",
                "name": "example.com",
                "target": "192.0.2.0",
                "isAlias": false,
                "type": "A"
            },
            {
                "id": "1703104243",
                "name": "example.com",
                "target": "ns-137.awsdns-17.com",
                "isAlias": false,
                "type": "NS"
            },
            {
                "id": "-1038331153",
                "name": "example.com",
                "target": "ns-1710.awsdns-21.co.uk",
                "isAlias": false,
                "type": "NS"
            },
            {
                "id": "-2107289565",
                "name": "example.com",
                "target": "ns-692.awsdns-22.net",
                "isAlias": false,
                "type": "NS"
            },
            {
                "id": "1582095705",
                "name": "example.com",
                "target": "ns-1436.awsdns-51.org",
                "isAlias": false,
                "type": "NS"
            },
            {
                "id": "-1769796132",
                "name": "example.com",
                "target": "ns-1710.awsdns-21.co.uk. awsdns-hostmaster.amazon.com. 1
7200 900 1209600 86400",
```

```
                "isAlias": false,
                "type": "SOA"
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte GetDomain en la Referencia de comandos de AWS CLI.

`get-domains`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-domains`.

AWS CLI

Para obtener información acerca de todos los dominios

En el siguiente ejemplo de `get-domains`, se muestran detalles sobre todos los dominios en la región de AWS configurada.

Nota: Las operaciones de API relacionadas con el dominio de Lightsail solo están disponibles en la región `us-east-1` de AWS. Si su perfil de CLI está configurado para usar una región diferente, debe incluir el parámetro `--region us-east-1` o el comando generará error.

```
aws lightsail get-domains \
    --region us-east-1
```

Salida:

```
{
    "domains": [
        {
            "name": "example.com",
            "arn":
 "arn:aws:lightsail:global:111122223333:Domain/28cda903-3f15-44b2-9baf-3EXAMPLEb304",
            "supportCode": "6EXAMPLE3362//hostedzone/ZEXAMPLEONGSC1",
            "createdAt": 1570728588.6,
            "location": {
                "availabilityZone": "all",
                "regionName": "global"
            },
```

```
            "resourceType": "Domain",
            "tags": [],
            "domainEntries": [
                {
                    "id": "-1682899164",
                    "name": "example.com",
                    "target": "192.0.2.0",
                    "isAlias": false,
                    "type": "A"
                },
                {
                    "id": "1703104243",
                    "name": "example.com",
                    "target": "ns-137.awsdns-17.com",
                    "isAlias": false,
                    "type": "NS"
                },
                {
                    "id": "-1038331153",
                    "name": "example.com",
                    "target": "ns-4567.awsdns-21.co.uk",
                    "isAlias": false,
                    "type": "NS"
                },
                {
                    "id": "-2107289565",
                    "name": "example.com",
                    "target": "ns-333.awsdns-22.net",
                    "isAlias": false,
                    "type": "NS"
                },
                {
                    "id": "1582095705",
                    "name": "example.com",
                    "target": "ns-1111.awsdns-51.org",
                    "isAlias": false,
                    "type": "NS"
                },
                {
                    "id": "-1769796132",
                    "name": "example.com",
                    "target": "ns-1234.awsdns-21.co.uk. awsdns-
hostmaster.amazon.com. 1 7200 900 1209600 86400",
                    "isAlias": false,
```

```
                    "type": "SOA"
                },
                {
                    "id": "1029454894",
                    "name": "_dead6a124ede046a0319eb44a4eb3cbc.example.com",
                    "target": "_be133b0a0899fb7b6bf79d9741d1a383.hkvuiqjoua.acm-
validations.aws",
                    "isAlias": false,
                    "type": "CNAME"
                }
            ]
        },
        {
            "name": "example.net",
            "arn": "arn:aws:lightsail:global:111122223333:Domain/9c9f0d70-
c92e-4753-86c2-6EXAMPLE029d",
            "supportCode": "6EXAMPLE3362//hostedzone/ZEXAMPLE5TPKMV",
            "createdAt": 1556661071.384,
            "location": {
                "availabilityZone": "all",
                "regionName": "global"
            },
            "resourceType": "Domain",
            "tags": [],
            "domainEntries": [
                {
                    "id": "-766320943",
                    "name": "example.net",
                    "target": "192.0.2.2",
                    "isAlias": false,
                    "type": "A"
                },
                {
                    "id": "-453913825",
                    "name": "example.net",
                    "target": "ns-123.awsdns-10.net",
                    "isAlias": false,
                    "type": "NS"
                },
                {
                    "id": "1553601564",
                    "name": "example.net",
                    "target": "ns-4444.awsdns-47.co.uk",
                    "isAlias": false,
```

```
                    "type": "NS"
                },
                {
                    "id": "1653797661",
                    "name": "example.net",
                    "target": "ns-7890.awsdns-61.org",
                    "isAlias": false,
                    "type": "NS"
                },
                {
                    "id": "706414698",
                    "name": "example.net",
                    "target": "ns-123.awsdns-44.com",
                    "isAlias": false,
                    "type": "NS"
                },
                {
                    "id": "337271745",
                    "name": "example.net",
                    "target": "ns-4444.awsdns-47.co.uk. awsdns-
hostmaster.amazon.com. 1 7200 900 1209600 86400",
                    "isAlias": false,
                    "type": "SOA"
                },
                {
                    "id": "-1785431096",
                    "name": "www.example.net",
                    "target": "192.0.2.2",
                    "isAlias": false,
                    "type": "A"
                }
            ]
        },
        {
            "name": "example.org",
            "arn": "arn:aws:lightsail:global:111122223333:Domain/
f0f13ba3-3df0-4fdc-8ebb-1EXAMPLEf26e",
            "supportCode": "6EXAMPLE3362//hostedzone/ZEXAMPLEAFO38",
            "createdAt": 1556661199.106,
            "location": {
                "availabilityZone": "all",
                "regionName": "global"
            },
            "resourceType": "Domain",
```

```
            "tags": [],
            "domainEntries": [
                {
                    "id": "2065301345",
                    "name": "example.org",
                    "target": "192.0.2.4",
                    "isAlias": false,
                    "type": "A"
                },
                {
                    "id": "-447198516",
                    "name": "example.org",
                    "target": "ns-123.awsdns-45.com",
                    "isAlias": false,
                    "type": "NS"
                },
                {
                    "id": "136463022",
                    "name": "example.org",
                    "target": "ns-9999.awsdns-15.co.uk",
                    "isAlias": false,
                    "type": "NS"
                },
                {
                    "id": "1395941679",
                    "name": "example.org",
                    "target": "ns-555.awsdns-01.net",
                    "isAlias": false,
                    "type": "NS"
                },
                {
                    "id": "872052569",
                    "name": "example.org",
                    "target": "ns-6543.awsdns-38.org",
                    "isAlias": false,
                    "type": "NS"
                },
                {
                    "id": "1001949377",
                    "name": "example.org",
                    "target": "ns-1234.awsdns-15.co.uk. awsdns-
hostmaster.amazon.com. 1 7200 900 1209600 86400",
                    "isAlias": false,
                    "type": "SOA"
```

```
                },
                {
                    "id": "1046191192",
                    "name": "www.example.org",
                    "target": "192.0.2.4",
                    "isAlias": false,
                    "type": "A"
                }
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetDomains en la Referencia de comandos de AWS CLI.

`get-export-snapshot-record`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-export-snapshot-record`.

AWS CLI

Para obtener los registros de las instantáneas exportadas a Amazon EC2

En el siguiente ejemplo de `get-export-snapshot-record`, se muestran detalles sobre la instantáneas de disco o instancia de Amazon Lightsail exportadas a Amazon EC2.

```
aws lightsail get-export-snapshot-records
```

Salida:

```
{
    "exportSnapshotRecords": [
        {
            "name": "ExportSnapshotRecord-d2da10ce-0b3c-4ae1-ab3a-2EXAMPLEa586",
            "arn": "arn:aws:lightsail:us-
west-2:111122223333:ExportSnapshotRecord/076c7060-b0cc-4162-98f0-2EXAMPLEe28e",
            "createdAt": 1543534665.678,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
```

```
            "resourceType": "ExportSnapshotRecord",
            "state": "Succeeded",
            "sourceInfo": {
                "resourceType": "InstanceSnapshot",
                "createdAt": 1540339310.706,
                "name": "WordPress-512MB-Oregon-1-1540339219",
                "arn": "arn:aws:lightsail:us-
west-2:111122223333:InstanceSnapshot/5446f534-ed60-4c17-b4a5-bEXAMPLEf8b7",
                "fromResourceName": "WordPress-512MB-Oregon-1",
                "fromResourceArn": "arn:aws:lightsail:us-
west-2:111122223333:Instance/4b8f1f24-e4d1-4cf3-88ff-cEXAMPLEa397",
                "instanceSnapshotInfo": {
                    "fromBundleId": "nano_2_0",
                    "fromBlueprintId": "wordpress_4_9_8",
                    "fromDiskInfo": [
                        {
                            "path": "/dev/sda1",
                            "sizeInGb": 20,
                            "isSystemDisk": true
                        }
                    ]
                }
            },
            "destinationInfo": {
                "id": "ami-0EXAMPLEc0d65058e",
                "service": "Aws::EC2::Image"
            }
        },
        {
            "name": "ExportSnapshotRecord-1c94e884-40ff-4fe1-9302-0EXAMPLE14c2",
            "arn": "arn:aws:lightsail:us-west-2:111122223333:ExportSnapshotRecord/
fb392ce8-6567-4013-9bfd-3EXAMPLE5b4c",
            "createdAt": 1543432110.2,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "resourceType": "ExportSnapshotRecord",
            "state": "Succeeded",
            "sourceInfo": {
                "resourceType": "InstanceSnapshot",
                "createdAt": 1540833603.545,
                "name": "LAMP_PHP_5-512MB-Oregon-1-1540833565",
```

```
                "arn": "arn:aws:lightsail:us-
west-2:111122223333:InstanceSnapshot/82334399-b5f2-49ec-8382-0EXAMPLEe45f",
                "fromResourceName": "LAMP_PHP_5-512MB-Oregon-1",
                "fromResourceArn": "arn:aws:lightsail:us-
west-2:111122223333:Instance/863b9f35-ab1e-4418-bdd2-1EXAMPLEbab2",
                "instanceSnapshotInfo": {
                    "fromBundleId": "nano_2_0",
                    "fromBlueprintId": "lamp_5_6_37_2",
                    "fromDiskInfo": [
                        {
                            "path": "/dev/sda1",
                            "sizeInGb": 20,
                            "isSystemDisk": true
                        }
                    ]
                }
            },
            "destinationInfo": {
                "id": "ami-0EXAMPLE7c5ec84e2",
                "service": "Aws::EC2::Image"
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetExportSnapshotRecord en la Referencia de comandos de la AWS CLI.

`get-instance-access-details`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-instance-access-details`.

AWS CLI

Para obtener información de claves de host de una instancia

En el siguiente ejemplo de `get-instance-access-details`, se muestra información de claves de host para la instancia `WordPress_Multisite-1`.

```
aws lightsail get-instance-access-details \
    --instance-name WordPress_Multisite-1
```

Salida:


```
{
    "accessDetails": {
        "certKey": "ssh-rsa-cert-v01@openssh.com
 AEXAMPLEaC1yc2EtY2VydC12MDFAb3BlbnNzaC5jb20AAAAgNf076Dt3ppmPd0fPxZVMmS491aEAYYH9cHqAJ3fNML8
vEXAMPLE2eBWJyQvn7ol/
i0+s966h5sx8qUD79lPB7q5UESd5VZGFtytrykfQJnjiwqe7EV5agzvjblLj26Fb37EKda9HVfCOu8pWbvky7Tyn9w29
+xMfQM9xVz0rXZmqx8uJidJpRgLCMTviofwQJU/
K1EXAMPLEAAAAAAAABAAAALS00MzMzMDU4MzA4ODg1MTY2NjM4Onp6UWlndHk4UElRSG9STitOTG5QSEE9PQAAAAsAAA
+LiB+ozNbUA0cdNL9Y67x7qPv/R7XhTc21+2A+8+GuVpK/Kz9dqDMKNAEXAMPLE+YYN
+tiXm7Y8OgziK+7iDB7xUuQ4vghmn4+qgz9mKwYgWvVe2+0XLuV7cnWPB7iUlHQg
+E3LUKrV4ZFw9pj7X2dFdNKfMxwWgI1ISWKimEXAMPLEeHjrf1Rqc/
QH6TpWCvPfcx8uvwVqdwTfkE/SfA5BCzbGGI1UmIUadh8nHcb5FamQ1hK7kECy47K/x9FMn/
KwmM7pCwJbSLDMO7n9bnbvck6m8ZoB2N2YLMG5dW7BerEXAMPLEobqfdtyYJHHel1EyyEJs1fWNU3D5JIGlgzcPAV
+ZlbQyUCZXf0oslSa+HE85fO/
FRq9SVSBSHrmbeb0frlPhgMzgSmqLeyhlbr6wwWIDbREXAMPLEJZ49H7RdQxdKyYrZPWvRgcr0qI2EL0tAajnpQQ8UZq
Aqter0xN5PhFL0J49OWTacwCGRAjLhibAx7K1t/1ZXWo6c+ijq8clll327EXAMPLE/
e89GC89KcmKCxfGQniDAUgF8UqofIbq3ZOUgiAAYCVXclI4L68NhVXyoWuQXPBRQSEXAMPLEWm74tDL9tFN3c7tSe/
Oz0cTR+4sAAAIPAAAAB3NzaC1yc2EAAAIAQnG/
L0DqiSnLrWhEox4aHqMgd0m0oLLAYx6OQH9F0TM9EXAMPLE961rzSCMon7ZgsWNnL0OwZQgDG
+rtJ4N0B7HOVwns4ynUFbzNQ3qFGGeE3lKwX1L41vV1iSy7sDk8aI0LmrKJi1LE1Qc1l8uboRlwoXOYEXAMPLEaUCeX
+10+WEXAMPLEg6Y4U4ZvE2B3xyRdpvysb5TGFNtk5qPslacnVkoLOGsZZXMpLGJnG4OBpQLLtpj9sNMxAgZPCAUjhkqk
+nxO9O4NUZ2pTWbVSUaV1gm6pug9xbwNO1Im21t34JeLlKTqxcJ6zzS8W0c0KKpAm5c4hWkseMbyutS2jav/4hiS
+BhrYgptzfwe5qRXEXAMPLEHZQr3YfGzYoBJ/
lLK3NHhxOihhsfAYwMei0BFZT1F/7CT3IH4iitEkIgodi06/
Mw6UDqMPozyQCK1lEA6LFhYCOZG9drWcoRa74lM4kY9TP028Za8gDMh1WpkXLq9Gixon5OHP8aM/
sEXAMPLEr2+fnkw+1BtoO5L6+VKoPlXaGqZ/fBYEXAMPLEAMQHjnLM1JYNvtEEPhp+TNzXHzuixWf/
Ht04m0AVpXrzIDXaS1O2tXY=",
        "ipAddress": "192.0.2.0",
        "privateKey": "-----BEGIN RSA PRIVATE KEY-----
\nEXAMPLEBAAKCAQEA+AD3qeU2toBy5O5v7wnRLVo/tngVickL5+6Jf4tPrPeuoebM
\nfKlA+/ZTwe6uVBEneVWRhbcra8pH0CZ44sKnuxFeWoM7425S49uhW9+xCnWvR1Xw
\njrvKVm75Mu08p/cNvfWugrBuaPB65DspgxNnOfZWMVxpIpSqOSPWmSwQHV597d6C
\nrEXAMPLEo8hJmqz2KFQ09X7fB2lBruGgr9aXiNPmWmovYKqwFmrnFvR7odFmDecq
\n5EXAMPLE9dyU1ZsrWhGby77eYrVaFl0GNGQ8qy1HGUiscquZ9NDIL49n4mXbfsTH
\n0EXAMPLE12ZqsfLiYnSaUYCwjE74qH8ECVPytQIDAQABAoIBAHeZV9Z58JHAjifz
\nCEXAMPLEEqC3doOVDgXSlkKI92qNo4z2VcUEho878paCuVVXVHcCGgSnGeyIh2tN
\nMEXAMPLESohR427BhH3YLA+3Z5SIvnejbTgYPfLC37B8khTaYqkqMvdZiFVZK5qn
\nIEXAMPLEM93oF9eSZCjcLKB/jGHsfb0eCDMP8BshHE2beuqzVMoK1DxOnvoP3+Fp
\nAEXAMPLESq6pDpCo9YVUX8g1u3Ro9cPl2LXHDy+oVEY5KhbZQJ7VU1I72WOvppWW
\nOEXAMPLEkgYlq7p6qYtYcSgTEjz14gDiMfQ7SyHB3alkIoNONQ9ZPaWHyJvymeud
\noQTNuz0CgYEA/LFWNTEZrzdzdR1kJmyNRmAermU0B6utyNENChAlHGSHkB+1lVSh
\nbEXAMPLEQo9ooUeW5UxO3YwacZLoDT1mwxw1Ptc1+PNycZoLe1fE9UdARrdmGTob
```

```
\n8l7CPLSXp3xuR8VqSp2fnIc7hfiQs/NrPX9gm/EOrB0we0RKyDSzWScCgYEA+z/r
\niob+nJZq0YbnOSuP6oMULP4vnWniWj8MIhUJU53LwSAM8DeJdONKDdkuiOd52aAL
\nVgn7nLo88rVWKhJwVc4tu/rNgZLcR3bP4+kL6zand0KQnMLyOzNA2Ys26aa5udH1\nqWl0WTt9WEm/
h10ndC1knOMectrvsG17b38y5sMCgYEA54NiRGGz8oCPW6GN/FZA
\nKEXAMPLE5tw34GEH3Uxlc9n3CejDaQmczOATwX4nIwRZDEqWyYZcS0btg1jhGiBD\nYEXAMPLEkc8Z71L/
agZEAaVCEog9FqfSqwB
+XTfoKh8qur74X1yCu9p6gof1q6k9\neEXAMPLEchJcNNOg4ETIfMkCgYBdVORRhE4mqvWpOdzA7v66FdEz2YSkjAXKk
\naEXAMPLE8Z/8yBSmuBv1Qv03XA12my462uB92uzzGAuW
+1yBc2Kn1sXqYTy0y1z0\ngEXAMPLEBogjw4MqHKL1bPKMHyQU8/
q24PaYgzHPzy13wlH6pTYf1XqlHdE2D6Vv\nyEXAMPLEgQC3i/
kVVhky/2XRwRVlC7JO2Bg3QGTx38hpmDa5IuofKANjA+Wa3/zy\nbEXAMPLE6ytQgD9GN/YtBq+uhO
+2ZkvXPL+CWRi0ZRXpPwYDBBFU9Cw0AuWWGlL8\nwEXAMPLExMlcysRgcWB9RNgf3AuOpFd2i6XT/
riNsvvkpmJ+VooU8g==\n-----END RSA PRIVATE KEY-----\n",
        "protocol": "ssh",
        "instanceName": "WordPress_Multisite-1",
        "username": "bitnami",
        "hostKeys": [
            {
                "algorithm": "ssh-rsa",
                "publicKey":
 "AEXAMPLEaC1yc2EAAAADAQABAAABAQCoeR9ieZTjQ3pXCHczuAYZFjlF7t
+uBkXuqeGMRex78pCvmS+DiEXAMPLEuJ1Q8dcKhrQL4HpXbD9dosVCTaJnJwb4MQqsuSVFdHFzy3guP
+BKclWqtxJEXAMPLEsBGqZZlrIv6a9bTA0TCplZ8AD+hSRTaSXXqg6FT
+Qf16IktH0XlMs7xIEXAMPLEmNtjCpzZiGXDHzytoMvUgwa8uHPp44Og36EUu4VqQxoUHPJKoXvcQizyk3K8ym0hP0Tp
Ot6y9HwvykEXAMPLEAfbKjbR42+u6+OSlkr4d339q2U1sTDytJhhs8HUel1wTfGRfp",
                "witnessedAt": 1570744377.699,
                "fingerprintSHA1": "SHA1:GEXAMPLEMoYgUg0ucadqU9Bt3Lk",
                "fingerprintSHA256": "SHA256:IEXAMPLEcB5vgxnAUoJawbdZ
+MwELhIp6FUxuwq/LIU"
            },
            {
                "algorithm": "ssh-ed25519",
                "publicKey":
 "AEXAMPLEaC1lZDI1NTE5AAAAIC1gwGPDfGaONxEXAMPLEJX3UNap781QxHQmn8nzlrUv",
                "witnessedAt": 1570744377.697,
                "fingerprintSHA1": "SHA1:VEXAMPLE5ReqSmTgv03sSUw9toU",
                "fingerprintSHA256": "SHA256:0EXAMPLEdE6tI95k3TJpG
+qhJbAoknB0yz9nAEaDt3A"
            },
            {
                "algorithm": "ecdsa-sha2-nistp256",
                "publicKey":
 "AEXAMPLEZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABEXAMPLE9B4mZy8YSsZW7cixCDq5yHSAAxjJkDo5
+EnKlDCsYtUkxxEXAMPLE6VOWL2z63RTKa2AUPgd8irjxWI=",
```

```
                "witnessedAt": 1570744377.707,
                "fingerprintSHA1": "SHA1:UEXAMPLEOYCfXsCf2G6tDg+7YG0",
                "fingerprintSHA256": "SHA256:wEXAMPLEQ9a/
iEXAMPLEhRufm6U9vFU4cpkMPHnBsNA"
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte GetInstanceAccessDetails en la Referencia de comandos de la AWS CLI.

`get-instance-metric-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-instance-metric-data`.

AWS CLI

Para obtener datos de métricas de una instancia

El siguiente ejemplo de `get-instance-metric-data` devuelve el porcentaje medio de `CPUUtilization` cada `7200` segundos (2 horas) entre `1571342400` y `1571428800` para la instancia `MEAN-1`.

Se recomienda utilizar un conversor de tiempo unix para identificar las horas de inicio y finalización.

```
aws lightsail get-instance-metric-data \
    --instance-name MEAN-1 \
    --metric-name CPUUtilization \
    --period 7200 \
    --start-time 1571342400 \
    --end-time 1571428800 \
    --unit Percent \
    --statistics Average
```

Salida:

```
{
    "metricName": "CPUUtilization",
    "metricData": [
        {
```

```
            "average": 0.26113718770120725,
            "timestamp": 1571342400.0,
            "unit": "Percent"
        },
        {
            "average": 0.26861268928111953,
            "timestamp": 1571392800.0,
            "unit": "Percent"
        },
        {
            "average": 0.28187475104748777,
            "timestamp": 1571378400.0,
            "unit": "Percent"
        },
        {
            "average": 0.2651936960458352,
            "timestamp": 1571421600.0,
            "unit": "Percent"
        },
        {
            "average": 0.2561856213712188,
            "timestamp": 1571371200.0,
            "unit": "Percent"
        },
        {
            "average": 0.3021383254607764,
            "timestamp": 1571356800.0,
            "unit": "Percent"
        },
        {
            "average": 0.2618381649223539,
            "timestamp": 1571407200.0,
            "unit": "Percent"
        },
        {
            "average": 0.26331929394825787,
            "timestamp": 1571400000.0,
            "unit": "Percent"
        },
        {
            "average": 0.2576348407007818,
            "timestamp": 1571385600.0,
            "unit": "Percent"
        },
```

```
        {
            "average": 0.2513008454658378,
            "timestamp": 1571364000.0,
            "unit": "Percent"
        },
        {
            "average": 0.26329974562758346,
            "timestamp": 1571414400.0,
            "unit": "Percent"
        },
        {
            "average": 0.2667092536656445,
            "timestamp": 1571349600.0,
            "unit": "Percent"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetInstanceMetricData en la Referencia de comandos de la AWS CLI.

`get-instance-port-states`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-instance-port-states`.

AWS CLI

Para obtener información de firewall de una instancia

El siguiente ejemplo de `get-instance-port-states` devuelve los puertos de firewall configurados para la instancia `MEAN-1`.

```
aws lightsail get-instance-port-states \
    --instance-name MEAN-1
```

Salida:

```
{
    "portStates": [
        {
            "fromPort": 80,
            "toPort": 80,
```

```
            "protocol": "tcp",
            "state": "open"
        },
        {
            "fromPort": 22,
            "toPort": 22,
            "protocol": "tcp",
            "state": "open"
        },
        {
            "fromPort": 443,
            "toPort": 443,
            "protocol": "tcp",
            "state": "open"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetInstancePortStates en la Referencia de comandos de la AWS CLI.

`get-instance-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-instance-snapshot`.

AWS CLI

Para obtener información sobre una instantánea de instancia especificada

En el ejemplo siguiente de `get-instance-snapshot`, se muestran detalles sobre la instantánea de instancia especificada.

```
aws lightsail get-instance-snapshot \
    --instance-snapshot-name MEAN-1-1571419854
```

Salida:

```
{
    "instanceSnapshot": {
        "name": "MEAN-1-1571419854",
        "arn": "arn:aws:lightsail:us-west-2:111122223333:InstanceSnapshot/
ac54700c-48a8-40fd-b065-2EXAMPLEac8f",
```

```
        "supportCode": "6EXAMPLE3362/ami-0EXAMPLE67a73020d",
        "createdAt": 1571419891.927,
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "resourceType": "InstanceSnapshot",
        "tags": [],
        "state": "available",
        "fromAttachedDisks": [],
        "fromInstanceName": "MEAN-1",
        "fromInstanceArn": "arn:aws:lightsail:us-west-2:111122223333:Instance/
bd470fc5-a68b-44c5-8dbc-8EXAMPLEbada",
        "fromBlueprintId": "mean",
        "fromBundleId": "medium_3_0",
        "isFromAutoSnapshot": false,
        "sizeInGb": 80
    }
}
```

- Para obtener información sobre la API, consulte GetInstanceSnapshot en la Referencia de comandos de la AWS CLI.

`get-instance-snapshots`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-instance-snapshots`.

AWS CLI

Para obtener información sobre todas las instantáneas de instancia

En el siguiente ejemplo de `get-instance-snapshots`, se muestran detalles sobre todas las instantáneas de instancia en la región de AWS configurada.

```
aws lightsail get-instance-snapshots
```

Salida:

```
{
    "instanceSnapshots": [
        {
            "name": "MEAN-1-1571421498",
```

```
            "arn": "arn:aws:lightsail:us-west-2:111122223333:InstanceSnapshot/
a20e6ebe-b0ee-4ae4-a750-3EXAMPLEcb0c",
            "supportCode": "6EXAMPLE3362/ami-0EXAMPLEe33cabfa1",
            "createdAt": 1571421527.755,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "resourceType": "InstanceSnapshot",
            "tags": [
                {
                    "key": "no_delete"
                }
            ],
            "state": "available",
            "fromAttachedDisks": [],
            "fromInstanceName": "MEAN-1",
            "fromInstanceArn": "arn:aws:lightsail:us-
west-2:111122223333:Instance/1761aa0a-6038-4f25-8b94-2EXAMPLE19fd",
            "fromBlueprintId": "wordpress",
            "fromBundleId": "micro_3_0",
            "isFromAutoSnapshot": false,
            "sizeInGb": 40
        },
        {
            "name": "MEAN-1-1571419854",
            "arn": "arn:aws:lightsail:us-west-2:111122223333:InstanceSnapshot/
ac54700c-48a8-40fd-b065-2EXAMPLEac8f",
            "supportCode": "6EXAMPLE3362/ami-0EXAMPLE67a73020d",
            "createdAt": 1571419891.927,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "resourceType": "InstanceSnapshot",
            "tags": [],
            "state": "available",
            "fromAttachedDisks": [],
            "fromInstanceName": "MEAN-1",
            "fromInstanceArn": "arn:aws:lightsail:us-west-2:111122223333:Instance/
bd470fc5-a68b-44c5-8dbc-8EXAMPLEbada",
            "fromBlueprintId": "mean",
            "fromBundleId": "medium_3_0",
            "isFromAutoSnapshot": false,
```

```
            "sizeInGb": 80
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetInstanceSnapshots en la Referencia de comandos de la AWS CLI.

`get-instance-state`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-instance-state`.

AWS CLI

Para obtener información sobre el estado de una instancia

En el siguiente ejemplo de `get-instance-state`, se devuelve el estado de la instancia especificada.

```
aws lightsail get-instance-state \
    --instance-name MEAN-1
```

Salida:

```
{
    "state": {
        "code": 16,
        "name": "running"
    }
}
```

- Para obtener información sobre la API, consulte GetInstanceState en la Referencia de comandos de la AWS CLI.

`get-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-instance`.

AWS CLI

Para obtener información sobre una instancia

En el siguiente ejemplo de `get-instance`, se muestran detalles sobre la instancia `MEAN-1`.

```
aws lightsail get-instance \
    --instance-name MEAN-1
```

Salida:

```
{
    "instance": {
        "name": "MEAN-1",
        "arn": "arn:aws:lightsail:us-west-2:111122223333:Instance/bd470fc5-
a68b-44c5-8dbc-EXAMPLE4bada",
        "supportCode": "6EXAMPLE3362/i-05EXAMPLE407c97d3",
        "createdAt": 1570635023.124,
        "location": {
            "availabilityZone": "us-west-2a",
            "regionName": "us-west-2"
        },
        "resourceType": "Instance",
        "tags": [],
        "blueprintId": "mean",
        "blueprintName": "MEAN",
        "bundleId": "medium_3_0",
        "isStaticIp": false,
        "privateIpAddress": "192.0.2.0",
        "publicIpAddress": "192.0.2.0",
        "hardware": {
            "cpuCount": 2,
            "disks": [
                {
                    "createdAt": 1570635023.124,
                    "sizeInGb": 80,
                    "isSystemDisk": true,
                    "iops": 240,
                    "path": "/dev/xvda",
                    "attachedTo": "MEAN-1",
                    "attachmentState": "attached"
                }
            ],
            "ramSizeInGb": 4.0
        },
        "networking": {
            "monthlyTransfer": {
```

```
                "gbPerMonthAllocated": 4096
            },
            "ports": [
                {
                    "fromPort": 80,
                    "toPort": 80,
                    "protocol": "tcp",
                    "accessFrom": "Anywhere (0.0.0.0/0)",
                    "accessType": "public",
                    "commonName": "",
                    "accessDirection": "inbound"
                },
                {
                    "fromPort": 22,
                    "toPort": 22,
                    "protocol": "tcp",
                    "accessFrom": "Anywhere (0.0.0.0/0)",
                    "accessType": "public",
                    "commonName": "",
                    "accessDirection": "inbound"
                },
                {
                    "fromPort": 443,
                    "toPort": 443,
                    "protocol": "tcp",
                    "accessFrom": "Anywhere (0.0.0.0/0)",
                    "accessType": "public",
                    "commonName": "",
                    "accessDirection": "inbound"
                }
            ]
        },
        "state": {
            "code": 16,
            "name": "running"
        },
        "username": "bitnami",
        "sshKeyName": "MyKey"
    }
}
```


- Para obtener información sobre la API, consulte GetInstance en la Referencia de comandos de la AWS CLI.

`get-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-instances`.

AWS CLI

Para obtener información sobre todas las instancias

En el siguiente ejemplo de `get-instances`, se muestran detalles sobre todas las instancias en la región de AWS configurada.

```
aws lightsail get-instances
```

Salida:

```
{
    "instances": [
        {
            "name": "Windows_Server_2022-1",
            "arn": "arn:aws:lightsail:us-
west-2:111122223333:Instance/0f44fbb9-8f55-4e47-a25e-EXAMPLE04763",
            "supportCode": "62EXAMPLE362/i-0bEXAMPLE71a686b9",
            "createdAt": 1571332358.665,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "resourceType": "Instance",
            "tags": [],
            "blueprintId": "windows_server_2022",
            "blueprintName": "Windows Server 2022",
            "bundleId": "large_win_3_0",
            "isStaticIp": false,
            "privateIpAddress": "192.0.2.0",
            "publicIpAddress": "192.0.2.0",
            "hardware": {
                "cpuCount": 1,
                "disks": [
                    {
                        "createdAt": 1571332358.665,
                        "sizeInGb": 160,
                        "isSystemDisk": true,
                        "iops": 180,
```

```
                        "path": "/dev/sda1",
                        "attachedTo": "Windows_Server_2022-1",
                        "attachmentState": "attached"
                    },
                    {
                        "name": "my-disk-for-windows-server",
                        "arn": "arn:aws:lightsail:us-
west-2:111122223333:Disk/4123a81c-484c-49ea-afea-5EXAMPLEda87",
                        "supportCode": "6EXAMPLE3362/vol-0EXAMPLEb2b99ca3d",
                        "createdAt": 1571355063.494,
                        "location": {
                            "availabilityZone": "us-west-2a",
                            "regionName": "us-west-2"
                        },
                        "resourceType": "Disk",
                        "tags": [],
                        "sizeInGb": 128,
                        "isSystemDisk": false,
                        "iops": 384,
                        "path": "/dev/xvdf",
                        "state": "in-use",
                        "attachedTo": "Windows_Server_2022-1",
                        "isAttached": true,
                        "attachmentState": "attached"
                    }
                ],
                "ramSizeInGb": 8.0
            },
            "networking": {
                "monthlyTransfer": {
                    "gbPerMonthAllocated": 3072
                },
                "ports": [
                    {
                        "fromPort": 80,
                        "toPort": 80,
                        "protocol": "tcp",
                        "accessFrom": "Anywhere (0.0.0.0/0)",
                        "accessType": "public",
                        "commonName": "",
                        "accessDirection": "inbound"
                    },
                    {
                        "fromPort": 22,
```

```
                        "toPort": 22,
                        "protocol": "tcp",
                        "accessFrom": "Anywhere (0.0.0.0/0)",
                        "accessType": "public",
                        "commonName": "",
                        "accessDirection": "inbound"
                    },
                    {
                        "fromPort": 3389,
                        "toPort": 3389,
                        "protocol": "tcp",
                        "accessFrom": "Anywhere (0.0.0.0/0)",
                        "accessType": "public",
                        "commonName": "",
                        "accessDirection": "inbound"
                    }
                ]
            },
            "state": {
                "code": 16,
                "name": "running"
            },
            "username": "Administrator",
            "sshKeyName": "LightsailDefaultKeyPair"
        },
        {
            "name": "MEAN-1",
            "arn": "arn:aws:lightsail:us-west-2:111122223333:Instance/bd470fc5-
a68b-44c5-8dbc-8EXAMPLEbada",
            "supportCode": "6EXAMPLE3362/i-0EXAMPLEa407c97d3",
            "createdAt": 1570635023.124,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "resourceType": "Instance",
            "tags": [],
            "blueprintId": "mean",
            "blueprintName": "MEAN",
            "bundleId": "medium_3_0",
            "isStaticIp": false,
            "privateIpAddress": "192.0.2.0",
            "publicIpAddress": "192.0.2.0",
            "hardware": {
```

```
                "cpuCount": 2,
                "disks": [
                    {
                        "name": "Disk-1",
                        "arn": "arn:aws:lightsail:us-west-2:111122223333:Disk/
c21cfb0a-07f2-44ae-9a23-bEXAMPLE8096",
                        "supportCode": "6EXAMPLE3362/vol-0EXAMPLEf2f88b32f",
                        "createdAt": 1566585439.587,
                        "location": {
                            "availabilityZone": "us-west-2a",
                            "regionName": "us-west-2"
                        },
                        "resourceType": "Disk",
                        "tags": [
                            {
                                "key": "test"
                            }
                        ],
                        "sizeInGb": 8,
                        "isSystemDisk": false,
                        "iops": 240,
                        "path": "/dev/xvdf",
                        "state": "in-use",
                        "attachedTo": "MEAN-1",
                        "isAttached": true,
                        "attachmentState": "attached"
                    },
                    {
                        "createdAt": 1570635023.124,
                        "sizeInGb": 80,
                        "isSystemDisk": true,
                        "iops": 240,
                        "path": "/dev/sda1",
                        "attachedTo": "MEAN-1",
                        "attachmentState": "attached"
                    }
                ],
                "ramSizeInGb": 4.0
            },
            "networking": {
                "monthlyTransfer": {
                    "gbPerMonthAllocated": 4096
                },
                "ports": [
```

```
                    {
                        "fromPort": 80,
                        "toPort": 80,
                        "protocol": "tcp",
                        "accessFrom": "Anywhere (0.0.0.0/0)",
                        "accessType": "public",
                        "commonName": "",
                        "accessDirection": "inbound"
                    },
                    {
                        "fromPort": 22,
                        "toPort": 22,
                        "protocol": "tcp",
                        "accessFrom": "Anywhere (0.0.0.0/0)",
                        "accessType": "public",
                        "commonName": "",
                        "accessDirection": "inbound"
                    },
                    {
                        "fromPort": 443,
                        "toPort": 443,
                        "protocol": "tcp",
                        "accessFrom": "Anywhere (0.0.0.0/0)",
                        "accessType": "public",
                        "commonName": "",
                        "accessDirection": "inbound"
                    }
                ]
            },
            "state": {
                "code": 16,
                "name": "running"
            },
            "username": "bitnami",
            "sshKeyName": "MyTestKey"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetInstances en la Referencia de comandos de la AWS CLI.

get-key-pair

En el siguiente ejemplo de código, se muestra cómo utilizar `get-key-pair`.

AWS CLI

Para obtener información sobre un par de claves

En el siguiente ejemplo de `get-key-pair`, se muestran detalles sobre el par de claves especificado.

```
aws lightsail get-key-pair \
    --key-pair-name MyKey1
```

Salida:

```
{
    "keyPair": {
        "name": "MyKey1",
        "arn": "arn:aws:lightsail:us-
west-2:111122223333:KeyPair/19a4efdf-3054-43d6-91fd-eEXAMPLE21bf",
        "supportCode": "6EXAMPLE3362/MyKey1",
        "createdAt": 1571255026.975,
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "resourceType": "KeyPair",
        "tags": [],
        "fingerprint": "00:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff:gg:hh:ii:jj"
    }
}
```

- Para obtener información sobre la API, consulte GetKeyPair en la Referencia de comandos de la AWS CLI.

get-key-pairs

En el siguiente ejemplo de código, se muestra cómo utilizar `get-key-pairs`.

AWS CLI

Para obtener información sobre todos los pares de claves

En el siguiente ejemplo de `get-key-pairs`, se muestran detalles sobre todos los pares de claves de la región de AWS configurada.

```
aws lightsail get-key-pairs
```

Salida:

```
{
    "keyPairs": [
        {
            "name": "MyKey1",
            "arn": "arn:aws:lightsail:us-
west-2:111122223333:KeyPair/19a4efdf-3054-43d6-91fd-eEXAMPLE21bf",
            "supportCode": "6EXAMPLE3362/MyKey1",
            "createdAt": 1571255026.975,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "resourceType": "KeyPair",
            "tags": [],
            "fingerprint":
 "00:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff:gg:hh:ii:jj"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetKeyPairs en la Referencia de comandos de la AWS CLI.

`get-load-balancer-tls-certificates`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-load-balancer-tls-certificates`.

AWS CLI

Para obtener información sobre certificados TLS para un equilibrador de carga

En el siguiente ejemplo de `get-load-balancer-tls-certificates`, se muestran detalles sobre los certificados TLS para el equilibrador de carga especificado.

```
aws lightsail get-load-balancer-tls-certificates \
    --load-balancer-name LoadBalancer-1
```

Salida:

```
{
    "tlsCertificates": [
        {
            "name": "example-com",
            "arn": "arn:aws:lightsail:us-
west-2:111122223333:LoadBalancerTlsCertificate/d7bf4643-6a02-4cd4-b3c4-
fEXAMPLE9b4d",
            "supportCode": "6EXAMPLE3362/arn:aws:acm:us-
west-2:333322221111:certificate/9af8e32c-a54e-4a67-8c63-cEXAMPLEb314",
            "createdAt": 1571678025.3,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "resourceType": "LoadBalancerTlsCertificate",
            "loadBalancerName": "LoadBalancer-1",
            "isAttached": false,
            "status": "ISSUED",
            "domainName": "example.com",
            "domainValidationRecords": [
                {
                    "name": "_dEXAMPLE4ede046a0319eb44a4eb3cbc.example.com.",
                    "type": "CNAME",
                    "value": "_bEXAMPLE0899fb7b6bf79d9741d1a383.hkvuiqjoua.acm-
validations.aws.",
                    "validationStatus": "SUCCESS",
                    "domainName": "example.com"
                }
            ],
            "issuedAt": 1571678070.0,
            "issuer": "Amazon",
            "keyAlgorithm": "RSA-2048",
            "notAfter": 1605960000.0,
            "notBefore": 1571616000.0,
            "serial": "00:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff",
```

```
            "signatureAlgorithm": "SHA256WITHRSA",
            "subject": "CN=example.com",
            "subjectAlternativeNames": [
                "example.com"
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetLoadBalancerTlsCertificates en la Referencia de comandos de la AWS CLI.

`get-load-balancer`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-load-balancer`.

AWS CLI

Para obtener información sobre un equilibrador de carga

En el siguiente ejemplo de `get-load-balancer`, se muestran detalles sobre el equilibrador de carga especificado.

```
aws lightsail get-load-balancer \
    --load-balancer-name LoadBalancer-1
```

Salida:

```
{
    "loadBalancer": {
        "name": "LoadBalancer-1",
        "arn": "arn:aws:lightsail:us-
west-2:111122223333:LoadBalancer/40486b2b-1ad0-4152-83e4-cEXAMPLE6f4b",
        "supportCode": "6EXAMPLE3362/arn:aws:elasticloadbalancing:us-
west-2:333322221111:loadbalancer/app/
bEXAMPLE128cb59d86f946a9395dd304/1EXAMPLE8dd9d77e",
        "createdAt": 1571677906.723,
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "resourceType": "LoadBalancer",
```

```
        "tags": [],
        "dnsName": "bEXAMPLE128cb59d86f946a9395dd304-1486911371.us-
west-2.elb.amazonaws.com",
        "state": "active",
        "protocol": "HTTP",
        "publicPorts": [
            80
        ],
        "healthCheckPath": "/",
        "instancePort": 80,
        "instanceHealthSummary": [
            {
                "instanceName": "MEAN-3",
                "instanceHealth": "healthy"
            },
            {
                "instanceName": "MEAN-1",
                "instanceHealth": "healthy"
            },
            {
                "instanceName": "MEAN-2",
                "instanceHealth": "healthy"
            }
        ],
        "tlsCertificateSummaries": [
            {
                "name": "example-com",
                "isAttached": false
            }
        ],
        "configurationOptions": {
            "SessionStickinessEnabled": "false",
            "SessionStickiness_LB_CookieDurationSeconds": "86400"
        }
    }
}
```

- Para obtener información sobre la API, consulte GetLoadBalancer en la Referencia de comandos de la AWS CLI.

`get-load-balancers`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-load-balancers`.

AWS CLI

Para obtener información sobre todos los equilibradores de carga

En el siguiente ejemplo de `get-load-balancers`, se muestran detalles sobre todos los equilibradores de carga de la región de AWS configurada.

```
aws lightsail get-load-balancers
```

Salida:

```
{
    "loadBalancers": [
        {
            "name": "LoadBalancer-1",
            "arn": "arn:aws:lightsail:us-
west-2:111122223333:LoadBalancer/40486b2b-1ad0-4152-83e4-cEXAMPLE6f4b",
            "supportCode": "6EXAMPLE3362/arn:aws:elasticloadbalancing:us-
west-2:333322221111:loadbalancer/app/
bEXAMPLE128cb59d86f946a9395dd304/1EXAMPLE8dd9d77e",
            "createdAt": 1571677906.723,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "resourceType": "LoadBalancer",
            "tags": [],
            "dnsName": "bEXAMPLE128cb59d86f946a9395dd304-1486911371.us-
west-2.elb.amazonaws.com",
            "state": "active",
            "protocol": "HTTP",
            "publicPorts": [
                80
            ],
            "healthCheckPath": "/",
            "instancePort": 80,
            "instanceHealthSummary": [
                {
                    "instanceName": "MEAN-3",
                    "instanceHealth": "healthy"
                },
                {
                    "instanceName": "MEAN-1",
```

```
                    "instanceHealth": "healthy"
                },
                {
                    "instanceName": "MEAN-2",
                    "instanceHealth": "healthy"
                }
            ],
            "tlsCertificateSummaries": [
                {
                    "name": "example-com",
                    "isAttached": false
                }
            ],
            "configurationOptions": {
                "SessionStickinessEnabled": "false",
                "SessionStickiness_LB_CookieDurationSeconds": "86400"
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetLoadBalancers en la Referencia de comandos de la AWS CLI.

`get-operation`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-operation`.

AWS CLI

Para obtener información sobre una operación

En el siguiente ejemplo de `get-operation`, se muestran detalles sobre la operación especificada.

```
aws lightsail get-operation \
    --operation-id e5700e8a-daf2-4b49-bc01-3EXAMPLE910a
```

Salida:

```
{
    "operation": {
```

```
        "id": "e5700e8a-daf2-4b49-bc01-3EXAMPLE910a",
        "resourceName": "Instance-1",
        "resourceType": "Instance",
        "createdAt": 1571679872.404,
        "location": {
            "availabilityZone": "us-west-2a",
            "regionName": "us-west-2"
        },
        "isTerminal": true,
        "operationType": "CreateInstance",
        "status": "Succeeded",
        "statusChangedAt": 1571679890.304
    }
}
```

- Para obtener información sobre la API, consulte GetOperation en la Referencia de comandos de la AWS CLI.

`get-operations-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-operations-for-resource`.

AWS CLI

Para obtener todas las operaciones de un recurso

En el siguiente ejemplo de `get-operations-for-resource`, se muestran detalles sobre todas operaciones del recurso especificado.

```
aws lightsail get-operations-for-resource \
    --resource-name LoadBalancer-1
```

Salida:

```
{
    "operations": [
        {
            "id": "e2973046-43f8-4252-a4b4-9EXAMPLE69ce",
            "resourceName": "LoadBalancer-1",
            "resourceType": "LoadBalancer",
            "createdAt": 1571678786.071,
            "location": {
```

```
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "MEAN-1",
            "operationType": "DetachInstancesFromLoadBalancer",
            "status": "Succeeded",
            "statusChangedAt": 1571679087.57
        },
        {
            "id": "2d742a18-0e7f-48c8-9705-3EXAMPLEf98a",
            "resourceName": "LoadBalancer-1",
            "resourceType": "LoadBalancer",
            "createdAt": 1571678782.784,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "MEAN-1",
            "operationType": "AttachInstancesToLoadBalancer",
            "status": "Succeeded",
            "statusChangedAt": 1571678798.465
        },
        {
            "id": "6c700fcc-4246-40ab-952b-1EXAMPLEdac2",
            "resourceName": "LoadBalancer-1",
            "resourceType": "LoadBalancer",
            "createdAt": 1571678775.297,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "MEAN-3",
            "operationType": "AttachInstancesToLoadBalancer",
            "status": "Succeeded",
            "statusChangedAt": 1571678842.806
        },
        ...
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetOperationsForResource en la Referencia de comandos de la AWS CLI.

`get-operations`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-operations`.

AWS CLI

Para obtener información sobre todas las operaciones

En el siguiente ejemplo de `get-operations`, se muestran detalles sobre todas las operaciones de la región de AWS configurada.

```
aws lightsail get-operations
```

Salida:

```
{
    "operations": [
        {
            "id": "e5700e8a-daf2-4b49-bc01-3EXAMPLE910a",
            "resourceName": "Instance-1",
            "resourceType": "Instance",
            "createdAt": 1571679872.404,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationType": "CreateInstance",
            "status": "Succeeded",
            "statusChangedAt": 1571679890.304
        },
        {
            "id": "701a3339-930e-4914-a9f9-7EXAMPLE68d7",
            "resourceName": "WordPress-1",
            "resourceType": "Instance",
            "createdAt": 1571678786.072,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
```

```
            },
            "isTerminal": true,
            "operationDetails": "LoadBalancer-1",
            "operationType": "DetachInstancesFromLoadBalancer",
            "status": "Succeeded",
            "statusChangedAt": 1571679086.399
        },
        {
            "id": "e2973046-43f8-4252-a4b4-9EXAMPLE69ce",
            "resourceName": "LoadBalancer-1",
            "resourceType": "LoadBalancer",
            "createdAt": 1571678786.071,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "WordPress-1",
            "operationType": "DetachInstancesFromLoadBalancer",
            "status": "Succeeded",
            "statusChangedAt": 1571679087.57
        },
        ...
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetOperations en la Referencia de comandos de la AWS CLI.

`get-regions`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-regions`.

AWS CLI

Para obtener todas las regiones de AWS para Amazon Lightsail

En el siguiente ejemplo de `get-regions`, se muestran detalles sobre todas regiones de AWS para Amazon Lightsail.

```
aws lightsail get-regions
```

Salida:


```
{
    "regions": [
        {
            "continentCode": "NA",
            "description": "This region is recommended to serve users in the eastern
 United States",
            "displayName": "Virginia",
            "name": "us-east-1",
            "availabilityZones": [],
            "relationalDatabaseAvailabilityZones": []
        },
        {
            "continentCode": "NA",
            "description": "This region is recommended to serve users in the eastern
 United States",
            "displayName": "Ohio",
            "name": "us-east-2",
            "availabilityZones": [],
            "relationalDatabaseAvailabilityZones": []
        },
        {
            "continentCode": "NA",
            "description": "This region is recommended to serve users in the
 northwestern United States, Alaska, and western Canada",
            "displayName": "Oregon",
            "name": "us-west-2",
            "availabilityZones": [],
            "relationalDatabaseAvailabilityZones": []
        },
        ...
        }
    ]
}
```


- Para obtener información sobre la API, consulte GetRegions en la Referencia de comandos de la AWS CLI.

get-relational-database-blueprints

En el siguiente ejemplo de código, se muestra cómo utilizar `get-relational-database-blueprints`.

AWS CLI

Para obtener los esquemas de nuevas bases de datos relacionales

En el siguiente ejemplo de `get-relational-database-blueprints`, se muestran detalles sobre todos los esquemas de bases de datos relacionales disponibles que se pueden utilizar para crear nuevas bases de datos relacionales en Amazon Lightsail.

```
aws lightsail get-relational-database-blueprints
```

Salida:

```
{
    "blueprints": [
        {
            "blueprintId": "mysql_5_6",
            "engine": "mysql",
            "engineVersion": "5.6.44",
            "engineDescription": "MySQL Community Edition",
            "engineVersionDescription": "MySQL 5.6.44",
            "isEngineDefault": false
        },
        {
            "blueprintId": "mysql_5_7",
            "engine": "mysql",
            "engineVersion": "5.7.26",
            "engineDescription": "MySQL Community Edition",
            "engineVersionDescription": "MySQL 5.7.26",
            "isEngineDefault": true
        },
        {
            "blueprintId": "mysql_8_0",
            "engine": "mysql",
            "engineVersion": "8.0.16",
            "engineDescription": "MySQL Community Edition",
            "engineVersionDescription": "MySQL 8.0.16",
            "isEngineDefault": false
        },
```

```
        {
            "blueprintId": "postgres_9_6",
            "engine": "postgres",
            "engineVersion": "9.6.15",
            "engineDescription": "PostgreSQL",
            "engineVersionDescription": "PostgreSQL 9.6.15-R1",
            "isEngineDefault": false
        },
        {
            "blueprintId": "postgres_10",
            "engine": "postgres",
            "engineVersion": "10.10",
            "engineDescription": "PostgreSQL",
            "engineVersionDescription": "PostgreSQL 10.10-R1",
            "isEngineDefault": false
        },
        {
            "blueprintId": "postgres_11",
            "engine": "postgres",
            "engineVersion": "11.5",
            "engineDescription": "PostgreSQL",
            "engineVersionDescription": "PostgreSQL 11.5-R1",
            "isEngineDefault": true
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetRelationalDatabaseBlueprints en la Referencia de comandos de la AWS CLI.

`get-relational-database-bundles`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-relational-database-bundles`.

AWS CLI

Para obtener las agrupaciones de nuevas bases de datos relacionales

En el siguiente ejemplo de `get-relational-database-bundles`, se muestran detalles sobre todas las agrupaciones de bases de datos relacionales disponibles que se pueden utilizar para crear nuevas bases de datos relacionales en Amazon Lightsail. Tenga en cuenta que la

respuesta no incluye las agrupaciones inactivas porque la marca `--include-inactive` no está especificada en el comando. No puede utilizar agrupaciones inactivas para crear nuevas bases de datos relacionales.

```
aws lightsail get-relational-database-bundles
```

Salida:

```
{
    "bundles": [
        {
            "bundleId": "micro_2_0",
            "name": "Micro",
            "price": 15.0,
            "ramSizeInGb": 1.0,
            "diskSizeInGb": 40,
            "transferPerMonthInGb": 100,
            "cpuCount": 2,
            "isEncrypted": true,
            "isActive": true
        },
        {
            "bundleId": "micro_ha_2_0",
            "name": "Micro with High Availability",
            "price": 30.0,
            "ramSizeInGb": 1.0,
            "diskSizeInGb": 40,
            "transferPerMonthInGb": 100,
            "cpuCount": 2,
            "isEncrypted": true,
            "isActive": true
        },
        {
            "bundleId": "small_2_0",
            "name": "Small",
            "price": 30.0,
            "ramSizeInGb": 2.0,
            "diskSizeInGb": 80,
            "transferPerMonthInGb": 100,
            "cpuCount": 2,
            "isEncrypted": true,
            "isActive": true
        },
```

```
        {
            "bundleId": "small_ha_2_0",
            "name": "Small with High Availability",
            "price": 60.0,
            "ramSizeInGb": 2.0,
            "diskSizeInGb": 80,
            "transferPerMonthInGb": 100,
            "cpuCount": 2,
            "isEncrypted": true,
            "isActive": true
        },
        {
            "bundleId": "medium_2_0",
            "name": "Medium",
            "price": 60.0,
            "ramSizeInGb": 4.0,
            "diskSizeInGb": 120,
            "transferPerMonthInGb": 100,
            "cpuCount": 2,
            "isEncrypted": true,
            "isActive": true
        },
        {
            "bundleId": "medium_ha_2_0",
            "name": "Medium with High Availability",
            "price": 120.0,
            "ramSizeInGb": 4.0,
            "diskSizeInGb": 120,
            "transferPerMonthInGb": 100,
            "cpuCount": 2,
            "isEncrypted": true,
            "isActive": true
        },
        {
            "bundleId": "large_2_0",
            "name": "Large",
            "price": 115.0,
            "ramSizeInGb": 8.0,
            "diskSizeInGb": 240,
            "transferPerMonthInGb": 200,
            "cpuCount": 2,
            "isEncrypted": true,
            "isActive": true
        },
```

```
        {
            "bundleId": "large_ha_2_0",
            "name": "Large with High Availability",
            "price": 230.0,
            "ramSizeInGb": 8.0,
            "diskSizeInGb": 240,
            "transferPerMonthInGb": 200,
            "cpuCount": 2,
            "isEncrypted": true,
            "isActive": true
        }
    ]
}
```

Para obtener más información, consulte Creación de una base de datos de Amazon Lightsail en la Guía para desarrolladores de Amazon Lightsail.

- Para obtener información sobre la API, consulte GetRelationalDatabaseBundles en la Referencia de comandos de la AWS CLI.

`get-relational-database-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-relational-database-events`.

AWS CLI

Para obtener los eventos de una base de datos relacional

El siguiente ejemplo de `get-relational-database-events` muestra detalles sobre los eventos de las últimas 17 horas (1020 minutos) para la base de datos relacional especificada.

```
aws lightsail get-relational-database-events \
    --relational-database-name Database-1 \
    --duration-in-minutes 1020
```

Salida:

```
{
    "relationalDatabaseEvents": [
        {
            "resource": "Database-1",
            "createdAt": 1571654146.553,
```

```
            "message": "Backing up Relational Database",
            "eventCategories": [
                "backup"
            ]
        },
        {
            "resource": "Database-1",
            "createdAt": 1571654249.98,
            "message": "Finished Relational Database backup",
            "eventCategories": [
                "backup"
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetRelationalDatabaseEvents en la Referencia de comandos de la AWS CLI.

`get-relational-database-log-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-relational-database-log-events`.

AWS CLI

Para obtener eventos de registro para una base de datos relacional

El siguiente ejemplo de `get-relational-database-log-events` muestra detalles sobre el registro especificado entre `1570733176` y `1571597176` para la base de datos relacional `Database1`. La información devuelta está configurada para empezar desde `head`.

Se recomienda utilizar un conversor de tiempo unix para identificar las horas de inicio y finalización.

```
aws lightsail get-relational-database-log-events \
    --relational-database-name Database1 \
    --log-stream-name error \
    --start-from-head \
    --start-time 1570733176 \
    --end-time 1571597176
```

Salida:


```
{
    "resourceLogEvents": [
        {
            "createdAt": 1570820267.0,
            "message": "2019-10-11 18:57:47 20969 [Warning] IP address '192.0.2.0'
 could not be resolved: Name or service not known"
        },
        {
            "createdAt": 1570860974.0,
            "message": "2019-10-12 06:16:14 20969 [Warning] IP address '8192.0.2.0'
 could not be resolved: Temporary failure in name resolution"
        },
        {
            "createdAt": 1570860977.0,
            "message": "2019-10-12 06:16:17 20969 [Warning] IP address '192.0.2.0'
 could not be resolved: Temporary failure in name resolution"
        },
        {
            "createdAt": 1570860979.0,
            "message": "2019-10-12 06:16:19 20969 [Warning] IP address '192.0.2.0'
 could not be resolved: Temporary failure in name resolution"
        },
        {
            "createdAt": 1570860981.0,
            "message": "2019-10-12 06:16:21 20969 [Warning] IP address '192.0.2.0'
 could not be resolved: Temporary failure in name resolution"
        },
        {
            "createdAt": 1570860982.0,
            "message": "2019-10-12 06:16:22 20969 [Warning] IP address '192.0.2.0'
 could not be resolved: Temporary failure in name resolution"
        },
        {
            "createdAt": 1570860984.0,
            "message": "2019-10-12 06:16:24 20969 [Warning] IP address '192.0.2.0'
 could not be resolved: Temporary failure in name resolution"
        },
        {
            "createdAt": 1570860986.0,
            "message": "2019-10-12 06:16:26 20969 [Warning] IP address '192.0.2.0'
 could not be resolved: Temporary failure in name resolution"
        },
```

```
            ...
            }
        ],
        "nextBackwardToken":
 "eEXAMPLEZXJUZXh0IjoiZnRWb3F3cUpRSlQ5NndMYThxelRUZlFhR3J6c2dKWEEvM2kvajZMZzVVVWpqRDN0YjFXTj
        "nextForwardToken":
 "eEXAMPLEZXJUZXh0IjoiT09Lb0Z6ZFRJbHhaNEQ5N2tPbkkwRmwwNUxPZjFTbFFwUklQbzlSaWgvMWVXbEk4aG56VH
}
```

- Para obtener información sobre la API, consulte GetRelationalDatabaseLogEvents en la Referencia de comandos de la AWS CLI.

`get-relational-database-log-streams`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-relational-database-log-streams`.

AWS CLI

Para obtener los flujos de registro para una base de datos relacional

En el siguiente ejemplo de `get-relational-database-log-streams`, se devuelven todos los flujos de registro disponibles para la base de datos relacional especificada.

```
aws lightsail get-relational-database-log-streams \
--relational-database-name Database1
```

Salida:

```
{
    "logStreams": [
        "audit",
        "error",
        "general",
        "slowquery"
    ]
}
```

- Para obtener información sobre la API, consulte GetRelationalDatabaseLogStreams en la Referencia de comandos de la AWS CLI.

get-relational-database-master-user-password

En el siguiente ejemplo de código, se muestra cómo utilizar `get-relational-database-master-user-password`.

AWS CLI

Para obtener la contraseña de usuario maestro de una base de datos relacional

En el siguiente ejemplo de `get-relational-database-master-user-password`, se devuelve información sobre la contraseña del usuario maestro de la base de datos relacional especificada.

```
aws lightsail get-relational-database-master-user-password \
    --relational-database-name Database-1
```

Salida:

```
{
    "masterUserPassword": "VEXAMPLEec.9qvx,_t<)Wkf)kwboM,>2",
    "createdAt": 1571259453.959
}
```

- Para obtener información sobre la API, consulte GetRelationalDatabaseMasterUserPassword en la Referencia de comandos de la AWS CLI.

get-relational-database-metric-data

En el siguiente ejemplo de código, se muestra cómo utilizar `get-relational-database-metric-data`.

AWS CLI

Para obtener datos de métricas de una base de datos relacional

El siguiente ejemplo de `get-relational-database-metric-data` devuelve la suma de recuento de la métrica `DatabaseConnections` durante un período de 24 horas (`86400` segundos) entre `1570733176` y `1571597176` para una base de datos relacional `Database1`.

Se recomienda utilizar un conversor de tiempo unix para identificar las horas de inicio y finalización.

```
aws lightsail get-relational-database-metric-data \
    --relational-database-name Database1 \
    --metric-name DatabaseConnections \
    --period 86400 \
    --start-time 1570733176 \
    --end-time 1571597176 \
    --unit Count \
    --statistics Sum
```

Salida:


```
{
    "metricName": "DatabaseConnections",
    "metricData": [
        {
            "sum": 1.0,
            "timestamp": 1571510760.0,
            "unit": "Count"
        },
        {
            "sum": 1.0,
            "timestamp": 1570733160.0,
            "unit": "Count"
        },
        {
            "sum": 1.0,
            "timestamp": 1570992360.0,
            "unit": "Count"
        },
        {
            "sum": 0.0,
            "timestamp": 1571251560.0,
            "unit": "Count"
        },
        {
            "sum": 721.0,
            "timestamp": 1570819560.0,
            "unit": "Count"
        },
        {
            "sum": 1.0,
            "timestamp": 1571078760.0,
            "unit": "Count"
```

```
        },
        {
            "sum": 2.0,
            "timestamp": 1571337960.0,
            "unit": "Count"
        },
        {
            "sum": 684.0,
            "timestamp": 1570905960.0,
            "unit": "Count"
        },
        {
            "sum": 0.0,
            "timestamp": 1571165160.0,
            "unit": "Count"
        },
        {
            "sum": 1.0,
            "timestamp": 1571424360.0,
            "unit": "Count"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetRelationalDatabaseMetricData en la Referencia de comandos de la AWS CLI.

`get-relational-database-parameters`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-relational-database-parameters`.

AWS CLI

Para obtener parámetros de una base de datos relacional

En el siguiente ejemplo de `get-relational-database-parameters`, se devuelve información sobre todos los parámetros disponibles para la base de datos relacional especificada.

```
aws lightsail get-relational-database-parameters \
    --relational-database-name Database-1
```

Salida:


```
{
    "parameters": [
        {
            "allowedValues": "0,1",
            "applyMethod": "pending-reboot",
            "applyType": "dynamic",
            "dataType": "boolean",
            "description": "Automatically set all granted roles as active after the
 user has authenticated successfully.",
            "isModifiable": true,
            "parameterName": "activate_all_roles_on_login",
            "parameterValue": "0"
        },
        {
            "allowedValues": "0,1",
            "applyMethod": "pending-reboot",
            "applyType": "static",
            "dataType": "boolean",
            "description": "Controls whether user-defined functions that have only
 an xxx symbol for the main function can be loaded",
            "isModifiable": false,
            "parameterName": "allow-suspicious-udfs"
        },
        {
            "allowedValues": "0,1",
            "applyMethod": "pending-reboot",
            "applyType": "dynamic",
            "dataType": "boolean",
            "description": "Sets the autocommit mode",
            "isModifiable": true,
            "parameterName": "autocommit"
        },
        {
            "allowedValues": "0,1",
            "applyMethod": "pending-reboot",
            "applyType": "static",
            "dataType": "boolean",
            "description": "Controls whether the server autogenerates SSL key and
 certificate files in the data directory, if they do not already exist.",
            "isModifiable": false,
            "parameterName": "auto_generate_certs"
        },
```

```
        ...
        }
    ]
}
```

Para obtener más información, consulte Actualización de parámetros de Amazon Lightsail en la Guía para desarrolladores de Lightsail.

- Para obtener información sobre la API, consulte GetRelationalDatabaseParameters en la Referencia de comandos de la AWS CLI.

`get-relational-database-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-relational-database-snapshot`.

AWS CLI

Para obtener información sobre una instantánea de base de datos relacional

El siguiente ejemplo de `get-relational-database-snapshot` muestra detalles sobre una instantánea de base de datos relacional especificada.

```
aws lightsail get-relational-database-snapshot \
    --relational-database-snapshot-name Database-1-1571350042
```

Salida:

```
{
    "relationalDatabaseSnapshot": {
        "name": "Database-1-1571350042",
        "arn": "arn:aws:lightsail:us-
west-2:111122223333:RelationalDatabaseSnapshot/0389bbad-4b85-4c3d-9EXAMPLEaee3643d2",
        "supportCode": "6EXAMPLE3362/ls-8EXAMPLE2ba7ad041451946fafc2ad19cfbd9eb2",
        "createdAt": 1571350046.238,
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "resourceType": "RelationalDatabaseSnapshot",
        "tags": [],
        "engine": "mysql",
```

```
        "engineVersion": "8.0.16",
        "sizeInGb": 40,
        "state": "available",
        "fromRelationalDatabaseName": "Database-1",
        "fromRelationalDatabaseArn": "arn:aws:lightsail:us-
west-2:111122223333:RelationalDatabase/7ea932b1-b85a-4bd5-9b3e-bEXAMPLE8cc4",
        "fromRelationalDatabaseBundleId": "micro_1_0",
        "fromRelationalDatabaseBlueprintId": "mysql_8_0"
    }
}
```

- Para obtener información sobre la API, consulte GetRelationalDatabaseSnapshot en la Referencia de comandos de la AWS CLI.

`get-relational-database-snapshots`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-relational-database-snapshots`.

AWS CLI

Para obtener información sobre todas las instantáneas de base de datos relacional

En el siguiente ejemplo de `get-relational-database-snapshots`, se muestran detalles sobre todas las instantáneas de base de datos relacional de la región de AWS configurada.

```
aws lightsail get-relational-database-snapshots
```

Salida:

```
{
    "relationalDatabaseSnapshots": [
        {
            "name": "Database-1-1571350042",
            "arn": "arn:aws:lightsail:us-
west-2:111122223333:RelationalDatabaseSnapshot/0389bbad-4b85-4c3d-9861-6EXAMPLE43d2",
            "supportCode": "6EXAMPLE3362/
ls-8EXAMPLE2ba7ad041451946fafc2ad19cfbd9eb2",
            "createdAt": 1571350046.238,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
```

```
            },
            "resourceType": "RelationalDatabaseSnapshot",
            "tags": [],
            "engine": "mysql",
            "engineVersion": "8.0.16",
            "sizeInGb": 40,
            "state": "available",
            "fromRelationalDatabaseName": "Database-1",
            "fromRelationalDatabaseArn": "arn:aws:lightsail:us-
west-2:111122223333:RelationalDatabase/7ea932b1-b85a-4bd5-9b3e-bEXAMPLE8cc4",
            "fromRelationalDatabaseBundleId": "micro_1_0",
            "fromRelationalDatabaseBlueprintId": "mysql_8_0"
        },
        {
            "name": "Database1-Console",
            "arn": "arn:aws:lightsail:us-
west-2:111122223333:RelationalDatabaseSnapshot/8b94136e-06ec-4b1a-
a3fb-5EXAMPLEe1e9",
            "supportCode": "6EXAMPLE3362/
ls-9EXAMPLE14b000d34c8d1c432734e137612d5b5c",
            "createdAt": 1571249981.025,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "resourceType": "RelationalDatabaseSnapshot",
            "tags": [
                {
                    "key": "test"
                }
            ],
            "engine": "mysql",
            "engineVersion": "5.6.44",
            "sizeInGb": 40,
            "state": "available",
            "fromRelationalDatabaseName": "Database1",
            "fromRelationalDatabaseArn": "arn:aws:lightsail:us-
west-2:111122223333:RelationalDatabase/a6161cb7-4535-4f16-9dcf-8EXAMPLE3d4e",
            "fromRelationalDatabaseBundleId": "micro_1_0",
            "fromRelationalDatabaseBlueprintId": "mysql_5_6"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetRelationalDatabaseSnapshots en la Referencia de comandos de la AWS CLI.

`get-relational-database`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-relational-database`.

AWS CLI

Para obtener información sobre una base de datos relacional

El siguiente ejemplo de `get-relational-database` muestra detalles sobre la base de datos relacional especificada.

```
aws lightsail get-relational-database \
    --relational-database-name Database-1
```

Salida:

```
{
    "relationalDatabase": {
        "name": "Database-1",
        "arn": "arn:aws:lightsail:us-
west-2:111122223333:RelationalDatabase/7ea932b1-b85a-4bd5-9b3e-bEXAMPLE8cc4",
        "supportCode": "6EXAMPLE3362/ls-9EXAMPLE8ad863723b62cc8901a8aa6e794ae0d2",
        "createdAt": 1571259453.795,
        "location": {
            "availabilityZone": "us-west-2a",
            "regionName": "us-west-2"
        },
        "resourceType": "RelationalDatabase",
        "tags": [],
        "relationalDatabaseBlueprintId": "mysql_8_0",
        "relationalDatabaseBundleId": "micro_1_0",
        "masterDatabaseName": "dbmaster",
        "hardware": {
            "cpuCount": 1,
            "diskSizeInGb": 40,
            "ramSizeInGb": 1.0
        },
        "state": "available",
        "backupRetentionEnabled": false,
```

```
        "pendingModifiedValues": {},
        "engine": "mysql",
        "engineVersion": "8.0.16",
        "masterUsername": "dbmasteruser",
        "parameterApplyStatus": "in-sync",
        "preferredBackupWindow": "10:01-10:31",
        "preferredMaintenanceWindow": "sat:11:14-sat:11:44",
        "publiclyAccessible": true,
        "masterEndpoint": {
            "port": 3306,
            "address": "ls-9EXAMPLE8ad863723b62ccEXAMPLEa6e794ae0d2.czowadgeezqi.us-
west-2.rds.amazonaws.com"
        },
        "pendingMaintenanceActions": []
    }
}
```

- Para obtener información sobre la API, consulte GetRelationalDatabase en la Referencia de comandos de la AWS CLI.

`get-relational-databases`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-relational-databases`.

AWS CLI

Para obtener información sobre todas las bases de datos relacionales

En el siguiente ejemplo de `get-relational-databases`, se muestran detalles sobre todas las bases de datos relacionales de la región de AWS configurada.

```
aws lightsail get-relational-databases
```

Salida:

```
{
    "relationalDatabases": [
        {
            "name": "MySQL",
            "arn": "arn:aws:lightsail:us-
west-2:111122223333:RelationalDatabase/8529020c-3ab9-4d51-92af-5EXAMPLE8979",
```

```
            "supportCode": "6EXAMPLE3362/
ls-3EXAMPLEa995d8c3b06b4501356e5f2f28e1aeba",
            "createdAt": 1554306019.155,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "resourceType": "RelationalDatabase",
            "tags": [],
            "relationalDatabaseBlueprintId": "mysql_8_0",
            "relationalDatabaseBundleId": "micro_1_0",
            "masterDatabaseName": "dbmaster",
            "hardware": {
                "cpuCount": 1,
                "diskSizeInGb": 40,
                "ramSizeInGb": 1.0
            },
            "state": "available",
            "backupRetentionEnabled": true,
            "pendingModifiedValues": {},
            "engine": "mysql",
            "engineVersion": "8.0.15",
            "latestRestorableTime": 1571686200.0,
            "masterUsername": "dbmasteruser",
            "parameterApplyStatus": "in-sync",
            "preferredBackupWindow": "07:51-08:21",
            "preferredMaintenanceWindow": "tue:12:18-tue:12:48",
            "publiclyAccessible": true,
            "masterEndpoint": {
                "port": 3306,
                "address":
 "ls-3EXAMPLEa995d8c3b06b4501356e5f2fEXAMPLEa.czowadgeezqi.us-
west-2.rds.amazonaws.com"
            },
            "pendingMaintenanceActions": []
        },
        {
            "name": "Postgres",
            "arn": "arn:aws:lightsail:us-west-2:111122223333:RelationalDatabase/
e9780b6b-d0ab-4af2-85f1-1EXAMPLEac68",
            "supportCode": "6EXAMPLE3362/
ls-3EXAMPLEb4fffb5cec056220c734713e14bd5fcd",
            "createdAt": 1554306000.814,
            "location": {
```

```
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "resourceType": "RelationalDatabase",
            "tags": [],
            "relationalDatabaseBlueprintId": "postgres_11",
            "relationalDatabaseBundleId": "micro_1_0",
            "masterDatabaseName": "dbmaster",
            "hardware": {
                "cpuCount": 1,
                "diskSizeInGb": 40,
                "ramSizeInGb": 1.0
            },
            "state": "available",
            "backupRetentionEnabled": true,
            "pendingModifiedValues": {},
            "engine": "postgres",
            "engineVersion": "11.1",
            "latestRestorableTime": 1571686339.0,
            "masterUsername": "dbmasteruser",
            "parameterApplyStatus": "in-sync",
            "preferredBackupWindow": "06:19-06:49",
            "preferredMaintenanceWindow": "sun:10:19-sun:10:49",
            "publiclyAccessible": false,
            "masterEndpoint": {
                "port": 5432,
                "address":
 "ls-3EXAMPLEb4fffb5cec056220c734713eEXAMPLEd.czowadgeezqi.us-
west-2.rds.amazonaws.com"
            },
            "pendingMaintenanceActions": []
        }
    ]
}
```


- Para obtener información sobre la API, consulte GetRelationalDatabases en la Referencia de comandos de la AWS CLI.

`get-static-ip`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-static-ip`.

AWS CLI

Para obtener información sobre una IP estática

En el siguiente ejemplo de `get-static-ip`, se muestran detalles sobre la IP estática especificada.

```
aws lightsail get-static-ip \
    --static-ip-name StaticIp-1
```

Salida:

```
{
    "staticIp": {
        "name": "StaticIp-1",
        "arn": "arn:aws:lightsail:us-
west-2:111122223333:StaticIp/2257cd76-1f0e-4ac0-82e2-2EXAMPLE23ad",
        "supportCode": "6EXAMPLE3362/192.0.2.0",
        "createdAt": 1571071325.076,
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "resourceType": "StaticIp",
        "ipAddress": "192.0.2.0",
        "isAttached": false
    }
}
```

- Para obtener información sobre la API, consulte GetStaticIp en la Referencia de comandos de la AWS CLI.

`get-static-ips`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-static-ips`.

AWS CLI

Para obtener información sobre todas las IP estáticas

En el siguiente ejemplo de `get-static-ips`, se muestran detalles sobre todas las IP estáticas de la región de AWS configurada.

```
aws lightsail get-static-ips
```

Salida:

```
{
    "staticIps": [
        {
            "name": "StaticIp-1",
            "arn": "arn:aws:lightsail:us-
west-2:111122223333:StaticIp/2257cd76-1f0e-4ac0-8EXAMPLE16f9423ad",
            "supportCode": "6EXAMPLE3362/192.0.2.0",
            "createdAt": 1571071325.076,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "resourceType": "StaticIp",
            "ipAddress": "192.0.2.0",
            "isAttached": false
        },
        {
            "name": "StaticIP-2",
            "arn": "arn:aws:lightsail:us-west-2:111122223333:StaticIp/c61edb40-
e5f0-4fd6-ae7c-8EXAMPLE19f8",
            "supportCode": "6EXAMPLE3362/192.0.2.2",
            "createdAt": 1568305385.681,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "resourceType": "StaticIp",
            "ipAddress": "192.0.2.2",
            "attachedTo": "WordPress-1",
            "isAttached": true
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetStaticIps en la Referencia de comandos de la AWS CLI.

`is-vpc-peered`

En el siguiente ejemplo de código, se muestra cómo utilizar `is-vpc-peered`.

AWS CLI

Para identificar si su nube privada virtual de Amazon Lightsail está interconectada

El siguiente ejemplo de `is-vpc-peered` devuelve el estado de interconexión de la nube privada virtual (VPC) de Amazon Lightsail de la región de AWS especificada.

```
aws lightsail is-vpc-peered \
    --region us-west-2
```

Salida:

```
{
    "isPeered": true
}
```

- Para obtener información sobre la API, consulte IsVpcPeered en la Referencia de comandos de la AWS CLI.

`open-instance-public-ports`

En el siguiente ejemplo de código, se muestra cómo utilizar `open-instance-public-ports`.

AWS CLI

Para abrir los puertos de firewall de una instancia

En el siguiente ejemplo de `open-instance-public-ports`, se abre el puerto TCP 22 de la instancia especificada.

```
aws lightsail open-instance-public-ports \
    --instance-name MEAN-2 \
    --port-info fromPort=22,protocol=TCP,toPort=22
```

Salida:

```
{
```

```
    "operation": {
        "id": "719744f0-a022-46f2-9f11-6EXAMPLE4642",
        "resourceName": "MEAN-2",
        "resourceType": "Instance",
        "createdAt": 1571072906.849,
        "location": {
            "availabilityZone": "us-west-2a",
            "regionName": "us-west-2"
        },
        "isTerminal": true,
        "operationDetails": "22/tcp",
        "operationType": "OpenInstancePublicPorts",
        "status": "Succeeded",
        "statusChangedAt": 1571072906.849
    }
}
```

- Para obtener información sobre la API, consulte OpenInstancePublicPorts en la Referencia de comandos de la AWS CLI.

`peer-vpc`

En el siguiente ejemplo de código, se muestra cómo utilizar `peer-vpc`.

AWS CLI

Para interconectar la nube privada virtual de Amazon Lightsail

El siguiente ejemplo de `peer-vpc` interconecta la nube privada virtual (VPC) de Amazon Lightsail de la región de AWS especificada.

```
aws lightsail peer-vpc \
    --region us-west-2
```

Salida:

```
{
    "operation": {
        "id": "787e846a-54ac-497f-bce2-9EXAMPLE5d91",
        "resourceName": "vpc-0EXAMPLEa5261efb3",
        "resourceType": "PeeredVpc",
```

```
        "createdAt": 1571694233.104,
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "isTerminal": true,
        "operationDetails": "vpc-e2b3eb9b",
        "operationType": "PeeredVpc",
        "status": "Succeeded",
        "statusChangedAt": 1571694233.104
    }
}
```

- Para obtener información sobre la API, consulte PeerVpc en la Referencia de comandos de la AWS CLI.

`reboot-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `reboot-instance`.

AWS CLI

Para reiniciar una instancia

En el siguiente ejemplo de `reboot-instance`, se reinicia la instancia especificada.

```
aws lightsail reboot-instance \
    --instance-name MEAN-1
```

Salida:

```
{
    "operations": [
        {
            "id": "2b679f1c-8b71-4bb4-8e97-8EXAMPLEed93",
            "resourceName": "MEAN-1",
            "resourceType": "Instance",
            "createdAt": 1571694445.49,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
```

```
            "isTerminal": true,
            "operationDetails": "",
            "operationType": "RebootInstance",
            "status": "Succeeded",
            "statusChangedAt": 1571694445.49
        }
    ]
}
```

- Para obtener información sobre la API, consulte RebootInstance en la Referencia de comandos de la AWS CLI.

`reboot-relational-database`

En el siguiente ejemplo de código, se muestra cómo utilizar `reboot-relational-database`.

AWS CLI

Para reiniciar una base de datos relacional

En el siguiente ejemplo de `reboot-relational-database`, se reinicia la base de datos relacional especificada.

```
aws lightsail reboot-relational-database \
    --relational-database-name Database-1
```

Salida:

```
{
    "operations": [
        {
            "id": "e4c980c0-3137-496c-9c91-1EXAMPLEdec2",
            "resourceName": "Database-1",
            "resourceType": "RelationalDatabase",
            "createdAt": 1571694532.91,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationDetails": "",
```

```
            "operationType": "RebootRelationalDatabase",
            "status": "Started",
            "statusChangedAt": 1571694532.91
        }
    ]
}
```

- Para obtener información sobre la API, consulte RebootRelationalDatabase en la Referencia de comandos de la AWS CLI.

`release-static-ip`

En el siguiente ejemplo de código, se muestra cómo utilizar `release-static-ip`.

AWS CLI

Para eliminar una IP estática

En el siguiente ejemplo de `release-static-ip`, se elimina la IP estática especificada.

```
aws lightsail release-static-ip \
    --static-ip-name StaticIp-1
```

Salida:

```
{
    "operations": [
        {
            "id": "e374c002-dc6d-4c7f-919f-2EXAMPLE13ce",
            "resourceName": "StaticIp-1",
            "resourceType": "StaticIp",
            "createdAt": 1571694962.003,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationType": "ReleaseStaticIp",
            "status": "Succeeded",
            "statusChangedAt": 1571694962.003
        }
    ]
```

```
}
```

- Para obtener información sobre la API, consulte ReleaseStaticIp en la Referencia de comandos de la AWS CLI.

`start-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-instance`.

AWS CLI

Para iniciar una instancia

En el siguiente ejemplo de `start-instance`, se inicia la instancia especificada.

```
aws lightsail start-instance \
    --instance-name WordPress-1
```

Salida:

```
{
    "operations": [
        {
            "id": "f88d2a93-7cea-4165-afce-2d688cb18f23",
            "resourceName": "WordPress-1",
            "resourceType": "Instance",
            "createdAt": 1571695583.463,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "StartInstance",
            "status": "Started",
            "statusChangedAt": 1571695583.463
        }
    ]
}
```

- Para obtener información sobre la API, consulte StartInstance en la Referencia de comandos de la AWS CLI.

`start-relational-database`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-relational-database`.

AWS CLI

Para iniciar una base de datos relacional

En el siguiente ejemplo de `start-relational-database`, se inicia la base de datos relacional especificada.

```
aws lightsail start-relational-database \
    --relational-database-name Database-1
```

Salida:

```
{
    "operations": [
        {
            "id": "4d5294ec-a38a-4fda-9e37-aEXAMPLE0d24",
            "resourceName": "Database-1",
            "resourceType": "RelationalDatabase",
            "createdAt": 1571695998.822,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "StartRelationalDatabase",
            "status": "Started",
            "statusChangedAt": 1571695998.822
        }
    ]
}
```

- Para obtener información sobre la API, consulte StartRelationalDatabase en la Referencia de comandos de la AWS CLI.

`stop-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-instance`.

AWS CLI

Para detener una instancia

En el siguiente ejemplo de `stop-instance`, se detiene la instancia especificada.

```
aws lightsail stop-instance \
--instance-name WordPress-1
```

Salida:

```
{
    "operations": [
        {
            "id": "265357e2-2943-4d51-888a-1EXAMPLE7585",
            "resourceName": "WordPress-1",
            "resourceType": "Instance",
            "createdAt": 1571695471.134,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "StopInstance",
            "status": "Started",
            "statusChangedAt": 1571695471.134
        }
    ]
}
```

- Para obtener información sobre la API, consulte StopInstance en la Referencia de comandos de la AWS CLI.

`stop-relational-database`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-relational-database`.

AWS CLI

Para detener una base de datos relacional

En el siguiente ejemplo de `stop-relational-database`, detiene la base de datos relacional especificada.

```
aws lightsail stop-relational-database \
    --relational-database-name Database-1
```

Salida:

```
{
    "operations": [
        {
            "id": "cc559c19-4adb-41e4-b75b-5EXAMPLE4e61",
            "resourceName": "Database-1",
            "resourceType": "RelationalDatabase",
            "createdAt": 1571695526.29,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "isTerminal": false,
            "operationType": "StopRelationalDatabase",
            "status": "Started",
            "statusChangedAt": 1571695526.29
        }
    ]
}
```

- Para obtener información sobre la API, consulte StopRelationalDatabase en la Referencia de comandos de la AWS CLI.

`unpeer-vpc`

En el siguiente ejemplo de código, se muestra cómo utilizar `unpeer-vpc`.

AWS CLI

Para desconectar la nube privada virtual de Amazon Lightsail

El siguiente ejemplo de `unpeer-vpc` desconecta la nube privada virtual (VPC) de Amazon Lightsail de la región de AWS especificada.

```
aws lightsail unpeer-vpc \
```

```
    --region us-west-2
```

Salida:

```
{
    "operation": {
        "id": "531aca64-7157-47ab-84c6-eEXAMPLEd898",
        "resourceName": "vpc-0EXAMPLEa5261efb3",
        "resourceType": "PeeredVpc",
        "createdAt": 1571694109.945,
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "isTerminal": true,
        "operationDetails": "vpc-e2b3eb9b",
        "operationType": "UnpeeredVpc",
        "status": "Succeeded",
        "statusChangedAt": 1571694109.945
    }
}
```

- Para obtener información sobre la API, consulte UnpeerVpc en la Referencia de comandos de la AWS CLI.

Ejemplos de Macie que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Macie.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`describe-buckets`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-buckets`.

AWS CLI

Para consultar datos sobre uno o más buckets de S3 que Amazon Macie supervisa y analiza para su cuenta

En el siguiente ejemplo de `describe-buckets`, se consultan metadatos de todos los buckets de S3 cuyos nombres comienzan por amzn-s3-demo-bucket y se encuentran en la región de AWS actual.

```
aws macie2 describe-buckets \
    --criteria '{"bucketName":{"prefix":"amzn-s3-demo-bucket"}}'
```

Salida:

```
{
    "buckets": [
        {
            "accountId": "123456789012",
            "allowsUnencryptedObjectUploads": "FALSE",
            "automatedDiscoveryMonitoringStatus": "MONITORED",
            "bucketArn": "arn:aws:s3:::amzn-s3-demo-bucket1",
            "bucketCreatedAt": "2020-05-18T19:54:00+00:00",
            "bucketName": "amzn-s3-demo-bucket1",
            "classifiableObjectCount": 13,
            "classifiableSizeInBytes": 1592088,
            "jobDetails": {
                "isDefinedInJob": "TRUE",
                "isMonitoredByJob": "TRUE",
                "lastJobId": "08c81dc4a2f3377fae45c9ddaEXAMPLE",
                "lastJobRunTime": "2024-08-19T14:55:30.270000+00:00"
            },
            "lastAutomatedDiscoveryTime": "2024-10-22T19:11:25.364000+00:00",
            "lastUpdated": "2024-10-25T07:33:06.337000+00:00",
            "objectCount": 13,
            "objectCountByEncryptionType": {
                "customerManaged": 0,
                "kmsManaged": 2,
```

```
                "s3Managed": 7,
                "unencrypted": 4,
                "unknown": 0
            },
            "publicAccess": {
                "effectivePermission": "NOT_PUBLIC",
                "permissionConfiguration": {
                    "accountLevelPermissions": {
                        "blockPublicAccess": {
                            "blockPublicAcls": true,
                            "blockPublicPolicy": true,
                            "ignorePublicAcls": true,
                            "restrictPublicBuckets": true
                        }
                    },
                    "bucketLevelPermissions": {
                        "accessControlList": {
                            "allowsPublicReadAccess": false,
                            "allowsPublicWriteAccess": false
                        },
                        "blockPublicAccess": {
                            "blockPublicAcls": true,
                            "blockPublicPolicy": true,
                            "ignorePublicAcls": true,
                            "restrictPublicBuckets": true
                        },
                        "bucketPolicy": {
                            "allowsPublicReadAccess": false,
                            "allowsPublicWriteAccess": false
                        }
                    }
                }
            },
            "region": "us-west-2",
            "replicationDetails": {
                "replicated": false,
                "replicatedExternally": false,
                "replicationAccounts": []
            },
            "sensitivityScore": 78,
            "serverSideEncryption": {
                "kmsMasterKeyId": null,
                "type": "NONE"
            },
```

```
            "sharedAccess": "NOT_SHARED",
            "sizeInBytes": 4549746,
            "sizeInBytesCompressed": 0,
            "tags": [
                {
                    "key": "Division",
                    "value": "HR"
                },
                {
                    "key": "Team",
                    "value": "Recruiting"
                }
            ],
            "unclassifiableObjectCount": {
                "fileType": 0,
                "storageClass": 0,
                "total": 0
            },
            "unclassifiableObjectSizeInBytes": {
                "fileType": 0,
                "storageClass": 0,
                "total": 0
            },
            "versioning": true
        },
        {
            "accountId": "123456789012",
            "allowsUnencryptedObjectUploads": "TRUE",
            "automatedDiscoveryMonitoringStatus": "MONITORED",
            "bucketArn": "arn:aws:s3:::amzn-s3-demo-bucket2",
            "bucketCreatedAt": "2020-11-25T18:24:38+00:00",
            "bucketName": "amzn-s3-demo-bucket2",
            "classifiableObjectCount": 8,
            "classifiableSizeInBytes": 133810,
            "jobDetails": {
                "isDefinedInJob": "TRUE",
                "isMonitoredByJob": "FALSE",
                "lastJobId": "188d4f6044d621771ef7d65f2EXAMPLE",
                "lastJobRunTime": "2024-07-09T19:37:11.511000+00:00"
            },
            "lastAutomatedDiscoveryTime": "2024-10-24T19:11:25.364000+00:00",
            "lastUpdated": "2024-10-25T07:33:06.337000+00:00",
            "objectCount": 8,
            "objectCountByEncryptionType": {
```

```
                "customerManaged": 0,
                "kmsManaged": 0,
                "s3Managed": 8,
                "unencrypted": 0,
                "unknown": 0
            },
            "publicAccess": {
                "effectivePermission": "NOT_PUBLIC",
                "permissionConfiguration": {
                    "accountLevelPermissions": {
                        "blockPublicAccess": {
                            "blockPublicAcls": true,
                            "blockPublicPolicy": true,
                            "ignorePublicAcls": true,
                            "restrictPublicBuckets": true
                        }
                    },
                    "bucketLevelPermissions": {
                        "accessControlList": {
                            "allowsPublicReadAccess": false,
                            "allowsPublicWriteAccess": false
                        },
                        "blockPublicAccess": {
                            "blockPublicAcls": true,
                            "blockPublicPolicy": true,
                            "ignorePublicAcls": true,
                            "restrictPublicBuckets": true
                        },
                        "bucketPolicy": {
                            "allowsPublicReadAccess": false,
                            "allowsPublicWriteAccess": false
                        }
                    }
                }
            },
            "region": "us-west-2",
            "replicationDetails": {
                "replicated": false,
                "replicatedExternally": false,
                "replicationAccounts": []
            },
            "sensitivityScore": 95,
            "serverSideEncryption": {
                "kmsMasterKeyId": null,
```

```
                "type": "AES256"
            },
            "sharedAccess": "EXTERNAL",
            "sizeInBytes": 175978,
            "sizeInBytesCompressed": 0,
            "tags": [
                {
                    "key": "Division",
                    "value": "HR"
                },
                {
                    "key": "Team",
                    "value": "Recruiting"
                }
            ],
            "unclassifiableObjectCount": {
                "fileType": 3,
                "storageClass": 0,
                "total": 3
            },
            "unclassifiableObjectSizeInBytes": {
                "fileType": 2999826,
                "storageClass": 0,
                "total": 2999826
            },
            "versioning": true
        }
    ]
}
```

Para obtener más información, consulte Filtering your S3 bucket inventory en la Guía del usuario de Amazon Macie.

- Para obtener información sobre la API, consulte DescribeBuckets en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon Managed Grafana que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon Managed Grafana.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`list-workspaces`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-workspaces`.

AWS CLI

Para enumerar los espacios de trabajo para la cuenta en la región especificada por la credencial de usuario

En el siguiente ejemplo de `list-workspaces`, se enumeran los espacios de trabajo de Grafana para la región de la cuenta.

```
aws grafana list-workspaces
```

Salida:

```
{
    "workspaces": [
        {
            "authentication": {
                "providers": [
                    "AWS_SSO"
                ]
            },
            "created": "2022-04-04T16:20:21.796000-07:00",
            "description": "to test tags",
            "endpoint": "g-949e7b44df.grafana-workspace.us-east-1.amazonaws.com",
            "grafanaVersion": "8.2",
            "id": "g-949e7b44df",
```

```
            "modified": "2022-04-04T16:20:21.796000-07:00",
            "name": "testtag2",
            "notificationDestinations": [
                "SNS"
            ],
            "status": "ACTIVE"
        },
        {
            "authentication": {
                "providers": [
                    "AWS_SSO"
                ]
            },
            "created": "2022-04-20T10:22:15.115000-07:00",
            "description": "ww",
            "endpoint": "g-bffa51ed1b.grafana-workspace.us-east-1.amazonaws.com",
            "grafanaVersion": "8.2",
            "id": "g-bffa51ed1b",
            "modified": "2022-04-20T10:22:15.115000-07:00",
            "name": "ww",
            "notificationDestinations": [
                "SNS"
            ],
            "status": "ACTIVE"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListWorkspaces en la Referencia de comandos de la AWS CLI.

Ejemplos de MediaConnect que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con MediaConnect.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-flow-outputs`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-flow-outputs`.

AWS CLI

Adición de salidas a un flujo

En el siguiente ejemplo de `add-flow-outputs`, se agregan salidas al flujo especificado.

```
aws mediaconnect add-flow-outputs \
--flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame \
--outputs Description='NYC
 stream',Destination=192.0.2.12,Name=NYC,Port=3333,Protocol=rtp-
fec,SmoothingLatency=100 Description='LA
 stream',Destination=203.0.113.9,Name=LA,Port=4444,Protocol=rtp-
fec,SmoothingLatency=100
```

Salida:

```
{
    "Outputs": [
        {
            "Port": 3333,
            "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:NYC",
            "Name": "NYC",
            "Description": "NYC stream",
            "Destination": "192.0.2.12",
            "Transport": {
                "Protocol": "rtp-fec",
                "SmoothingLatency": 100
            }
        },
        {
            "Port": 4444,
```

```
            "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-987655dEF67hiJ89-c34de5fG678h:LA",
            "Name": "LA",
            "Description": "LA stream",
            "Destination": "203.0.113.9",
            "Transport": {
                "Protocol": "rtp-fec",
                "SmoothingLatency": 100
            }
        }
    ],
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame"
}
```

Para obtener más información, consulte Adding Outputs to a Flow en la Guía del usuario de AWS Elemental MediaConnect.

- Para obtener información sobre la API, consulte AddFlowOutputs en la Referencia de comandos de la AWS CLI.

`create-flow`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-flow`.

AWS CLI

Para crear un flujo

En el siguiente ejemplo de `create-flow`, se crea un flujo con la configuración especificada.

```
aws mediaconnect create-flow \
    --availability-zone us-west-2c \
    --name ExampleFlow \
    --source Description='Example source,
 backup',IngestPort=1055,Name=BackupSource,Protocol=rtp,WhitelistCidr=10.24.34.0/23
```

Salida:

```
{
    "Flow": {
        "FlowArn": "arn:aws:mediaconnect:us-
east-1:123456789012:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:ExampleFlow",
```

```
        "AvailabilityZone": "us-west-2c",
        "EgressIp": "54.245.71.21",
        "Source": {
            "IngestPort": 1055,
            "SourceArn": "arn:aws:mediaconnect:us-
east-1:123456789012:source:2-3aBC45dEF67hiJ89-c34de5fG678h:BackupSource",
            "Transport": {
                "Protocol": "rtp",
                "MaxBitrate": 80000000
            },
            "Description": "Example source, backup",
            "IngestIp": "54.245.71.21",
            "WhitelistCidr": "10.24.34.0/23",
            "Name": "mySource"
        },
        "Entitlements": [],
        "Name": "ExampleFlow",
        "Outputs": [],
        "Status": "STANDBY",
        "Description": "Example source, backup"
    }
}
```

Para obtener más información, consulte Creating a Flow en la Guía del usuario de AWS Elemental MediaConnect.

- Para obtener información sobre la API, consulte CreateFlow en la Referencia de comandos de la AWS CLI.

`delete-flow`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-flow`.

AWS CLI

Para eliminar un flujo

En el siguiente ejemplo de `delete-flow`, se elimina el flujo especificado.

```
aws mediaconnect delete-flow \
    --flow-arn arn:aws:mediaconnect:us-
east-1:123456789012:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow
```

Salida:

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:123456789012:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow",
    "Status": "DELETING"
}
```

Para obtener más información, consulte Deleting a Flow en la Guía del usuario de AWS Elemental MediaConnect.

- Para obtener información sobre la API, consulte DeleteFlow en la Referencia de comandos de la AWS CLI.

`describe-flow`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-flow`.

AWS CLI

Para consultar los detalles de un flujo

En el siguiente ejemplo de `describe-flow`, se muestran los detalles del flujo especificado, como ARN, zona de disponibilidad, estado, origen, derechos y salidas.

```
aws mediaconnect describe-flow \
    --flow-arn arn:aws:mediaconnect:us-
east-1:123456789012:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow
```

Salida:

```
{
    "Flow": {
        "EgressIp": "54.201.4.39",
        "AvailabilityZone": "us-west-2c",
        "Status": "ACTIVE",
        "FlowArn": "arn:aws:mediaconnect:us-
east-1:123456789012:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow",
        "Entitlements": [
            {
                "EntitlementArn": "arn:aws:mediaconnect:us-
west-2:123456789012:entitlement:1-AaBb11CcDd22EeFf-34DE5fG12AbC:MyEntitlement",
```

```
                "Description": "Assign to this account",
                "Name": "MyEntitlement",
                "Subscribers": [
                    "444455556666"
                ]
            }
        ],
        "Description": "NYC awards show",
        "Name": "AwardsShow",
        "Outputs": [
            {
                "Port": 2355,
                "Name": "NYC",
                "Transport": {
                    "SmoothingLatency": 0,
                    "Protocol": "rtp-fec"
                },
                "OutputArn": "arn:aws:mediaconnect:us-
east-1:123456789012:output:2-3aBC45dEF67hiJ89-c34de5fG678h:NYC",
                "Destination": "192.0.2.0"
            },
            {
                "Port": 3025,
                "Name": "LA",
                "Transport": {
                    "SmoothingLatency": 0,
                    "Protocol": "rtp-fec"
                },
                "OutputArn": "arn:aws:mediaconnect:us-
east-1:123456789012:output:2-987655dEF67hiJ89-c34de5fG678h:LA",
                "Destination": "192.0.2.0"
            }
        ],
        "Source": {
            "IngestIp": "54.201.4.39",
            "SourceArn": "arn:aws:mediaconnect:us-
east-1:123456789012:source:3-4aBC56dEF78hiJ90-4de5fG6Hi78Jk:ShowSource",
            "Transport": {
                "MaxBitrate": 80000000,
                "Protocol": "rtp"
            },
            "IngestPort": 1069,
            "Description": "Saturday night show",
            "Name": "ShowSource",
```

```
            "WhitelistCidr": "10.24.34.0/23"
        }
    }
}
```

Para obtener más información, consulte Viewing the Details of a Flow en la Guía del usuario de AWS Elemental MediaConnect.

- Para obtener información sobre la API, consulte DescribeFlow en la Referencia de comandos de la AWS CLI.

`grant-flow-entitlements`

En el siguiente ejemplo de código, se muestra cómo utilizar `grant-flow-entitlements`.

AWS CLI

Para conceder un derecho para un flujo

En el siguiente ejemplo de `grant-flow-entitlements`, se concede un derecho al flujo existente especificado para compartir el contenido con otra cuenta de AWS.

```
aws mediaconnect grant-flow-entitlements \
    --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame \
    --entitlements Description='For
 AnyCompany',Encryption={"Algorithm=aes128,KeyType=static-
key,RoleArn=arn:aws:iam::111122223333:role/MediaConnect-
ASM,SecretArn=arn:aws:secretsmanager:us-
west-2:111122223333:secret:mySecret1"},Name=AnyCompany_Entitlement,Subscribers=444455556666
 Description='For Example Corp',Name=ExampleCorp,Subscribers=777788889999
```

Salida:

```
{
    "Entitlements": [
        {
            "Name": "AnyCompany_Entitlement",
            "EntitlementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:AnyCompany_Entitlement",
            "Subscribers": [
                "444455556666"
```

```
            ],
            "Description": "For AnyCompany",
            "Encryption": {
                "SecretArn": "arn:aws:secretsmanager:us-
west-2:111122223333:secret:mySecret1",
                "Algorithm": "aes128",
                "RoleArn": "arn:aws:iam::111122223333:role/MediaConnect-ASM",
                "KeyType": "static-key"
            }
        },
        {
            "Name": "ExampleCorp",
            "EntitlementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-3333cccc4444dddd-1111aaaa2222:ExampleCorp",
            "Subscribers": [
                "777788889999"
            ],
            "Description": "For Example Corp"
        }
    ],
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame"
}
```

Para obtener más información, consulte Granting an Entitlement on a Flow en la Guía del usuario de AWS Elemental MediaConnect.

- Para obtener información sobre la API, consulte GrantFlowEntitlements en la Referencia de comandos de la AWS CLI.

`list-entitlements`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-entitlements`.

AWS CLI

Para ver una lista de derechos

En el siguiente ejemplo de `list-entitlements`, se muestra una lista de todos los derechos que se han concedido a la cuenta.

```
aws mediaconnect list-entitlements
```

Salida:

```
{
    "Entitlements": [
        {
            "EntitlementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:MyEntitlement",
            "EntitlementName": "MyEntitlement"
        }
    ]
}
```

Para obtener más información, consulte ListEntitlements en la Referencia de la API de AWS Elemental MediaConnect.

- Para obtener información sobre la API, consulte ListEntitlements en la Referencia de comandos de la AWS CLI.

`list-flows`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-flows`.

AWS CLI

Para ver una lista de flujos

En el siguiente ejemplo de `list-flows`, se muestra una lista de flujos.

```
aws mediaconnect list-flows
```

Salida:

```
{
    "Flows": [
        {
            "Status": "STANDBY",
            "SourceType": "OWNED",
            "AvailabilityZone": "us-west-2a",
            "Description": "NYC awards show",
            "Name": "AwardsShow",
            "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow"
```

```
        },
        {
            "Status": "STANDBY",
            "SourceType": "OWNED",
            "AvailabilityZone": "us-west-2c",
            "Description": "LA basketball game",
            "Name": "BasketballGame",
            "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame"
        }
    ]
}
```

Para obtener más información, consulte Viewing a List of Flows en la Guía del usuario de AWS Elemental MediaConnect.

- Para obtener información sobre la API, consulte ListFlows en la Referencia de comandos de AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para mostrar etiquetas de un recurso de MediaConnect

En el siguiente ejemplo de `list-tags-for-resource`, se muestran las claves y los valores de etiqueta asociados al recurso de MediaConnect especificado.

```
aws mediaconnect list-tags-for-resource \
    --resource-arn arn:aws:mediaconnect:us-
east-1:123456789012:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame
```

Salida:

```
{
    "Tags": {
        "region": "west",
        "stage": "prod"
    }
}
```

Para obtener más información, consulte ListTagsForResource, TagResource, UntagResource en la Referencia de la API de AWS Elemental MediaConnect.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`remove-flow-output`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-flow-output`.

AWS CLI

Para eliminar una salida de un flujo

En el siguiente ejemplo de `remove-flow-output`, se elimina un resultado del flujo especificado.

```
aws mediaconnect remove-flow-output \
    --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame \
    --output-arn arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:NYC
```

Salida:

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame",
    "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:NYC"
}
```

Para obtener más información, consulte Removing Outputs from a Flow en la Guía del usuario de AWS Elemental MediaConnect.

- Para obtener información sobre la API, consulte RemoveFlowOutput en la Referencia de comandos de la AWS CLI.

`revoke-flow-entitlement`

En el siguiente ejemplo de código, se muestra cómo utilizar `revoke-flow-entitlement`.

AWS CLI

Para revocar un derecho

En el siguiente ejemplo de `revoke-flow-entitlement`, se revoca un derecho en el flujo especificado.

```
aws mediaconnect revoke-flow-entitlement \
    --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame \
    --entitlement-arn arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:AnyCompany_Entitlement
```

Salida:

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame",
    "EntitlementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:AnyCompany_Entitlement"
}
```

Para obtener más información, consulte Revoking an Entitlement en la Guía del usuario de AWS Elemental MediaConnect.

- Para obtener información sobre la API, consulte RevokeFlowEntitlement en la Referencia de comandos de AWS CLI.

`start-flow`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-flow`.

AWS CLI

Para iniciar un flujo

En el siguiente ejemplo de `start-flow`, se inicia el flujo especificado.

```
aws mediaconnect start-flow \
    --flow-arn arn:aws:mediaconnect:us-
east-1:123456789012:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow
```

Este comando no genera ninguna salida. Salida:

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:123456789012:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow",
    "Status": "STARTING"
}
```

Para obtener más información, consulte Starting a Flow en la Guía del usuario de AWS Elemental MediaConnect.

- Para obtener más información sobre la API, consulte StartFlow en Referencia de comandos de la AWS CLI.

`stop-flow`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-flow`.

AWS CLI

Para detener un flujo

En el siguiente ejemplo de `stop-flow`, se detiene el flujo especificado.

```
aws mediaconnect stop-flow \
    --flow-arn arn:aws:mediaconnect:us-
east-1:123456789012:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow
```

Salida:

```
{
    "Status": "STOPPING",
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:123456789012:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow"
}
```

Para obtener más información, consulte Stopping a Flow en la Guía del usuario de AWS Elemental MediaConnect.

- Para obtener información sobre la API, consulte StopFlow en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para añadir etiquetas a un recurso de MediaConnect

El siguiente ejemplo de `tag-resource` añade una etiqueta con un nombre de clave y un valor al recurso de MediaConnect especificado.

```
aws mediaconnect tag-resource \
    --resource-arn arn:aws:mediaconnect:us-
east-1:123456789012:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame
    --tags region=west
```

Este comando no genera ninguna salida.

Para obtener más información, consulte ListTagsForResource, TagResource, UntagResource en la Referencia de la API de AWS Elemental MediaConnect.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar etiquetas de un recurso de MediaConnect

En el siguiente ejemplo de `untag-resource`, se elimina la etiqueta con el nombre de clave especificado y su valor asociado desde el recurso de MediaConnect.

```
aws mediaconnect untag-resource \
    --resource-arn arn:aws:mediaconnect:us-
east-1:123456789012:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame \
    --tag-keys region
```

Este comando no genera ninguna salida.

Para obtener más información, consulte ListTagsForResource, TagResource, UntagResource en la Referencia de la API de AWS Elemental MediaConnect.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-flow-entitlement

En el siguiente ejemplo de código, se muestra cómo utilizar `update-flow-entitlement`.

AWS CLI

Para actualizar un derecho

En el siguiente ejemplo de `update-flow-entitlement`, se actualiza el derecho especificado con una descripción y un suscriptor nuevos.

```
aws mediaconnect update-flow-entitlement \
    --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame \
    --entitlement-arn arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:AnyCompany_Entitlement
 \
    --description 'For AnyCompany Affiliate' \
    --subscribers 777788889999
```

Salida:

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame",
    "Entitlement": {
        "Name": "AnyCompany_Entitlement",
        "Description": "For AnyCompany Affiliate",
        "EntitlementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:AnyCompany_Entitlement",
        "Encryption": {
            "KeyType": "static-key",
            "Algorithm": "aes128",
            "RoleArn": "arn:aws:iam::111122223333:role/MediaConnect-ASM",
            "SecretArn": "arn:aws:secretsmanager:us-
west-2:111122223333:secret:mySecret1"
```

```
        },
        "Subscribers": [
            "777788889999"
        ]
    }
}
```

Para obtener más información, consulte Updating an Entitlement en la Guía del usuario de AWS Elemental MediaConnect.

- Para obtener información sobre la API, consulte UpdateFlowEntitlement en la Referencia de comandos de la AWS CLI.

`update-flow-output`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-flow-output`.

AWS CLI

Para actualizar un resultado de un flujo

En el siguiente ejemplo de `update-flow-output`, se actualiza un resultado del flujo especificado.

```
aws mediaconnect update-flow-output \
    --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame \
    --output-arn arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:NYC \
    --port 3331
```

Salida:

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame",
    "Output": {
        "Name": "NYC",
        "Port": 3331,
        "Description": "NYC stream",
        "Transport": {
            "Protocol": "rtp-fec",
```

```
            "SmoothingLatency": 100
        },
        "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:NYC",
        "Destination": "192.0.2.12"
    }
}
```

Para obtener más información, consulte Updating Outputs to a Flow en la Guía del usuario de AWS Elemental MediaConnect.

- Para obtener información sobre la API, consulte UpdateFlowOutput en la Referencia de comandos de la AWS CLI.

`update-flow-source`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-flow-source`.

AWS CLI

Para actualizar el origen de un flujo existente

En el siguiente ejemplo de `update-flow-source`, se actualiza el origen de un flujo existente.,

```
aws mediaconnect update-flow-source \
    --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow \
    --source-arn arn:aws:mediaconnect:us-
east-1:111122223333:source:3-4aBC56dEF78hiJ90-4de5fG6Hi78Jk:ShowSource \
    --description 'Friday night show' \
    --ingest-port 3344 \
    --protocol rtp-fec \
    --whitelist-cidr 10.24.34.0/23
```

Salida:

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow",
    "Source": {
        "IngestIp": "34.210.136.56",
        "WhitelistCidr": "10.24.34.0/23",
```

```
        "Transport": {
            "Protocol": "rtp-fec"
        },
        "IngestPort": 3344,
        "Name": "ShowSource",
        "Description": "Friday night show",
        "SourceArn": "arn:aws:mediaconnect:us-
east-1:111122223333:source:3-4aBC56dEF78hiJ90-4de5fG6Hi78Jk:ShowSource"
    }
}
```

Para obtener más información, consulte Updating the Source of a Flow en la Guía del usuario de AWS Elemental MediaConnect.

- Para obtener información sobre la API, consulte UpdateFlowSource en la Referencia de comandos de la AWS CLI.

Ejemplos de MediaConvert que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con MediaConvert.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`cancel-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-job`.

AWS CLI

Para cancelar un trabajo que está en una cola

En el siguiente ejemplo de `cancel-job`, se cancela un trabajo con el ID `1234567891234-abc123`. No se puede cancelar un trabajo cuando el servicio comience a procesarlo.

```
aws mediaconvert cancel-job \
    --endpoint-url https://abcd1234.mediaconvert.region-name-1.amazonaws.com \
    --region region-name-1 \
    --id 1234567891234-abc123
```

Para obtener el punto de conexión específico de su cuenta, utilice `describe-endpoints` o envíe el comando sin el punto de conexión. El servicio devuelve un error y su punto de conexión.

Para obtener más información, consulte Trabajar con AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener más información sobre la API, consulte CancelJob en la Referencia de comandos de la AWS CLI.

`create-job-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-job-template`.

AWS CLI

Para crear una nueva plantilla de trabajo

En el siguiente ejemplo de `create-job-template`, se crea una plantilla de trabajos con la configuración de transcodificación especificada en un archivo `job-template.json` que reside en el sistema.

```
aws mediaconvert create-job-template \
    --endpoint-url https://abcd1234.mediaconvert.region-name-1.amazonaws.com \
    --region region-name-1 \
    --name JobTemplate1 \
    --cli-input-json file://~/job-template.json
```

Si crea el archivo JSON de plantilla de trabajos utilizando `get-job-template` y, a continuación, modifica el archivo, elimine el objeto `JobTemplate`, pero mantenga el objeto secundario de Configuración dentro de él. Asimismo, asegúrese de eliminar los siguientes pares de clave-valor: `LastUpdated`, `Arn`, `Type` y `CreatedAt`. Puede especificar la categoría, la descripción, el nombre y la cola en el archivo JSON o en la línea de comandos.

Para obtener el punto de conexión específico de su cuenta, utilice `describe-endpoints` o envíe el comando sin el punto de conexión. El servicio devuelve un error y su punto de conexión.

Si la solicitud se realiza correctamente, el servicio devuelve la especificación JSON para la plantilla de trabajos que ha creado.

Para obtener más información, consulte Uso de plantillas de tarea de AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte CreateJobTemplate en la Referencia de comandos de la AWS CLI.

`create-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-job`.

AWS CLI

Creación de un trabajo

En el siguiente ejemplo de `create-job` se crea un trabajo de transcodificación con la configuración especificada en un archivo `job.json` que reside en el sistema desde el que se envía el comando. Esta especificación de trabajo de JSON puede especificar cada configuración de forma individual, hacer referencia a una plantilla de trabajo o hacer referencia a ajustes preestablecidos de salida.

```
aws mediaconvert create-job \
    --endpoint-url https://abcd1234.mediaconvert.region-name-1.amazonaws.com \
    --region region-name-1 \
    --cli-input-json file://~/job.json
```

Puede utilizar la consola de AWS Elemental MediaConvert para generar la especificación de trabajo de JSON eligiendo la configuración del trabajo y, a continuación, eligiendo Mostrar JSON del trabajo en la parte inferior de la sección Trabajo.

Para obtener el punto de conexión específico de su cuenta, utilice `describe-endpoints` o envíe el comando sin el punto de conexión. El servicio devuelve un error y su punto de conexión.

Si la solicitud se realiza correctamente, el servicio devuelve la especificación de trabajo JSON que envió con la solicitud.

Para obtener más información, consulte Trabajar con AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener más información sobre la API, consulte CreateJob en la Referencia de comandos de la AWS CLI.

`create-preset`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-preset`.

AWS CLI

Para crear un elemento preestablecido de salida personalizado

En el siguiente ejemplo de `create-preset`, se crea un elemento preestablecido de salida personalizado basado en la configuración de salida especificada en el archivo `preset.json`. Puede especificar la categoría, la descripción y el nombre en el archivo JSON o en la línea de comandos.

```
aws mediaconvert create-preset \
    --endpoint-url https://abcd1234.mediaconvert.region-name-1.amazonaws.com
    --region region-name-1 \
    --cli-input-json file://~/preset.json
```

Si crea el archivo JSON preestablecido utilizando `get-preset` y, a continuación, modificando el archivo de salida, asegúrese de eliminar los siguientes pares clave-valor: `LastUpdated`, `Arn`, `Type` y `CreatedAt`.

Para obtener el punto de conexión específico de su cuenta, utilice `describe-endpoints` o envíe el comando sin el punto de conexión. El servicio devuelve un error y su punto de conexión.

Para obtener más información, consulte Trabajar con elementos preestablecidos de salida de AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte CreatePreset en la Referencia de comandos de la AWS CLI.

`create-queue`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-queue`.

AWS CLI

Para crear una cola

En el siguiente ejemplo de `create-queue`, se crea una cola de transcodificación personalizada.

```
aws mediaconvert create-queue \
    --endpoint-url https://abcd1234.mediaconvert.region-name-1.amazonaws.com \
    --region region-name-1 \
    --name Queue1 \
    --description "Keep this queue empty unless job is urgent."
```

Para obtener el punto de conexión específico de su cuenta, utilice `describe-endpoints` o envíe el comando sin el punto de conexión. El servicio devuelve un error y su punto de conexión.

Salida:

```
{
    "Queue": {
        "Status": "ACTIVE",
        "Name": "Queue1",
        "LastUpdated": 1518034928,
        "Arn": "arn:aws:mediaconvert:region-name-1:012345678998:queues/Queue1",
        "Type": "CUSTOM",
        "CreatedAt": 1518034928,
        "Description": "Keep this queue empty unless job is urgent."
    }
}
```

Para obtener más información, consulte Trabajar con colas en AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte CreateQueue en la Referencia de comandos de la AWS CLI.

`delete-job-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-job-template`.

AWS CLI

Para eliminar una plantilla de trabajo

En el siguiente ejemplo de `delete-job-template`, se elimina la plantilla de trabajo personalizada especificada.

```
aws mediaconvert delete-job-template \
    --name "DASH Streaming" \
    --endpoint-url https://abcd1234.mediaconvert.us-west-2.amazonaws.com
```

Este comando no genera ninguna salida. Ejecute `aws mediaconvert list-job-templates` para confirmar que se ha eliminado la plantilla.

Para obtener más información, consulte Uso de plantillas de tarea de AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte DeleteJobTemplate en la Referencia de comandos de la AWS CLI.

`delete-preset`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-preset`.

AWS CLI

Para eliminar una cola bajo demanda personalizada

En el siguiente ejemplo de `delete-preset`, se elimina el elemento preestablecido especificado.

```
aws mediaconvert delete-preset \
    --name SimpleMP4 \
    --endpoint-url  https://abcd1234.mediaconvert.us-west-2.amazonaws.com
```

Este comando no genera ninguna salida. Ejecute `aws mediaconvert list-presets` para confirmar que se ha eliminado el elemento preestablecido.

Para obtener más información, consulte Trabajar con elementos preestablecidos de salida de AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte DeletePreset en la Referencia de comandos de la AWS CLI.

`delete-queue`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-queue`.

AWS CLI

Para eliminar una cola bajo demanda personalizada

En el siguiente ejemplo de `delete-queue`, se elimina la cola bajo demanda personalizada especificada.

No puede eliminar la cola predeterminada. No se puede eliminar una cola reservada que tenga un plan de precios activo o que contenga tareas sin procesar.

```
aws mediaconvert delete-queue \
    --name Customer1 \
    --endpoint-url https://abcd1234.mediaconvert.us-west-2.amazonaws.com
```

Este comando no genera ninguna salida. Ejecute `aws mediaconvert list-queues` para confirmar que se ha eliminado la cola.

Para obtener más información, consulte Trabajar con colas en AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte DeleteQueue en la Referencia de comandos de la AWS CLI.

`describe-endpoints`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-endpoints`.

AWS CLI

Para obtener un punto de conexión específico de la cuenta

En el siguiente ejemplo de `describe-endpoints`, se recupera el punto de conexión que necesita para enviar cualquier otra solicitud al servicio.

```
aws mediaconvert describe-endpoints
```

Salida:

```
{
    "Endpoints": [
        {
            "Url": "https://abcd1234.mediaconvert.region-name-1.amazonaws.com"
```

```
        }
    ]
}
```

Para obtener más información, consulte la Getting Started with MediaConvert Using the API en la AWSReferencia de la API de MediaConvert.

- Para obtener detalles sobre la API, consulte DescribeEndpoints en la Referencia de comandos de la AWS CLI.

`get-job-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-job-template`.

AWS CLI

Para obtener detalles sobre una plantilla de trabajo

En el siguiente ejemplo de `get-job-template`, se muestra la definición JSON de la plantilla de trabajo personalizada especificada.

```
aws mediaconvert get-job-template \
    --name "DASH Streaming" \
    --endpoint-url https://abcd1234.mediaconvert.us-east-1.amazonaws.com
```

Salida:

```
{
    "JobTemplate": {
        "StatusUpdateInterval": "SECONDS_60",
        "LastUpdated": 1568652998,
        "Description": "Create a DASH streaming ABR stack",
        "CreatedAt": 1568652998,
        "Priority": 0,
        "Name": "DASH Streaming",
        "Settings": {
            ...<truncatedforbrevity>...
        },
        "Arn": "arn:aws:mediaconvert:us-west-2:123456789012:jobTemplates/DASH
 Streaming",
        "Type": "CUSTOM"
    }
```

```
}
```

Para obtener más información, consulte Uso de plantillas de tarea de AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte GetJobTemplate en la Referencia de comandos de la AWS CLI.

`get-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-job`.

AWS CLI

Obtención de los detalles de un trabajo en particular

En el siguiente ejemplo, se solicita la información del trabajo con el ID `1234567890987-1ab2c3`, que en este ejemplo finalizó con un error.

```
aws mediaconvert get-job \
    --endpoint-url https://abcd1234.mediaconvert.region-name-1.amazonaws.com \
    --region region-name-1 \
    --id 1234567890987-1ab2c3
```

Para obtener el punto de conexión específico de su cuenta, utilice `describe-endpoints` o envíe el comando sin el punto de conexión. El servicio devuelve un error y su punto de conexión.

Si la solicitud se realiza correctamente, el servicio devuelve un archivo JSON con la información del trabajo, incluida la configuración de este, los errores devueltos y otros datos del trabajo, de la siguiente manera:

```
{
    "Job": {
        "Status": "ERROR",
        "Queue": "arn:aws:mediaconvert:region-name-1:012345678998:queues/Queue1",
        "Settings": {
            ...<truncated for brevity>...
        },
        "ErrorMessage": "Unable to open input file [s3://my-input-bucket/file-
name.mp4]: [Failed probe/open: [Failed to read data: AssumeRole failed]]",
        "ErrorCode": 1434,
        "Role": "arn:aws:iam::012345678998:role/MediaConvertServiceRole",
```

```
        "Arn": "arn:aws:mediaconvert:us-
west-1:012345678998:jobs/1234567890987-1ab2c3",
        "UserMetadata": {},
        "Timing": {
            "FinishTime": 1517442131,
            "SubmitTime": 1517442103,
            "StartTime": 1517442104
        },
        "Id": "1234567890987-1ab2c3",
        "CreatedAt": 1517442103
    }
}
```

Para obtener más información, consulte Trabajar con AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener más información sobre la API, consulte GetJob en la Referencia de comandos de la AWS CLI.

`get-preset`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-preset`.

AWS CLI

Para obtener detalles de un elemento preestablecido en particular

En el siguiente ejemplo de `get-preset`, se solicita la definición JSON del elemento preestablecido personalizado especificado.

```
aws mediaconvert get-preset \
    --name SimpleMP4 \
    --endpoint-url https://abcd1234.mediaconvert.us-west-2.amazonaws.com
```

Salida:

```
{
    "Preset": {
        "Description": "Creates basic MP4 file. No filtering or preproccessing.",
        "Arn": "arn:aws:mediaconvert:us-west-2:123456789012:presets/SimpleMP4",
        "LastUpdated": 1568843141,
        "Name": "SimpleMP4",
        "Settings": {
```

```
            "ContainerSettings": {
                "Mp4Settings": {
                    "FreeSpaceBox": "EXCLUDE",
                    "CslgAtom": "INCLUDE",
                    "MoovPlacement": "PROGRESSIVE_DOWNLOAD"
                },
                "Container": "MP4"
            },
            "AudioDescriptions": [
                {
                    "LanguageCodeControl": "FOLLOW_INPUT",
                    "AudioTypeControl": "FOLLOW_INPUT",
                    "CodecSettings": {
                        "AacSettings": {
                            "RawFormat": "NONE",
                            "CodecProfile": "LC",
                            "AudioDescriptionBroadcasterMix": "NORMAL",
                            "SampleRate": 48000,
                            "Bitrate": 96000,
                            "RateControlMode": "CBR",
                            "Specification": "MPEG4",
                            "CodingMode": "CODING_MODE_2_0"
                        },
                        "Codec": "AAC"
                    }
                }
            ],
            "VideoDescription": {
                "RespondToAfd": "NONE",
                "TimecodeInsertion": "DISABLED",
                "Sharpness": 50,
                "ColorMetadata": "INSERT",
                "CodecSettings": {
                    "H264Settings": {
                        "FramerateControl": "INITIALIZE_FROM_SOURCE",
                        "SpatialAdaptiveQuantization": "ENABLED",
                        "Softness": 0,
                        "Telecine": "NONE",
                        "CodecLevel": "AUTO",
                        "QualityTuningLevel": "SINGLE_PASS",
                        "UnregisteredSeiTimecode": "DISABLED",
                        "Slices": 1,
                        "Syntax": "DEFAULT",
                        "GopClosedCadence": 1,
```

```
                        "AdaptiveQuantization": "HIGH",
                        "EntropyEncoding": "CABAC",
                        "InterlaceMode": "PROGRESSIVE",
                        "ParControl": "INITIALIZE_FROM_SOURCE",
                        "NumberBFramesBetweenReferenceFrames": 2,
                        "GopSizeUnits": "FRAMES",
                        "RepeatPps": "DISABLED",
                        "CodecProfile": "MAIN",
                        "FieldEncoding": "PAFF",
                        "GopSize": 90.0,
                        "SlowPal": "DISABLED",
                        "SceneChangeDetect": "ENABLED",
                        "GopBReference": "DISABLED",
                        "RateControlMode": "CBR",
                        "FramerateConversionAlgorithm": "DUPLICATE_DROP",
                        "FlickerAdaptiveQuantization": "DISABLED",
                        "DynamicSubGop": "STATIC",
                        "MinIInterval": 0,
                        "TemporalAdaptiveQuantization": "ENABLED",
                        "Bitrate": 400000,
                        "NumberReferenceFrames": 3
                    },
                    "Codec": "H_264"
                },
                "AfdSignaling": "NONE",
                "AntiAlias": "ENABLED",
                "ScalingBehavior": "DEFAULT",
                "DropFrameTimecode": "ENABLED"
            }
        },
        "Type": "CUSTOM",
        "CreatedAt": 1568841521
    }
}
```

Para obtener más información, consulte Trabajar con elementos preestablecidos de salida de AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte GetPreset en la Referencia de comandos de AWS CLI.

`get-queue`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-queue`.

AWS CLI

Para obtener información de una cola

En el siguiente ejemplo de `get-queue`, se recuperan los detalles sobre la cola personalizada especificada.

```
aws mediaconvert get-queue \
    --name Customer1 \
    --endpoint-url https://abcd1234.mediaconvert.us-west-2.amazonaws.com
```

Salida:

```
{
    "Queue": {
        "LastUpdated": 1526428502,
        "Type": "CUSTOM",
        "SubmittedJobsCount": 0,
        "Status": "ACTIVE",
        "PricingPlan": "ON_DEMAND",
        "CreatedAt": 1526428502,
        "ProgressingJobsCount": 0,
        "Arn": "arn:aws:mediaconvert:us-west-2:123456789012:queues/Customer1",
        "Name": "Customer1"
    }
}
```

Para obtener más información, consulte Trabajar con colas en AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte GetQueue en la Referencia de comandos de la AWS CLI.

`list-job-templates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-job-templates`.

AWS CLI

Ejemplo 1: mostrar plantillas de trabajo personalizadas

En el siguiente ejemplo de `list-job-templates`, se muestran todas las plantillas de trabajos personalizadas de la región actual. Para ver una lista de las plantillas de trabajo del sistema, consulte el siguiente ejemplo.

```
aws mediaconvert list-job-templates \
    --endpoint-url https://abcd1234.mediaconvert.us-west-2.amazonaws.com
```

Salida:

```
{
    "JobTemplates": [
        {
            "Description": "Create a DASH streaming ABR stack",
            "Arn": "arn:aws:mediaconvert:us-west-2:123456789012:jobTemplates/DASH
 Streaming",
            "Name": "DASH Streaming",
            "LastUpdated": 1568653007,
            "Priority": 0,
            "Settings": {
                ...<truncatedforbrevity>...
            },
            "Type": "CUSTOM",
            "StatusUpdateInterval": "SECONDS_60",
            "CreatedAt": 1568653007
        },
        {
            "Description": "Create a high-res file",
            "Arn": "arn:aws:mediaconvert:us-west-2:123456789012:jobTemplates/File",
            "Name": "File",
            "LastUpdated": 1568653007,
            "Priority": 0,
            "Settings": {
                ...<truncatedforbrevity>...
            },
            "Type": "CUSTOM",
            "StatusUpdateInterval": "SECONDS_60",
            "CreatedAt": 1568653023
        }
    ]
```

```
}
```

Ejemplo 2: mostrar las plantillas de trabajo del sistema de MediaConvert

En el siguiente ejemplo de `list-job-templates`, se muestran todas las plantillas de trabajo del sistema.

```
aws mediaconvert list-job-templates \
    --endpoint-url https://abcd1234.mediaconvert.us-east-1.amazonaws.com \
    --list-by SYSTEM
```

Salida:

```
{
    "JobTemplates": [
        {
            "CreatedAt": 1568321779,
            "Arn": "arn:aws:mediaconvert:us-east-1:123456789012:jobTemplates/System-
Generic_Mp4_Hev1_Avc_Aac_Sdr_Qvbr",
            "Name": "System-Generic_Mp4_Hev1_Avc_Aac_Sdr_Qvbr",
            "Description": "GENERIC, MP4, AVC + HEV1(HEVC,SDR), AAC, SDR, QVBR",
            "Category": "GENERIC",
            "Settings": {
                "AdAvailOffset": 0,
                "OutputGroups": [
                    {
                        "Outputs": [
                            {
                                "Extension": "mp4",
                                "Preset": "System-
Generic_Hd_Mp4_Avc_Aac_16x9_Sdr_1280x720p_30Hz_5Mbps_Qvbr_Vq9",
                                "NameModifier":
 "_Generic_Hd_Mp4_Avc_Aac_16x9_Sdr_1280x720p_30Hz_5000Kbps_Qvbr_Vq9"
                            },
                            {
                                "Extension": "mp4",
                                "Preset": "System-
Generic_Hd_Mp4_Avc_Aac_16x9_Sdr_1920x1080p_30Hz_10Mbps_Qvbr_Vq9",
                                "NameModifier":
 "_Generic_Hd_Mp4_Avc_Aac_16x9_Sdr_1920x1080p_30Hz_10000Kbps_Qvbr_Vq9"
                            },
                            {
                                "Extension": "mp4",
```

```
                                "Preset": "System-
Generic_Sd_Mp4_Avc_Aac_16x9_Sdr_640x360p_30Hz_0.8Mbps_Qvbr_Vq7",
                                "NameModifier":
 "_Generic_Sd_Mp4_Avc_Aac_16x9_Sdr_640x360p_30Hz_800Kbps_Qvbr_Vq7"
                            },
                            {
                                "Extension": "mp4",
                                "Preset": "System-
Generic_Hd_Mp4_Hev1_Aac_16x9_Sdr_1280x720p_30Hz_4Mbps_Qvbr_Vq9",
                                "NameModifier":
 "_Generic_Hd_Mp4_Hev1_Aac_16x9_Sdr_1280x720p_30Hz_4000Kbps_Qvbr_Vq9"
                            },
                            {
                                "Extension": "mp4",
                                "Preset": "System-
Generic_Hd_Mp4_Hev1_Aac_16x9_Sdr_1920x1080p_30Hz_8Mbps_Qvbr_Vq9",
                                "NameModifier":
 "_Generic_Hd_Mp4_Hev1_Aac_16x9_Sdr_1920x1080p_30Hz_8000Kbps_Qvbr_Vq9"
                            },
                            {
                                "Extension": "mp4",
                                "Preset": "System-
Generic_Uhd_Mp4_Hev1_Aac_16x9_Sdr_3840x2160p_30Hz_12Mbps_Qvbr_Vq9",
                                "NameModifier":
 "_Generic_Uhd_Mp4_Hev1_Aac_16x9_Sdr_3840x2160p_30Hz_12000Kbps_Qvbr_Vq9"
                            }
                        ],
                        "OutputGroupSettings": {
                            "FileGroupSettings": {

                            },
                            "Type": "FILE_GROUP_SETTINGS"
                        },
                        "Name": "File Group"
                    }
                ]
            },
            "Type": "SYSTEM",
            "LastUpdated": 1568321779
        },
        ...<truncatedforbrevity>...
    ]
}
```

Para obtener más información, consulte Uso de plantillas de tarea de AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte ListJobTemplates en la Referencia de comandos de la AWS CLI.

`list-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-jobs`.

AWS CLI

Obtención de los detalles de todos los trabajos de una región

En el siguiente ejemplo se solicita la información de todos los trabajos de la región especificada.

```
aws mediaconvert list-jobs \
    --endpoint-url https://abcd1234.mediaconvert.region-name-1.amazonaws.com \
    --region region-name-1
```

Para obtener el punto de conexión específico de su cuenta, utilice `describe-endpoints` o envíe el comando sin el punto de conexión. El servicio devuelve un error y su punto de conexión.

Para obtener más información, consulte Trabajar con AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte ListJobs en la Referencia de comandos de la AWS CLI.

`list-presets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-presets`.

AWS CLI

Ejemplo 1: mostrar los elementos preestablecidos de salida personalizados

En el siguiente ejemplo de `list-presets`, se muestran los elementos preestablecidos de salida personalizados. Para ver una lista de los elementos preestablecidos del sistema, consulte el siguiente ejemplo.

```
aws mediaconvert list-presets \
    --endpoint-url https://abcd1234.mediaconvert.us-west-2.amazonaws.com
```

Salida:

```
{
    "Presets": [
        {
            "Name": "SimpleMP4",
            "CreatedAt": 1568841521,
            "Settings": {
                ......
            },
            "Arn": "arn:aws:mediaconvert:us-east-1:003235472598:presets/SimpleMP4",
            "Type": "CUSTOM",
            "LastUpdated": 1568843141,
            "Description": "Creates basic MP4 file. No filtering or preproccessing."
        },
        {
            "Name": "SimpleTS",
            "CreatedAt": 1568843113,
            "Settings": {
                ... truncated for brevity ...
            },
            "Arn": "arn:aws:mediaconvert:us-east-1:003235472598:presets/SimpleTS",
            "Type": "CUSTOM",
            "LastUpdated": 1568843113,
            "Description": "Create a basic transport stream."
        }
    ]
}
```

Ejemplo 2: mostrar los elementos preestablecidos de salida del sistema

El siguiente ejemplo de `list-presets` muestra los elementos preestablecidos disponibles del sistema de MediaConvert. Para ver una lista de los elementos preestablecidos personalizados, consulte el ejemplo anterior.

```
aws mediaconvert list-presets \
    --list-by SYSTEM \
    --endpoint-url https://abcd1234.mediaconvert.us-west-2.amazonaws.com
```

Salida:

```
{
    "Presets": [
        {
            "Arn": "arn:aws:mediaconvert:us-west-2:123456789012:presets/System-
Avc_16x9_1080p_29_97fps_8500kbps",
            "Name": "System-Avc_16x9_1080p_29_97fps_8500kbps",
            "CreatedAt": 1568321789,
            "Description": "Wifi, 1920x1080, 16:9, 29.97fps, 8500kbps",
            "LastUpdated": 1568321789,
            "Type": "SYSTEM",
            "Category": "HLS",
            "Settings": {
            ...<output settings removed for brevity>...
            }
        },

        ...<list of presets shortened for brevity>...

        {
            "Arn": "arn:aws:mediaconvert:us-east-1:123456789012:presets/System-
Xdcam_HD_1080i_29_97fps_35mpbs",
            "Name": "System-Xdcam_HD_1080i_29_97fps_35mpbs",
            "CreatedAt": 1568321790,
            "Description": "XDCAM MPEG HD, 1920x1080i, 29.97fps, 35mbps",
            "LastUpdated": 1568321790,
            "Type": "SYSTEM",
            "Category": "MXF",
            "Settings": {
            ...<output settings removed for brevity>...
            }
        }
    ]
}
```

Para obtener más información, consulte Trabajar con elementos preestablecidos de salida de AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte ListPresets en la Referencia de comandos de la AWS CLI.

`list-queues`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-queues`.

AWS CLI

Para mostrar colas

En el siguiente ejemplo de `list-queues`, se muestran todas las colas de MediaConvert.

```
aws mediaconvert list-queues \
    --endpoint-url https://abcd1234.mediaconvert.us-west-2.amazonaws.com
```

Salida:

```
{
    "Queues": [
        {
            "PricingPlan": "ON_DEMAND",
            "Type": "SYSTEM",
            "Status": "ACTIVE",
            "CreatedAt": 1503451595,
            "Name": "Default",
            "SubmittedJobsCount": 0,
            "ProgressingJobsCount": 0,
            "Arn": "arn:aws:mediaconvert:us-west-2:123456789012:queues/Default",
            "LastUpdated": 1534549158
        },
        {
            "PricingPlan": "ON_DEMAND",
            "Type": "CUSTOM",
            "Status": "ACTIVE",
            "CreatedAt": 1537460025,
            "Name": "Customer1",
            "SubmittedJobsCount": 0,
            "Description": "Jobs we run for our cusotmer.",
            "ProgressingJobsCount": 0,
            "Arn": "arn:aws:mediaconvert:us-west-2:123456789012:queues/Customer1",
            "LastUpdated": 1537460025
        },
        {
            "ProgressingJobsCount": 0,
            "Status": "ACTIVE",
            "Name": "transcode-library",
```

```
            "SubmittedJobsCount": 0,
            "LastUpdated": 1564066204,
            "ReservationPlan": {
                "Status": "ACTIVE",
                "ReservedSlots": 1,
                "PurchasedAt": 1564066203,
                "Commitment": "ONE_YEAR",
                "ExpiresAt": 1595688603,
                "RenewalType": "EXPIRE"
            },
            "PricingPlan": "RESERVED",
            "Arn": "arn:aws:mediaconvert:us-west-2:123456789012:queues/transcode-
library",
            "Type": "CUSTOM",
            "CreatedAt": 1564066204
        }
    ]
}
```

Para obtener más información, consulte Trabajar con colas en AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte ListQueues en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para mostrar las etiquetas de una cola, plantilla de trabajo o elemento preestablecido de salida de MediaConvert

En el siguiente ejemplo de `list-tags-for-resource`, se muestran las etiquetas del elemento preestablecido de salida especificado.

```
aws mediaconvert list-tags-for-resource \
    --arn arn:aws:mediaconvert:us-west-2:123456789012:presets/SimpleMP4 \
    --endpoint-url https://abcd1234.mediaconvert.us-west-2.amazonaws.com
```

Salida:

```
{
    "ResourceTags": {
        "Tags": {
            "customer": "zippyVideo"
        },
        "Arn": "arn:aws:mediaconvert:us-west-2:123456789012:presets/SimpleMP4"
    }
}
```

Para obtener más información, consulte Etiquetado de recursos de AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`update-job-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-job-template`.

AWS CLI

Para cambiar una plantilla de trabajo

En el siguiente ejemplo de `update-job-template`, se reemplaza la definición de JSON de la plantilla de trabajo personalizada especificada por la definición de JSON del archivo proporcionado.

aws mediaconvert update-job-template --name File1 --endpoint-url https://abcd1234.mediaconvert.us-west-2.amazonaws.com --cli-input-json file://~/job-template-update.json

Contenido de `job-template-update.json`:

```
{
    "Description": "A simple job template that generates a single file output.",
    "Queue": "arn:aws:mediaconvert:us-east-1:012345678998:queues/Default",
    "Name": "SimpleFile",
    "Settings": {
      "OutputGroups": [
        {
          "Name": "File Group",
          "Outputs": [
```

```
            {
              "ContainerSettings": {
                "Container": "MP4",
                "Mp4Settings": {
                  "CslgAtom": "INCLUDE",
                  "FreeSpaceBox": "EXCLUDE",
                  "MoovPlacement": "PROGRESSIVE_DOWNLOAD"
                }
              },
              "VideoDescription": {
                "ScalingBehavior": "DEFAULT",
                "TimecodeInsertion": "DISABLED",
                "AntiAlias": "ENABLED",
                "Sharpness": 50,
                "CodecSettings": {
                  "Codec": "H_264",
                  "H264Settings": {
                    "InterlaceMode": "PROGRESSIVE",
                    "NumberReferenceFrames": 3,
                    "Syntax": "DEFAULT",
                    "Softness": 0,
                    "GopClosedCadence": 1,
                    "GopSize": 90,
                    "Slices": 1,
                    "GopBReference": "DISABLED",
                    "SlowPal": "DISABLED",
                    "SpatialAdaptiveQuantization": "ENABLED",
                    "TemporalAdaptiveQuantization": "ENABLED",
                    "FlickerAdaptiveQuantization": "DISABLED",
                    "EntropyEncoding": "CABAC",
                    "Bitrate": 400000,
                    "FramerateControl": "INITIALIZE_FROM_SOURCE",
                    "RateControlMode": "CBR",
                    "CodecProfile": "MAIN",
                    "Telecine": "NONE",
                    "MinIInterval": 0,
                    "AdaptiveQuantization": "HIGH",
                    "CodecLevel": "AUTO",
                    "FieldEncoding": "PAFF",
                    "SceneChangeDetect": "ENABLED",
                    "QualityTuningLevel": "SINGLE_PASS",
                    "FramerateConversionAlgorithm": "DUPLICATE_DROP",
                    "UnregisteredSeiTimecode": "DISABLED",
                    "GopSizeUnits": "FRAMES",
```

```
                    "ParControl": "INITIALIZE_FROM_SOURCE",
                    "NumberBFramesBetweenReferenceFrames": 2,
                    "RepeatPps": "DISABLED",
                    "DynamicSubGop": "STATIC"
                  }
                },
                "AfdSignaling": "NONE",
                "DropFrameTimecode": "ENABLED",
                "RespondToAfd": "NONE",
                "ColorMetadata": "INSERT"
              },
              "AudioDescriptions": [
                {
                  "AudioTypeControl": "FOLLOW_INPUT",
                  "CodecSettings": {
                    "Codec": "AAC",
                    "AacSettings": {
                      "AudioDescriptionBroadcasterMix": "NORMAL",
                      "Bitrate": 96000,
                      "RateControlMode": "CBR",
                      "CodecProfile": "LC",
                      "CodingMode": "CODING_MODE_2_0",
                      "RawFormat": "NONE",
                      "SampleRate": 48000,
                      "Specification": "MPEG4"
                    }
                  },
                  "LanguageCodeControl": "FOLLOW_INPUT"
                }
              ]
            }
          ],
          "OutputGroupSettings": {
            "Type": "FILE_GROUP_SETTINGS",
            "FileGroupSettings": {}
          }
        }
      ],
      "AdAvailOffset": 0
    },
    "StatusUpdateInterval": "SECONDS_60",
    "Priority": 0
}
```

El sistema devuelve la carga útil de JSON que usted envía con la solicitud, incluso si la solicitud produce un error. Por tanto, el JSON devuelto no es necesariamente la nueva definición de la plantilla de trabajo.

Dado que la carga útil de JSON puede ser larga, es posible que tenga que desplazarse hacia arriba para ver los mensajes de error.

Para obtener más información, consulte Uso de plantillas de tarea de AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte UpdateJobTemplate en la Referencia de comandos de la AWS CLI.

`update-preset`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-preset`.

AWS CLI

Para cambiar un elemento preestablecido

En el siguiente ejemplo de `update-preset`, se reemplaza la descripción del elemento preestablecido especificado.

```
aws mediaconvert update-preset \
--name Customer1 \
--description "New description text."
--endpoint-url https://abcd1234.mediaconvert.us-west-2.amazonaws.com
```

Este comando no genera ninguna salida. Salida:

```
{
    "Preset": {
        "Arn": "arn:aws:mediaconvert:us-east-1:003235472598:presets/SimpleMP4",
        "Settings": {
        ...<output settings removed for brevity>...
        },
        "Type": "CUSTOM",
        "LastUpdated": 1568938411,
        "Description": "New description text.",
        "Name": "SimpleMP4",
```

```
        "CreatedAt": 1568938240
    }
}
```

Para obtener más información, consulte Trabajar con elementos preestablecidos de salida de AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte UpdatePreset en la Referencia de comandos de la AWS CLI.

`update-queue`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-queue`.

AWS CLI

Para cambiar una cola

En el siguiente ejemplo de `update-queue`, se pausa la cola especificada, cambiando su estado a PAUSED.

```
aws mediaconvert update-queue \
--name Customer1 \
--status PAUSED
--endpoint-url https://abcd1234.mediaconvert.us-west-2.amazonaws.com
```

Salida:

```
{
    "Queue": {
        "LastUpdated": 1568839845,
        "Status": "PAUSED",
        "ProgressingJobsCount": 0,
        "CreatedAt": 1526428516,
        "Arn": "arn:aws:mediaconvert:us-west-1:123456789012:queues/Customer1",
        "Name": "Customer1",
        "SubmittedJobsCount": 0,
        "PricingPlan": "ON_DEMAND",
        "Type": "CUSTOM"
    }
}
```

Para obtener más información, consulte Trabajar con colas en AWS Elemental MediaConvert en la Guía del usuario de AWS Elemental MediaConvert.

- Para obtener información sobre la API, consulte UpdateQueue en la Referencia de comandos de la AWS CLI.

Ejemplos de MediaLive que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo ejecutar acciones e implementar escenarios comunes usando AWS Command Line Interface con MediaLive.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-channel`.

AWS CLI

Para crear un canal

En el siguiente ejemplo de `create-channel`, se crea un canal pasando un archivo JSON que contiene los parámetros que desea especificar.

El canal de este ejemplo ingiere una entrada HLS PULL que se conecta a un origen que contiene vídeo, audio y subtítulos incrustados. El canal crea un grupo de salida HLS con un servidor de Akamai como destino. El grupo de salida contiene dos salidas: una para el vídeo H.265 y el audio AAC, y otra para los subtítulos Web-VTT, solo en inglés.

El JSON de este canal de ejemplo incluye los parámetros mínimos necesarios para un canal que utilice una entrada HLS PULL y que genere un grupo de salidas HLS con Akamai como destino. El JSON contiene las siguientes secciones principales:

`InputAttachments`, que especifica un origen para el audio y un origen para los subtítulos. No especifica un selector de vídeo, lo que significa que MediaLive extrae el primer vídeo que encuentra en el origen. `Destinations`, que contiene las dos direcciones IP (URL) del único grupo de salida de este canal. Estas direcciones requieren contraseñas. `EncoderSettings`, que contiene subsecciones. `AudioDescriptions`, que especifica que el canal contiene un activo de salida de audio, que utiliza el origen de InputAttachments y produce audio en formato AAC. `CaptionDescriptions`, que especifica que el canal contiene un activo de salida de subtítulos, que utiliza el origen de InputAttachments y produce subtítulos en formato Web-VTT. `VideoDescriptions`, que especifica que el canal contiene un activo de salida de vídeo con la resolución especificada. `OutputGroups`, que especifica los grupos de salida. En este ejemplo hay un grupo llamado `Akamai`. La conexión se realiza mediante HLS PUT. El grupo de salida contiene dos salidas. Una salida es para el activo de vídeo (llamado `Video_high`) y el activo de audio (llamado `Audio_EN`). Una salida es para el activo de subtítulos (llamado `WebVTT_EN`).

En este ejemplo, algunos de los parámetros no contienen ningún valor o contienen parámetros vacíos anidados. Por ejemplo, OutputSettings para la salida `Video_and_audio` contiene varios parámetros anidados que terminan en un parámetro vacío M3u8Settings. Este parámetro debe estar incluido, pero puede omitir uno, varios o todos sus elementos secundarios, lo que significa que el elemento secundario tomará su valor predeterminado o será nulo.

Todos los parámetros que se apliquen a este canal de ejemplo pero que no estén especificados en este archivo tomarán el valor predeterminado, se establecerán en nulo o tomarán un valor único generado por MediaLive.

```
aws medialive create-channel \
    --cli-input-json file://channel-in-hls-out-hls-akamai.json
```

Contenido de `channel-in-hls-out-hls-akamai.json`:

```
{
    "Name": "News_West",
    "RoleArn": "arn:aws:iam::111122223333:role/MediaLiveAccessRole",
    "InputAttachments": [
        {
            "InputAttachmentName": "local_news",
```

```
            "InputId": "1234567",
            "InputSettings": {
                "AudioSelectors": [
                    {
                        "Name": "English-Audio",
                        "SelectorSettings": {
                            "AudioLanguageSelection": {
                                "LanguageCode": "EN"
                            }
                        }
                    }
                ],
                "CaptionSelectors": [
                    {
                        "LanguageCode": "ENE",
                        "Name": "English_embedded"
                    }
                ]
            }
        }
    ],
    "Destinations": [
        {
            "Id": "akamai-server-west",
            "Settings": [
                {
                    "PasswordParam": "/medialive/examplecorp1",
                    "Url": "http://203.0.113.55/news/news_west",
                    "Username": "examplecorp"
                },
                {
                    "PasswordParam": "/medialive/examplecorp2",
                    "Url": "http://203.0.113.82/news/news_west",
                    "Username": "examplecorp"
                }
            ]
        }
    ],
    "EncoderSettings": {
        "AudioDescriptions": [
            {
                "AudioSelectorName": "English-Audio",
                "CodecSettings": {
                    "AacSettings": {}
```

```
                },
                "Name": "Audio_EN"
            }
        ],
        "CaptionDescriptions": [
            {
                "CaptionSelectorName": "English_embedded",
                "DestinationSettings": {
                    "WebvttDestinationSettings": {}
                },
                "Name": "WebVTT_EN"
            }
        ],
        "VideoDescriptions": [
            {
                "Height": 720,
                "Name": "Video_high",
                "Width": 1280
            }
        ],
        "OutputGroups": [
            {
                "Name": "Akamai",
                "OutputGroupSettings": {
                    "HlsGroupSettings": {
                        "Destination": {
                            "DestinationRefId": "akamai-server-west"
                        },
                        "HlsCdnSettings": {
                            "HlsBasicPutSettings": {}
                        }
                    }
                },
                "Outputs": [
                    {
                        "AudioDescriptionNames": [
                            "Audio_EN"
                        ],
                        "OutputName": "Video_and_audio",
                        "OutputSettings": {
                            "HlsOutputSettings": {
                                "HlsSettings": {
                                    "StandardHlsSettings": {
                                        "M3u8Settings": {}
```

```
                                    }
                                },
                                "NameModifier": "_1"
                            }
                        },
                        "VideoDescriptionName": "Video_high"
                    },
                    {
                        "CaptionDescriptionNames": [
                            "WebVTT_EN"
                        ],
                        "OutputName": "Captions-WebVTT",
                        "OutputSettings": {
                            "HlsOutputSettings": {
                                "HlsSettings": {
                                    "StandardHlsSettings": {
                                        "M3u8Settings": {}
                                    }
                                },
                                "NameModifier": "_2"
                            }
                        }
                    }
                ]
            }
        ],
        "TimecodeConfig": {
            "Source": "EMBEDDED"
        }
    }
}
```

Salida:

La salida repite el contenido del archivo JSON más los valores siguientes. Todos los parámetros están ordenados alfabéticamente.

ARN para el canal. La última parte del ARN es el ID de canal único. `EgressEndpoints` está en blanco en este canal de ejemplo porque solo se usa para entradas PUSH. Cuando se aplica, muestra las direcciones de MediaLive a las que se envía el contenido.`OutputGroups`, `Outputs`. Muestran todos los parámetros del grupo de salida y las salidas, incluidos las que no incluyó pero que son relevantes para este canal. Es posible que los parámetros estén vacíos (lo que podría indicar que el parámetro o la característica están deshabilitados en esta configuración de

canal) o pueden mostrar el valor predeterminado que se aplicará. `LogLevel` está establecido en el valor predeterminado (DISABLED). `Tags` está establecido en el valor predeterminado (null). `PipelinesRunningCount` y `State` muestran el estado actual del canal.

Para obtener más información, consulte Creación de un canal desde cero en la Guía del usuario de AWS Elemental MediaLive.

- Para obtener información sobre la API, consulte CreateChannel en la Referencia de comandos de la AWS CLI.

`create-input`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-input`.

AWS CLI

Para crear una entrada

En el siguiente ejemplo de `create-input`, se crea una entrada `HLS PULL` pasando un archivo JSON que contiene los parámetros que se aplican a este tipo de entrada. El JSON de esta entrada de ejemplo especifica dos orígenes (direcciones) para la entrada, a fin de admitir la redundancia en la ingesta. Estas direcciones requieren contraseña.

```
aws medialive create-input \
    --cli-input-json file://input-hls-pull-news.json
```

Contenido de `input-hls-pull-news.json`:

```
{
    "Name": "local_news",
    "RequestId": "cli000059",
    "Sources": [
            {
                    "Url": "https://203.0.113.13/newschannel/anytownusa.m3u8",
                    "Username": "examplecorp",
                    "PasswordParam": "/medialive/examplecorp1"
            },
       {
                    "Url": "https://198.51.100.54/fillervideos/oceanwaves.mp4",
                    "Username": "examplecorp",
                    "PasswordParam": "examplecorp2"
```

```
            }
    ],
    "Type": "URL_PULL"
}
```

Salida:

La salida repite el contenido del archivo JSON más los valores siguientes. Todos los parámetros están ordenados alfabéticamente.

`Arn` para la entrada. La última parte del ARN es el ID de entrada único. `Attached Channels`, que siempre está vacío para una entrada recién creada. `Destinations`, que está vacío en este ejemplo porque solo se usa con una entrada PUSH. `Id` para la entrada, igual que el ID del ARN. `MediaConnectFlows`, que está vacío en este ejemplo porque solo se usa con una entrada de tipo MediaConnect. `SecurityGroups`, que está vacío en este ejemplo porque solo se usa con una entrada PUSH. `State` de esta entrada. `Tags`, que está vacío (el valor predeterminado para este parámetro).

Para obtener más información, consulte Creating an Input en la Guía del usuario de AWS Elemental MediaLive.

- Para obtener más información sobre la API, consulte CreateInput en la Referencia de comandos de la AWS CLI.

Ejemplos de MediaPackage que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios habituales mediante el AWS Command Line Interface con MediaPackage.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-channel`.

AWS CLI

Para crear un canal

El siguiente comando `create-channel` crea un canal llamado `sportschannel` en la cuenta actual.

```
aws mediapackage create-channel --id sportschannel
```

Salida:

```
{
   "Arn": "arn:aws:mediapackage:us-
west-2:111222333:channels/6d345804ec3f46c9b454a91d4a80d0e0",
   "HlsIngest": {
        "IngestEndpoints": [
            {
                "Id": "6d345804ec3f46c9b454a91d4a80d0e0",
                "Password": "generatedwebdavpassword1",
                "Url": "https://f31c86aed53b815a.mediapackage.us-
west-2.amazonaws.com/in/
v2/6d345804ec3f46c9b454a91d4a80d0e0/6d345804ec3f46c9b454a91d4a80d0e0/channel",
                "Username": "generatedwebdavusername1"
            },
            {
                "Id": "2daa32878af24803b24183727211b8ff",
                "Password": "generatedwebdavpassword2",
                "Url": "https://6ebbe7e04c4b0afa.mediapackage.us-
west-2.amazonaws.com/in/
v2/6d345804ec3f46c9b454a91d4a80d0e0/2daa32878af24803b24183727211b8ff/channel",
                "Username": "generatedwebdavusername2"
            }
        ]
    },
    "Id": "sportschannel",
    "Tags": {
        "region": "west"
```

```
    }
}
```

Para obtener más información, consulte Creating a Channel en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte CreateChannel en la Referencia de comandos de la AWS CLI.

`create-origin-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-origin-endpoint`.

AWS CLI

Para crear un punto de conexión de origen

El siguiente comando `create-origin-endpoint` crea un punto de conexión de origen llamado `cmafsports` con la configuración del paquete proporcionada en un archivo JSON y la configuración de punto de conexión especificada.

```
aws mediapackage create-origin-endpoint \
    --channel-id sportschannel \
    --id cmafsports \
    --cmaf-package file://file/path/cmafpkg.json --description "cmaf output of
 sports" \
    --id cmaf_sports \
    --manifest-name sports_channel \
    --startover-window-seconds 300 \
    --tags region=west,media=sports \
    --time-delay-seconds 10
```

Salida:

```
{
    "Arn": "arn:aws:mediapackage:us-
west-2:111222333:origin_endpoints/1dc6718be36f4f34bb9cd86bc50925e6",
    "ChannelId": "sportschannel",
    "CmafPackage": {
        "HlsManifests": [
            {
```

```
                "AdMarkers": "PASSTHROUGH",
                "Id": "cmaf_sports_endpoint",
                "IncludeIframeOnlyStream": true,
                "ManifestName": "index",
                "PlaylistType": "EVENT",
                "PlaylistWindowSeconds": 300,
                "ProgramDateTimeIntervalSeconds": 300,
                "Url": "https://c4af3793bf76b33c.mediapackage.us-
west-2.amazonaws.com/out/v1/1dc6718be36f4f34bb9cd86bc50925e6/cmaf_sports_endpoint/
index.m3u8"
            }
        ],
        "SegmentDurationSeconds": 2,
        "SegmentPrefix": "sportschannel"
    },
    "Description": "cmaf output of sports",
    "Id": "cmaf_sports",
    "ManifestName": "sports_channel",
    "StartoverWindowSeconds": 300,
    "Tags": {
        "region": "west",
        "media": "sports"
    },
    "TimeDelaySeconds": 10,
    "Url": "",
    "Whitelist": []
}
```

Para obtener más información, consulte Creating an Endpoint en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte CreateOriginEndpoint en la Referencia de comandos de la AWS CLI.

`delete-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-channel`.

AWS CLI

Para eliminar un canal

El siguiente comando `delete-channel` elimina el canal llamado `test`.

```
aws mediapackage delete-channel \
    --id test
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting a Channel en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte DeleteChannel en la Referencia de comandos de la AWS CLI.

`delete-origin-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-origin-endpoint`.

AWS CLI

Para eliminar un punto de conexión de origen

El siguiente comando `delete-origin-endpoint` elimina el punto de conexión de origen llamado `tester2`.

```
aws mediapackage delete-origin-endpoint \
    --id tester2
```

Para obtener más información, consulte Deleting an Endpoint en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte DeleteOriginEndpoint en la Referencia de comandos de la AWS CLI.

`describe-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-channel`.

AWS CLI

Para describir un canal

El siguiente comando `describe-channel` muestra todos los detalles del canal llamado `test`.

```
aws mediapackage describe-channel \
    --id test
```

Salida:

```
{
    "Arn": "arn:aws:mediapackage:us-
west-2:111222333:channels/584797f1740548c389a273585dd22a63",
    "HlsIngest": {
        "IngestEndpoints": [
            {
                "Id": "584797f1740548c389a273585dd22a63",
                "Password": "webdavgeneratedpassword1",
                "Url": "https://9be9c4405c474882.mediapackage.us-
west-2.amazonaws.com/in/
v2/584797f1740548c389a273585dd22a63/584797f1740548c389a273585dd22a63/channel",
                "Username": "webdavgeneratedusername1"
            },
            {
                "Id": "7d187c8616fd455f88aaa5a9fcf74442",
                "Password": "webdavgeneratedpassword2",
                "Url": "https://7bf454c57220328d.mediapackage.us-
west-2.amazonaws.com/in/
v2/584797f1740548c389a273585dd22a63/7d187c8616fd455f88aaa5a9fcf74442/channel",
                "Username": "webdavgeneratedusername2"
            }
        ]
    },
    "Id": "test",
    "Tags": {}
}
```

Para obtener más información, consulte Viewing Channel Details<https://docs.aws.amazon.com/mediapackage/latest/ug/channels-view.html> en la Guía del usuario de AWS Elemental MediaPackage

- Para obtener información sobre la API, consulte DescribeChannel en la Referencia de comandos de la AWS CLI.

`describe-origin-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-origin-endpoint`.

AWS CLI

Para describir un punto de conexión de origen

El siguiente comando `describe-origin-endpoint` muestra todos los detalles del punto de conexión de origen llamado `cmaf_sports`.

```
aws mediapackage describe-origin-endpoint \
    --id cmaf_sports
```

Salida:

```
{
    "Arn": "arn:aws:mediapackage:us-
west-2:111222333:origin_endpoints/1dc6718be36f4f34bb9cd86bc50925e6",
    "ChannelId": "sportschannel",
    "CmafPackage": {
        "HlsManifests": [
            {
                "AdMarkers": "NONE",
                "Id": "cmaf_sports_endpoint",
                "IncludeIframeOnlyStream": false,
                "PlaylistType": "EVENT",
                "PlaylistWindowSeconds": 60,
                "ProgramDateTimeIntervalSeconds": 0,
                "Url": "https://c4af3793bf76b33c.mediapackage.us-
west-2.amazonaws.com/out/v1/1dc6718be36f4f34bb9cd86bc50925e6/cmaf_sports_endpoint/
index.m3u8"
            }
        ],
        "SegmentDurationSeconds": 2,
        "SegmentPrefix": "sportschannel"
    },
    "Id": "cmaf_sports",
    "ManifestName": "index",
    "StartoverWindowSeconds": 0,
    "Tags": {
        "region": "west",
        "media": "sports"
    },
    "TimeDelaySeconds": 0,
    "Url": "",
    "Whitelist": []
```

```
}
```

Para obtener más información, consulte Viewing a Single Endpoint en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte DescribeOriginEndpoint en la Referencia de comandos de la AWS CLI.

`list-channels`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-channels`.

AWS CLI

Creación de una lista de todos los canales

El siguiente comando `list-channels` muestra todos los canales que están configurados en la cuenta de AWS actual.

```
aws mediapackage list-channels
```

Salida:

```
{
    "Channels": [
        {
            "Arn": "arn:aws:mediapackage:us-
west-2:111222333:channels/584797f1740548c389a273585dd22a63",
            "HlsIngest": {
                "IngestEndpoints": [
                    {
                        "Id": "584797f1740548c389a273585dd22a63",
                        "Password": "webdavgeneratedpassword1",
                        "Url": "https://9be9c4405c474882.mediapackage.us-
west-2.amazonaws.com/in/
v2/584797f1740548c389a273585dd22a63/584797f1740548c389a273585dd22a63/channel",
                        "Username": "webdavgeneratedusername1"
                    },
                    {
                        "Id": "7d187c8616fd455f88aaa5a9fcf74442",
                        "Password": "webdavgeneratedpassword2",
```

```
                        "Url": "https://7bf454c57220328d.mediapackage.us-
west-2.amazonaws.com/in/
v2/584797f1740548c389a273585dd22a63/7d187c8616fd455f88aaa5a9fcf74442/channel",
                        "Username": "webdavgeneratedusername2"
                    }
                ]
            },
            "Id": "test",
            "Tags": {}
        }
    ]
}
```

Para obtener más información, consulte Viewing Channel Details en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte ListChannels en la Referencia de comandos de la AWS CLI.

`list-origin-endpoints`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-origin-endpoints`.

AWS CLI

Creación de una lista de todos los puntos de conexión de origen de un canal

El siguiente comando `list-origin-endpoints` muestra todos los puntos de conexión de origen que están configurados en el canal denominado `test`.

```
aws mediapackage list-origin-endpoints \
    --channel-id test
```

Salida:

```
{
    "OriginEndpoints": [
        {
            "Arn": "arn:aws:mediapackage:us-
west-2:111222333:origin_endpoints/247cff871f2845d3805129be22f2c0a2",
            "ChannelId": "test",
            "DashPackage": {
                "ManifestLayout": "FULL",
```

```
                "ManifestWindowSeconds": 60,
                "MinBufferTimeSeconds": 30,
                "MinUpdatePeriodSeconds": 15,
                "PeriodTriggers": [],
                "Profile": "NONE",
                "SegmentDurationSeconds": 2,
                "SegmentTemplateFormat": "NUMBER_WITH_TIMELINE",
                "StreamSelection": {
                    "MaxVideoBitsPerSecond": 2147483647,
                    "MinVideoBitsPerSecond": 0,
                    "StreamOrder": "ORIGINAL"
                },
                "SuggestedPresentationDelaySeconds": 25
            },
            "Id": "tester2",
            "ManifestName": "index",
            "StartoverWindowSeconds": 0,
            "Tags": {},
            "TimeDelaySeconds": 0,
            "Url": "https://8343f7014c0ea438.mediapackage.us-west-2.amazonaws.com/
out/v1/247cff871f2845d3805129be22f2c0a2/index.mpd",
            "Whitelist": []
        },
        {
            "Arn": "arn:aws:mediapackage:us-
west-2:111222333:origin_endpoints/869e237f851549e9bcf10e3bc2830839",
            "ChannelId": "test",
            "HlsPackage": {
                "AdMarkers": "NONE",
                "IncludeIframeOnlyStream": false,
                "PlaylistType": "EVENT",
                "PlaylistWindowSeconds": 60,
                "ProgramDateTimeIntervalSeconds": 0,
                "SegmentDurationSeconds": 6,
                "StreamSelection": {
                    "MaxVideoBitsPerSecond": 2147483647,
                    "MinVideoBitsPerSecond": 0,
                    "StreamOrder": "ORIGINAL"
                },
                "UseAudioRenditionGroup": false
            },
            "Id": "tester",
            "ManifestName": "index",
            "StartoverWindowSeconds": 0,
```

```
            "Tags": {},
            "TimeDelaySeconds": 0,
            "Url": "https://8343f7014c0ea438.mediapackage.us-west-2.amazonaws.com/
out/v1/869e237f851549e9bcf10e3bc2830839/index.m3u8",
            "Whitelist": []
        }
    ]
}
```

Para obtener más información, consulte Viewing all Endpoints Associated with a Channel en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte ListOriginEndpoints en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas asignadas a un recurso

El siguiente comando `list-tags-for-resource` enumera todas las etiquetas asignadas al recurso especificado.

```
aws mediapackage list-tags-for-resource \
    --resource-arn arn:aws:mediapackage:us-
west-2:111222333:channels/6d345804ec3f46c9b454a91d4a80d0e0
```

Salida:

```
{
    "Tags": {
        "region": "west"
    }
}
```

Para obtener más información, consulte Tagging Resources in AWS Elemental MediaPackage en la Guía del usuario de AWS Elemental MediaPackage.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`rotate-ingest-endpoint-credentials`

En el siguiente ejemplo de código, se muestra cómo utilizar `rotate-ingest-endpoint-credentials`.

AWS CLI

Para rotar las credenciales de ingesta

El siguiente comando `rotate-ingest-endpoint-credentials` rota el nombre de usuario y la contraseña de WebDAV para el punto de conexión de ingesta especificado.

```
aws mediapackage rotate-ingest-endpoint-credentials \
    --id test \
    --ingest-endpoint-id 584797f1740548c389a273585dd22a63
```

Salida:

```
{
    "Arn": "arn:aws:mediapackage:us-
west-2:111222333:channels/584797f1740548c389a273585dd22a63",
    "HlsIngest": {
        "IngestEndpoints": [
            {
                "Id": "584797f1740548c389a273585dd22a63",
                "Password": "webdavregeneratedpassword1",
                "Url": "https://9be9c4405c474882.mediapackage.us-
west-2.amazonaws.com/in/
v2/584797f1740548c389a273585dd22a63/584797f1740548c389a273585dd22a63/channel",
                "Username": "webdavregeneratedusername1"
            },
            {
                "Id": "7d187c8616fd455f88aaa5a9fcf74442",
                "Password": "webdavgeneratedpassword2",
                "Url": "https://7bf454c57220328d.mediapackage.us-
west-2.amazonaws.com/in/
v2/584797f1740548c389a273585dd22a63/7d187c8616fd455f88aaa5a9fcf74442/channel",
                "Username": "webdavgeneratedusername2"
```

```
            }
        ]
    },
    "Id": "test",
    "Tags": {}
}
```

Para obtener más información, consulte Rotating Credentials on an Input URL en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener más información sobre la API, consulte RotateIngestEndpointCredentials en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Cómo añadir una etiqueta a un recurso

Los siguientes comandos `tag-resource` agregan un par de clave y valor `region=west` al recurso especificado.

```
aws mediapackage tag-resource \
    --resource-arn arn:aws:mediapackage:us-
west-2:111222333:channels/6d345804ec3f46c9b454a91d4a80d0e0 \
    --tags region=west
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging Resources in AWS Elemental MediaPackage en la Guía del usuario de AWS Elemental MediaPackage.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar una etiqueta de un recurso

El siguiente comando `untag-resource` elimina la etiqueta con la clave `region` del canal especificado.

```
aws mediapackage untag-resource \
    --resource-arn arn:aws:mediapackage:us-
west-2:111222333:channels/6d345804ec3f46c9b454a91d4a80d0e0 \
    --tag-keys region
```

Para obtener más información, consulte Tagging Resources in AWS Elemental MediaPackage en la Guía del usuario de AWS Elemental MediaPackage.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-channel`.

AWS CLI

Para actualizar un canal

El siguiente comando `update-channel` actualiza el canal llamado `sportschannel` para incluir la descripción `24x7 sports`.

```
aws mediapackage update-channel \
    --id sportschannel \
    --description "24x7 sports"
```

Salida:

```
{
    "Arn": "arn:aws:mediapackage:us-
west-2:111222333:channels/6d345804ec3f46c9b454a91d4a80d0e0",
    "Description": "24x7 sports",
    "HlsIngest": {
```

```
        "IngestEndpoints": [
            {
                "Id": "6d345804ec3f46c9b454a91d4a80d0e0",
                "Password": "generatedwebdavpassword1",
                "Url": "https://f31c86aed53b815a.mediapackage.us-
west-2.amazonaws.com/in/
v2/6d345804ec3f46c9b454a91d4a80d0e0/6d345804ec3f46c9b454a91d4a80d0e0/channel",
                "Username": "generatedwebdavusername1"
            },
            {
                "Id": "2daa32878af24803b24183727211b8ff",
                "Password": "generatedwebdavpassword2",
                "Url": "https://6ebbe7e04c4b0afa.mediapackage.us-
west-2.amazonaws.com/in/
v2/6d345804ec3f46c9b454a91d4a80d0e0/2daa32878af24803b24183727211b8ff/channel",
                "Username": "generatedwebdavusername2"
            }
        ]
    },
    "Id": "sportschannel",
    "Tags": {}
}
```

Para obtener más información, consulte Editing a Channel en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte UpdateChannel en la Referencia de comandos de la AWS CLI.

update-origin-endpoint

En el siguiente ejemplo de código, se muestra cómo utilizar `update-origin-endpoint`.

AWS CLI

Para actualizar un punto de conexión de origen

El siguiente comando `update-origin-endpoint` actualiza el punto de conexión de origen denominado `cmaf_sports`. Cambia el retardo de tiempo a `0` segundos.

```
aws mediapackage update-origin-endpoint \
    --id cmaf_sports \
```

```
    --time-delay-seconds 0
```

Salida:

```
{
    "Arn": "arn:aws:mediapackage:us-
west-2:111222333:origin_endpoints/1dc6718be36f4f34bb9cd86bc50925e6",
    "ChannelId": "sportschannel",
    "CmafPackage": {
        "HlsManifests": [
            {
                "AdMarkers": "NONE",
                "Id": "cmaf_sports_endpoint",
                "IncludeIframeOnlyStream": false,
                "PlaylistType": "EVENT",
                "PlaylistWindowSeconds": 60,
                "ProgramDateTimeIntervalSeconds": 0,
                "Url": "https://c4af3793bf76b33c.mediapackage.us-
west-2.amazonaws.com/out/v1/1dc6718be36f4f34bb9cd86bc50925e6/cmaf_sports_endpoint/
index.m3u8"
            }
        ],
        "SegmentDurationSeconds": 2,
        "SegmentPrefix": "sportschannel"
    },
    "Id": "cmaf_sports",
    "ManifestName": "index",
    "StartoverWindowSeconds": 0,
    "Tags": {
        "region": "west",
        "media": "sports"
    },
    "TimeDelaySeconds": 0,
    "Url": "",
    "Whitelist": []
}
```

Para obtener más información, consulte Editing an Endpoint en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte UpdateOriginEndpoint en la Referencia de comandos de AWS CLI.

Ejemplos de VOD de MediaPackage que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios habituales mediante el AWS Command Line Interface con VOD de MediaPackage.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-asset`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-asset`.

AWS CLI

Para crear un activo

En el siguiente ejemplo de `create-asset`, se crea un activo llamado `Chicken_Asset` en la cuenta actual de AWS. El activo ingiere el archivo `30sec_chicken.smil` en MediaPackage.

```
aws mediapackage-vod create-asset \
    --id chicken_asset \
    --packaging-group-id hls_chicken_gp \
    --source-role-arn arn:aws:iam::111122223333:role/EMP_Vod \
    --source-arn arn:aws:s3::111122223333:video-bucket/A/30sec_chicken.smil
```

Salida:

```
{
    "Arn":"arn:aws:mediapackage-vod:us-west-2:111122223333:assets/chicken_asset",
    "Id":"chicken_asset",
    "PackagingGroupId":"hls_chicken_gp",
    "SourceArn":"arn:aws:s3::111122223333:video-bucket/A/30sec_chicken.smil",
```

```
    "SourceRoleArn":"arn:aws:iam::111122223333:role/EMP_Vod",
    "EgressEndpoints":[
        {
            "PackagingConfigurationId":"New_config_1",
            "Url":"https://c75ea2668ab49d02bca7ae10ef31c59e.egress.mediapackage-
vod.us-west-2.amazonaws.com/out/
v1/6644b55df1744261ab3732a8e5cdaf07/904b06a58c7645e08d57d40d064216ac/
f5b2e633ff4942228095d164c10074f3/index.m3u8"
        },
        {
            "PackagingConfigurationId":"new_hls",
            "Url":" https://c75ea2668ab49d02bca7ae10ef31c59e.egress.mediapackage-
vod.us-west-2.amazonaws.com/out/v1/6644b55df1744261ab3732a8e5cdaf07/
fe8f1f00a80e424cb4f8da4095835e9e/7370ec57432343af816332356d2bd5c6/string.m3u8"
        }
    ]
}
```

Para obtener más información, consulte Ingest an Asset en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte CreateAsset en la Referencia de comandos de la AWS CLI.

`create-packaging-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-packaging-configuration`.

AWS CLI

Para crear una configuración de empaquetado

En el siguiente ejemplo de `create-packaging-configuration`, se crea una configuración de empaquetado llamada `new_hls` en el grupo de empaquetado llamado `hls_chicken`. En este ejemplo se utiliza un archivo en el disco llamado `hls_pc.json` para proporcionar los detalles.

```
aws mediapackage-vod create-packaging-configuration \
    --id new_hls \
    --packaging-group-id hls_chicken \
    --hls-package file://hls_pc.json
```

Contenido de `hls_pc.json`:

```
{
    "HlsManifests":[
        {
            "AdMarkers":"NONE",
            "IncludeIframeOnlyStream":false,
            "ManifestName":"string",
            "ProgramDateTimeIntervalSeconds":60,
            "RepeatExtXKey":true,
            "StreamSelection":{
                "MaxVideoBitsPerSecond":1000,
                "MinVideoBitsPerSecond":0,
                "StreamOrder":"ORIGINAL"
            }
        }
    ],
    "SegmentDurationSeconds":6,
    "UseAudioRenditionGroup":false
}
```

Salida:

```
{
    "Arn":"arn:aws:mediapackage-vod:us-west-2:111122223333:packaging-configurations/
new_hls",
    "Id":"new_hls",
    "PackagingGroupId":"hls_chicken",
    "HlsManifests":{
        "SegmentDurationSeconds":6,
        "UseAudioRenditionGroup":false,
        "HlsMarkers":[
            {
                "AdMarkers":"NONE",
                "IncludeIframeOnlyStream":false,
                "ManifestName":"string",
                "ProgramDateTimeIntervalSeconds":60,
                "RepeatExtXKey":true,
                "StreamSelection":{
                    "MaxVideoBitsPerSecond":1000,
                    "MinVideoBitsPerSecond":0,
                    "StreamOrder":"ORIGINAL"
                }
            }
        ]
```

```
    }
}
```

Para obtener más información, consulte Creating a Packaging Configuration en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte CreatePackagingConfiguration en la Referencia de comandos de la AWS CLI.

`create-packaging-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-packaging-group`.

AWS CLI

Para crear un grupo de empaquetado

En el siguiente ejemplo de `create-packaging-group`, se muestran todos los grupos de empaquetado que están configurados en la cuenta actual de AWS.

```
aws mediapackage-vod create-packaging-group \
    --id hls_chicken
```

Salida:

```
{
    "Arn": "arn:aws:mediapackage-vod:us-west-2:111122223333:packaging-groups/
hls_chicken",
    "Id": "hls_chicken"
}
```

Para obtener más información, consulte Creating a Packaging Group en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte CreatePackagingGroup en la Referencia de comandos de la AWS CLI.

`delete-asset`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-asset`.

AWS CLI

Para eliminar un activo

En el siguiente ejemplo de `delete-asset`, se elimina el activo llamado `30sec_chicken`.

```
aws mediapackage-vod delete-asset \
    --id 30sec_chicken
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting an Asset en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte DeleteAsset en la Referencia de comandos de la AWS CLI.

`delete-packaging-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-packaging-configuration`.

AWS CLI

Para eliminar una configuración de empaquetado

En el siguiente ejemplo de `delete-packaging-configuration`, se elimina la configuración de empaquetado llamada `CMAF`.

```
aws mediapackage-vod delete-packaging-configuration \
    --id CMAF
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting a Packaging Configuration en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte DeletePackagingConfiguration en la Referencia de comandos de la AWS CLI.

`delete-packaging-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-packaging-group`.

AWS CLI

Para eliminar un grupo de empaquetado

En el siguiente ejemplo de `delete-packaging-group`, se elimina el grupo de empaquetado llamado `Dash_widevine`.

```
aws mediapackage-vod delete-packaging-group \
    --id Dash_widevine
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting a Packaging Group en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte DeletePackagingGroup en la Referencia de comandos de la AWS CLI.

`describe-asset`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-asset`.

AWS CLI

Para describir un activo

En el siguiente ejemplo de `describe-asset`, se muestran todos los detalles del activo llamado `30sec_chicken`.

```
aws mediapackage-vod describe-asset \
    --id 30sec_chicken
```

Salida:

```
{
    "Arn":"arn:aws:mediapackage-vod:us-west-2:111122223333:assets/30sec_chicken",
    "Id":"30sec_chicken",
    "PackagingGroupId":"Packaging_group_1",
    "SourceArn":"arn:aws:s3::111122223333:video-bucket/A/30sec_chicken.smil",
    "SourceRoleArn":"arn:aws:iam::111122223333:role/EMP_Vod",
    "EgressEndpoints":[
        {
```

```
            "PackagingConfigurationId":"DASH",
            "Url":"https://a5f46a44118ba3e3724ef39ef532e701.egress.mediapackage-
vod.us-west-2.amazonaws.com/out/v1/
aad7962c569946119c2d5a691be5663c/66c25aff456d463aae0855172b3beb27/4ddfda6da17c4c279a1b8401cb
index.mpd"
        },
        {
            "PackagingConfigurationId":"HLS",
            "Url":"https://a5f46a44118ba3e3724ef39ef532e701.egress.mediapackage-
vod.us-west-2.amazonaws.com/out/v1/
aad7962c569946119c2d5a691be5663c/6e5bf286a3414254a2bf0d22ae148d7e/06b5875b4d004c3cbdc4da2dc4
index.m3u8"
        },
        {
            "PackagingConfigurationId":"CMAF",
            "Url":"https://a5f46a44118ba3e3724ef39ef532e701.egress.mediapackage-
vod.us-west-2.amazonaws.com/out/v1/
aad7962c569946119c2d5a691be5663c/628fb5d8d89e4702958b020af27fde0e/05eb062214064238ad6330a443
index.m3u8"
        }
    ]
}
```

Para obtener más información, consulte Viewing Asset Details en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte DescribeAsset en la Referencia de comandos de la AWS CLI.

`describe-packaging-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-packaging-configuration`.

AWS CLI

Para describir una configuración de empaquetado

En el siguiente ejemplo de `describe-packaging-configuration`, se muestran todos los detalles de la configuración de empaquetado llamada `DASH`.

```
aws mediapackage-vod describe-packaging-configuration \
```

```
    --id DASH
```

Salida:

```
{
    "Arn":"arn:aws:mediapackage-vod:us-west-2:111122223333:packaging-configurations/
DASH",
    "Id":"DASH",
    "PackagingGroupId":"Packaging_group_1",
    "DashPackage":[
        {
            "SegmentDurationSeconds":"2"
        },
        {
            "DashManifests":{
                "ManifestName":"index",
                "MinBufferTimeSeconds":"30",
                "Profile":"NONE"
            }
        }
    ]
}
```

Para obtener más información, consulte Viewing Packaging Configuration Details en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte DescribePackagingConfiguration en la Referencia de comandos de la AWS CLI.

`describe-packaging-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-packaging-group`.

AWS CLI

Para describir un grupo de empaquetado

En el siguiente ejemplo de `describe-packaging-group`, se muestran todos los detalles del grupo de de empaquetado llamado `Packaging_group_1`.

```
aws mediapackage-vod describe-packaging-group \
    --id Packaging_group_1
```

Salida:

```
{
    "Arn": "arn:aws:mediapackage-vod:us-west-2:111122223333:packaging-groups/
Packaging_group_1",
    "Id": "Packaging_group_1"
}
```

Para obtener más información, consulte Viewing Packaging Group Details en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte DescribePackagingGroup en la Referencia de comandos de la AWS CLI.

`list-assets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-assets`.

AWS CLI

Para enumerar todos los activos

En el siguiente ejemplo de `list-assets`, se muestran todos los activos que están configurados en la cuenta actual de AWS.

```
aws mediapackage-vod list-assets
```

Salida:

```
{
    "Assets": [
        "Arn": "arn:aws:mediapackage-vod:us-
west-2:111122223333:assets/30sec_chicken",
        "Id": "30sec_chicken",
        "PackagingGroupId": "Packaging_group_1",
        "SourceArn": "arn:aws:s3::111122223333:video-bucket/A/30sec_chicken.smil",
        "SourceRoleArn": "arn:aws:iam::111122223333:role/EMP_Vod"
    ]
}
```

Para obtener más información, consulte Viewing Asset Details en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte ListAssets en la Referencia de comandos de la AWS CLI.

`list-packaging-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-packaging-configurations`.

AWS CLI

Para enumerar todas las configuraciones de empaquetado

En el siguiente ejemplo de `list-packaging-configurations`, se muestran todas las configuraciones de empaquetado que están configuradas en el grupo de empaquetado llamado `Packaging_group_1`.

```
aws mediapackage-vod list-packaging-configurations \
    --packaging-group-id Packaging_group_1
```

Salida:

```
{
    "PackagingConfigurations":[
        {
            "Arn":"arn:aws:mediapackage-vod:us-west-2:111122223333:packaging-
configurations/CMAF",
            "Id":"CMAF",
            "PackagingGroupId":"Packaging_group_1",
            "CmafPackage":[
                {
                    "SegmentDurationSeconds":"2"
                },
                {
                    "HlsManifests":{
                        "AdMarkers":"NONE",
                        "RepeatExtXKey":"False",
                        "ManifestName":"index",
                        "ProgramDateTimeIntervalSeconds":"0",
                        "IncludeIframeOnlyStream":"False"
                    }
                }
            ]
        },
```

```
        {
            "Arn":"arn:aws:mediapackage-vod:us-west-2:111122223333:packaging-
configurations/DASH",
            "Id":"DASH",
            "PackagingGroupId":"Packaging_group_1",
            "DashPackage":[
                {
                    "SegmentDurationSeconds":"2"
                },
                {
                    "DashManifests":{
                        "ManifestName":"index",
                        "MinBufferTimeSeconds":"30",
                        "Profile":"NONE"
                    }
                }
            ]
        },
        {
            "Arn":"arn:aws:mediapackage-vod:us-west-2:111122223333:packaging-
configurations/HLS",
            "Id":"HLS",
            "PackagingGroupId":"Packaging_group_1",
            "HlsPackage":[
                {
                    "SegmentDurationSeconds":"6",
                    "UseAudioRenditionGroup":"False"
                },
                {
                    "HlsManifests":{
                        "AdMarkers":"NONE",
                        "RepeatExtXKey":"False",
                        "ManifestName":"index",
                        "ProgramDateTimeIntervalSeconds":"0",
                        "IncludeIframeOnlyStream":"False"
                    }
                }
            ]
        },
        {
            "Arn":"arn:aws:mediapackage-vod:us-west-2:111122223333:packaging-
configurations/New_config_0_copy",
            "Id":"New_config_0_copy",
            "PackagingGroupId":"Packaging_group_1",
```

```
            "HlsPackage":[
                {
                    "SegmentDurationSeconds":"6",
                    "UseAudioRenditionGroup":"False"
                },
                {
                    "Encryption":{
                        "EncryptionMethod":"AWS_128",
                        "SpekeKeyProvider":{
                           "RoleArn":"arn:aws:iam:111122223333::role/SPEKERole",
                            "Url":"https://lfgubdvs97.execute-api.us-
west-2.amazonaws.com/EkeStage/copyProtection/",
                            "SystemIds":[
                                "81376844-f976-481e-a84e-cc25d39b0b33"
                            ]
                        }
                    }
                },
                {
                    "HlsManifests":{
                        "AdMarkers":"NONE",
                        "RepeatExtXKey":"False",
                        "ManifestName":"index",
                        "ProgramDateTimeIntervalSeconds":"0",
                        "IncludeIframeOnlyStream":"False"
                    }
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Viewing Packaging Configuration Details en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener más información sobre la API, consulte ListPackagingConfigurations en Referencia de comandos de la AWS CLI.

`list-packaging-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-packaging-groups`.

AWS CLI

Para enumerar todos los grupos de empaquetado

En el siguiente ejemplo de `list-packaging-groups`, se muestran todos los grupos de empaquetado que están configurados en la cuenta actual de AWS.

```
aws mediapackage-vod list-packaging-groups
```

Salida:

```
{
    "PackagingGroups": [
        {
            "Arn": "arn:aws:mediapackage-vod:us-west-2:111122223333:packaging-
groups/Dash_widevine",
            "Id": "Dash_widevine"
        },
        {
            "Arn": "arn:aws:mediapackage-vod:us-west-2:111122223333:packaging-
groups/Encrypted_HLS",
            "Id": "Encrypted_HLS"
        },
        {
            "Arn": "arn:aws:mediapackage-vod:us-west-2:111122223333:packaging-
groups/Packaging_group_1",
            "Id": "Packaging_group_1"
        }
    ]
}
```

Para obtener más información, consulte Viewing Packaging Group Details en la Guía del usuario de AWS Elemental MediaPackage.

- Para obtener información sobre la API, consulte ListPackagingGroups en la Referencia de comandos de la AWS CLI.

Ejemplos de planos de datos de MediaStore que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo ejecutar acciones e implementar escenarios comunes usando AWS Command Line Interface con plano de datos de MediaStore.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`delete-object`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-object`.

AWS CLI

Para eliminar un objeto

En el siguiente ejemplo de `delete-object`, se elimina el objeto especificado.

```
aws mediastore-data delete-object \
    --endpoint=https://aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com \
    --path=/folder_name/README.md
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting an Object en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte DeleteObject en la Referencia de comandos de AWS CLI.

`describe-object`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-object`.

AWS CLI

Para ver los encabezados de un objeto

En el siguiente ejemplo de `describe-object`, se muestran los encabezados de un objeto en la ruta especificada.

```
aws mediastore-data describe-object \
    --endpoint https://aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com \
    --path events/baseball/setup.jpg
```

Salida:

```
{
    "LastModified": "Fri, 19 Jul 2019 21:50:31 GMT",
    "ContentType": "image/jpeg",
    "ContentLength": "3860266",
    "ETag": "2aa333bbcc8d8d22d777e999c88d4aa9eeeeee4dd89ff7f555555555555da6d3"
}
```

Para obtener más información, consulte Viewing the Details of an Object en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte DescribeObject en la Referencia de comandos de la AWS CLI.

`get-object`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-object`.

AWS CLI

Ejemplo 1: descargar un objeto completo

En el siguiente ejemplo de `get-object`, se descarga el objeto especificado.

```
aws mediastore-data get-object \
    --endpoint https://aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com \
    --path events/baseball/setup.jpg setup.jpg
```

Salida:

```
{
    "ContentType": "image/jpeg",
    "StatusCode": 200,
```

```
    "ETag": "2aa333bbcc8d8d22d777e999c88d4aa9eeeeee4dd89ff7f555555555555da6d3",
    "ContentLength": "3860266",
    "LastModified": "Fri, 19 Jul 2019 21:50:31 GMT"
}
```

Ejemplo 2: descargar parte de un objeto

En el siguiente ejemplo de `get-object`, se descarga la parte especificada de un objeto.

```
aws mediastore-data get-object \
    --endpoint https://aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com \
    --path events/baseball/setup.jpg setup.jpg \
    --range "bytes=0-100"
```

Salida:

```
{
    "StatusCode": 206,
    "LastModified": "Fri, 19 Jul 2019 21:50:31 GMT",
    "ContentType": "image/jpeg",
    "ContentRange": "bytes 0-100/3860266",
    "ETag": "2aa333bbcc8d8d22d777e999c88d4aa9eeeeee4dd89ff7f555555555555da6d3",
    "ContentLength": "101"
}
```

Para obtener más información, consulte Downloading an Object en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte GetObject en la Referencia de comandos de AWS CLI.

`list-items`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-items`.

AWS CLI

Ejemplo 1: ver una lista de elementos (objetos y carpetas) almacenados en un contenedor

En el siguiente ejemplo de `list-items`, se muestra una lista de elementos (objetos y carpetas) almacenados en el contenedor especificado.

```
aws mediastore-data list-items \
    --endpoint https://aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com
```

Salida:

```
{
    "Items": [
        {
            "Type": "OBJECT",
            "ContentLength": 3784,
            "Name": "setup.jpg",
            "ETag":
 "2aa333bbcc8d8d22d777e999c88d4aa9eeeeee4dd89ff7f555555555555da6d3",
            "ContentType": "image/jpeg",
            "LastModified": 1563571859.379
        },
        {
            "Type": "FOLDER",
            "Name": "events"
        }
    ]
}
```

Ejemplo 2: ver una lista de elementos (objetos y carpetas) almacenados en una carpeta

En el siguiente ejemplo de `list-items`, se muestra una lista de elementos (objetos y carpetas) almacenados en la carpeta especificada.

```
aws mediastore-data list-items \
    --endpoint https://aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com \
    --path events/baseball
```

Salida:

```
{
    "Items": [
        {
            "ETag":
 "2aa333bbcc8d8d22d777e999c88d4aa9eeeeee4dd89ff7f555555555555da6d3",
            "ContentType": "image/jpeg",
            "Type": "OBJECT",
            "ContentLength": 3860266,
```

```
            "LastModified": 1563573031.872,
            "Name": "setup.jpg"
        }
    ]
}
```

Para obtener más información, consulte Viewing a List of Objects en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte ListItems en la Referencia de comandos de la AWS CLI.

`put-object`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-object`.

AWS CLI

Ejemplo 1: cargar un objeto en un contenedor

En el siguiente ejemplo de `put-object`, se carga un objeto en el contenedor especificado.

```
aws mediastore-data put-object \
    --endpoint https://aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com \
    --body ReadMe.md \
    --path ReadMe.md \
    --cache-control "max-age=6, public" \
    --content-type binary/octet-stream
```

Salida:

```
{
    "ContentSHA256":
 "f29bc64a9d3732b4b9035125fdb3285f5b6455778edca72414671e0ca3b2e0de",
    "StorageClass": "TEMPORAL",
    "ETag": "2aa333bbcc8d8d22d777e999c88d4aa9eeeeee4dd89ff7f555555555555da6d3"
}
```

Ejemplo 2: cargar un objeto en una carpeta dentro de un contenedor

En el siguiente ejemplo de `put-object`, se carga un objeto en la carpeta especificada dentro de un contenedor.

```
aws mediastore-data put-object \
    --endpoint https://aaabbbcccdddee.data.mediastore.us-west-2.amazonaws.com \
    --body ReadMe.md \
    --path /september-events/ReadMe.md \
    --cache-control "max-age=6, public" \
    --content-type binary/octet-stream
```

Salida:

```
{
    "ETag": "2aa333bbcc8d8d22d777e999c88d4aa9eeeeee4dd89ff7f555555555555da6d3",
    "ContentSHA256":
 "f29bc64a9d3732b4b9035125fdb3285f5b6455778edca72414671e0ca3b2e0de",
    "StorageClass": "TEMPORAL"
}
```

Para obtener más información, consulte Uploading an Object en la Guía del usuario de AWS Elemental MediaStore.

- Para obtener información sobre la API, consulte PutObject en la Referencia de comandos de AWS CLI.

Ejemplos de MediaTailor que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con MediaTailor.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`delete-playback-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-playback-configuration`.

AWS CLI

Para eliminar una configuración

El siguiente `delete-playback-configuration` elimina una configuración llamada `campaign_short`.

```
aws mediatailor delete-playback-configuration \
    --name campaign_short
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting a Configuration en la Guía del usuario de AWS Elemental MediaTailor.

- Para obtener información sobre la API, consulte DeletePlaybackConfiguration en la Referencia de comandos de la AWS CLI.

`get-playback-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-playback-configuration`.

AWS CLI

Descripción de una configuración

El siguiente `get-playback-configuration` muestra todos los detalles de la configuración llamada `west_campaign`.

```
aws mediatailor get-playback-configuration \
    --name west_campaign
```

Salida:

```
{
```

```
    "AdDecisionServerUrl": "http://your.ads.url",
    "CdnConfiguration": {},
    "DashConfiguration": {
        "ManifestEndpointPrefix":
 "https://170c14299689462897d0cc45fc2000bb.mediatailor.us-west-2.amazonaws.com/v1/
dash/1cbfeaaecb69778e0c167d0505a2bc57da2b1754/west_campaign/",
        "MpdLocation": "EMT_DEFAULT",
        "OriginManifestType": "MULTI_PERIOD"
    },
    "HlsConfiguration": {
        "ManifestEndpointPrefix":
 "https://170c14299689462897d0cc45fc2000bb.mediatailor.us-west-2.amazonaws.com/v1/
master/1cbfeaaecb69778e0c167d0505a2bc57da2b1754/west_campaign/"
    },
    "Name": "west_campaign",
    "PlaybackConfigurationArn": "arn:aws:mediatailor:us-
west-2:123456789012:playbackConfiguration/west_campaign",
    "PlaybackEndpointPrefix":
 "https://170c14299689462897d0cc45fc2000bb.mediatailor.us-west-2.amazonaws.com",
    "SessionInitializationEndpointPrefix":
 "https://170c14299689462897d0cc45fc2000bb.mediatailor.us-west-2.amazonaws.com/v1/
session/1cbfeaaecb69778e0c167d0505a2bc57da2b1754/west_campaign/",
    "Tags": {},
    "VideoContentSourceUrl": "https://8343f7014c0ea438.mediapackage.us-
west-2.amazonaws.com/out/v1/683f0f2ff7cd43a48902e6dcd5e16dcf/index.m3u8"
}
```

Para obtener más información, consulte Viewing a Configuration en la Guía del usuario de AWS Elemental MediaTailor.

- Para obtener información sobre la API, consulte GetPlaybackConfiguration en la Referencia de comandos de la AWS CLI.

`list-playback-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-playback-configurations`.

AWS CLI

Para enumerar todas las configuraciones

El siguiente `list-playback-configurations` muestra todos los detalles de la configuración en la cuenta actual de AWS.

```
aws mediatailor list-playback-configurations
```

Salida:

```
{
    "Items": [
        {
            "AdDecisionServerUrl": "http://your.ads.url",
            "CdnConfiguration": {},
            "DashConfiguration": {
                "ManifestEndpointPrefix":
 "https://170c14299689462897d0cc45fc2000bb.mediatailor.us-west-2.amazonaws.com/v1/
dash/1cbfeaaecb69778e0c167d0505a2bc57da2b1754/west_campaign/",
                "MpdLocation": "EMT_DEFAULT",
                "OriginManifestType": "MULTI_PERIOD"
            },
            "HlsConfiguration": {
                "ManifestEndpointPrefix":
 "https://170c14299689462897d0cc45fc2000bb.mediatailor.us-west-2.amazonaws.com/v1/
master/1cbfeaaecb69778e0c167d0505a2bc57da2b1754/west_campaign/"
            },
            "Name": "west_campaign",
            "PlaybackConfigurationArn": "arn:aws:mediatailor:us-
west-2:123456789012:playbackConfiguration/west_campaign",
            "PlaybackEndpointPrefix":
 "https://170c14299689462897d0cc45fc2000bb.mediatailor.us-west-2.amazonaws.com",
            "SessionInitializationEndpointPrefix":
 "https://170c14299689462897d0cc45fc2000bb.mediatailor.us-west-2.amazonaws.com/v1/
session/1cbfeaaecb69778e0c167d0505a2bc57da2b1754/west_campaign/",
            "Tags": {},
            "VideoContentSourceUrl": "https://8343f7014c0ea438.mediapackage.us-
west-2.amazonaws.com/out/v1/683f0f2ff7cd43a48902e6dcd5e16dcf/index.m3u8"
        },
        {
            "AdDecisionServerUrl": "http://your.ads.url",
            "CdnConfiguration": {},
            "DashConfiguration": {
                "ManifestEndpointPrefix":
 "https://73511f91d6a24ca2b93f3cf1d7cedd67.mediatailor.us-west-2.amazonaws.com/v1/
dash/1cbfeaaecb69778e0c167d0505a2bc57da2b1754/sports_campaign/",
                "MpdLocation": "DISABLED",
                "OriginManifestType": "MULTI_PERIOD"
            },
```

```
            "HlsConfiguration": {
                "ManifestEndpointPrefix":
 "https://73511f91d6a24ca2b93f3cf1d7cedd67.mediatailor.us-west-2.amazonaws.com/v1/
master/1cbfeaaecb69778e0c167d0505a2bc57da2b1754/sports_campaign/"
            },
            "Name": "sports_campaign",
            "PlaybackConfigurationArn": "arn:aws:mediatailor:us-
west-2:123456789012:playbackConfiguration/sports_campaign",
            "PlaybackEndpointPrefix":
 "https://73511f91d6a24ca2b93f3cf1d7cedd67.mediatailor.us-west-2.amazonaws.com",
            "SessionInitializationEndpointPrefix":
 "https://73511f91d6a24ca2b93f3cf1d7cedd67.mediatailor.us-west-2.amazonaws.com/v1/
session/1cbfeaaecb69778e0c167d0505a2bc57da2b1754/sports_campaign/",
            "SlateAdUrl": "http://s3.bucket/slate_ad.mp4",
            "Tags": {},
            "VideoContentSourceUrl": "https://c4af3793bf76b33c.mediapackage.us-
west-2.amazonaws.com/out/v1/1dc6718be36f4f34bb9cd86bc50925e6/sports_endpoint/
index.m3u8"
        }
    ]
}
```

Para obtener más información, consulte Viewing a Configuration<https://docs.aws.amazon.com/mediatailor/latest/ug/configurations-view.html> en la Guía del usuario de AWS Elemental MediaTailor.

- Para obtener información sobre la API, consulte ListPlaybackConfigurations en la Referencia de comandos de la AWS CLI.

`put-playback-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-playback-configuration`.

AWS CLI

Para crear una configuración

El siguiente `put-playback-configuration` crea una configuración llamada `campaign_short`.

```
aws mediatailor put-playback-configuration \
    --name campaign_short \
```

```
    --ad-decision-server-url http://your.ads.url \
    --video-content-source-url http://video.bucket/index.m3u8
```

Salida:

```
{
    "AdDecisionServerUrl": "http://your.ads.url",
    "CdnConfiguration": {},
    "DashConfiguration": {
         "ManifestEndpointPrefix":
 "https://13484114d38f4383bc0d6a7cb879bd00.mediatailor.us-west-2.amazonaws.com/v1/
dash/1cbfeaaecb69778e0c167d0505a2bc57da2b1754/campaign_short/",
         "MpdLocation": "EMT_DEFAULT",
         "OriginManifestType": "MULTI_PERIOD"
    },
    "HlsConfiguration": {
        "ManifestEndpointPrefix":
 "https://13484114d38f4383bc0d6a7cb879bd00.mediatailor.us-west-2.amazonaws.com/v1/
master/1cbfeaaecb69778e0c167d0505a2bc57da2b1754/campaign_short/"
    },
    "Name": "campaign_short",
    "PlaybackConfigurationArn": "arn:aws:mediatailor:us-
west-2:123456789012:playbackConfiguration/campaign_short",
    "PlaybackEndpointPrefix":
 "https://13484114d38f4383bc0d6a7cb879bd00.mediatailor.us-west-2.amazonaws.com",
    "SessionInitializationEndpointPrefix":
 "https://13484114d38f4383bc0d6a7cb879bd00.mediatailor.us-west-2.amazonaws.com/v1/
session/1cbfeaaecb69778e0c167d0505a2bc57da2b1754/campaign_short/",
    "Tags": {},
    "VideoContentSourceUrl": "http://video.bucket/index.m3u8"
}
```

Para obtener más información, consulte Creating a Configuration en la Guía del usuario de AWS Elemental MediaTailor.

- Para obtener información sobre la API, consulte PutPlaybackConfiguration en la Referencia de comandos de la AWS CLI.

Ejemplos de MemoryDB que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con MemoryDB.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`copy-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-snapshot`.

AWS CLI

Copia de una instantánea

El siguiente ejemplo de `copy-snapshot` crea una copia de una instantánea.

```
aws memorydb copy-snapshot \
    --source-snapshot-name my-cluster-snapshot \
    --target-snapshot-name my-cluster-snapshot-copy
```

Output

```
{
    "Snapshot": {
        "Name": "my-cluster-snapshot-copy",
        "Status": "creating",
        "Source": "manual",
        "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:snapshot/my-cluster-
snapshot-copy",
        "ClusterConfiguration": {
            "Name": "my-cluster",
            "Description": " ",
            "NodeType": "db.r6g.large",
            "EngineVersion": "6.2",
            "MaintenanceWindow": "wed:03:00-wed:04:00",
            "Port": 6379,
```

```
            "ParameterGroupName": "default.memorydb-redis6",
            "SubnetGroupName": "my-sg",
            "VpcId": "vpc-xx2574fc",
            "SnapshotRetentionLimit": 0,
            "SnapshotWindow": "04:30-05:30",
            "NumShards": 2
        }
    }
}
```

Para obtener más información, consulte Copying a snapshot en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte CopySnapshot en la Referencia de comandos de la AWS CLI.

`create-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-acl`.

AWS CLI

Para crear una ACL

El siguiente ejemplo de `create-acl` crea una lista de control de acceso.

```
aws memorydb create-acl \
    --acl-name "new-acl-1" \
    --user-names "my-user"
```

Salida:

```
{
    "ACL": {
        "Name": "new-acl-1",
        "Status": "creating",
        "UserNames": [
            "my-user"
        ],
        "MinimumEngineVersion": "6.2",
        "Clusters": [],
        "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:acl/new-acl-1"
```

```
    }
}
```

Para obtener más información, consulte Authenticating users with Access Control Lists en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte CreateAcl en la Referencia de comandos de la AWS CLI.

`create-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-cluster`.

AWS CLI

Para crear un clúster

El siguiente ejemplo de `create-cluster` crea un nuevo clúster.

```
aws memorydb create-cluster \
    --cluster-name my-new-cluster \
    --node-type db.r6g.large \
    --acl-name my-acl \
    --subnet-group my-sg
```

Salida:

```
{
    "Cluster": {
        "Name": "my-new-cluster",
        "Status": "creating",
        "NumberOfShards": 1,
        "AvailabilityMode": "MultiAZ",
        "ClusterEndpoint": {
            "Port": 6379
        },
        "NodeType": "db.r6g.large",
        "EngineVersion": "6.2",
        "EnginePatchVersion": "6.2.6",
        "ParameterGroupName": "default.memorydb-redis6",
        "ParameterGroupStatus": "in-sync",
        "SubnetGroupName": "my-sg",
        "TLSEnabled": true,
```

```
        "ARN": "arn:aws:memorydb:us-east-1:49165xxxxxx:cluster/my-new-cluster",
        "SnapshotRetentionLimit": 0,
        "MaintenanceWindow": "sat:10:00-sat:11:00",
        "SnapshotWindow": "07:30-08:30",
        "ACLName": "my-acl",
        "AutoMinorVersionUpgrade": true
    }
}
```

Para obtener más información, consulte Managing Clusters en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte CreateCluster en la Referencia de comandos de la AWS CLI.

`create-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-parameter-group`.

AWS CLI

Para crear un grupo de parámetros

El siguiente ejemplo de `create-parameter-group` crea un grupo de parámetros.

```
aws memorydb create-parameter-group \
    --parameter-group-name myRedis6x \
    --family memorydb_redis6 \
    --description "my-parameter-group"
```

Salida:

```
{
    "ParameterGroup": {
        "Name": "myredis6x",
        "Family": "memorydb_redis6",
        "Description": "my-parameter-group",
        "ARN": "arn:aws:memorydb:us-east-1:49165xxxxxx:parametergroup/myredis6x"
    }
}
```

Para obtener más información, consulte Creating a parameter group en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte CreateParameterGroup en la Referencia de comandos de la AWS CLI.

`create-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-snapshot`.

AWS CLI

Para crear una instantánea

El siguiente ejemplo de `create-snapshot` crea una instantánea.

```
aws memorydb create-snapshot \
    --cluster-name my-cluster \
    --snapshot-name my-cluster-snapshot
```

Salida:

```
{
    "Snapshot": {
        "Name": "my-cluster-snapshot1",
        "Status": "creating",
        "Source": "manual",
        "ARN": "arn:aws:memorydb:us-east-1:49165xxxxxx:snapshot/my-cluster-
snapshot",
        "ClusterConfiguration": {
            "Name": "my-cluster",
            "Description": "",
            "NodeType": "db.r6g.large",
            "EngineVersion": "6.2",
            "MaintenanceWindow": "wed:03:00-wed:04:00",
            "Port": 6379,
            "ParameterGroupName": "default.memorydb-redis6",
            "SubnetGroupName": "my-sg",
            "VpcId": "vpc-862xxxxc",
            "SnapshotRetentionLimit": 0,
            "SnapshotWindow": "04:30-05:30",
            "NumShards": 2
        }
    }
}
```

Para obtener más información, consulte Making manual snapshots en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte CreateSnapshot en la Referencia de comandos de la AWS CLI.

`create-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-subnet-group`.

AWS CLI

Para crear un grupo de subredes

En el siguiente ejemplo de `create-subnet-group` se crea un grupo de subredes.

```
aws memorydb create-subnet-group \
    --subnet-group-name mysubnetgroup \
    --description "my subnet group" \
    --subnet-ids subnet-5623xxxx
```

Salida:

```
{
    "SubnetGroup": {
        "Name": "mysubnetgroup",
        "Description": "my subnet group",
        "VpcId": "vpc-86257xxx",
        "Subnets": [
            {
                "Identifier": "subnet-5623xxxx",
                "AvailabilityZone": {
                    "Name": "us-east-1a"
                }
            }
        ],
        "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:subnetgroup/mysubnetgroup"
    }
}
```

Para obtener más información, consulte Creating a subnet group en la Guía del usuario de MemoryDB.

- Para obtener detalles sobre la API, consulte CreateSubnetGroup en la Referencia de comandos de la AWS CLI.

`create-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-user`.

AWS CLI

Para crear un usuario

En el siguiente ejemplo de `create-user` se crea un nuevo usuario.

```
aws memorydb create-user \
    --user-name user-name-1 \
    --access-string "~objects:* ~items:* ~public:*" \
     --authentication-mode \
         Passwords="enterapasswordhere",Type=password
```

Salida:

```
{
    "User": {
        "Name": "user-name-1",
        "Status": "active",
        "AccessString": "off ~objects:* ~items:* ~public:* resetchannels -@all",
        "ACLNames": [],
        "MinimumEngineVersion": "6.2",
        "Authentication": {
            "Type": "password",
            "PasswordCount": 1
        },
        "ARN": "arn:aws:memorydb:us-west-2:491658xxxxxx:user/user-name-1"
    }
}
```

Para obtener más información, consulte Authenticating users with Access Control Lists en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte CreateUser en la Referencia de comandos de la AWS CLI.

`delete-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-acl`.

AWS CLI

Para eliminar una ACL

En el siguiente ejemplo de `delete-acl` se elimina una lista de control de acceso.

```
aws memorydb delete-acl \
    --acl-name "new-acl-1"
```

Salida:

```
{
    "ACL": {
        "Name": "new-acl-1",
        "Status": "deleting",
        "UserNames": [
            "pat"
        ],
        "MinimumEngineVersion": "6.2",
        "Clusters": [],
        "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:acl/new-acl-1"
    }
}
```

Para obtener más información, consulte Authenticating users with Access Control Lists en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte DeleteAcl en la Referencia de comandos de la AWS CLI.

`delete-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-cluster`.

AWS CLI

Para eliminar un clúster

En el siguiente ejemplo de `delete-cluster` se elimina un clúster.

```
aws memorydb delete-cluster \
    --cluster-name my-new-cluster
```

Salida:

```
{
    "Cluster": {
        "Name": "my-new-cluster",
        "Status": "deleting",
        "NumberOfShards": 1,
        "ClusterEndpoint": {
            "Address": "clustercfg.my-new-cluster.xxxxx.memorydb.us-
east-1.amazonaws.com",
            "Port": 6379
        },
        "NodeType": "db.r6g.large",
        "EngineVersion": "6.2",
        "EnginePatchVersion": "6.2.6",
        "ParameterGroupName": "default.memorydb-redis6",
        "ParameterGroupStatus": "in-sync",
        "SubnetGroupName": "my-sg",
        "TLSEnabled": true,
        "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:cluster/my-new-cluster",
        "SnapshotRetentionLimit": 0,
        "MaintenanceWindow": "sat:10:00-sat:11:00",
        "SnapshotWindow": "07:30-08:30",
        "AutoMinorVersionUpgrade": true
    }
}
```

Para obtener más información, consulte Deleting a cluster en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte DeleteCluster en la Referencia de comandos de la AWS CLI.

`delete-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-parameter-group`.

AWS CLI

Para eliminar un grupo de parámetros

En el siguiente ejemplo de `delete-parameter-group` se elimina un grupo de parámetros.

```
aws memorydb delete-parameter-group \
    --parameter-group-name myRedis6x
```

Salida:

```
{
    "ParameterGroup": {
        "Name": "myredis6x",
        "Family": "memorydb_redis6",
        "Description": "my-parameter-group",
        "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:parametergroup/myredis6x"
    }
}
```

Para obtener más información, consulte Deleting a parameter group en la Guía del usuario de MemoryDB.

- Para obtener detalles sobre la API, consulte DeleteParameterGroup en la Referencia de comandos de la AWS CLI.

`delete-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-snapshot`.

AWS CLI

Eliminar una instantánea

En el siguiente ejemplo de `delete-snapshot` se elimina una instantánea.

```
aws memorydb delete-snapshot \
    --snapshot-name my-cluster-snapshot
```

Salida:

```
{
    "Snapshot": {
        "Name": "my-cluster-snapshot",
        "Status": "deleting",
        "Source": "manual",
```

```
        "ARN": "arn:aws:memorydb:us-east-1:49165xxxxxx:snapshot/my-cluster-
snapshot",
        "ClusterConfiguration": {
            "Name": "my-cluster",
            "Description": "",
            "NodeType": "db.r6g.large",
            "EngineVersion": "6.2",
            "MaintenanceWindow": "wed:03:00-wed:04:00",
            "Port": 6379,
            "ParameterGroupName": "default.memorydb-redis6",
            "SubnetGroupName": "my-sg",
            "VpcId": "vpc-862xxxxc",
            "SnapshotRetentionLimit": 0,
            "SnapshotWindow": "04:30-05:30",
            "NumShards": 2
        }
    }
}
```

Para obtener más información, consulte Deleting a snapshot en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte DeleteSnapshot en la Referencia de comandos de la AWS CLI.

`delete-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-subnet-group`.

AWS CLI

Para eliminar un grupo de subredes

En el siguiente ejemplo de `delete-subnet-group` se elimina una subred.

```
aws memorydb delete-subnet-group \
    --subnet-group-name mysubnetgroup
```

Salida:

```
{
    "SubnetGroup": {
```

```
        "Name": "mysubnetgroup",
        "Description": "my subnet group",
        "VpcId": "vpc-86xxxx4fc",
        "Subnets": [
            {
                "Identifier": "subnet-56xxx61b",
                "AvailabilityZone": {
                    "Name": "us-east-1a"
                }
            }
        ],
        "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:subnetgroup/mysubnetgroup"
    }
}
```

Para obtener más información, consulte Deleting a subnet group en la Guía del usuario de MemoryDB.

- Para obtener más información sobre la API, consulte DeleteSubnetGroup en la Referencia de comandos de la AWS CLI.

`delete-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-user`.

AWS CLI

Cómo eliminar un usuario

En el siguiente ejemplo de `delete-user` se elimina un usuario.

```
aws memorydb delete-user \
    --user-name my-user
```

Salida:

```
{
    "User": {
        "Name": "my-user",
        "Status": "deleting",
        "AccessString": "on ~app::* resetchannels -@all +@read",
        "ACLNames": [
```

```
            "my-acl"
        ],
        "MinimumEngineVersion": "6.2",
        "Authentication": {
            "Type": "password",
            "PasswordCount": 1
        },
        "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:user/my-user"
    }
}
```

Para obtener más información, consulte Authenticating users with Access Control Lists en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte DeleteUser en la Referencia de comandos de la AWS CLI.

`describe-acls`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-acls`.

AWS CLI

Para devolver una lista de ACL

El siguiente describe-acls` devuelve una lista de ACL.

```
aws memorydb describe-acls
```

Salida:

```
{
    "ACLs": [
        {
            "Name": "open-access",
            "Status": "active",
            "UserNames": [
                "default"
            ],
            "MinimumEngineVersion": "6.2",
            "Clusters": [],
            "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:acl/open-access"
```

```
        },
        {
            "Name": my-acl",
            "Status": "active",
            "UserNames": [],
            "MinimumEngineVersion": "6.2",
            "Clusters": [
                "my-cluster"
            ],
            "ARN": "arn:aws:memorydb:us-east-1:49165xxxxxxx:acl/my-acl"
        }
    ]
}
```

Para obtener más información, consulte Authenticating users with Access Control Lists en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte DescribeAcls en la Referencia de comandos de la AWS CLI.

`describe-clusters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-clusters`.

AWS CLI

Para devolver una lista de clústeres

El siguiente describe-clusters` devuelve una lista de clústeres.

```
aws memorydb describe-clusters
```

Salida:

```
{
    "Clusters": [
        {
                "Name": "my-cluster",
                "Status": "available",
                "NumberOfShards": 2,
                "ClusterEndpoint": {
                    "Address": "clustercfg.my-cluster.llru6f.memorydb.us-
east-1.amazonaws.com",
```

```
                    "Port": 6379
                },
                "NodeType": "db.r6g.large",
                "EngineVersion": "6.2",
                "EnginePatchVersion": "6.2.6",
                "ParameterGroupName": "default.memorydb-redis6",
                "ParameterGroupStatus": "in-sync",
                "SecurityGroups": [
                    {
                        "SecurityGroupId": "sg-0a1434xxxxxc9fae",
                        "Status": "active"
                    }
                ],
                "SubnetGroupName": "pat-sg",
                "TLSEnabled": true,
                "ARN": "arn:aws:memorydb:us-east-1:49165xxxxxx:cluster/my-cluster",
                "SnapshotRetentionLimit": 0,
                "MaintenanceWindow": "wed:03:00-wed:04:00",
                "SnapshotWindow": "04:30-05:30",
                "ACLName": "my-acl",
                "AutoMinorVersionUpgrade": true
        }
    ]
}
```

Para obtener más información, consulte Managing clusters en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte DescribeClusters en la Referencia de comandos de la AWS CLI.

`describe-engine-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-engine-versions`.

AWS CLI

Para devolver una lista de versiones del motor

El siguiente describe-engine-versions` devuelve una lista de las versiones del motor.

```
aws memorydb describe-engine-versions
```

Salida:

```
{
    "EngineVersions": [
        {
            "EngineVersion": "6.2",
            "EnginePatchVersion": "6.2.6",
            "ParameterGroupFamily": "memorydb_redis6"
        }
    ]
}
```

Para obtener más información, consulte Engine versions and upgrading en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte DescribeEngineVersions en la Referencia de comandos de la AWS CLI.

`describe-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-events`.

AWS CLI

Para devolver una lista de eventos

El siguiente describe-acls` devuelve una lista de eventos.

```
aws memorydb describe-events
```

Salida:

```
{
    "Events": [
        {
            "SourceName": "my-cluster",
            "SourceType": "cluster",
            "Message": "Increase replica count started for replication group my-
cluster on 2022-07-22T14:09:01.440Z",
            "Date": "2022-07-22T07:09:01.443000-07:00"
        },
        {
            "SourceName": "my-user",
            "SourceType": "user",
```

```
            "Message": "Create user my-user operation completed.",
            "Date": "2022-07-22T07:00:02.975000-07:00"
        }
    ]
}
```

Para obtener más información, consulte Monitoring events en la Guía del usuario de MemoryDB.

- Para obtener detalles sobre la API, consulte DescribeEvents en la Referencia de comandos de la AWS CLI.

`describe-parameter-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-parameter-groups`.

AWS CLI

Para devolver una lista de grupos de parámetros

El siguiente describe-parameter-groups` devuelve una lista de grupos de parámetros.

```
aws memorydb describe-parameter-groups
```

Salida:

```
{
    "ParameterGroups": [
        {
            "Name": "default.memorydb-redis6",
            "Family": "memorydb_redis6",
            "Description": "Default parameter group for memorydb_redis6",
            "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:parametergroup/
default.memorydb-redis6"
        }
    ]
}
```

Para obtener más información, consulte Configuring engine parameters using parameter groups en la Guía del usuario de MemoryDB.

- Para obtener detalles sobre la API, consulte DescribeParameterGroups en la Referencia de comandos de la AWS CLI.

describe-parameters

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-parameters`.

AWS CLI

Para devolver una lista de parámetros

El siguiente describe-parameters` devuelve una lista de parámetros.

```
aws memorydb describe-parameters
```

Salida:

```
{
    "Parameters": [
        {
            "Name": "acllog-max-len",
            "Value": "128",
            "Description": "The maximum length of the ACL Log",
            "DataType": "integer",
            "AllowedValues": "1-10000",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "activedefrag",
            "Value": "no",
            "Description": "Enabled active memory defragmentation",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "active-defrag-cycle-max",
            "Value": "75",
            "Description": "Maximal effort for defrag in CPU percentage",
            "DataType": "integer",
            "AllowedValues": "1-75",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "active-defrag-cycle-min",
            "Value": "5",
            "Description": "Minimal effort for defrag in CPU percentage",
```

```
            "DataType": "integer",
            "AllowedValues": "1-75",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "active-defrag-ignore-bytes",
            "Value": "104857600",
            "Description": "Minimum amount of fragmentation waste to start active
defrag",
            "DataType": "integer",
            "AllowedValues": "1048576-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "active-defrag-max-scan-fields",
            "Value": "1000",
            "Description": "Maximum number of set/hash/zset/list fields that will be
processed from the main dictionary scan",
            "DataType": "integer",
            "AllowedValues": "1-1000000",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "active-defrag-threshold-lower",
            "Value": "10",
            "Description": "Minimum percentage of fragmentation to start active
defrag",
            "DataType": "integer",
            "AllowedValues": "1-100",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "active-defrag-threshold-upper",
            "Value": "100",
            "Description": "Maximum percentage of fragmentation at which we use
maximum effort",
            "DataType": "integer",
            "AllowedValues": "1-100",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "active-expire-effort",
            "Value": "1",
```

```
            "Description": "The amount of effort that redis uses to expire items in
the active expiration job",
            "DataType": "integer",
            "AllowedValues": "1-10",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "activerehashing",
            "Value": "yes",
            "Description": "Apply rehashing or not",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "client-output-buffer-limit-normal-hard-limit",
            "Value": "0",
            "Description": "Normal client output buffer hard limit in bytes",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "client-output-buffer-limit-normal-soft-limit",
            "Value": "0",
            "Description": "Normal client output buffer soft limit in bytes",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "client-output-buffer-limit-normal-soft-seconds",
            "Value": "0",
            "Description": "Normal client output buffer soft limit in seconds",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "client-output-buffer-limit-pubsub-hard-limit",
            "Value": "33554432",
            "Description": "Pubsub client output buffer hard limit in bytes",
            "DataType": "integer",
            "AllowedValues": "0-",
```

```
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "client-output-buffer-limit-pubsub-soft-limit",
            "Value": "8388608",
            "Description": "Pubsub client output buffer soft limit in bytes",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "client-output-buffer-limit-pubsub-soft-seconds",
            "Value": "60",
            "Description": "Pubsub client output buffer soft limit in seconds",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "hash-max-ziplist-entries",
            "Value": "512",
            "Description": "The maximum number of hash entries in order for the
dataset to be compressed",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "hash-max-ziplist-value",
            "Value": "64",
            "Description": "The threshold of biggest hash entries in order for the
dataset to be compressed",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "hll-sparse-max-bytes",
            "Value": "3000",
            "Description": "HyperLogLog sparse representation bytes limit",
            "DataType": "integer",
            "AllowedValues": "1-16000",
            "MinimumEngineVersion": "6.2.4"
        },
```

```
        {
            "Name": "lazyfree-lazy-eviction",
            "Value": "no",
            "Description": "Perform an asynchronous delete on evictions",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "lazyfree-lazy-expire",
            "Value": "no",
            "Description": "Perform an asynchronous delete on expired keys",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "lazyfree-lazy-server-del",
            "Value": "no",
            "Description": "Perform an asynchronous delete on key updates",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "lazyfree-lazy-user-del",
            "Value": "no",
            "Description": "Specifies whether the default behavior of DEL command
acts the same as UNLINK",
            "DataType": "string",
            "AllowedValues": "yes,no",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "lfu-decay-time",
            "Value": "1",
            "Description": "The amount of time in minutes to decrement the key
counter for LFU eviction policyd",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "lfu-log-factor",
```

```
            "Value": "10",
            "Description": "The log factor for incrementing key counter for LFU
 eviction policy",
            "DataType": "integer",
            "AllowedValues": "1-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "list-compress-depth",
            "Value": "0",
            "Description": "Number of quicklist ziplist nodes from each side of
 the list to exclude from compression. The head and tail of the list are always
 uncompressed for fast push/pop operations",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "maxmemory-policy",
            "Value": "noeviction",
            "Description": "Max memory policy",
            "DataType": "string",
            "AllowedValues": "volatile-lru,allkeys-lru,volatile-lfu,allkeys-
lfu,volatile-random,allkeys-random,volatile-ttl,noeviction",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "maxmemory-samples",
            "Value": "3",
            "Description": "Max memory samples",
            "DataType": "integer",
            "AllowedValues": "1-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "notify-keyspace-events",
            "Description": "The keyspace events for Redis to notify Pub/Sub clients
 about. By default all notifications are disabled",
            "DataType": "string",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "set-max-intset-entries",
            "Value": "512",
```

```
            "Description": "The limit in the size of the set in order for the
dataset to be compressed",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "slowlog-log-slower-than",
            "Value": "10000",
            "Description": "The execution time, in microseconds, to exceed in order
for the command to get logged. Note that a negative number disables the slow log,
while a value of zero forces the logging of every command",
            "DataType": "integer",
            "AllowedValues": "-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "slowlog-max-len",
            "Value": "128",
            "Description": "The length of the slow log. There is no limit to this
length. Just be aware that it will consume memory. You can reclaim memory used by
the slow log with SLOWLOG RESET.",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "stream-node-max-bytes",
            "Value": "4096",
            "Description": "The maximum size of a single node in a stream in bytes",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "stream-node-max-entries",
            "Value": "100",
            "Description": "The maximum number of items a single node in a stream
can contain",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
```

```
            "Name": "tcp-keepalive",
            "Value": "300",
            "Description": "If non-zero, send ACKs every given number of seconds",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "timeout",
            "Value": "0",
            "Description": "Close connection if client is idle for a given number of
seconds, or never if 0",
            "DataType": "integer",
            "AllowedValues": "0,20-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "tracking-table-max-keys",
            "Value": "1000000",
            "Description": "The maximum number of keys allowed for the tracking
table for client side caching",
            "DataType": "integer",
            "AllowedValues": "1-100000000",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "zset-max-ziplist-entries",
            "Value": "128",
            "Description": "The maximum number of sorted set entries in order for
the dataset to be compressed",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        },
        {
            "Name": "zset-max-ziplist-value",
            "Value": "64",
            "Description": "The threshold of biggest sorted set entries in order for
the dataset to be compressed",
            "DataType": "integer",
            "AllowedValues": "0-",
            "MinimumEngineVersion": "6.2.4"
        }
    ]
```

```
}
```

Para obtener más información, consulte Configuring engine parameters using parameter groups en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte DescribeParameters en la Referencia de comandos de la AWS CLI.

`describe-snapshots`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-snapshots`.

AWS CLI

Para devolver una lista de instantáneas

El siguiente describe-snapshots` devuelve una lista de instantáneas.

```
aws memorydb describe-snapshots
```

Salida:

```
{
"Snapshots": [
    {
        "Name": "my-cluster-snapshot",
        "Status": "available",
        "Source": "manual",
        "ARN": "arn:aws:memorydb:us-east-1:491658xxxxx2:snapshot/my-cluster-
snapshot",
        "ClusterConfiguration": {
            "Name": "my-cluster",
            "Description": " ",
            "NodeType": "db.r6g.large",
            "EngineVersion": "6.2",
            "MaintenanceWindow": "wed:03:00-wed:04:00",
            "Port": 6379,
            "ParameterGroupName": "default.memorydb-redis6",
            "SubnetGroupName": "my-sg",
            "VpcId": "vpc-862574fc",
            "SnapshotRetentionLimit": 0,
            "SnapshotWindow": "04:30-05:30",
            "NumShards": 2
```

```
        }
    }
}
```

Para obtener más información, consulte Snapshot and restore en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte DescribeSnapshots en la Referencia de comandos de la AWS CLI.

`describe-subnet-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-subnet-groups`.

AWS CLI

Para devolver una lista de grupos de subredes

El siguiente describe-subnet-groups` devuelve una lista de grupos de subredes.

```
aws memorydb describe-subnet-groups
```

Output

```
{
    "SubnetGroups": [
        {
            "Name": "my-sg",
            "Description": "pat-sg",
            "VpcId": "vpc-86xxx4fc",
            "Subnets": [
                {
                    "Identifier": "subnet-faxx84a6",
                    "AvailabilityZone": {
                        "Name": "us-east-1b"
                    }
                },
                {
                    "Identifier": "subnet-56xxf61b",
                    "AvailabilityZone": {
                        "Name": "us-east-1a"
                    }
                }
```

```
            ],
            "ARN": "arn:aws:memorydb:us-east-1:49165xxxxxx:subnetgroup/my-sg"
        }
    ]
}
```

Para obtener más información, consulte Subnets and subnet groups en la Guía del usuario de MemoryDB.

- Para obtener detalles sobre la API, consulte DescribeSubnetGroups en la Referencia de comandos de la AWS CLI.

`describe-users`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-users`.

AWS CLI

Para devolver una lista de usuarios

El siguiente describe-users` devuelve una lista de usuarios.

```
aws memorydb describe-users
```

Output

```
{
    "Users": [
        {
            "Name": "default",
            "Status": "active",
            "AccessString": "on ~* &* +@all",
            "ACLNames": [
                "open-access"
            ],
            "MinimumEngineVersion": "6.0",
            "Authentication": {
                "Type": "no-password"
            },
            "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:user/default"
        },
        {
            "Name": "my-user",
```

```
            "Status": "active",
            "AccessString": "off ~objects:* ~items:* ~public:* resetchannels -@all",
            "ACLNames": [],
            "MinimumEngineVersion": "6.2",
            "Authentication": {
                "Type": "password",
                "PasswordCount": 2
            },
            "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:user/my-user"
        }
    ]
}
```

Para obtener más información, consulte Authenticating users with Access Control Lists en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte DescribeUsers en la Referencia de comandos de la AWS CLI.

`failover-shard`

En el siguiente ejemplo de código, se muestra cómo utilizar `failover-shard`.

AWS CLI

Para realizar conmutación por error de una partición

El siguiente failover-shard` realiza conmutación por error de una partición.

```
aws memorydb failover-shard \
    --cluster-name my-cluster --shard-name 0001
```

Salida:

```
{
    "Cluster": {
        "Name": "my-cluster",
        "Status": "available",
        "NumberOfShards": 2,
        "ClusterEndpoint": {
            "Address": "clustercfg.my-cluster.xxxxxx.memorydb.us-
east-1.amazonaws.com",
            "Port": 6379
```

```
        },
        "NodeType": "db.r6g.large",
        "EngineVersion": "6.2",
        "EnginePatchVersion": "6.2.6",
        "ParameterGroupName": "default.memorydb-redis6",
        "ParameterGroupStatus": "in-sync",
        "SecurityGroups": [
            {
                "SecurityGroupId": "sg-0a143xxxx45c9fae",
                "Status": "active"
            }
        ],
        "SubnetGroupName": "my-sg",
        "TLSEnabled": true,
        "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:cluster/my-cluster",
        "SnapshotRetentionLimit": 0,
        "MaintenanceWindow": "wed:03:00-wed:04:00",
        "SnapshotWindow": "04:30-05:30",
        "AutoMinorVersionUpgrade": true
    }
}
```

Para obtener más información, consulte Minimizing downtime with MultiAZ en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte FailoverShard en la Referencia de comandos de la AWS CLI.

`list-allowed-node-type-updates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-allowed-node-type-updates`.

AWS CLI

Para devolver una lista de actualizaciones de tipo de nodo permitidas

El siguiente list-allowed-node-type-updates devuelve una lista de actualizaciones de tipo de nodo disponibles.

```
aws memorydb list-allowed-node-type-updates
```

Salida:

```
{
    "Cluster": {
        "Name": "my-cluster",
        "Status": "available",
        "NumberOfShards": 2,
        "ClusterEndpoint": {
            "Address": "clustercfg.my-cluster.xxxxxx.memorydb.us-
east-1.amazonaws.com",
            "Port": 6379
        },
        "NodeType": "db.r6g.large",
        "EngineVersion": "6.2",
        "EnginePatchVersion": "6.2.6",
        "ParameterGroupName": "default.memorydb-redis6",
        "ParameterGroupStatus": "in-sync",
        "SecurityGroups": [
            {
                "SecurityGroupId": "sg-0a143xxxx45c9fae",
                "Status": "active"
            }
        ],
        "SubnetGroupName": "my-sg",
        "TLSEnabled": true,
        "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:cluster/my-cluster",
        "SnapshotRetentionLimit": 0,
        "MaintenanceWindow": "wed:03:00-wed:04:00",
        "SnapshotWindow": "04:30-05:30",
        "AutoMinorVersionUpgrade": true
    }
}
```

Para obtener más información, consulte Scaling en la Guía del usuario de MemoryDB .

- Para obtener información sobre la API, consulte ListAllowedNodeTypeUpdates en la Referencia de comandos de la AWS CLI.

`list-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags`.

AWS CLI

Para devolver una lista de etiquetas

El siguiente list-tags devuelve una lista de etiquetas.

```
aws memorydb list-tags \
    --resource-arn arn:aws:memorydb:us-east-1:491658xxxxxx:cluster/my-cluster
```

Salida:

```
{
    "TagList": [
        {
            "Key": "mytag",
            "Value": "myvalue"
        }
    ]
}
```

Para obtener más información, consulte Tagging resources en la Guía del usuario de MemoryDB.

- Para obtener más información sobre la API, consulte ListTags en la Referencia de comandos de la AWS CLI.

`reset-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-parameter-group`.

AWS CLI

Para restablecer un grupo de parámetros

El siguiente reset-parameter-group` restablece un grupo de parámetros.

```
aws memorydb reset-parameter-group \
    --parameter-group-name my-parameter-group \
    --all-parameters
```

Salida:

```
{
    "ParameterGroup": {
        "Name": "my-parameter-group",
```

```
        "Family": "memorydb_redis6",
        "Description": "my parameter group",
        "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:parametergroup/my-parameter-
group"
    }
}
```

Para obtener más información, consulte Configuring engine parameters using parameter groups en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte ResetParameterGroup en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para etiquetar un recurso

El siguiente tag-resource` agrega una etiqueta a un recurso.

```
aws memorydb tag-resource \
    --resource-arn arn:aws:memorydb:us-east-1:491658xxxxxx:cluster/my-cluster \
    --tags Key="mykey",Value="myvalue"
```

Salida:

```
{
    "TagList": [
        {
            "Key": "mytag",
            "Value": "myvalue"
        },
        {
            "Key": "mykey",
            "Value": "myvalue"
        }
    ]
}
```

Para obtener más información, consulte Tagging resources en la Guía del usuario de MemoryDB.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para actualizar una ACL

El siguiente update-acl` actualiza una ACL añadiendo un usuario.

```
aws memorydb untag-resource \
    --resource-arn arn:aws:memorydb:us-east-1:491658xxxxx:cluster/my-cluster \
    --tag-keys mykey
```

Salida:

```
{
    "TagList": [
        {
            "Key": "mytag",
            "Value": "myvalue"
        }
    ]
}
```

Para obtener más información, consulte Tagging resources en la Guía del usuario de MemoryDB.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-cluster`.

AWS CLI

Para actualizar un clúster

El siguiente update-cluster`` actualiza el grupo de parámetros de un clúster a my-parameter-group.

```
aws memorydb update-cluster \
    --cluster-name my-cluster \
    --parameter-group-name my-parameter-group
```

Salida:

```
{
    "Cluster": {
        "Name": "my-cluster",
        "Status": "available",
        "NumberOfShards": 2,
        "AvailabilityMode": "MultiAZ",
        "ClusterEndpoint": {
            "Address": "clustercfg.my-cluster.llru6f.memorydb.us-
east-1.amazonaws.com",
            "Port": 6379
        },
        "NodeType": "db.r6g.large",
        "EngineVersion": "6.2",
        "EnginePatchVersion": "6.2.6",
        "ParameterGroupName": "my-parameter-group",
        "ParameterGroupStatus": "in-sync",
        "SecurityGroups": [
            {
                "SecurityGroupId": "sg-0a143xxxxxc9fae",
                "Status": "active"
            }
        ],
        "SubnetGroupName": "pat-sg",
        "TLSEnabled": true,
        "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:cluster/my-cluster",
        "SnapshotRetentionLimit": 0,
        "MaintenanceWindow": "wed:03:00-wed:04:00",
        "SnapshotWindow": "04:30-05:30",
        "ACLName": "my-acl",
        "AutoMinorVersionUpgrade": true
    }
}
```

Para obtener más información, consulte Modifying a cluster en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte UpdateCluster en la Referencia de comandos de la AWS CLI.

`update-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-parameter-group`.

AWS CLI

Para actualizar un grupo de parámetros

El siguiente update-parameter-group`` actualiza un grupo de parámetros.

```
aws memorydb update-parameter-group \
    --parameter-group-name my-parameter-group \
    --parameter-name-values "ParameterName=activedefrag, ParameterValue=no"
```

Salida:

```
{
    "ParameterGroup": {
        "Name": "my-parameter-group",
        "Family": "memorydb_redis6",
        "Description": "my parameter group",
        "ARN": "arn:aws:memorydb:us-east-1:49165xxxxxx:parametergroup/my-parameter-
group"
    }
}
```

Para obtener más información, consulte Modifying a parameter group en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte UpdateParameterGroup en la Referencia de comandos de AWS CLI.

`update-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-subnet-group`.

AWS CLI

Para actualizar un grupo de subredes

El siguiente update-subnet-group` actualiza el ID de subred de un grupo de subredes.

```
aws memorydb update-subnet-group \
    --subnet-group-name my-sg \
    --subnet-ids subnet-01f29d458f3xxxxx
```

Salida:

```
{
    "SubnetGroup": {
        "Name": "my-sg-1",
        "Description": "my-sg",
        "VpcId": "vpc-09d2cfc01xxxxxxx",
        "Subnets": [
            {
                "Identifier": "subnet-01f29d458fxxxxxx",
                "AvailabilityZone": {
                    "Name": "us-east-1a"
                }
            }
        ],
        "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:subnetgroup/my-sg"
    }
}
```

Para obtener más información, consulte Subnets and subnet groups en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte UpdateSubnetGroup en la Referencia de comandos de la AWS CLI.

update-user

En el siguiente ejemplo de código, se muestra cómo utilizar `update-user`.

AWS CLI

Para actualizar un usuario

El siguiente `update-user` modifica la cadena de acceso de un usuario.

```
aws memorydb update-user \
```

```
    --user-name my-user \
    --access-string "off ~objects:* ~items:* ~public:* resetchannels -@all"
```

Salida:

```
{
    "User": {
        "Name": "my-user",
        "Status": "modifying",
        "AccessString": "off ~objects:* ~items:* ~public:* resetchannels -@all",
        "ACLNames": [
            "myt-acl"
        ],
        "MinimumEngineVersion": "6.2",
        "Authentication": {
            "Type": "password",
            "PasswordCount": 2
        },
        "ARN": "arn:aws:memorydb:us-east-1:491658xxxxxx:user/my-user"
    }
}
```

Para obtener más información, consulte Authenticating users with Access Control Lists en la Guía del usuario de MemoryDB.

- Para obtener información sobre la API, consulte UpdateUser en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon MSK que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon MSK.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-cluster`.

AWS CLI

Para crear un clúster de Amazon MSK

En el siguiente ejemplo de `create-cluster`, se crea un clúster de MSK denominado `MessagingCluster` con tres nodos de agente. Un archivo JSON denominado `brokernodegroupinfo.json` especifica las tres subredes en las que desea que Amazon MSK distribuya los nodos de agente. En este ejemplo no se especifica el nivel de supervisión, por lo que el clúster obtiene el nivel `DEFAULT`.

```
aws kafka create-cluster \
    --cluster-name "MessagingCluster" \
    --broker-node-group-info file://brokernodegroupinfo.json \
    --kafka-version "2.2.1" \
    --number-of-broker-nodes 3
```

Contenido de `brokernodegroupinfo.json`:

```
{
    "InstanceType": "kafka.m5.xlarge",
    "BrokerAZDistribution": "DEFAULT",
    "ClientSubnets": [
        "subnet-0123456789111abcd",
        "subnet-0123456789222abcd",
        "subnet-0123456789333abcd"
    ]
}
```

Salida:

```
{
    "ClusterArn": "arn:aws:kafka:us-west-2:123456789012:cluster/MessagingCluster/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE-2",
```

```
    "ClusterName": "MessagingCluster",
    "State": "CREATING"
}
```

Para obtener más información, consulte Creación de un clúster de Amazon MSK aprovisionado en la Guía para desarrolladores de Amazon Managed Streaming para Apache Kafka.

- Para obtener información sobre la API, consulte CreateCluster en la Referencia de comandos de la AWS CLI.

`create-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-configuration`.

AWS CLI

Para crear una configuración personalizada de Amazon MSK

En el siguiente ejemplo de `create-configuration`, se crea una configuración de MSK personalizada con las propiedades del servidor que se especifican en el archivo de entrada.

```
aws kafka create-configuration \
    --name "CustomConfiguration" \
    --description "Topic autocreation enabled; Apache ZooKeeper timeout 2000 ms; Log
 rolling 604800000 ms." \
    --kafka-versions "2.2.1" \
    --server-properties file://configuration.txt
```

Contenido de `configuration.txt`:

```
auto.create.topics.enable = true
zookeeper.connection.timeout.ms = 2000
log.roll.ms = 604800000
```

Este comando no genera ninguna salida. Salida:

```
{
    "Arn": "arn:aws:kafka:us-west-2:123456789012:configuration/CustomConfiguration/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE-2",
    "CreationTime": "2019-10-09T15:26:05.548Z",
    "LatestRevision":
        {
```

```
            "CreationTime": "2019-10-09T15:26:05.548Z",
            "Description": "Topic autocreation enabled; Apache ZooKeeper timeout
 2000 ms; Log rolling 604800000 ms.",
            "Revision": 1
        },
    "Name": "CustomConfiguration"
}
```

Para obtener más información, consulte Operaciones de configuración de Amazon MSK en la Guía para desarrolladores de Amazon Managed Streaming para Apache Kafka.

- Para obtener información sobre la API, consulte CreateConfiguration en la Referencia de comandos de la AWS CLI.

`describe-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cluster`.

AWS CLI

Para describir un clúster

En el siguiente ejemplo de `describe-cluster`, se describe un clúster de Amazon MSK.

```
aws kafka describe-cluster \
    --cluster-arn arn:aws:kafka:us-east-1:123456789012:cluster/demo-
cluster-1/6357e0b2-0e6a-4b86-a0b4-70df934c2e31-5
```

Salida:

```
{
    "ClusterInfo": {
        "BrokerNodeGroupInfo": {
            "BrokerAZDistribution": "DEFAULT",
            "ClientSubnets": [
                "subnet-cbfff283",
                "subnet-6746046b"
            ],
            "InstanceType": "kafka.m5.large",
            "SecurityGroups": [
                "sg-f839b688"
            ],
            "StorageInfo": {
```

```
                "EbsStorageInfo": {
                    "VolumeSize": 100
                }
            }
        },
        "ClusterArn": "arn:aws:kafka:us-east-1:123456789012:cluster/demo-
cluster-1/6357e0b2-0e6a-4b86-a0b4-70df934c2e31-5",
        "ClusterName": "demo-cluster-1",
        "CreationTime": "2020-07-09T02:31:36.223000+00:00",
        "CurrentBrokerSoftwareInfo": {
            "KafkaVersion": "2.2.1"
        },
        "CurrentVersion": "K3AEGXETSR30VB",
        "EncryptionInfo": {
            "EncryptionAtRest": {
                "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a7ca56d5-0768-4b64-a670-339a9fbef81c"
            },
            "EncryptionInTransit": {
                "ClientBroker": "TLS_PLAINTEXT",
                "InCluster": true
            }
        },
        "EnhancedMonitoring": "DEFAULT",
        "OpenMonitoring": {
            "Prometheus": {
                "JmxExporter": {
                    "EnabledInBroker": false
                },
                "NodeExporter": {
                    "EnabledInBroker": false
                }
            }
        },
        "NumberOfBrokerNodes": 2,
        "State": "ACTIVE",
        "Tags": {},
        "ZookeeperConnectString": "z-2.demo-cluster-1.xuy0sb.c5.kafka.us-
east-1.amazonaws.com:2181,z-1.demo-cluster-1.xuy0sb.c5.kafka.us-
east-1.amazonaws.com:2181,z-3.demo-cluster-1.xuy0sb.c5.kafka.us-
east-1.amazonaws.com:2181"
    }
}
```

Para obtener más información, consulte Enumeración de clústeres de Amazon MSK en la Guía para desarrolladores de Amazon Managed Streaming para Apache Kafka.

- Para obtener información sobre la API, consulte DescribeCluster en la Referencia de comandos de la AWS CLI.

`get-bootstrap-brokers`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bootstrap-brokers`.

AWS CLI

Para obtener los agentes de arranque

En el siguiente ejemplo de `get-bootstrap-brokers`, se recupera la información del agente de arranque para un clúster de Amazon MSK.

```
aws kafka get-bootstrap-brokers \
    --cluster-arn arn:aws:kafka:us-east-1:123456789012:cluster/demo-cluster-1/6357e0b2-0e6a-4b86-a0b4-70df934c2e31-5
```

Salida:

```
{
    "BootstrapBrokerString": "b-1.demo-cluster-1.xuy0sb.c5.kafka.us-east-1.amazonaws.com:9092,b-2.demo-cluster-1.xuy0sb.c5.kafka.us-east-1.amazonaws.com:9092",
    "BootstrapBrokerStringTls": "b-1.demo-cluster-1.xuy0sb.c5.kafka.us-east-1.amazonaws.com:9094,b-2.demo-cluster-1.xuy0sb.c5.kafka.us-east-1.amazonaws.com:9094"
}
```

Para obtener más información, consulte Obtención de agentes de arranque para un clúster de Amazon MSK en la Guía para desarrolladores de Amazon Managed Streaming para Apache Kafka.

- Para obtener información sobre la API, consulte GetBootstrapBrokers en la Referencia de comandos de la AWS CLI.

`list-clusters`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-clusters`.

AWS CLI

Para enumerar los clústeres disponibles

En el siguiente ejemplo de `list-clusters`, se enumeran todos los clústeres de Amazon MSK de su cuenta de AWS.

```
aws kafka list-clusters
```

Salida:

```
{
    "ClusterInfoList": [
        {
            "BrokerNodeGroupInfo": {
                "BrokerAZDistribution": "DEFAULT",
                "ClientSubnets": [
                    "subnet-cbfff283",
                    "subnet-6746046b"
                ],
                "InstanceType": "kafka.m5.large",
                "SecurityGroups": [
                    "sg-f839b688"
                ],
                "StorageInfo": {
                    "EbsStorageInfo": {
                        "VolumeSize": 100
                    }
                }
            },
            "ClusterArn": "arn:aws:kafka:us-east-1:123456789012:cluster/demo-
cluster-1/6357e0b2-0e6a-4b86-a0b4-70df934c2e31-5",
            "ClusterName": "demo-cluster-1",
            "CreationTime": "2020-07-09T02:31:36.223000+00:00",
            "CurrentBrokerSoftwareInfo": {
                "KafkaVersion": "2.2.1"
            },
            "CurrentVersion": "K3AEGXETSR30VB",
            "EncryptionInfo": {
                "EncryptionAtRest": {
                    "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a7ca56d5-0768-4b64-a670-339a9fbef81c"
                },
```

```
                "EncryptionInTransit": {
                    "ClientBroker": "TLS_PLAINTEXT",
                    "InCluster": true
                }
            },
            "EnhancedMonitoring": "DEFAULT",
            "OpenMonitoring": {
                "Prometheus": {
                    "JmxExporter": {
                        "EnabledInBroker": false
                    },
                    "NodeExporter": {
                        "EnabledInBroker": false
                    }
                }
            },
            "NumberOfBrokerNodes": 2,
            "State": "ACTIVE",
            "Tags": {},
            "ZookeeperConnectString": "z-2.demo-cluster-1.xuy0sb.c5.kafka.us-
east-1.amazonaws.com:2181,z-1.demo-cluster-1.xuy0sb.c5.kafka.us-
east-1.amazonaws.com:2181,z-3.demo-cluster-1.xuy0sb.c5.kafka.us-
east-1.amazonaws.com:2181"
        }
    ]
}
```

Para obtener más información, consulte Enumeración de clústeres de Amazon MSK en la Guía para desarrolladores de Amazon Managed Streaming para Apache Kafka.

- Para obtener información sobre la API, consulte ListClusters en la Referencia de comandos de la AWS CLI.

`update-broker-storage`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-broker-storage`.

AWS CLI

Para actualizar el almacenamiento de EBS para agentes

En el siguiente ejemplo de `update-broker-storage`, se actualiza la cantidad de almacenamiento de EBS para todos los agentes del clúster. Amazon MSK establece la misma

cantidad de almacenamiento objetivo para cada agente que la cantidad especificada en el ejemplo. Para obtener la versión actual del clúster, descríbalo o enumere todos los clústeres.

```
aws kafka update-broker-storage \
    --cluster-arn "arn:aws:kafka:us-west-2:123456789012:cluster/MessagingCluster/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE-2" \
    --current-version "K21V3IB1VIZYYH" \
    --target-broker-ebs-volume-info "KafkaBrokerNodeId=ALL,VolumeSizeGB=1100"
```

La salida devuelve un ARN para esta operación `update-broker-storage`. Para determinar si la operación se ha completado, utilice el comando `describe-cluster-operation` con este ARN como entrada.

```
{
    "ClusterArn": "arn:aws:kafka:us-west-2:123456789012:cluster/MessagingCluster/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE-2",
    "ClusterOperationArn": "arn:aws:kafka:us-west-2:123456789012:cluster-
operation/V123450123/a1b2c3d4-1234-abcd-cdef-22222EXAMPLE-2/a1b2c3d4-abcd-1234-
bcde-33333EXAMPLE"
}
```

Para obtener más información, consulte Escalado vertical del almacenamiento del agente de Amazon MSK en la Guía para desarrolladores de Amazon Managed Streaming para Apache Kafka.

- Para obtener información sobre la API, consulte UpdateBrokerStorage en la Referencia de comandos de la AWS CLI.

`update-cluster-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-cluster-configuration`.

AWS CLI

Para actualizar la configuración de un clúster de Amazon MSK

En el siguiente ejemplo de `update-cluster-configuration`, se actualiza la configuración del clúster de MSK existente especificado. Utiliza una configuración de MSK personalizada.

```
aws kafka update-cluster-configuration \
```

```
    --cluster-arn "arn:aws:kafka:us-west-2:123456789012:cluster/MessagingCluster/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE-2" \
    --configuration-info file://configuration-info.json \
    --current-version "K21V3IB1VIZYYH"
```

Contenido de `configuration-info.json`:

```
{
    "Arn": "arn:aws:kafka:us-west-2:123456789012:configuration/CustomConfiguration/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE-2",
    "Revision": 1
}
```

La salida devuelve un ARN para esta operación `update-cluster-configuration`. Para determinar si la operación se ha completado, utilice el comando `describe-cluster-operation` con este ARN como entrada.

```
{
    "ClusterArn": "arn:aws:kafka:us-west-2:123456789012:cluster/MessagingCluster/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE-2",
    "ClusterOperationArn": "arn:aws:kafka:us-west-2:123456789012:cluster-
operation/V123450123/a1b2c3d4-1234-abcd-cdef-22222EXAMPLE-2/a1b2c3d4-abcd-1234-
bcde-33333EXAMPLE"
}
```

Para obtener más información, consulte Update the Configuration of an Amazon MSK Cluster en la Guía para desarrolladores de Amazon Managed Streaming para Apache Kafka.

- Para obtener información acerca de la API, consulte UpdateClusterConfiguration en la Referencia de comandos de la AWS CLI.

Ejemplos de monitor del flujo de red mediante AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios comunes mediante la AWS Command Line Interface con monitor de flujo de red.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-monitor`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-monitor`.

AWS CLI

Creación de un monitor

En el siguiente ejemplo de `create-monitor`, se crea un monitor denominado demo en la cuenta especificada.

```
aws networkflowmonitor create-monitor \
    --monitor-name demo \
    --local-resources type="AWS::EC2::VPC",identifier="arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-03ea55eeda25adbb0"  \
    --scope-arn arn:aws:networkflowmonitor:us-east-1:123456789012:scope/
e21cda79-30a0-4c12-9299-d8629d76d8cf
```

Salida:

```
{
    "monitorArn": "arn:aws:networkflowmonitor:us-east-1:123456789012:monitor/demo",
    "monitorName": "demo",
    "monitorStatus": "ACTIVE",
    "tags": {}
}
```

Para obtener más información, consulte Creación de un monitor en monitor de flujo de red en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte CreateMonitor en la Referencia de comandos de la AWS CLI.

`create-scope`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-scope`.

AWS CLI

Creación de un alcance

En el siguiente ejemplo de `create-scope`, se crea un ámbito que incluye un conjunto de recursos para los que el monitor de flujo de red generará métricas de tráfico de red.

```
aws networkflowmonitor create-scope \
    --targets '[{"targetIdentifier":{"targetId":
{"accountId":"123456789012"},"targetType":"ACCOUNT"},"region":"us-east-1"}]'
```

Salida:

```
{
    "scopeId": "97626f8d-8a21-4b5d-813a-1a0962dd4615",
    "status": "IN_PROGRESS",
    "tags": {}
}
```

Para obtener más información, consulte Componentes y características de un monitor de flujo de red en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte CreateScope en la Referencia de comandos de la AWS CLI.

`delete-monitor`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-monitor`.

AWS CLI

Para eliminar un monitor

En el siguiente ejemplo de `delete-monitor`, se elimina un monitor denominado demo en la cuenta especificada.

```
aws networkflowmonitor delete-monitor \
    --monitor-name demo
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de un monitor en monitor de flujo de red en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DeleteMonitor en la Referencia de comandos de AWS CLI.

`delete-scope`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-scope`.

AWS CLI

Eliminación de un alcance

En el siguiente ejemplo de `delete-scope`, se elimina el alcance especificado.

```
aws networkflowmonitor delete-scope \
    --scope-id fdc20616-6bb4-4242-a24e-a748e65ca7ac
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Componentes y características de un monitor de flujo de red en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte DeleteScope en la Referencia de comandos de la AWS CLI.

`get-monitor`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-monitor`.

AWS CLI

Recuperación de información sobre un monitor

En el siguiente ejemplo de `get-monitor`, se muestra información acerca del monitor denominado `demo` en la cuenta especificada.

```
aws networkflowmonitor get-monitor \
    --monitor-name Demo
```

Salida:

```
{
    "monitorArn": "arn:aws:networkflowmonitor:us-east-1:123456789012:monitor/Demo",
    "monitorName": "Demo",
    "monitorStatus": "ACTIVE",
    "localResources": [
        {
            "type": "AWS::EC2::VPC",
            "identifier": "arn:aws:ec2:us-east-1:123456789012:vpc/
vpc-03ea55eeda25adbb0"
        }
    ],
    "remoteResources": [],
    "createdAt": "2024-12-09T12:21:51.616000-06:00",
    "modifiedAt": "2024-12-09T12:21:55.412000-06:00",
    "tags": {}
}
```

Para obtener más información, consulte Componentes y características de un monitor de flujo de red en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetMonitor en la Referencia de comandos de la AWS CLI.

`get-query-results-workload-insights-top-contributors-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-query-results-workload-insights-top-contributors-data`.

AWS CLI

Recuperación de los datos de los principales colaboradores sobre la información de la carga de trabajo

En el siguiente ejemplo de `get-query-results-workload-insights-top-contributors-data`, se devuelven los datos de la consulta especificada.

```
aws networkflowmonitor get-query-results-workload-insights-top-contributors-data \
    --scope-id e21cda79-30a0-4c12-9299-d8629d76d8cf \
    --query-id cc4f4ab3-3103-33b8-80ff-d6597a0c6cea
```

Salida:

```
{
    "datapoints": [
        {
            "timestamps": [
                "2024-12-09T19:00:00+00:00",
                "2024-12-09T19:05:00+00:00",
                "2024-12-09T19:10:00+00:00"
            ],
            "values": [
                259943.0,
                194856.0,
                216432.0
            ],
            "label": "use1-az6"
        }
    ],
    "unit": "Bytes"
}
```

Para obtener más información, consulte Evaluate network flows with workload insights en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetQueryResultsWorkloadInsightsTopContributorsData en la Referencia de comandos de la AWS CLI.

`get-query-results-workload-insights-top-contributors`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-query-results-workload-insights-top-contributors`.

AWS CLI

Recuperación de los colaboradores principales sobre la información de la carga de trabajo

En el siguiente ejemplo de `get-query-results-workload-insights-top-contributors`, se devuelven los datos de la consulta especificada.

```
aws networkflowmonitor get-query-results-workload-insights-top-contributors \
    --scope-id e21cda79-30a0-4c12-9299-d8629d76d8cf \
```

```
    --query-id 1fc423d3-b144-37a6-80e6-e2c7d26eea0c
```

Salida:

```
{
    "topContributors": [
        {
            "accountId": "123456789012",
            "localSubnetId": "subnet-0a5b30fb95dca2c14",
            "localAz": "use1-az6",
            "localVpcId": "vpc-03ea55eeda25adbb0",
            "localRegion": "us-east-1",
            "remoteIdentifier": "",
            "value": 908443,
            "localSubnetArn": "arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0a5b30fb95dca2c14",
            "localVpcArn": "arn:aws:ec2:us-east-1:123456789012:vpc/
vpc-03ea55eeda25adbb0"
        }
    ]
}
```

Para obtener más información, consulte Evaluate network flows with workload insights en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetQueryResultsWorkloadInsightsTopContributors en la Referencia de comandos de la AWS CLI.

`get-query-status-monitor-top-contributors`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-query-status-monitor-top-contributors`.

AWS CLI

Recuperación del estado de la consulta

En el siguiente ejemplo de `get-query-status-monitor-top-contributors`, se muestra el estado actual de la consulta en la cuenta especificada.

```
aws networkflowmonitor get-query-status-monitor-top-contributors \
```

```
    --monitor-name Demo \
    --query-id 5398eabd-bc40-3f5f-aba3-bcb639d3c7ca
```

Salida:

```
{
    "status": "SUCCEEDED"
}
```

Para obtener más información, consulte Evaluate network flows with workload insights en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetQueryStatusMonitorTopContributors en la Referencia de comandos de la AWS CLI.

`get-query-status-workload-insights-top-contributors-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-query-status-workload-insights-top-contributors-data`.

AWS CLI

Recuperación del estado de la consulta

En el siguiente ejemplo de `get-query-status-workload-insights-top-contributors-data`, se muestra el estado actual de la consulta en la cuenta especificada.

```
aws networkflowmonitor get-query-status-workload-insights-top-contributors-data \
    --scope-id e21cda79-30a0-4c12-9299-d8629d76d8cf \
    --query-id 4333754d-8ae1-3f29-b6b7-c36db2e7f8ac
```

Salida:

```
{
    "status": "SUCCEEDED"
}
```

Para obtener más información, consulte Evaluate network flows with workload insights en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetQueryStatusWorkloadInsightsTopContributorsData en la Referencia de comandos de la AWS CLI.

`get-query-status-workload-insights-top-contributors`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-query-status-workload-insights-top-contributors`.

AWS CLI

Recuperación del estado de la consulta

En el siguiente ejemplo de `get-query-status-workload-insights-top-contributors`, se muestra el estado actual de la consulta en la cuenta especificada.

```
aws networkflowmonitor get-query-status-workload-insights-top-contributors \
    --scope-id e21cda79-30a0-4c12-9299-d8629d76d8cf \
    --query-id f2a87c70-3e5a-362e-8beb-4747d13d8419
```

Salida:

```
{
    "status": "SUCCEEDED"
}
```

Para obtener más información, consulte Evaluate network flows with workload insights en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetQueryStatusWorkloadInsightsTopContributors en la Referencia de comandos de la AWS CLI.

`get-scope`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-scope`.

AWS CLI

Recuperación de información sobre un alcance

En el siguiente ejemplo de `get-scope`, se muestra información sobre un alcance, como el estado, las etiquetas, el nombre y los detalles de destino.

```
aws networkflowmonitor get-scope \
    --scope-id e21cda79-30a0-4c12-9299-d8629d76d8cf
```

Salida:

```
{
    "scopeId": "e21cda79-30a0-4c12-9299-d8629d76d8cf",
    "status": "SUCCEEDED",
    "scopeArn": "arn:aws:networkflowmonitor:us-east-1:123456789012:scope/
e21cda79-30a0-4c12-9299-d8629d76d8cf",
    "targets": [
        {
            "targetIdentifier": {
                "targetId": {
                    "accountId": "123456789012"
                },
                "targetType": "ACCOUNT"
            },
            "region": "us-east-1"
        }
    ],
    "tags": {}
}
```

Para obtener más información, consulte Componentes y características de un monitor de flujo de red en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte GetScope en la Referencia de comandos de la AWS CLI.

`list-monitors`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-monitors`.

AWS CLI

Recuperación de una lista de monitores

En el siguiente ejemplo de `list-monitors`, se devuelven todos los monitores de la cuenta especificada.

```
aws networkflowmonitor list-monitors
```

Salida:

```
{
    "monitors": [
        {
            "monitorArn": "arn:aws:networkflowmonitor:us-
east-1:123456789012:monitor/Demo",
            "monitorName": "Demo",
            "monitorStatus": "ACTIVE"
        }
    ]
}
```

Para obtener más información, consulte Componentes y características de un monitor de flujo de red en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListMonitors en la Referencia de comandos de la AWS CLI.

`list-scopes`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-scopes`.

AWS CLI

Recuperación de una lista de alcances

En el siguiente ejemplo de `list-scopes`, se muestran todos los alcances de la cuenta especificada.

```
aws networkflowmonitor list-scopes
```

Salida:

```
{
    "scopes": [
        {
```

```
            "scopeId": "fdc20616-6bb4-4242-a24e-a748e65ca7ac",
            "status": "SUCCEEDED",
            "scopeArn": "arn:aws:networkflowmonitor:us-east-1:123456789012:scope/
fdc20616-6bb4-4242-a24e-a748e65ca7ac"
        }
    ]
}
```

Para obtener más información, consulte Componentes y características de un monitor de flujo de red en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte ListScopes en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Muestra de las etiquetas

En el siguiente ejemplo de `list-tags-for-resource`, se devuelven todas las etiquetas asociadas al recurso especificado.

```
aws networkflowmonitor list-tags-for-resource \
    --resource-arn arn:aws:networkflowmonitor:us-east-1:123456789012:monitor/Demo
```

Salida:

```
{
    "tags": {
        "Value": "Production",
        "Key": "stack"
    }
}
```

Para obtener más información, consulte Etiquetado de los recursos de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`start-query-monitor-top-contributors`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-query-monitor-top-contributors`.

AWS CLI

Inicio de una consulta

En el siguiente ejemplo de `start-query-monitor-top-contributors`, se inicia la consulta que devuelve un ID de consulta para recuperar los colaboradores principales.

```
aws networkflowmonitor start-query-monitor-top-contributors \
    --monitor-name Demo \
    --start-time 2024-12-09T19:00:00Z \
    --end-time 2024-12-09T19:15:00Z \
    --metric-name DATA_TRANSFERRED \
    --destination-category UNCLASSIFIED
```

Salida:

```
{
    "queryId": "aecd3a88-0283-35b0-a17d-6e944dc8531d"
}
```

Para obtener más información, consulte Evaluate network flows with workload insights en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte StartQueryMonitorTopContributors en la Referencia de comandos de la AWS CLI.

`start-query-workload-insights-top-contributors-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-query-workload-insights-top-contributors-data`.

AWS CLI

Inicio de una consulta

En el siguiente ejemplo de `start-query-workload-insights-top-contributors-data`, se inicia la consulta que devuelve un ID de consulta para recuperar los colaboradores principales.

```
aws networkflowmonitor start-query-workload-insights-top-contributors-data \
    --scope-id e21cda79-30a0-4c12-9299-d8629d76d8cf \
    --start-time 2024-12-09T19:00:00Z \
    --end-time 2024-12-09T19:15:00Z \
    --metric-name DATA_TRANSFERRED \
    --destination-category UNCLASSIFIED
```

Salida:

```
{
    "queryId": "cc4f4ab3-3103-33b8-80ff-d6597a0c6cea"
}
```

Para obtener más información, consulte Evaluate network flows with workload insights en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte StartQueryWorkloadInsightsTopContributorsData en la Referencia de comandos de la AWS CLI.

`start-query-workload-insights-top-contributors`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-query-workload-insights-top-contributors`.

AWS CLI

Inicio de una consulta

En el siguiente ejemplo de `start-query-workload-insights-top-contributors`, se inicia la consulta que devuelve un ID de consulta para recuperar los colaboradores principales.

```
aws networkflowmonitor start-query-workload-insights-top-contributors \
    --scope-id e21cda79-30a0-4c12-9299-d8629d76d8cf \
    --start-time 2024-12-09T19:00:00Z \
    --end-time 2024-12-09T19:15:00Z \
    --metric-name DATA_TRANSFERRED \
    --destination-category UNCLASSIFIED
```

Salida:

```
{
    "queryId": "1fc423d3-b144-37a6-80e6-e2c7d26eea0c"
}
```

Para obtener más información, consulte Evaluate network flows with workload insights en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte StartQueryWorkloadInsightsTopContributors en la Referencia de comandos de la AWS CLI.

`stop-query-monitor-top-contributors`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-query-monitor-top-contributors`.

AWS CLI

Detención de una consulta

En el siguiente ejemplo de `stop-query-monitor-top-contributors`, se detiene la consulta en la cuenta especificada.

```
aws networkflowmonitor stop-query-monitor-top-contributors \
    --monitor-name Demo \
    --query-id aecd3a88-0283-35b0-a17d-6e944dc8531d
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Evaluate network flows with workload insights en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte StopQueryMonitorTopContributors en la Referencia de comandos de la AWS CLI.

`stop-query-workload-insights-top-contributors-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-query-workload-insights-top-contributors-data`.

AWS CLI

Detención de una consulta

En el siguiente ejemplo de `stop-query-workload-insights-top-contributors-data`, se detiene la consulta en la cuenta especificada.

```
aws networkflowmonitor stop-query-workload-insights-top-contributors-data \
    --scope-id e21cda79-30a0-4c12-9299-d8629d76d8cf \
    --query-id cc4f4ab3-3103-33b8-80ff-d6597a0c6cea
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Evaluate network flows with workload insights en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte StopQueryWorkloadInsightsTopContributorsData en la Referencia de comandos de la AWS CLI.

`stop-query-workload-insights-top-contributors`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-query-workload-insights-top-contributors`.

AWS CLI

Detención de una consulta

En el siguiente ejemplo de `stop-query-workload-insights-top-contributors`, se detiene la consulta en la cuenta especificada.

```
aws networkflowmonitor stop-query-workload-insights-top-contributors \
    --scope-id e21cda79-30a0-4c12-9299-d8629d76d8cf \
    --query-id 1fc423d3-b144-37a6-80e6-e2c7d26eea0c
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Evaluate network flows with workload insights en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte StopQueryWorkloadInsightsTopContributors en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Adición de una etiqueta al recurso especificado

En el siguiente ejemplo de `tag-resource`, se agrega una etiqueta al monitor en la cuenta especificada.

```
aws networkflowmonitor tag-resource \
    --resource-arn arn:aws:networkflowmonitor:us-east-1:123456789012:monitor/Demo \
    --tags Key=stack,Value=Production
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de los recursos de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de una etiqueta del recurso especificado

En el siguiente ejemplo de `untag-resource`, se elimina una etiqueta del monitor en la cuenta especificada.

```
aws networkflowmonitor untag-resource \
    --resource-arn arn:aws:networkflowmonitor:us-east-1:123456789012:monitor/Demo \
    --tag-keys stack
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de los recursos de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-monitor`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-monitor`.

AWS CLI

Actualización de un monitor existente

En el siguiente ejemplo de `update-monitor`, se actualiza el monitor denominado `Demo` en la cuenta especificada.

```
aws networkflowmonitor update-monitor \
    --monitor-name Demo \
    --local-resources-to-add type="AWS::EC2::VPC",identifier="arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-048d08dfbec623f94"
```

Salida:

```
{
    "monitorArn": "arn:aws:networkflowmonitor:us-east-1:123456789012:monitor/Demo",
    "monitorName": "Demo",
    "monitorStatus": "ACTIVE",
    "tags": {
        "Value": "Production",
        "Key": "stack"
    }
}
```

Para obtener más información, consulte Componentes y características de un monitor de flujo de red en la Guía del usuario de Amazon CloudWatch.

- Para obtener información sobre la API, consulte UpdateMonitor en la Referencia de comandos de la AWS CLI.

Ejemplos de Network Manager que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Administrador de red.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-customer-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-customer-gateway`.

AWS CLI

Para asociar una puerta de enlace de cliente

El siguiente ejemplo de `associate-customer-gateway` asocia la puerta de enlace de cliente `cgw-11223344556677889` de la red global especificada con el dispositivo `device-07f6fd08867abc123`.

```
aws networkmanager associate-customer-gateway \
    --customer-gateway-arn arn:aws:ec2:us-west-2:123456789012:customer-gateway/
cgw-11223344556677889  \
    --global-network-id global-network-01231231231231231 \
    --device-id device-07f6fd08867abc123 \
    --region us-west-2
```

Salida:

```
{
    "CustomerGatewayAssociation": {
```

```
        "CustomerGatewayArn": "arn:aws:ec2:us-west-2:123456789012:customer-gateway/
cgw-11223344556677889",
        "GlobalNetworkId": "global-network-01231231231231231",
        "DeviceId": "device-07f6fd08867abc123",
        "State": "PENDING"
    }
}
```

Para obtener más información, consulte Customer Gateway Associations en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte AssociateCustomerGateway en la Referencia de comandos de la AWS CLI.

`associate-link`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-link`.

AWS CLI

Para asociar un enlace

En el siguiente ejemplo de `associate-link` se asocia el enlace `link-11112222aaaabbbb1` al dispositivo `device-07f6fd08867abc123`. El enlace y el dispositivo se encuentran en la red global especificada.

```
aws networkmanager associate-link \
    --global-network-id global-network-01231231231231231 \
    --device-id device-07f6fd08867abc123 \
    --link-id link-11112222aaaabbbb1 \
    --region us-west-2
```

Salida:

```
{
    "LinkAssociation": {
        "GlobalNetworkId": "global-network-01231231231231231",
        "DeviceId": "device-07f6fd08867abc123",
        "LinkId": "link-11112222aaaabbbb1",
        "LinkAssociationState": "PENDING"
    }
```

```
}
```

Para obtener más información, consulte Device and Link Associations en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte AssociateLink en la Referencia de comandos de la AWS CLI.

`create-core-network`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-core-network`.

AWS CLI

Para crear una red principal

En el siguiente ejemplo de `create-core-network` se crea una red principal con una descripción y etiquetas opcionales dentro de una red global WAN en la nube de AWS.

```
aws networkmanager create-core-network \
    --global-network-id global-network-cdef-EXAMPLE22222 \
    --description "Main headquarters location" \
    --tags Key=Name,Value="New York City office"
```

Salida:

```
{
    "CoreNetwork": {
        "GlobalNetworkId": "global-network-cdef-EXAMPLE22222",
        "CoreNetworkId": "core-network-cdef-EXAMPLE33333",
        "CoreNetworkArn": "arn:aws:networkmanager::987654321012:core-network/core-
network-cdef-EXAMPLE33333",
        "Description": "Main headquarters location",
        "CreatedAt": "2022-01-10T19:53:59+00:00",
        "State": "AVAILABLE",
        "Tags": [
            {
                "Key": "Name",
                "Value": "New York City office"
            }
        ]
    }
```

```
}
```

Para obtener más información, consulte Global and core networks en la Guía del usuario de AWS WAN en la nube.

- Para obtener información sobre la API, consulte CreateCoreNetwork en la Referencia de comandos de la AWS CLI.

`create-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-device`.

AWS CLI

Para crear un dispositivo

En el ejemplo siguiente de `create-device` se crea un dispositivo en la red global especificada. Los detalles del dispositivo incluyen descripción, tipo, proveedor, modelo y número de serie.

```
aws networkmanager create-device
    --global-network-id global-network-01231231231231231 \
    --description "New York office device" \
    --type "office device" \
    --vendor "anycompany" \
    --model "abcabc" \
    --serial-number "1234" \
    --region us-west-2
```

Salida:

```
{
    "Device": {
        "DeviceId": "device-07f6fd08867abc123",
        "DeviceArn": "arn:aws:networkmanager::123456789012:device/global-
network-01231231231231231/device-07f6fd08867abc123",
        "GlobalNetworkId": "global-network-01231231231231231",
        "Description": "New York office device",
        "Type": "office device",
        "Vendor": "anycompany",
        "Model": "abcabc",
        "SerialNumber": "1234",
        "CreatedAt": 1575554005.0,
```

```
        "State": "PENDING"
    }
}
```

Para obtener más información, consulte Working with Devices en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte CreateDevice en la Referencia de comandos de AWS CLI.

`create-global-network`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-global-network`.

AWS CLI

Para crear una red global

En el siguiente ejemplo de `create-global-network` se crea una nueva red global. El estado inicial tras la creación es `PENDING`.

```
aws networkmanager create-global-network
```

Salida:

```
{
    "GlobalNetwork": {
        "GlobalNetworkId": "global-network-00a77fc0f722dae74",
        "GlobalNetworkArn": "arn:aws:networkmanager::987654321012:global-network/
global-network-00a77fc0f722dae74",
        "CreatedAt": "2022-03-14T20:31:56+00:00",
        "State": "PENDING"
    }
}
```

- Para obtener información sobre la API, consulte CreateGlobalNetwork en la Referencia de comandos de la AWS CLI.

`create-link`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-link`.

AWS CLI

Para crear un enlace

En el ejemplo siguiente de `create-link` se crea un enlace en la red global especificada. El enlace incluye una descripción y detalles sobre el tipo de enlace, el ancho de banda y el proveedor. El ID del sitio indica el sitio al que está asociado el enlace.

```
aws networkmanager create-link \
    --global-network-id global-network-01231231231231231 \
    --description "VPN Link" \
    --type "broadband" \
    --bandwidth UploadSpeed=10,DownloadSpeed=20 \
    --provider "AnyCompany" \
    --site-id site-444555aaabbb11223 \
    --region us-west-2
```

Salida:

```
{
    "Link": {
        "LinkId": "link-11112222aaaabbbb1",
        "LinkArn": "arn:aws:networkmanager::123456789012:link/global-
network-01231231231231231/link-11112222aaaabbbb1",
        "GlobalNetworkId": "global-network-01231231231231231",
        "SiteId": "site-444555aaabbb11223",
        "Description": "VPN Link",
        "Type": "broadband",
        "Bandwidth": {
            "UploadSpeed": 10,
            "DownloadSpeed": 20
        },
        "Provider": "AnyCompany",
        "CreatedAt": 1575555811.0,
        "State": "PENDING"
    }
}
```

Para obtener más información, consulte Working with Links en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte CreateLink en la Referencia de comandos de la AWS CLI.

`create-site`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-site`.

AWS CLI

Para crear un sitio

En el ejemplo siguiente de `create-site` se crea un sitio en la red global especificada. Los detalles del sitio incluyen una descripción e información de ubicación.

```
aws networkmanager create-site \
    --global-network-id global-network-01231231231231231 \
    --description  "New York head office" \
    --location Latitude=40.7128,Longitude=-74.0060 \
    --region us-west-2
```

Salida:

```
{
    "Site": {
        "SiteId": "site-444555aaabbb11223",
        "SiteArn": "arn:aws:networkmanager::123456789012:site/global-
network-01231231231231231/site-444555aaabbb11223",
        "GlobalNetworkId": "global-network-01231231231231231",
        "Description": "New York head office",
        "Location": {
            "Latitude": "40.7128",
            "Longitude": "-74.0060"
        },
        "CreatedAt": 1575554300.0,
        "State": "PENDING"
    }
}
```

Para obtener más información, consulte Working with Sites en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte CreateSite en la Referencia de comandos de la AWS CLI.

`create-vpc-attachment`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-vpc-attachment`.

AWS CLI

Para crear una asociación a VPC

En el siguiente ejemplo de `create-vpc-attachment` se crea una asociación a VPC compatible con IPv6 en una red principal.

```
aws networkmanager create-vpc-attachment \
    --core-network-id core-network-0fab62fe438d94db6 \
    --vpc-arn arn:aws:ec2:us-east-1:987654321012:vpc/vpc-09f37f69e2786eeb8  \
    --subnet-arns arn:aws:ec2:us-east-1:987654321012:subnet/subnet-04ca4e010857e7bb7
 \
    --Ipv6Support=true
```

Salida:

```
{
    "VpcAttachment": {
        "Attachment": {
            "CoreNetworkId": "core-network-0fab62fe438d94db6",
            "AttachmentId": "attachment-05e1da6eba87a06e6",
            "OwnerAccountId": "987654321012",
            "AttachmentType": "VPC",
            "State": "CREATING",
            "EdgeLocation": "us-east-1",
            "ResourceArn": "arn:aws:ec2:us-east-1:987654321012:vpc/
vpc-09f37f69e2786eeb8",
            "Tags": [],
            "CreatedAt": "2022-03-10T20:59:14+00:00",
            "UpdatedAt": "2022-03-10T20:59:14+00:00"
        },
        "SubnetArns": [
            "arn:aws:ec2:us-east-1:987654321012:subnet/subnet-04ca4e010857e7bb7"
        ],
        "Options": {
            "Ipv6Support": true
        }
    }
}
```

Para obtener más información, consulte Create an attachment en la Guía del usuario de WAN en la nube.

- Para obtener información sobre la API, consulte CreateVpcAttachment en la Referencia de comandos de la AWS CLI.

`delete-attachment`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-attachment`.

AWS CLI

Para eliminar una asociación

En el siguiente ejemplo de `delete-attachment` se elimina una asociación a Connect.

```
aws networkmanager delete-attachment \
    --attachment-id attachment-01feddaeae26ab68c
```

Salida:

```
{
    "Attachment": {
        "CoreNetworkId": "core-network-0f4b0a9d5ee7761d1",
        "AttachmentId": "attachment-01feddaeae26ab68c",
        "OwnerAccountId": "987654321012",
        "AttachmentType": "CONNECT",
        "State": "DELETING",
        "EdgeLocation": "us-east-1",
        "ResourceArn": "arn:aws:networkmanager::987654321012:attachment/
attachment-02c3964448fedf5aa",
        "CreatedAt": "2022-03-15T19:18:41+00:00",
        "UpdatedAt": "2022-03-15T19:28:59+00:00"
    }
}
```

Para obtener más información, consulte Delete attachments en la Guía del usuario de WAN en la nube.

- Para obtener información sobre la API, consulte DeleteAttachment en la Referencia de comandos de la AWS CLI.

`delete-bucket-analytics-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bucket-analytics-configuration`.

AWS CLI

Eliminar una configuración de análisis de un bucket

En el siguiente ejemplo de `delete-bucket-analytics-configuration`, se elimina la configuración de análisis para el bucket e ID especificados.

```
aws s3api delete-bucket-analytics-configuration \
    --bucket amzn-s3-demo-bucket \
    --id 1
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteBucketAnalyticsConfiguration en la Referencia de comandos de la AWS CLI.

`delete-bucket-metrics-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bucket-metrics-configuration`.

AWS CLI

Eliminar una configuración de métricas de un bucket

En el siguiente ejemplo de `delete-bucket-metrics-configuration`, se elimina la configuración de métricas para el bucket e ID especificados.

```
aws s3api delete-bucket-metrics-configuration \
    --bucket amzn-s3-demo-bucket \
    --id 123
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteBucketMetricsConfiguration en la Referencia de comandos de la AWS CLI.

`delete-core-network`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-core-network`.

AWS CLI

Para eliminar una red principal

En el siguiente ejemplo de `delete-core-network` se elimina una red principal de una red global de WAN en la nube.

```
aws networkmanager delete-core-network \
    --core-network-id core-network-0fab62fe438d94db6
```

Salida:

```
{
    "CoreNetwork": {
        "GlobalNetworkId": "global-network-0d59060f16a73bc41",
        "CoreNetworkId": "core-network-0fab62fe438d94db6",
        "Description": "Main headquarters location",
        "CreatedAt": "2021-12-09T18:31:11+00:00",
        "State": "DELETING",
        "Segments": [
            {
                "Name": "dev",
                "EdgeLocations": [
                    "us-east-1"
                ],
                "SharedSegments": []
            }
        ],
        "Edges": [
            {
                "EdgeLocation": "us-east-1",
                "Asn": 64512,
                "InsideCidrBlocks": []
            }
        ]
    }
}
```

Para obtener más información, consulte Core networks en la Guía del usuario de WAN en la nube.

- Para obtener información sobre la API, consulte DeleteCoreNetwork en la Referencia de comandos de la AWS CLI.

`delete-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-device`.

AWS CLI

Para eliminar un dispositivo

En el siguiente ejemplo de `delete-device` se elimina el dispositivo especificado de la red global indicada.

```
aws networkmanager delete-device \
    --global-network-id global-network-01231231231231231 \
    --device-id device-07f6fd08867abc123 \
    --region us-west-2
```

Salida:

```
{
    "Device": {
        "DeviceId": "device-07f6fd08867abc123",
        "DeviceArn": "arn:aws:networkmanager::123456789012:device/global-
network-01231231231231231/device-07f6fd08867abc123",
        "GlobalNetworkId": "global-network-01231231231231231",
        "Description": "New York office device",
        "Type": "office device",
        "Vendor": "anycompany",
        "Model": "abcabc",
        "SerialNumber": "1234",
        "SiteId": "site-444555aaabbb11223",
        "CreatedAt": 1575554005.0,
        "State": "DELETING"
    }
}
```

Para obtener más información, consulte Working with Devices en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte DeleteDevice en la Referencia de comandos de AWS CLI.

`delete-global-network`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-global-network`.

AWS CLI

Para eliminar una red global

En el siguiente ejemplo de `delete-global-network` se crea una red global.

```
aws networkmanager delete-global-network \
    --global-network-id global-network-052bedddccb193b6b
```

Salida:

```
{
    "GlobalNetwork": {
        "GlobalNetworkId": "global-network-052bedddccb193b6b",
        "GlobalNetworkArn": "arn:aws:networkmanager::987654321012:global-network/
global-network-052bedddccb193b6b",
        "CreatedAt": "2021-12-09T18:19:12+00:00",
        "State": "DELETING"
    }
}
```

- Para obtener información sobre la API, consulte DeleteGlobalNetwork en la Referencia de comandos de la AWS CLI.

`delete-link`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-link`.

AWS CLI

Para eliminar un enlace

En el siguiente ejemplo de `delete-link` se elimina el enlace especificado de la red global indicada.

```
aws networkmanager delete-link \
    --global-network-id global-network-01231231231231231  \
    --link-id link-11112222aaaabbbb1 \
    --region us-west-2
```

Salida:

```
{
    "Link": {
        "LinkId": "link-11112222aaaabbbb1",
        "LinkArn": "arn:aws:networkmanager::123456789012:link/global-
network-01231231231231231/link-11112222aaaabbbb1",
        "GlobalNetworkId": "global-network-01231231231231231",
        "SiteId": "site-444555aaabbb11223",
        "Description": "VPN Link",
        "Type": "broadband",
        "Bandwidth": {
            "UploadSpeed": 20,
            "DownloadSpeed": 20
        },
        "Provider": "AnyCompany",
        "CreatedAt": 1575555811.0,
        "State": "DELETING"
    }
}
```

Para obtener más información, consulte Working with Links en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte DeleteLink en la Referencia de comandos de la AWS CLI.

`delete-public-access-block`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-public-access-block`.

AWS CLI

Eliminar la configuración de bloqueo de acceso público de un bucket

En el siguiente ejemplo de `delete-public-access-block`, se elimina la configuración de bloqueo de acceso público en el bucket especificado.

```
aws s3api delete-public-access-block \
    --bucket amzn-s3-demo-bucket
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeletePublicAccessBlock en la Referencia de comandos de la AWS CLI.

`delete-site`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-site`.

AWS CLI

Para eliminar un sitio

En el siguiente ejemplo de `delete-site` se elimina el sitio especificado (`site-444555aaabbb11223`) de la red global indicada.

```
aws networkmanager delete-site \
    --global-network-id global-network-01231231231231231  \
    --site-id site-444555aaabbb11223 \
    --region us-west-2
```

Salida:

```
{
    "Site": {
        "SiteId": "site-444555aaabbb11223",
        "SiteArn": "arn:aws:networkmanager::123456789012:site/global-
network-01231231231231231/site-444555aaabbb11223",
        "GlobalNetworkId": "global-network-01231231231231231",
        "Description": "New York head office",
        "Location": {
            "Latitude": "40.7128",
            "Longitude": "-74.0060"
        },
        "CreatedAt": 1575554300.0,
        "State": "DELETING"
```

```
    }
}
```

Para obtener más información, consulte Working with Sites en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte DeleteSite en la Referencia de comandos de la AWS CLI.

`deregister-transit-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-transit-gateway`.

AWS CLI

Para anular el registro de una puerta de enlace de tránsito de una red global

En el siguiente ejemplo de `deregister-transit-gateway` se anula el registro de la puerta de enlace de tránsito especificada de la red global indicada.

```
aws networkmanager deregister-transit-gateway \
    --global-network-id global-network-01231231231231231 \
    --transit-gateway-arn arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-123abc05e04123abc \
    --region us-west-2
```

Salida:

```
{
    "TransitGatewayRegistration": {
        "GlobalNetworkId": "global-network-01231231231231231",
        "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-123abc05e04123abc",
        "State": {
            "Code": "DELETING"
        }
    }
}
```

Para obtener más información, consulte Transit Gateway Registrations en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte DeregisterTransitGateway en la Referencia de comandos de la AWS CLI.

`describe-global-networks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-global-networks`.

AWS CLI

Para describir sus redes globales

En el siguiente ejemplo de `describe-global-networks` se describen todas las redes globales de su cuenta.

```
aws networkmanager describe-global-networks \
    --region us-west-2
```

Salida:

```
{
    "GlobalNetworks": [
        {
            "GlobalNetworkId": "global-network-01231231231231231",
            "GlobalNetworkArn": "arn:aws:networkmanager::123456789012:global-
network/global-network-01231231231231231",
            "Description": "Company 1 global network",
            "CreatedAt": 1575553525.0,
            "State": "AVAILABLE"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeGlobalNetworks en la Referencia de comandos de la AWS CLI.

`disassociate-customer-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-customer-gateway`.

AWS CLI

Para desasociar una puerta de enlace de cliente

En el siguiente ejemplo de `disassociate-customer-gateway` se desasocia la puerta de enlace de cliente especificada (`cgw-11223344556677889`) de la red global indicada.

```
aws networkmanager disassociate-customer-gateway \
    --global-network-id global-network-01231231231231231 \
    --customer-gateway-arn arn:aws:ec2:us-west-2:123456789012:customer-gateway/
cgw-11223344556677889 \
    --region us-west-2
```

Salida:

```
{
    "CustomerGatewayAssociation": {
        "CustomerGatewayArn": "arn:aws:ec2:us-west-2:123456789012:customer-gateway/
cgw-11223344556677889",
        "GlobalNetworkId": "global-network-01231231231231231",
        "DeviceId": "device-07f6fd08867abc123",
        "State": "DELETING"
    }
}
```

Para obtener más información, consulte Customer Gateway Associations en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte DisassociateCustomerGateway en la Referencia de comandos de la AWS CLI.

`disassociate-link`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-link`.

AWS CLI

Para desasociar un enlace

En el siguiente ejemplo de `disassociate-link` se desasocia el enlace especificado del dispositivo `device-07f6fd08867abc123` de la red global indicada.

```
aws networkmanager disassociate-link \
    --global-network-id global-network-01231231231231231 \
    --device-id device-07f6fd08867abc123 \
    --link-id link-11112222aaaabbbb1 \
    --region us-west-2
```

Salida:

```
{
    "LinkAssociation": {
        "GlobalNetworkId": "global-network-01231231231231231",
        "DeviceId": "device-07f6fd08867abc123",
        "LinkId": "link-11112222aaaabbbb1",
        "LinkAssociationState": "DELETING"
    }
}
```

Para obtener más información, consulte Device and Link Associations en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte DisassociateLink en la Referencia de comandos de la AWS CLI.

`get-bucket-analytics-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-analytics-configuration`.

AWS CLI

Recuperar la configuración de análisis de un bucket con un ID específico

En el siguiente ejemplo de `get-bucket-analytics-configuration`, se muestra la configuración de análisis para el bucket e ID especificados.

```
aws s3api get-bucket-analytics-configuration \
    --bucket amzn-s3-demo-bucket \
    --id 1
```

Salida:

```
{
    "AnalyticsConfiguration": {
        "StorageClassAnalysis": {},
        "Id": "1"
    }
}
```

- Para obtener información sobre la API, consulte GetBucketAnalyticsConfiguration en la Referencia de comandos de la AWS CLI.

`get-bucket-metrics-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-metrics-configuration`.

AWS CLI

Recuperar la configuración de métricas de un bucket con un ID específico

En el siguiente ejemplo de `get-bucket-metrics-configuration`, se muestra la configuración de métricas para el bucket e ID especificados.

```
aws s3api get-bucket-metrics-configuration \
    --bucket amzn-s3-demo-bucket \
    --id 123
```

Salida:

```
{
    "MetricsConfiguration": {
        "Filter": {
            "Prefix": "logs"
        },
        "Id": "123"
    }
}
```

- Para obtener información sobre la API, consulte GetBucketMetricsConfiguration en la Referencia de comandos de la AWS CLI.

`get-customer-gateway-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-customer-gateway-associations`.

AWS CLI

Para obtener sus asociaciones de puerta de enlace de cliente

En el siguiente ejemplo de `get-customer-gateway-associations` se obtienen asociaciones de puerta de enlace de cliente para la red global especificada.

```
aws networkmanager get-customer-gateway-associations \
    --global-network-id global-network-01231231231231231 \
    --region us-west-2
```

Salida:

```
{
    "CustomerGatewayAssociations": [
        {
            "CustomerGatewayArn": "arn:aws:ec2:us-west-2:123456789012:customer-
gateway/cgw-11223344556677889",
            "GlobalNetworkId": "global-network-01231231231231231",
            "DeviceId": "device-07f6fd08867abc123",
            "State": "AVAILABLE"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetCustomerGatewayAssociations en la Referencia de comandos de la AWS CLI.

`get-devices`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-devices`.

AWS CLI

Para configurar los dispositivos

En el siguiente ejemplo de `get-devices` se obtienen los dispositivos en la red global especificada.

```
aws networkmanager get-devices \
    --global-network-id global-network-01231231231231231 \
    --region us-west-2
```

Salida:

```
{
    "Devices": [
        {
            "DeviceId": "device-07f6fd08867abc123",
            "DeviceArn": "arn:aws:networkmanager::123456789012:device/global-
network-01231231231231231/device-07f6fd08867abc123",
            "GlobalNetworkId": "global-network-01231231231231231",
            "Description": "NY office device",
            "Type": "office device",
            "Vendor": "anycompany",
            "Model": "abcabc",
            "SerialNumber": "1234",
            "CreatedAt": 1575554005.0,
            "State": "AVAILABLE"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetDevices en la Referencia de comandos de la AWS CLI.

`get-link-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-link-associations`.

AWS CLI

Para obtener sus asociaciones de enlaces

En el siguiente ejemplo de `get-link-associations` se obtienen asociaciones de enlace de la red global especificada.

```
aws networkmanager get-link-associations \
```

```
    --global-network-id global-network-01231231231231231 \
    --region us-west-2
```

Salida:

```
{
    "LinkAssociations": [
        {
            "GlobalNetworkId": "global-network-01231231231231231",
            "DeviceId": "device-07f6fd08867abc123",
            "LinkId": "link-11112222aaaabbbb1",
            "LinkAssociationState": "AVAILABLE"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetLinkAssociations en la Referencia de comandos de la AWS CLI.

`get-links`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-links`.

AWS CLI

Para obtener sus enlaces

En el siguiente ejemplo de `get-links` se obtienen los enlaces de la red global especificada.

```
aws networkmanager get-links \
    --global-network-id global-network-01231231231231231 \
    --region us-west-2
```

Salida:

```
{
    "Links": [
        {
            "LinkId": "link-11112222aaaabbbb1",
            "LinkArn": "arn:aws:networkmanager::123456789012:link/global-
network-01231231231231231/link-11112222aaaabbbb1",
```

```
            "GlobalNetworkId": "global-network-01231231231231231",
            "SiteId": "site-444555aaabbb11223",
            "Description": "VPN Link",
            "Type": "broadband",
            "Bandwidth": {
                "UploadSpeed": 10,
                "DownloadSpeed": 20
            },
            "Provider": "AnyCompany",
            "CreatedAt": 1575555811.0,
            "State": "AVAILABLE"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetLinks en la Referencia de comandos de la AWS CLI.

`get-object-retention`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-object-retention`.

AWS CLI

Para recuperar la configuración de retención de un objeto

En el siguiente ejemplo de `get-object-retention`, se recupera la configuración de retención del objeto especificado.

```
aws s3api get-object-retention \
    --bucket amzn-s3-demo-bucket-with-object-lock \
    --key doc1.rtf
```

Salida:

```
{
    "Retention": {
        "Mode": "GOVERNANCE",
        "RetainUntilDate": "2025-01-01T00:00:00.000Z"
    }
}
```

- Para obtener información sobre la API, consulte GetObjectRetention en la Referencia de comandos de la AWS CLI.

`get-public-access-block`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-public-access-block`.

AWS CLI

Establecer o modificar la configuración de bloqueo de acceso público de un bucket

En el siguiente ejemplo de `get-public-access-block`, se elimina la configuración de bloqueo de acceso público del bucket especificado.

```
aws s3api get-public-access-block --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "PublicAccessBlockConfiguration": {
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "BlockPublicAcls": true,
        "RestrictPublicBuckets": true
    }
}
```

- Para obtener información sobre la API, consulte GetPublicAccessBlock en la Referencia de comandos de la AWS CLI.

`get-sites`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-sites`.

AWS CLI

Para obtener sus sitios

En el siguiente ejemplo de `get-sites` se obtienen los sitios de la red global especificada.

```
aws networkmanager get-sites \
```

```
    --global-network-id global-network-01231231231231231 \
    --region us-west-2
```

Salida:

```
{
    "Sites": [
        {
            "SiteId": "site-444555aaabbb11223",
            "SiteArn": "arn:aws:networkmanager::123456789012:site/global-
network-01231231231231231/site-444555aaabbb11223",
            "GlobalNetworkId": "global-network-01231231231231231",
            "Description": "NY head office",
            "Location": {
                "Latitude": "40.7128",
                "Longitude": "-74.0060"
            },
            "CreatedAt": 1575554528.0,
            "State": "AVAILABLE"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetSites en la Referencia de comandos de la AWS CLI.

`get-transit-gateway-registrations`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-transit-gateway-registrations`.

AWS CLI

Para obtener sus registros de puerta de enlace de tránsito

En el siguiente ejemplo de `get-transit-gateway-registrations`, se obtienen las puertas de enlace de tránsito que están registradas en la red global especificada.

```
aws networkmanager get-transit-gateway-registrations \
    --global-network-id global-network-01231231231231231 \
    --region us-west-2
```

Salida:

```
{
    "TransitGatewayRegistrations": [
        {
            "GlobalNetworkId": "global-network-01231231231231231",
            "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-
gateway/tgw-123abc05e04123abc",
            "State": {
                "Code": "AVAILABLE"
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetTransitGatewayRegistrations en la Referencia de comandos de la AWS CLI.

`get-vpc-attachment`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-vpc-attachment`.

AWS CLI

Para obtener una asociación a VPC

El siguiente ejemplo de `get-vpc-attachment` devuelve información sobre una asociación a VPC.

```
aws networkmanager get-vpc-attachment \
    --attachment-id  attachment-03b7ea450134787da
```

Salida:

```
{
    "VpcAttachment": {
        "Attachment": {
            "CoreNetworkId": "core-network-0522de1b226a5d7b3",
            "AttachmentId": "attachment-03b7ea450134787da",
            "OwnerAccountId": "987654321012",
            "AttachmentType": "VPC",
            "State": "CREATING",
```

```
            "EdgeLocation": "us-east-1",
            "ResourceArn": "arn:aws:ec2:us-east-1:987654321012:vpc/vpc-a7c4bbda",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "DevVPC"
                }
            ],
            "CreatedAt": "2022-03-11T17:48:58+00:00",
            "UpdatedAt": "2022-03-11T17:48:58+00:00"
        },
        "SubnetArns": [
            "arn:aws:ec2:us-east-1:987654321012:subnet/subnet-202cde6c",
            "arn:aws:ec2:us-east-1:987654321012:subnet/subnet-e5022dba",
            "arn:aws:ec2:us-east-1:987654321012:subnet/subnet-2387ae02",
            "arn:aws:ec2:us-east-1:987654321012:subnet/subnet-cda9dffc"
        ],
        "Options": {
            "Ipv6Support": false
        }
    }
}
```

Para obtener más información, consulte Attachments en la Guía del usuario de WAN en la nube.

- Para obtener información sobre la API, consulte GetVpcAttachment en la Referencia de comandos de la AWS CLI.

`list-bucket-analytics-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-bucket-analytics-configurations`.

AWS CLI

Recuperar una lista de configuraciones de análisis para un bucket

El siguiente `list-bucket-analytics-configurations` recupera una lista de configuraciones de análisis para el bucket especificado.

```
aws s3api list-bucket-analytics-configurations \
    --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "AnalyticsConfigurationList": [
        {
            "StorageClassAnalysis": {},
            "Id": "1"
        }
    ],
    "IsTruncated": false
}
```

- Para obtener información sobre la API, consulte ListBucketAnalyticsConfigurations en la Referencia de comandos de la AWS CLI.

`list-bucket-metrics-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-bucket-metrics-configurations`.

AWS CLI

Para recuperar una lista de las configuraciones de métricas para un bucket

En el siguiente ejemplo de `list-bucket-metrics-configurations` se recupera una lista de configuraciones de métricas para el bucket especificado.

```
aws s3api list-bucket-metrics-configurations \
    --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "IsTruncated": false,
    "MetricsConfigurationList": [
        {
            "Filter": {
                "Prefix": "logs"
            },
            "Id": "123"
        },
```

```
        {
            "Filter": {
                "Prefix": "tmp"
            },
            "Id": "234"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListBucketMetricsConfigurations en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un recurso

En el siguiente ejemplo de `list-tags-for-resource` se enumeran las etiquetas del recurso de dispositivo especificado (`device-07f6fd08867abc123`).

```
aws networkmanager list-tags-for-resource \
    --resource-arn arn:aws:networkmanager::123456789012:device/global-network-01231231231231231/device-07f6fd08867abc123 \
    --region us-west-2
```

Salida:

```
{
    "TagList": [
        {
            "Key": "Network",
            "Value": "Northeast"
        }
    ]
}
```

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-bucket-metrics-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-metrics-configuration`.

AWS CLI

Para establecer una configuración de métricas para un bucket

En el siguiente ejemplo de `put-bucket-metrics-configuration` se establece una configuración de métricas para ID 123 para el bucket especificado.

```
aws s3api put-bucket-metrics-configuration \
    --bucket amzn-s3-demo-bucket \
    --id 123 \
    --metrics-configuration '{"Id": "123", "Filter": {"Prefix": "logs"}}'
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutBucketMetricsConfiguration en la Referencia de comandos de la AWS CLI.

`put-object-retention`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-object-retention`.

AWS CLI

Para establecer la configuración de retención de un objeto

En el siguiente ejemplo de `put-object-retention`, se establece una configuración de retención del objeto especificado hasta el 1 de enero de 2025.

```
aws s3api put-object-retention \
    --bucket amzn-s3-demo-bucket-with-object-lock \
    --key doc1.rtf \
    --retention '{ "Mode": "GOVERNANCE", "RetainUntilDate": "2025-01-01T00:00:00" }'
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutObjectRetention en la Referencia de comandos de la AWS CLI.

`put-public-access-block`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-public-access-block`.

AWS CLI

Para establecer la configuración de bloqueo de acceso público para un bucket

En el siguiente ejemplo de `put-public-access-block` se establece una configuración de bloqueo de acceso público restrictiva para el bucket especificado.

```
aws s3api put-public-access-block \
    --bucket amzn-s3-demo-bucket \
    --public-access-block-
configuration "BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPub
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutPublicAccessBlock en la Referencia de comandos de la AWS CLI.

`register-transit-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-transit-gateway`.

AWS CLI

Para registrar una puerta de enlace de tránsito en una red global

En el siguiente ejemplo de `register-transit-gateway` se registra la puerta de enlace de tránsito `tgw-123abc05e04123abc` en la red global especificada.

```
aws networkmanager register-transit-gateway \
    --global-network-id global-network-01231231231231231 \
    --transit-gateway-arn arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-123abc05e04123abc \
    --region us-west-2
```

Salida:

```
{
    "TransitGatewayRegistration": {
        "GlobalNetworkId": "global-network-01231231231231231",
```

```
        "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-123abc05e04123abc",
        "State": {
            "Code": "PENDING"
        }
    }
}
```

Para obtener más información, consulte Transit Gateway Registrations en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte RegisterTransitGateway en la Referencia de comandos de la AWS CLI.

`reject-attachment`

En el siguiente ejemplo de código, se muestra cómo utilizar `reject-attachment`.

AWS CLI

Para rechazar una asociación

En el siguiente ejemplo de `reject-attachment` se rechaza una solicitud de asociación a VPC.

```
aws networkmanager reject-attachment \
    --attachment-id  attachment-03b7ea450134787da
```

Salida:

```
{
    "Attachment": {
        "CoreNetworkId": "core-network-0522de1b226a5d7b3",
        "AttachmentId": "attachment-03b7ea450134787da",
        "OwnerAccountId": "987654321012",
        "AttachmentType": "VPC",
        "State": "AVAILABLE",
        "EdgeLocation": "us-east-1",
        "ResourceArn": "arn:aws:ec2:us-east-1:987654321012:vpc/vpc-a7c4bbda",
        "CreatedAt": "2022-03-11T17:48:58+00:00",
        "UpdatedAt": "2022-03-11T17:51:25+00:00"
    }
}
```

Para obtener más información, consulte Attachment acceptance en la Guía del usuario de WAN en la nube.

- Para obtener información sobre la API, consulte RejectAttachment en la Referencia de comandos de la AWS CLI.

`start-route-analysis`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-route-analysis`.

AWS CLI

Para iniciar análisis de rutas

En el siguiente ejemplo de `start-route-analysis` se inicia el análisis entre un origen y un destino, incluida la `include-return-path` opcional.

```
aws networkmanager start-route-analysis \
    --global-network-id global-network-00aa0aaa0b0aaa000 \
    --source TransitGatewayAttachmentArn=arn:aws:ec2:us-east-1:503089527312:transit-gateway-attachment/tgw-attach-0d4a2d491bf68c093,IpAddress=10.0.0.0 \
    --destination TransitGatewayAttachmentArn=arn:aws:ec2:us-west-1:503089527312:transit-gateway-attachment/tgw-attach-002577f30bb181742,IpAddress=11.0.0.0 \
    --include-return-path
```

Salida:

```
{
    "RouteAnalysis": {
        "GlobalNetworkId": "global-network-00aa0aaa0b0aaa000
        "OwnerAccountId": "1111222233333",
        "RouteAnalysisId": "a1873de1-273c-470c-1a2bc2345678",
        "StartTimestamp": 1695760154.0,
        "Status": "RUNNING",
        "Source": {
            "TransitGatewayAttachmentArn": "arn:aws:ec2:us-east-1:111122223333:transit-gateway-attachment/tgw-attach-1234567890abcdef0,
            "TransitGatewayArn": "arn:aws:ec2:us-east-1:111122223333:transit-gateway/tgw-abcdef01234567890",
            "IpAddress": "10.0.0.0"
        },
        "Destination": {
```

```
            "TransitGatewayAttachmentArn": "arn:aws:ec2:us-
west-1:555555555555:transit-gateway-attachment/tgw-attach-021345abcdef6789",
            "TransitGatewayArn": "arn:aws:ec2:us-west-1:111122223333:transit-
gateway/tgw-09876543210fedcba0",
            "IpAddress": "11.0.0.0"
        },
        "IncludeReturnPath": true,
        "UseMiddleboxes": false
    }
}
```

Para obtener más información, consulte Route Analyzer en la Guía del usuario de AWS Global Networks for Transit Gateways.

- Para obtener información sobre la API, consulte StartRouteAnalysis en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para aplicar etiquetas a un recurso

En el siguiente ejemplo de `tag-resource` se aplica la etiqueta `Network=Northeast` al dispositivo `device-07f6fd08867abc123`.

```
aws networkmanager tag-resource \
    --resource-arn arn:aws:networkmanager::123456789012:device/global-
network-0123123123123231/device-07f6fd08867abc123 \
    --tags Key=Network,Value=Northeast \
    --region us-west-2
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar etiquetas de un recurso

En el siguiente ejemplo de `untag-resource` se elimina la etiqueta con la clave `Network` del dispositivo `device-07f6fd08867abc123`.

```
aws networkmanager untag-resource \
    --resource-arn arn:aws:networkmanager::123456789012:device/global-network-01231231231231231/device-07f6fd08867abc123 ]
    --tag-keys Network \
    --region us-west-2
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-device`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-device`.

AWS CLI

Para actualizar un dispositivo

El siguiente ejemplo de `update-device` actualiza el dispositivo `device-07f6fd08867abc123` especificando un ID de sitio para el dispositivo.

```
aws networkmanager update-device \
    --global-network-id global-network-01231231231231231 \
    --device-id device-07f6fd08867abc123 \
    --site-id site-444555aaabbb11223 \
    --region us-west-2
```

Salida:

```
{
    "Device": {
        "DeviceId": "device-07f6fd08867abc123",
        "DeviceArn": "arn:aws:networkmanager::123456789012:device/global-network-01231231231231231/device-07f6fd08867abc123",
```

```
        "GlobalNetworkId": "global-network-01231231231231231",
        "Description": "NY office device",
        "Type": "Office device",
        "Vendor": "anycompany",
        "Model": "abcabc",
        "SerialNumber": "1234",
        "SiteId": "site-444555aaabbb11223",
        "CreatedAt": 1575554005.0,
        "State": "UPDATING"
    }
}
```

Para obtener más información, consulte Working with Devices en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte UpdateDevice en la Referencia de comandos de la AWS CLI.

`update-global-network`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-global-network`.

AWS CLI

Para actualizar una red global

En el siguiente ejemplo de `update-global-network` se actualiza la descripción de la red global `global-network-01231231231231231`.

```
aws networkmanager update-global-network \
    --global-network-id global-network-01231231231231231 \
    --description "Head offices" \
    --region us-west-2
```

Salida:

```
{
    "GlobalNetwork": {
        "GlobalNetworkId": "global-network-01231231231231231",
        "GlobalNetworkArn": "arn:aws:networkmanager::123456789012:global-network/
global-network-01231231231231231",
        "Description": "Head offices",
```

```
        "CreatedAt": 1575553525.0,
        "State": "UPDATING"
    }
}
```

Para obtener más información, consulte Global Networks en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte UpdateGlobalNetwork en la Referencia de comandos de la AWS CLI.

update-link

En el siguiente ejemplo de código, se muestra cómo utilizar `update-link`.

AWS CLI

Para actualizar un enlace

El siguiente ejemplo de `update-link` actualiza la información de ancho de banda del enlace `link-11112222aaaabbbb1`.

```
aws networkmanager update-link \
    --global-network-id global-network-01231231231231231 \
    --link-id link-11112222aaaabbbb1 \
    --bandwidth  UploadSpeed=20,DownloadSpeed=20 \
    --region us-west-2
```

Salida:

```
{
    "Link": {
        "LinkId": "link-11112222aaaabbbb1",
        "LinkArn": "arn:aws:networkmanager::123456789012:link/global-
network-01231231231231231/link-11112222aaaabbbb1",
        "GlobalNetworkId": "global-network-01231231231231231",
        "SiteId": "site-444555aaabbb11223",
        "Description": "VPN Link",
        "Type": "broadband",
        "Bandwidth": {
            "UploadSpeed": 20,
            "DownloadSpeed": 20
```

```
        },
        "Provider": "AnyCompany",
        "CreatedAt": 1575555811.0,
        "State": "UPDATING"
    }
}
```

Para obtener más información, consulte Working with Links en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte UpdateLink en la Referencia de comandos de la AWS CLI.

`update-site`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-site`.

AWS CLI

Para actualizar un sitio

En el siguiente ejemplo de `update-site` se actualiza la descripción del sitio `site-444555aaabbb11223` en la red global especificada.

```
aws networkmanager update-site \
    --global-network-id global-network-01231231231231231 \
    --site-id site-444555aaabbb11223 \
    --description "New York Office site" \
    --region us-west-2
```

Salida:

```
{
    "Site": {
        "SiteId": "site-444555aaabbb11223",
        "SiteArn": "arn:aws:networkmanager::123456789012:site/global-
network-01231231231231231/site-444555aaabbb11223",
        "GlobalNetworkId": "global-network-01231231231231231",
        "Description": "New York Office site",
        "Location": {
            "Latitude": "40.7128",
            "Longitude": "-74.0060"
```

```
        },
        "CreatedAt": 1575554528.0,
        "State": "UPDATING"
    }
}
```

Para obtener más información, consulte Working with Sites en la Guía de Transit Gateway Network Manager.

- Para obtener información sobre la API, consulte UpdateSite en la Referencia de comandos de la AWS CLI.

Ejemplos de OpenSearch Service que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con OpenSearch Service.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-elasticsearch-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-elasticsearch-domain`.

AWS CLI

Para crear un dominio de Amazon Elasticsearch Service

En el siguiente comando de `create-elasticsearch-domain`, se crea un nuevo dominio de Amazon Elasticsearch Service dentro de una VPC y restringe el acceso a un único usuario. Amazon ES infiere el ID de VPC a partir de los ID de subred y grupo de seguridad especificados.

```
aws es create-elasticsearch-domain \
    --domain-name vpc-cli-example \
    --elasticsearch-version 6.2 \
    --elasticsearch-cluster-
config InstanceType=m4.large.elasticsearch,InstanceCount=1 \
    --ebs-options EBSEnabled=true,VolumeType=standard,VolumeSize=10 \
    --access-policies '{"Version":"2012-10-17",        "Statement": [ { "Effect":
 "Allow", "Principal": {"AWS": "arn:aws:iam::123456789012:root" }, "Action":"es:*",
 "Resource": "arn:aws:es:us-west-1:123456789012:domain/vpc-cli-example/*" } ] }' \
    --vpc-options SubnetIds=subnet-1a2a3a4a,SecurityGroupIds=sg-2a3a4a5a
```

Salida:

```
{
    "DomainStatus": {
        "ElasticsearchClusterConfig": {
            "DedicatedMasterEnabled": false,
            "InstanceCount": 1,
            "ZoneAwarenessEnabled": false,
            "InstanceType": "m4.large.elasticsearch"
        },
        "DomainId": "123456789012/vpc-cli-example",
        "CognitoOptions": {
            "Enabled": false
        },
        "VPCOptions": {
            "SubnetIds": [
                "subnet-1a2a3a4a"
            ],
            "VPCId": "vpc-3a4a5a6a",
            "SecurityGroupIds": [
                "sg-2a3a4a5a"
            ],
            "AvailabilityZones": [
                "us-west-1c"
            ]
        },
        "Created": true,
        "Deleted": false,
        "EBSOptions": {
            "VolumeSize": 10,
            "VolumeType": "standard",
            "EBSEnabled": true
```

```
        },
        "Processing": true,
        "DomainName": "vpc-cli-example",
        "SnapshotOptions": {
            "AutomatedSnapshotStartHour": 0
        },
        "ElasticsearchVersion": "6.2",
        "AccessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":
\"Allow\",\"Principal\":{\"AWS\":\"arn:aws:iam::123456789012:root\"},\"Action\":
\"es:*\",\"Resource\":\"arn:aws:es:us-west-1:123456789012:domain/vpc-cli-example/*
\"}]}",
        "AdvancedOptions": {
            "rest.action.multi.allow_explicit_index": "true"
        },
        "EncryptionAtRestOptions": {
            "Enabled": false
        },
        "ARN": "arn:aws:es:us-west-1:123456789012:domain/vpc-cli-example"
    }
}
```

Para obtener más información, consulte Creating and Managing Amazon Elasticsearch Service Domains en la Guía para desarrolladores de Amazon Elasticsearch Service.

- Para obtener información sobre la API, consulte CreateElasticsearchDomain en la Referencia de comandos de la AWS CLI.

`describe-elasticsearch-domain-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-elasticsearch-domain-config`.

AWS CLI

Para obtener los detalles de la configuración del dominio

En el siguiente ejemplo de `describe-elasticsearch-domain-config` se proporcionan los detalles de configuración de un dominio determinado, junto con la información del estado de cada componente de dominio individual.

```
aws es describe-elasticsearch-domain-config \
    --domain-name cli-example
```

Salida:


```
{
    "DomainConfig": {
        "ElasticsearchVersion": {
            "Options": "7.4",
            "Status": {
                "CreationDate": 1589395034.946,
                "UpdateDate": 1589395827.325,
                "UpdateVersion": 8,
                "State": "Active",
                "PendingDeletion": false
            }
        },
        "ElasticsearchClusterConfig": {
            "Options": {
                "InstanceType": "c5.large.elasticsearch",
                "InstanceCount": 1,
                "DedicatedMasterEnabled": true,
                "ZoneAwarenessEnabled": false,
                "DedicatedMasterType": "c5.large.elasticsearch",
                "DedicatedMasterCount": 3,
                "WarmEnabled": true,
                "WarmType": "ultrawarm1.medium.elasticsearch",
                "WarmCount": 2
            },
            "Status": {
                "CreationDate": 1589395034.946,
                "UpdateDate": 1589395827.325,
                "UpdateVersion": 8,
                "State": "Active",
                "PendingDeletion": false
            }
        },
        "EBSOptions": {
            "Options": {
                "EBSEnabled": true,
                "VolumeType": "gp2",
                "VolumeSize": 10
            },
            "Status": {
                "CreationDate": 1589395034.946,
                "UpdateDate": 1589395827.325,
                "UpdateVersion": 8,
```

```
                "State": "Active",
                "PendingDeletion": false
            }
        },
        "AccessPolicies": {
            "Options": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Principal\":{\"AWS\":\"*\"},\"Action\":\"es:*\",\"Resource\":
\"arn:aws:es:us-east-1:123456789012:domain/cli-example/*\"}]}",
            "Status": {
                "CreationDate": 1589395034.946,
                "UpdateDate": 1589395827.325,
                "UpdateVersion": 8,
                "State": "Active",
                "PendingDeletion": false
            }
        },
        "SnapshotOptions": {
            "Options": {
                "AutomatedSnapshotStartHour": 0
            },
            "Status": {
                "CreationDate": 1589395034.946,
                "UpdateDate": 1589395827.325,
                "UpdateVersion": 8,
                "State": "Active",
                "PendingDeletion": false
            }
        },
        "VPCOptions": {
            "Options": {},
            "Status": {
                "CreationDate": 1591210426.162,
                "UpdateDate": 1591210426.162,
                "UpdateVersion": 18,
                "State": "Active",
                "PendingDeletion": false
            }
        },
        "CognitoOptions": {
            "Options": {
                "Enabled": false
            },
            "Status": {
                "CreationDate": 1591210426.163,
```

```
                "UpdateDate": 1591210426.163,
                "UpdateVersion": 18,
                "State": "Active",
                "PendingDeletion": false
            }
        },
        "EncryptionAtRestOptions": {
            "Options": {
                "Enabled": true,
                "KmsKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1a2a3a4a-1a2a-1a2a-1a2a-1a2a3a4a5a6a"
            },
            "Status": {
                "CreationDate": 1589395034.946,
                "UpdateDate": 1589395827.325,
                "UpdateVersion": 8,
                "State": "Active",
                "PendingDeletion": false
            }
        },
        "NodeToNodeEncryptionOptions": {
            "Options": {
                "Enabled": true
            },
            "Status": {
                "CreationDate": 1589395034.946,
                "UpdateDate": 1589395827.325,
                "UpdateVersion": 8,
                "State": "Active",
                "PendingDeletion": false
            }
        },
        "AdvancedOptions": {
            "Options": {
                "rest.action.multi.allow_explicit_index": "true"
            },
            "Status": {
                "CreationDate": 1589395034.946,
                "UpdateDate": 1589395827.325,
                "UpdateVersion": 8,
                "State": "Active",
                "PendingDeletion": false
            }
        },
```

```
        "LogPublishingOptions": {
            "Options": {},
            "Status": {
                "CreationDate": 1591210426.164,
                "UpdateDate": 1591210426.164,
                "UpdateVersion": 18,
                "State": "Active",
                "PendingDeletion": false
            }
        },
        "DomainEndpointOptions": {
            "Options": {
                "EnforceHTTPS": true,
                "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07"
            },
            "Status": {
                "CreationDate": 1589395034.946,
                "UpdateDate": 1589395827.325,
                "UpdateVersion": 8,
                "State": "Active",
                "PendingDeletion": false
            }
        },
        "AdvancedSecurityOptions": {
            "Options": {
                "Enabled": true,
                "InternalUserDatabaseEnabled": true
            },
            "Status": {
                "CreationDate": 1589395034.946,
                "UpdateDate": 1589827485.577,
                "UpdateVersion": 14,
                "State": "Active",
                "PendingDeletion": false
            }
        }
    }
}
```

Para obtener más información, consulte Creating and Managing Amazon Elasticsearch Service Domains en la Guía para desarrolladores de Amazon Elasticsearch Service.

- Para obtener información sobre la API, consulte DescribeElasticsearchDomainConfig en la Referencia de comandos de la AWS CLI.

`describe-elasticsearch-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-elasticsearch-domain`.

AWS CLI

Para obtener los detalles para un dominio único

En el siguiente ejemplo de `describe-elasticsearch-domain`, se proporcionan los detalles de configuración para un dominio determinado.

```
aws es describe-elasticsearch-domain \
    --domain-name cli-example
```

Salida:

```
{
    "DomainStatus": {
        "DomainId": "123456789012/cli-example",
        "DomainName": "cli-example",
        "ARN": "arn:aws:es:us-east-1:123456789012:domain/cli-example",
        "Created": true,
        "Deleted": false,
        "Endpoint": "search-cli-example-1a2a3a4a5a6a7a8a9a0a.us-
east-1.es.amazonaws.com",
        "Processing": false,
        "UpgradeProcessing": false,
        "ElasticsearchVersion": "7.4",
        "ElasticsearchClusterConfig": {
            "InstanceType": "c5.large.elasticsearch",
            "InstanceCount": 1,
            "DedicatedMasterEnabled": true,
            "ZoneAwarenessEnabled": false,
            "DedicatedMasterType": "c5.large.elasticsearch",
            "DedicatedMasterCount": 3,
            "WarmEnabled": true,
            "WarmType": "ultrawarm1.medium.elasticsearch",
            "WarmCount": 2
        },
        "EBSOptions": {
            "EBSEnabled": true,
            "VolumeType": "gp2",
            "VolumeSize": 10
```

```
        },
        "AccessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Principal\":{\"AWS\":\"*\"},\"Action\":\"es:*\",\"Resource\":
\"arn:aws:es:us-east-1:123456789012:domain/cli-example/*\"}]}",
        "SnapshotOptions": {
            "AutomatedSnapshotStartHour": 0
        },
        "CognitoOptions": {
            "Enabled": false
        },
        "EncryptionAtRestOptions": {
            "Enabled": true,
            "KmsKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1a2a3a4a-1a2a-1a2a-1a2a-1a2a3a4a5a6a"
        },
        "NodeToNodeEncryptionOptions": {
            "Enabled": true
        },
        "AdvancedOptions": {
            "rest.action.multi.allow_explicit_index": "true"
        },
        "ServiceSoftwareOptions": {
            "CurrentVersion": "R20200522",
            "NewVersion": "",
            "UpdateAvailable": false,
            "Cancellable": false,
            "UpdateStatus": "COMPLETED",
            "Description": "There is no software update available for this domain.",
            "AutomatedUpdateDate": 0.0
        },
        "DomainEndpointOptions": {
            "EnforceHTTPS": true,
            "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07"
        },
        "AdvancedSecurityOptions": {
            "Enabled": true,
            "InternalUserDatabaseEnabled": true
        }
    }
}
```

Para obtener más información, consulte Creating and Managing Amazon Elasticsearch Service Domains en la Guía para desarrolladores de Amazon Elasticsearch Service.

- Para obtener información sobre la API, consulte DescribeElasticsearchDomain en la Referencia de comandos de la AWS CLI.

`describe-elasticsearch-domains`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-elasticsearch-domains`.

AWS CLI

Para obtener los detalles para uno o más dominios

En el siguiente ejemplo de `describe-elasticsearch-domains`, se proporcionan los detalles de configuración para uno o más dominios.

```
aws es describe-elasticsearch-domains \
    --domain-names cli-example-1 cli-example-2
```

Salida:

```
{
    "DomainStatusList": [{
            "DomainId": "123456789012/cli-example-1",
            "DomainName": "cli-example-1",
            "ARN": "arn:aws:es:us-east-1:123456789012:domain/cli-example-1",
            "Created": true,
            "Deleted": false,
            "Endpoint": "search-cli-example-1-1a2a3a4a5a6a7a8a9a0a.us-
east-1.es.amazonaws.com",
            "Processing": false,
            "UpgradeProcessing": false,
            "ElasticsearchVersion": "7.4",
            "ElasticsearchClusterConfig": {
                "InstanceType": "c5.large.elasticsearch",
                "InstanceCount": 1,
                 "DedicatedMasterEnabled": true,
                "ZoneAwarenessEnabled": false,
                "DedicatedMasterType": "c5.large.elasticsearch",
                "DedicatedMasterCount": 3,
                "WarmEnabled": true,
                "WarmType": "ultrawarm1.medium.elasticsearch",
                "WarmCount": 2
            },
```

```
            "EBSOptions": {
                "EBSEnabled": true,
                "VolumeType": "gp2",
                "VolumeSize": 10
            },
            "AccessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Principal\":{\"AWS\":\"*\"},\"Action\":\"es:*\",\"Resource\":
\"arn:aws:es:us-east-1:123456789012:domain/cli-example-1/*\"}]}",
            "SnapshotOptions": {
                "AutomatedSnapshotStartHour": 0
            },
            "CognitoOptions": {
                "Enabled": false
            },
            "EncryptionAtRestOptions": {
                "Enabled": true,
                "KmsKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1a2a3a4a-1a2a-1a2a-1a2a-1a2a3a4a5a6a"
            },
            "NodeToNodeEncryptionOptions": {
                "Enabled": true
            },
            "AdvancedOptions": {
                "rest.action.multi.allow_explicit_index": "true"
            },
            "ServiceSoftwareOptions": {
                "CurrentVersion": "R20200522",
                "NewVersion": "",
                "UpdateAvailable": false,
                "Cancellable": false,
                "UpdateStatus": "COMPLETED",
                "Description": "There is no software update available for this
 domain.",
                "AutomatedUpdateDate": 0.0
            },
            "DomainEndpointOptions": {
                "EnforceHTTPS": true,
                "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07"
            },
            "AdvancedSecurityOptions": {
                "Enabled": true,
                "InternalUserDatabaseEnabled": true
            }
        },
```

```
        {
            "DomainId": "123456789012/cli-example-2",
            "DomainName": "cli-example-2",
            "ARN": "arn:aws:es:us-east-1:123456789012:domain/cli-example-2",
            "Created": true,
            "Deleted": false,
            "Processing": true,
            "UpgradeProcessing": false,
            "ElasticsearchVersion": "7.4",
            "ElasticsearchClusterConfig": {
                "InstanceType": "r5.large.elasticsearch",
                "InstanceCount": 1,
                "DedicatedMasterEnabled": false,
                "ZoneAwarenessEnabled": false,
                "WarmEnabled": false
            },
            "EBSOptions": {
                "EBSEnabled": true,
                "VolumeType": "gp2",
                "VolumeSize": 10
            },
            "AccessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Deny\",\"Principal\":{\"AWS\":\"*\"},\"Action\":\"es:*\",\"Resource\":
\"arn:aws:es:us-east-1:123456789012:domain/cli-example-2/*\"}]}",
            "SnapshotOptions": {
                "AutomatedSnapshotStartHour": 0
            },
            "CognitoOptions": {
                "Enabled": false
            },
            "EncryptionAtRestOptions": {
                "Enabled": false
            },
            "NodeToNodeEncryptionOptions": {
                "Enabled": false
            },
            "AdvancedOptions": {
                "rest.action.multi.allow_explicit_index": "true"
            },
            "ServiceSoftwareOptions": {
                "CurrentVersion": "",
                "NewVersion": "",
                "UpdateAvailable": false,
                "Cancellable": false,
```

```
                "UpdateStatus": "COMPLETED",
                "Description": "There is no software update available for this
 domain.",
                "AutomatedUpdateDate": 0.0
            },
            "DomainEndpointOptions": {
                "EnforceHTTPS": false,
                "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07"
            },
            "AdvancedSecurityOptions": {
                "Enabled": false,
                "InternalUserDatabaseEnabled": false
            }
        }
    ]
}
```

Para obtener más información, consulte Creating and Managing Amazon Elasticsearch Service Domains en la Guía para desarrolladores de Amazon Elasticsearch Service.

- Para obtener información sobre la API, consulte DescribeElasticsearchDomains en la Referencia de comandos de la AWS CLI.

`describe-reserved-elasticsearch-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-reserved-elasticsearch-instances`.

AWS CLI

Para ver todas las instancias reservadas

En el siguiente ejemplo de `describe-elasticsearch-domains`, se proporciona un resumen de todas las instancias que ha reservado en una región.

```
aws es describe-reserved-elasticsearch-instances
```

Salida:

```
{
    "ReservedElasticsearchInstances": [{
        "FixedPrice": 100.0,
```

```
        "ReservedElasticsearchInstanceOfferingId":
 "1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a",
        "ReservationName": "my-reservation",
        "PaymentOption": "PARTIAL_UPFRONT",
        "UsagePrice": 0.0,
        "ReservedElasticsearchInstanceId": "9a8a7a6a-5a4a-3a2a-1a0a-9a8a7a6a5a4a",
        "RecurringCharges": [{
            "RecurringChargeAmount": 0.603,
            "RecurringChargeFrequency": "Hourly"
        }],
        "State": "payment-pending",
        "StartTime": 1522872571.229,
        "ElasticsearchInstanceCount": 3,
        "Duration": 31536000,
        "ElasticsearchInstanceType": "m4.2xlarge.elasticsearch",
        "CurrencyCode": "USD"
    }]
}
```

Para obtener más información, consulte Reserved Instances en la Guía para desarrolladores de Amazon Elasticsearch Service.

- Para obtener información sobre la API, consulte DescribeReservedElasticsearchInstances en la Referencia de comandos de la AWS CLI.

`list-domain-names`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-domain-names`.

AWS CLI

Para enumerar todos los dominios

En el siguiente ejemplo de `list-domain-names` se proporciona un resumen rápido de todos los dominios de la región.

```
aws es list-domain-names
```

Salida:

```
{
    "DomainNames": [{
            "DomainName": "cli-example-1"
```

```
        },
        {
            "DomainName": "cli-example-2"
        }
    ]
}
```

Para obtener más información, consulte Creating and Managing Amazon Elasticsearch Service Domains en la Guía para desarrolladores de Amazon Elasticsearch Service.

- Para obtener información sobre la API, consulte ListDomainNames en la Referencia de comandos de la AWS CLI.

Ejemplos de Organizations que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Organizations.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`accept-handshake`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-handshake`.

AWS CLI

Para aceptar un protocolo de enlace de otra cuenta

Bill, el propietario de una organización, había invitado a la cuenta de Juan a unirse a su organización. En el siguiente ejemplo, se muestra a la cuenta de Juan aceptando el protocolo de enlace y, por lo tanto, aceptando la invitación.

```
aws organizations accept-handshake --handshake-id h-examplehandshakeid111
```

En el resultado se observa lo siguiente:

```
{
        "Handshake": {
                "Action": "INVITE",
                "Arn": "arn:aws:organizations::111111111111:handshake/o-
exampleorgid/invite/h-examplehandshakeid111",
                "RequestedTimestamp": 1481656459.257,
                "ExpirationTimestamp": 1482952459.257,
                "Id": "h-examplehandshakeid111",
                "Parties": [
                        {
                                "Id": "o-exampleorgid",
                                "Type": "ORGANIZATION"
                        },
                        {
                                "Id": "juan@example.com",
                                "Type": "EMAIL"
                        }
                ],
                "Resources": [
                        {
                                "Resources": [
                                        {
                                                "Type": "MASTER_EMAIL",
                                                "Value": "bill@amazon.com"
                                        },
                                        {
                                                "Type": "MASTER_NAME",
                                                "Value": "Org Master Account"
                                        },
                                        {
                                                "Type": "ORGANIZATION_FEATURE_SET",
                                                "Value": "ALL"
                                        }
                                ],
                                "Type": "ORGANIZATION",
                                "Value": "o-exampleorgid"
                        },
                        {
                                "Type": "EMAIL",
```

```
                                "Value": "juan@example.com"
                        }
                ],
                "State": "ACCEPTED"
        }
}
```

- Para obtener información sobre la API, consulte AcceptHandshake en la Referencia de comandos de la AWS CLI.

`attach-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `attach-policy`.

AWS CLI

Asociación de una política a un nodo raíz, unidad organizativa o cuenta

Ejemplo 1

El siguiente ejemplo de código muestra cómo adjuntar una política de control de servicio (SCP) a una unidad organizativa.

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id ou-examplerootid111-exampleouid111
```

Ejemplo 2

El siguiente ejemplo de código muestra cómo adjuntar una política de control de servicio directamente a una cuenta:

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id 333333333333
```

- Para obtener información sobre la API, consulte AttachPolicy en la Referencia de comandos de la AWS CLI.

`cancel-handshake`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-handshake`.

AWS CLI

Para cancelar un protocolo de enlace enviado desde otra cuenta

Bill había enviado una invitación a la cuenta de Susan para unirse a su organización, pero cambia de opinión y decide cancelar la invitación antes de que Susan la acepte. El siguiente ejemplo muestra la cancelación de Bill:

```
aws organizations cancel-handshake --handshake-id h-examplehandshakeid111
```

El resultado incluye un objeto de protocolo de enlace que muestra que el estado ahora es `CANCELED`:

```
{
        "Handshake": {
                "Id": "h-examplehandshakeid111",
                "State":"CANCELED",
                "Action": "INVITE",
                "Arn": "arn:aws:organizations::111111111111:handshake/o-
exampleorgid/invite/h-examplehandshakeid111",
                "Parties": [
                        {
                                "Id": "o-exampleorgid",
                                "Type": "ORGANIZATION"
                        },
                        {
                                "Id": "susan@example.com",
                                "Type": "EMAIL"
                        }
                ],
                "Resources": [
                        {
                                "Type": "ORGANIZATION",
                                "Value": "o-exampleorgid",
                                "Resources": [
                                        {
                                                "Type": "MASTER_EMAIL",
                                                "Value": "bill@example.com"
```

```
                                        },
                                        {
                                                "Type": "MASTER_NAME",
                                                "Value": "Master Account"
                                        },
                                        {
                                                "Type": "ORGANIZATION_FEATURE_SET",
                                                "Value": "CONSOLIDATED_BILLING"
                                        }
                                ]
                        },
                        {
                                "Type": "EMAIL",
                                "Value": "anika@example.com"
                        },
                        {
                                "Type": "NOTES",
                                "Value": "This is a request for Susan's account to
 join Bob's organization."
                        }
                ],
                "RequestedTimestamp": 1.47008383521E9,
                "ExpirationTimestamp": 1.47137983521E9
        }
}
```

- Para obtener información sobre la API, consulte CancelHandshake en la Referencia de comandos de la AWS CLI.

`create-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-account`.

AWS CLI

Creación de una cuenta de miembro que forme parte automáticamente de la organización

En el siguiente ejemplo se muestra cómo crear una cuenta de miembro en una organización. La cuenta de miembro se configura con el nombre Production Account y la dirección de correo electrónico susan@example.com. Organizations crea automáticamente un rol de IAM con el nombre predeterminado de OrganizationAccountAccessRole porque no se especifica el parámetro roleName. Además, la configuración que permite a los usuarios o roles de IAM con

permisos suficientes acceder a los datos de facturación de la cuenta se establece en el valor predeterminado de ALLOW porque no se especifica el parámetro IamUserAccessToBilling. Organizations envía automáticamente a Susan un correo electrónico “Le damos la bienvenida a AWS”:

```
aws organizations create-account --email susan@example.com --account-
name "Production Account"
```

La salida incluye un objeto de solicitud que muestra que el estado ahora es `IN_PROGRESS`:

```
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

Más adelante, puede consultar el estado actual de la solicitud proporcionando el valor de respuesta de ID al comando describe-create-account-status como valor del parámetro create-account-request-id.

Para obtener más información, consulte Creación de una cuenta de AWS en su organización en la Guía del usuario de AWS Organizations.

- Para obtener información sobre la API, consulte CreateAccount en la Referencia de comandos de la AWS CLI.

`create-organization`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-organization`.

AWS CLI

Ejemplo 1: Creación de una nueva organización

Bill quiere crear una organización con las credenciales de la cuenta 111111111111. En el siguiente ejemplo se muestra que la cuenta se convierte en la cuenta maestra de la nueva organización. Puesto que no especifica un conjunto de características, la nueva organización tiene habilitadas todas las características de forma predeterminada y las políticas de control de servicios están habilitadas en la raíz.

```
aws organizations create-organization
```

El resultado incluye un objeto de organización con detalles sobre la nueva organización:

```
{
        "Organization": {
                "AvailablePolicyTypes": [
                        {
                                "Status": "ENABLED",
                                "Type": "SERVICE_CONTROL_POLICY"
                        }
                ],
                "MasterAccountId": "111111111111",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "FeatureSet": "ALL",
                "Id": "o-exampleorgid",
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
        }
}
```

Ejemplo 2: Creación de una nueva organización con solo las características de facturación consolidada habilitadas

En el siguiente ejemplo se crea una organización que solo admite las características de facturación consolidada:

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

El resultado incluye un objeto de organización con detalles sobre la nueva organización:

```
{
        "Organization": {
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
                "AvailablePolicyTypes": [],
                "Id": "o-exampleorgid",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/111111111111",
```

```
                "MasterAccountEmail": "bill@example.com",
                "MasterAccountId": "111111111111",
                "FeatureSet": "CONSOLIDATED_BILLING"
        }
}
```

Para obtener más información, consulte Creación de una organización en la Guía del usuario de AWS Organizations.

- Para obtener información sobre la API, consulte CreateOrganization en la Referencia de comandos de la AWS CLI.

`create-organizational-unit`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-organizational-unit`.

AWS CLI

Creación de una unidad organizativa en raíz o UO principal

En el siguiente ejemplo se muestra cómo crear una unidad organizativa que se denomina AccountingOU:

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

El resultado incluye un objeto organizationalUnit con detalles sobre la nueva unidad organizativa:

```
{
        "OrganizationalUnit": {
                "Id": "ou-examplerootid111-exampleouid111",
                "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
                "Name": "AccountingOU"
        }
}
```

- Para obtener información sobre la API, consulte CreateOrganizationalUnit en la Referencia de comandos de la AWS CLI.

`create-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-policy`.

AWS CLI

Ejemplo 1: Creación de una política con un archivo fuente de texto para la política JSON

En el siguiente ejemplo se muestra cómo crear una política de control de servicios (SCP) denominada `AllowAllS3Actions`. El contenido de la política se extrae de un archivo del equipo local denominado `policy.json`.

```
aws organizations create-policy --content file://policy.json --
name AllowAllS3Actions, --type SERVICE_CONTROL_POLICY --description "Allows
 delegation of all S3 actions"
```

La salida incluye un objeto de política con detalles sobre la nueva política:

```
{
        "Policy": {
                "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":
\"Allow\",\"Action\":[\"s3:*\"],\"Resource\":[\"*\"]}]}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::o-exampleorgid:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Allows delegation of all S3 actions",
                        "Name": "AllowAllS3Actions",
                        "Type":"SERVICE_CONTROL_POLICY"
                }
        }
}
```

Ejemplo 2: Creación de una política con una política JSON como parámetro

En el siguiente ejemplo se muestra cómo crear el mismo SCP, esta vez integrando el contenido de la política como una cadena JSON en el parámetro. La cadena debe aplicar una secuencia de escape con barras diagonales antes de las comillas dobles para garantizar que se traten como literales en el parámetro, que a su vez queda rodeado de comillas dobles:

```
aws organizations create-policy --content "{\"Version\":\"2012-10-17\",\"Statement
\":[{\"Effect\":\"Allow\",\"Action\":[\"s3:*\"],\"Resource\":[\"*\"]}]}" --
```

```
name AllowAllS3Actions --type SERVICE_CONTROL_POLICY --description "Allows
 delegation of all S3 actions"
```

Para obtener más información sobre la creación y el uso de políticas en su organización, consulte Administración de políticas de la organización en la Guía del usuario de AWS Organizations.

- Para obtener información sobre la API, consulte CreatePolicy en la Referencia de comandos de la AWS CLI.

`decline-handshake`

En el siguiente ejemplo de código, se muestra cómo utilizar `decline-handshake`.

AWS CLI

Para cancelar un protocolo de enlace enviado desde otra cuenta

En el siguiente ejemplo, se muestra que Susan, una administradora propietaria de la cuenta 222222222222, rechaza una invitación para unirse a la organización de Bill. La operación DeclineHandshake devuelve un objeto de protocolo de enlace que muestra que el estado ahora es DECLINED:

```
aws organizations decline-handshake --handshake-id h-examplehandshakeid111
```

El resultado incluye un objeto de protocolo de enlace que muestra que el estado ahora es DECLINED:

```
{
        "Handshake": {
                "Id": "h-examplehandshakeid111",
                "State": "DECLINED",
                "Resources": [
                        {
                                "Type": "ORGANIZATION",
                                "Value": "o-exampleorgid",
                                "Resources": [
                                        {
                                                "Type": "MASTER_EMAIL",
                                                "Value": "bill@example.com"
                                        },
                                        {
```

```
                                                "Type": "MASTER_NAME",
                                                "Value": "Master Account"
                                        }
                                ]
                        },
                        {
                                "Type": "EMAIL",
                                "Value": "susan@example.com"
                        },
                        {
                                "Type": "NOTES",
                                "Value": "This is an invitation to Susan's account
 to join the Bill's organization."
                        }
                ],
                "Parties": [
                        {
                                "Type": "EMAIL",
                                "Id": "susan@example.com"
                        },
                        {
                                "Type": "ORGANIZATION",
                                "Id": "o-exampleorgid"
                        }
                ],
                "Action": "INVITE",
                "RequestedTimestamp": 1470684478.687,
                "ExpirationTimestamp": 1471980478.687,
                "Arn": "arn:aws:organizations::111111111111:handshake/o-
exampleorgid/invite/h-examplehandshakeid111"
        }
}
```

- Para obtener más información sobre la API, consulte DeclineHandshake en la Referencia de comandos de la AWS CLI.

`delete-organization`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-organization`.

AWS CLI

Eliminación de una organización

En el siguiente ejemplo se muestra cómo eliminar una organización. Para realizar esta operación, debe ser administrador de la cuenta maestra de la organización. En el ejemplo se supone que anteriormente se eliminaron todas las cuentas, unidades organizativas y políticas de los miembros de la organización:

```
aws organizations delete-organization
```

- Para obtener información sobre la API, consulte DeleteOrganization en la Referencia de comandos de la AWS CLI.

`delete-organizational-unit`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-organizational-unit`.

AWS CLI

Eliminación de una unidad organizativa

En el ejemplo siguiente se muestra cómo se elimina una OU. En el ejemplo se supone que anteriormente se eliminaron todas las cuentas y demás unidades organizativas de la unidad organizativa:

```
aws organizations delete-organizational-unit --organizational-unit-id ou-examplerootid111-exampleouid111
```

- Para obtener información sobre la API, consulte DeleteOrganizationalUnit en la Referencia de comandos de la AWS CLI.

`delete-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-policy`.

AWS CLI

Eliminación de una política

En el siguiente ejemplo se muestra cómo eliminar una política de una organización. En el ejemplo se asume que anteriormente se ha desvinculado la política de todas las entidades:

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- Para obtener información sobre la API, consulte DeletePolicy en la Referencia de comandos de la AWS CLI.

`describe-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-account`.

AWS CLI

Para obtener los detalles de una cuenta

El siguiente ejemplo muestra cómo recuperar los detalles de una cuenta:

```
aws organizations describe-account --account-id 555555555555
```

El resultado muestra un objeto de cuenta con los detalles de la cuenta:

```
{
        "Account": {
                "Id": "555555555555",
                "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/555555555555",
                "Name": "Beta account",
                "Email": "anika@example.com",
                "JoinedMethod": "INVITED",
                "JoinedTimeStamp": 1481756563.134,
                "Status": "ACTIVE"
        }
}
```

- Para obtener información sobre la API, consulte DescribeAccount en la Referencia de comandos de la AWS CLI.

`describe-create-account-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-create-account-status`.

AWS CLI

Para obtener el estado más reciente de una solicitud de creación de cuenta

En el siguiente ejemplo se muestra cómo solicitar el estado más reciente de una solicitud anterior para crear una cuenta en una organización. El --request-id especificado proviene de la respuesta de la llamada original a create-account. La solicitud de creación de cuenta muestra en el campo de estado que Organizations completó correctamente la creación de la cuenta.

Comando:

```
aws organizations describe-create-account-status --create-account-request-id car-examplecreateaccountrequestid111
```

Salida:

```
{
  "CreateAccountStatus": {
    "State": "SUCCEEDED",
    "AccountId": "555555555555",
    "AccountName": "Beta account",
    "RequestedTimestamp": 1470684478.687,
    "CompletedTimestamp": 1470684532.472,
    "Id": "car-examplecreateaccountrequestid111"
  }
}
```

- Para obtener información sobre la API, consulte DescribeCreateAccountStatus en la Referencia de comandos de la AWS CLI.

`describe-handshake`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-handshake`.

AWS CLI

Obtención de información sobre un protocolo de enlace

El siguiente ejemplo muestra cómo recuperar los detalles de un protocolo de enlace. El identificador del protocolo de enlace proviene de la llamada original a `InviteAccountToOrganization` o de una llamada a `ListHandshakesForAccount` o `ListHandshakesForOrganization`.

```
aws organizations describe-handshake --handshake-id h-examplehandshakeid111
```

El resultado incluye un objeto de protocolo de enlace que contiene todos los detalles sobre el protocolo de enlace solicitado:

```
{
        "Handshake": {
                "Id": "h-examplehandshakeid111",
                "State": "OPEN",
                "Resources": [
                        {
                                "Type": "ORGANIZATION",
                                "Value": "o-exampleorgid",
                                "Resources": [
                                        {
                                                "Type": "MASTER_EMAIL",
                                                "Value": "bill@example.com"
                                        },
                                        {
                                                "Type": "MASTER_NAME",
                                                "Value": "Master Account"
                                        }
                                ]
                        },
                        {
                                "Type": "EMAIL",
                                "Value": "anika@example.com"
                        }
                ],
                "Parties": [
                        {
                                "Type": "ORGANIZATION",
                                "Id": "o-exampleorgid"
                        },
                        {
                                "Type": "EMAIL",
                                "Id": "anika@example.com"
                        }
                ],
                "Action": "INVITE",
                "RequestedTimestamp": 1470158698.046,
                "ExpirationTimestamp": 1471454698.046,
                "Arn": "arn:aws:organizations::111111111111:handshake/o-
exampleorgid/invite/h-examplehandshakeid111"
        }
```

```
}
```

- Para obtener información sobre la API, consulte DescribeHandshake en la Referencia de comandos de la AWS CLI.

`describe-organization`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-organization`.

AWS CLI

Para obtener información sobre la organización actual

El siguiente ejemplo muestra cómo solicitar detalles de una organización:

```
aws organizations describe-organization
```

El resultado incluye un objeto de organización con los detalles sobre la organización:

```
{
        "Organization": {
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "MasterAccountId": "111111111111",
                "Id": "o-exampleorgid",
                "FeatureSet": "ALL",
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
                "AvailablePolicyTypes": [
                        {
                                "Status": "ENABLED",
                                "Type": "SERVICE_CONTROL_POLICY"
                        }
                ]
        }
}
```

- Para obtener información sobre la API, consulte DescribeOrganization en la Referencia de comandos de la AWS CLI.

`describe-organizational-unit`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-organizational-unit`.

AWS CLI

Para obtener información sobre una unidad organizativa

En el siguiente ejemplo de `describe-organizational-unit` se solicitan detalles sobre una unidad organizativa.

```
aws organizations describe-organizational-unit \
    --organizational-unit-id ou-examplerootid111-exampleouid111
```

Salida:

```
{
    "OrganizationalUnit": {
        "Name": "Accounting Group",
        "Arn": "arn:aws:organizations::123456789012:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
        "Id": "ou-examplerootid111-exampleouid111"
    }
}
```

- Para obtener información sobre la API, consulte DescribeOrganizationalUnit en la Referencia de comandos de la AWS CLI.

`describe-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-policy`.

AWS CLI

Obtención de información acerca de una política

En el siguiente ejemplo se muestra cómo solicitar información acerca de una política:

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

El resultado incluye un objeto de política que contiene detalles acerca de la política:

```
{
        "Policy": {
                "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n
    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n      \"Resource\":
 \"*\"\n    }\n  ]\n}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::111111111111:policy/o-
exampleorgid/service_control_policy/p-examplepolicyid111",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-examplepolicyid111",
                        "AwsManaged": false,
                        "Name": "AllowAllS3Actions",
                        "Description": "Enables admins to delegate S3 permissions"
                }
        }
}
```

- Para obtener información sobre la API, consulte DescribePolicy en la Referencia de comandos de la AWS CLI.

`detach-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `detach-policy`.

AWS CLI

Desasociación de una política de un nodo raíz, unidad organizativa o cuenta

En el siguiente ejemplo se muestra cómo desasociar una política de una unidad organizativa:

```
aws organizations  detach-policy  --target-id ou-examplerootid111-exampleouid111 --
policy-id p-examplepolicyid111
```

- Para obtener información sobre la API, consulte DetachPolicy en la Referencia de comandos de la AWS CLI.

`disable-policy-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-policy-type`.

AWS CLI

Para deshabilitar un tipo de política en una raíz

El siguiente ejemplo muestra cómo deshabilitar el tipo de política llamado política de control de servicios (SCP) en una raíz:

```
aws organizations disable-policy-type --root-id r-examplerootid111 --policy-
type SERVICE_CONTROL_POLICY
```

El resultado muestra que el elemento de respuesta PolicyTypes ya no incluye SERVICE_CONTROL_POLICY:

```
{
        "Root": {
                "PolicyTypes": [],
                "Name": "Root",
                "Id": "r-examplerootid111",
                "Arn": "arn:aws:organizations::111111111111:root/o-exampleorgid/r-
examplerootid111"
        }
}
```

- Para obtener más detalles sobre la API, consulte DisablePolicyType en la Referencia de comandos de la AWS CLI.

`enable-all-features`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-all-features`.

AWS CLI

Para habilitar todas las características en una organización

En este ejemplo, se muestra al administrador pidiendo a todas las cuentas invitadas de la organización que aprueben la habilitación de todas las características de la organización. AWS Organizations envía un correo electrónico a la dirección registrada con cada cuenta de miembro invitada pidiendo al propietario que apruebe el cambio en todas las características aceptando el protocolo de enlace enviado. Una vez que todas las cuentas de los miembros invitadas aceptan el protocolo de enlace, el administrador de la organización podrá finalizar el cambio a todas

las características y, quienes dispongan de los permisos adecuados, podrán crear políticas y aplicarlas a las raíces, las unidades organizativas y las cuentas:

```
aws organizations enable-all-features
```

El resultado es un objeto de protocolo de enlace que se envía a todas las cuentas de los miembros invitadas para su aprobación:

```
{
        "Handshake": {
                "Action": "ENABLE_ALL_FEATURES",
                "Arn":"arn:aws:organizations::111111111111:handshake/o-exampleorgid/
enable_all_features/h-examplehandshakeid111",
                "ExpirationTimestamp":1.483127868609E9,
                "Id":"h-examplehandshakeid111",
                "Parties": [
                        {
                                "id":"o-exampleorgid",
                                "type":"ORGANIZATION"
                        }
                ],
                "requestedTimestamp":1.481831868609E9,
                "resources": [
                        {
                                "type":"ORGANIZATION",
                                "value":"o-exampleorgid"
                        }
                ],
                "state":"REQUESTED"
        }
}
```

- Para obtener información sobre las API, consulte EnableAllFeatures en la Referencia de comandos de la AWS CLI.

`enable-policy-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-policy-type`.

AWS CLI

Para habilitar el uso de un tipo de política en una raíz

El siguiente ejemplo muestra cómo habilitar el tipo de política llamado política de control de servicios (SCP) en una raíz:

```
aws organizations enable-policy-type --root-id r-examplerootid111 --policy-
type SERVICE_CONTROL_POLICY
```

El resultado muestra un objeto raíz con un elemento de respuesta policyTypes que indica que los SCP ya están habilitados:

```
{
        "Root": {
                "PolicyTypes": [
                        {
                                "Status":"ENABLED",
                                "Type":"SERVICE_CONTROL_POLICY"
                        }
                ],
                "Id": "r-examplerootid111",
                "Name": "Root",
                "Arn": "arn:aws:organizations::111111111111:root/o-exampleorgid/r-
examplerootid111"
        }
}
```

- Para obtener información sobre la API, consulte EnablePolicyType en la Referencia de comandos de la AWS CLI.

`invite-account-to-organization`

En el siguiente ejemplo de código, se muestra cómo utilizar `invite-account-to-organization`.

AWS CLI

Para invitar a una cuenta a unirse a una organización

En el siguiente ejemplo, se muestra la cuenta maestra propiedad de bill@example.com que invita a la cuenta propiedad de juan@example.com a unirse a una organización:

```
aws organizations invite-account-to-organization --target '{"Type": "EMAIL", "Id":
 "juan@example.com"}' --notes "This is a request for Juan's account to join Bill's
 organization."
```

El resultado incluye una estructura de protocolo de enlace que muestra lo que se envía a la cuenta invitada:

```
{
        "Handshake": {
                "Action": "INVITE",
                "Arn": "arn:aws:organizations::111111111111:handshake/o-
exampleorgid/invite/h-examplehandshakeid111",
                "ExpirationTimestamp": 1482952459.257,
                "Id": "h-examplehandshakeid111",
                "Parties": [
                        {
                                "Id": "o-exampleorgid",
                                "Type": "ORGANIZATION"
                        },
                        {
                                "Id": "juan@example.com",
                                "Type": "EMAIL"
                        }
                ],
                "RequestedTimestamp": 1481656459.257,
                "Resources": [
                        {
                                "Resources": [
                                        {
                                                "Type": "MASTER_EMAIL",
                                                "Value": "bill@amazon.com"
                                        },
                                        {
                                                "Type": "MASTER_NAME",
                                                "Value": "Org Master Account"
                                        },
                                        {
                                                "Type": "ORGANIZATION_FEATURE_SET",
                                                "Value": "FULL"
                                        }
                                ],
                                "Type": "ORGANIZATION",
                                "Value": "o-exampleorgid"
                        },
                        {
                                "Type": "EMAIL",
                                "Value": "juan@example.com"
```

```
                        }
                ],
                "State": "OPEN"
        }
}
```

- Para obtener información sobre la API, consulte InviteAccountToOrganization en la Referencia de comandos de la AWS CLI.

`leave-organization`

En el siguiente ejemplo de código, se muestra cómo utilizar `leave-organization`.

AWS CLI

Para abandonar una organización como cuenta de miembro

En el siguiente ejemplo, se muestra al administrador de una cuenta de miembro que solicita abandonar la organización de la que es miembro actualmente:

```
aws organizations leave-organization
```

- Para obtener más información sobre la API, consulte LeaveOrganization en la Referencia de comandos de la AWS CLI.

`list-accounts-for-parent`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-accounts-for-parent`.

AWS CLI

Para recuperar una lista de todas las cuentas en una raíz o unidad organizativa principal especificada

En el siguiente ejemplo se muestra cómo solicitar una lista de las cuentas de una unidad organizativa:

```
aws organizations list-accounts-for-parent --parent-id ou-examplerootid111-
exampleouid111
```

La salida incluye una lista de objetos de resumen de cuenta.

```
{
        "Accounts": [
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/333333333333",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835795.536,
                        "Id": "333333333333",
                        "Name": "Development Account",
                        "Email": "juan@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/444444444444",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835812.143,
                        "Id": "444444444444",
                        "Name": "Test Account",
                        "Email": "anika@example.com",
                        "Status": "ACTIVE"
                }
        ]
}
```

- Para obtener información sobre la API, consulte ListAccountsForParent en la Referencia de comandos de la AWS CLI.

`list-accounts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-accounts`.

AWS CLI

Para recuperar una lista de todas las cuentas de una organización

En el siguiente ejemplo se muestra cómo solicitar una lista de las cuentas de una organización:

```
aws organizations list-accounts
```

La salida incluye una lista de objetos de resumen de cuenta.

```
{
        "Accounts": [
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/111111111111",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481830215.45,
                        "Id": "111111111111",
                        "Name": "Master Account",
                        "Email": "bill@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/222222222222",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835741.044,
                        "Id": "222222222222",
                        "Name": "Production Account",
                        "Email": "alice@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/333333333333",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835795.536,
                        "Id": "333333333333",
                        "Name": "Development Account",
                        "Email": "juan@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/444444444444",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835812.143,
                        "Id": "444444444444",
                        "Name": "Test Account",
                        "Email": "anika@example.com",
                        "Status": "ACTIVE"
                }
```

```
        ]
}
```

- Para obtener información sobre la API, consulte ListAccounts en la Referencia de comandos de la AWS CLI.

`list-children`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-children`.

AWS CLI

Para recuperar las cuentas secundarias y las unidades organizativas de una unidad organizativa principal o raíz

En el siguiente ejemplo, se muestra cómo enumerar la raíz o la unidad organizativa que contiene esa cuenta 444444444444:

```
aws organizations list-children --child-type ORGANIZATIONAL_UNIT --parent-id ou-examplerootid111-exampleouid111
```

El resultado muestra las dos unidades organizativas secundarias que contiene la unidad principal:

```
{
        "Children": [
                {
                        "Id": "ou-examplerootid111-exampleouid111",
                        "Type":"ORGANIZATIONAL_UNIT"
                },
                {
                        "Id":"ou-examplerootid111-exampleouid222",
                        "Type":"ORGANIZATIONAL_UNIT"
                }
        ]
}
```

- Para obtener información sobre la API, consulte ListChildren en la Referencia de comandos de la AWS CLI.

`list-create-account-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-create-account-status`.

AWS CLI

Ejemplo 1: recuperar una lista de las solicitudes de creación de cuentas realizadas en la organización actual

En el siguiente ejemplo se muestra cómo solicitar una lista de solicitudes de creación de cuentas para una organización que se han completado correctamente:

```
aws organizations list-create-account-status --states SUCCEEDED
```

El resultado incluye una matriz de objetos con información sobre cada solicitud.

```
{
        "CreateAccountStatuses": [
                {
                        "AccountId": "444444444444",
                        "AccountName": "Developer Test Account",
                        "CompletedTimeStamp": 1481835812.143,
                        "Id": "car-examplecreateaccountrequestid111",
                        "RequestedTimeStamp": 1481829432.531,
                        "State": "SUCCEEDED"
                }
        ]
}
```

Ejemplo 2: recuperar una lista de las solicitudes de creación de cuentas en curso en la organización actual

En el siguiente ejemplo se obtiene una lista de las solicitudes de creación de cuentas en curso para una organización:

```
aws organizations list-create-account-status --states IN_PROGRESS
```

El resultado incluye una matriz de objetos con información sobre cada solicitud.

```
{
        "CreateAccountStatuses": [
```

```
                {
                  "State": "IN_PROGRESS",
                  "Id": "car-examplecreateaccountrequestid111",
                  "RequestedTimeStamp": 1481829432.531,
                  "AccountName": "Production Account"
                }
        ]
}
```

- Para obtener información sobre la API, consulte ListCreateAccountStatus en la Referencia de comandos de la AWS CLI.

`list-handshakes-for-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-handshakes-for-account`.

AWS CLI

Para recuperar una lista de los protocolos de enlace enviados a una cuenta

En el siguiente ejemplo se muestra cómo obtener una lista de todos los protocolos de enlace que se han asociado a la cuenta de las credenciales que se usaron para llamar a la operación:

```
aws organizations list-handshakes-for-account
```

El resultado incluye una lista de estructuras de protocolos de enlace con información sobre cada protocolo, incluido su estado actual:

```
{
        "Handshake": {
                "Action": "INVITE",
                "Arn": "arn:aws:organizations::111111111111:handshake/o-
exampleorgid/invite/h-examplehandshakeid111",
                "ExpirationTimestamp": 1482952459.257,
                "Id": "h-examplehandshakeid111",
                "Parties": [
                        {
                                "Id": "o-exampleorgid",
                                "Type": "ORGANIZATION"
                        },
                        {
                                "Id": "juan@example.com",
```

```
                                "Type": "EMAIL"
                        }
                ],
                "RequestedTimestamp": 1481656459.257,
                "Resources": [
                        {
                                "Resources": [
                                        {
                                                "Type": "MASTER_EMAIL",
                                                "Value": "bill@amazon.com"
                                        },
                                        {
                                                "Type": "MASTER_NAME",
                                                "Value": "Org Master Account"
                                        },
                                        {
                                                "Type": "ORGANIZATION_FEATURE_SET",
                                                "Value": "FULL"
                                        }
                                ],
                                "Type": "ORGANIZATION",
                                "Value": "o-exampleorgid"
                        },
                        {
                                "Type": "EMAIL",
                                "Value": "juan@example.com"
                        }
                ],
                "State": "OPEN"
        }
}
```

- Para obtener detalles sobre la API, consulte ListHandshakesForAccount en la Referencia de comandos de la AWS CLI.

`list-handshakes-for-organization`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-handshakes-for-organization`.

AWS CLI

Para recuperar una lista de los protocolos de enlace asociados a una organización

En el siguiente ejemplo se muestra cómo obtener una lista de protocolos de enlace que están asociados a la organización actual:

```
aws organizations list-handshakes-for-organization
```

El resultado muestra dos protocolos de enlace. El primero es una invitación a la cuenta de Juan y muestra un estado ABIERTO. La segunda es una invitación a la cuenta de Anika y muestra el estado ACEPTADO:

```
{
        "Handshakes": [
                {
                        "Action": "INVITE",
                        "Arn": "arn:aws:organizations::111111111111:handshake/o-
exampleorgid/invite/h-examplehandshakeid111",
                        "ExpirationTimestamp": 1482952459.257,
                        "Id": "h-examplehandshakeid111",
                        "Parties": [
                                {
                                        "Id": "o-exampleorgid",
                                        "Type": "ORGANIZATION"
                                },
                                {
                                        "Id": "juan@example.com",
                                        "Type": "EMAIL"
                                }
                        ],
                        "RequestedTimestamp": 1481656459.257,
                        "Resources": [
                                {
                                        "Resources": [
                                                {
                                                        "Type": "MASTER_EMAIL",
                                                        "Value": "bill@amazon.com"
                                                },
                                                {
                                                        "Type": "MASTER_NAME",
                                                        "Value": "Org Master
 Account"
                                                },
                                                {
                                                        "Type":
 "ORGANIZATION_FEATURE_SET",
```

```
                                                        "Value": "FULL"
                                                }
                                        ],
                                        "Type": "ORGANIZATION",
                                        "Value": "o-exampleorgid"
                                },
                                {
                                        "Type": "EMAIL",
                                        "Value": "juan@example.com"
                                },
                                {
                                        "Type":"NOTES",
                                        "Value":"This is an invitation to Juan's
 account to join Bill's organization."
                                }
                        ],
                        "State": "OPEN"
                },
                {
                        "Action": "INVITE",
                        "State":"ACCEPTED",
                        "Arn": "arn:aws:organizations::111111111111:handshake/o-
exampleorgid/invite/h-examplehandshakeid111",
                        "ExpirationTimestamp": 1.471797437427E9,
                        "Id": "h-examplehandshakeid222",
                        "Parties": [
                                {
                                        "Id": "o-exampleorgid",
                                        "Type": "ORGANIZATION"
                                },
                                {
                                        "Id": "anika@example.com",
                                        "Type": "EMAIL"
                                }
                        ],
                        "RequestedTimestamp": 1.469205437427E9,
                        "Resources": [
                                {
                                        "Resources": [
                                                {
                                                        "Type":"MASTER_EMAIL",
                                                        "Value":"bill@example.com"
                                                },
                                                {
```

```
                                                "Type":"MASTER_NAME",
                                                "Value":"Master Account"
                                        }
                                ],
                                "Type":"ORGANIZATION",
                                "Value":"o-exampleorgid"
                        },
                        {
                                "Type":"EMAIL",
                                "Value":"anika@example.com"
                        },
                        {
                                "Type":"NOTES",
                                "Value":"This is an invitation to Anika's
 account to join Bill's organization."
                        }
                ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListHandshakesForOrganization en la Referencia de comandos de la AWS CLI.

`list-organizational-units-for-parent`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-organizational-units-for-parent`.

AWS CLI

Para recuperar una lista de las unidades organizativas de una unidad organizativa principal o nodo raíz

El siguiente ejemplo muestra cómo obtener una lista de unidades organizativas en un nodo raíz específico:

```
aws organizations list-organizational-units-for-parent --parent-id r-
examplerootid111
```

El resultado muestra que el nodo raíz especificado contiene dos unidades organizativas y muestra los detalles de cada una de ellas:

```
{
        "OrganizationalUnits": [
                {
                        "Name": "AccountingDepartment",
                        "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-
examplerootid111/ou-examplerootid111-exampleouid111"
                },
                {
                        "Name": "ProductionDepartment",
                        "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-
examplerootid111/ou-examplerootid111-exampleouid222"
                }
        ]
}
```

- Para obtener información sobre la API, consulte ListOrganizationalUnitsForParent en la Referencia de comandos de la AWS CLI.

`list-parents`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-parents`.

AWS CLI

Para enumerar las unidades organizativas o raíces principales de una cuenta o unidad organizativa secundaria

En el siguiente ejemplo, se muestra cómo enumerar la raíz o la unidad organizativa principal que contiene esa cuenta 444444444444:

```
aws organizations list-parents --child-id 444444444444
```

El resultado muestra que la cuenta especificada está en la unidad organizativa con un ID especificado:

```
{
  "Parents": [
        {
          "Id": "ou-examplerootid111-exampleouid111",
          "Type": "ORGANIZATIONAL_UNIT"
```

```
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListParents en la Referencia de comandos de la AWS CLI.

`list-policies-for-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-policies-for-target`.

AWS CLI

Para recuperar una lista de los SCP asociados directamente a una cuenta

En el siguiente ejemplo se muestra cómo obtener una lista de todas las políticas de control de servicios (SCP), como se especifica en el parámetro Filtro, que se asocian directamente a una cuenta:

```
aws organizations list-policies-for-target --filter SERVICE_CONTROL_POLICY --target-
id 444444444444
```

La salida incluye una lista de estructuras de políticas con información resumida sobre las políticas. La lista no incluye las políticas que se aplican a la cuenta porque se heredan de su ubicación en una jerarquía de unidades organizativas:

```
{
        "Policies": [
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllEC2Actions",
                        "AwsManaged", false,
                        "Id": "p-examplepolicyid222",
                        "Arn": "arn:aws:organizations::o-exampleorgid:policy/
service_control_policy/p-examplepolicyid222",
                        "Description": "Enables account admins to delegate
 permissions for any EC2 actions to users and roles in their accounts."
                }
        ]
}
```

- Para obtener información sobre la API, consulte ListPoliciesForTarget en la Referencia de comandos de la AWS CLI.

`list-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-policies`.

AWS CLI

Recuperación de una lista de todas las políticas de una organización de un tipo determinado

En el siguiente ejemplo se muestra cómo obtener una lista de SCP, como se especifica en el parámetro de filtro:

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

La salida incluye una lista de políticas con información resumida:

```
{
        "Policies": [
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllS3Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid111",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Enables account admins to delegate
 permissions for any S3 actions to users and roles in their accounts."
                },
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllEC2Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid222",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid222",
                        "Description": "Enables account admins to delegate
 permissions for any EC2 actions to users and roles in their accounts."
                },
                {
                        "AwsManaged": true,
```

```
                        "Description": "Allows access to every operation",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-FullAWSAccess",
                        "Arn": "arn:aws:organizations::aws:policy/
service_control_policy/p-FullAWSAccess",
                        "Name": "FullAWSAccess"
                }
        ]
}
```

- Para obtener información sobre la API, consulte ListPolicies en la Referencia de comandos de la AWS CLI.

`list-roots`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-roots`.

AWS CLI

Para recuperar una lista de las raíces de una organización

En este ejemplo se muestra cómo obtener la lista de raíces de una organización:

```
aws organizations list-roots
```

El resultado incluye una lista de estructuras de políticas con información resumida:

```
{
        "Roots": [
                {
                        "Name": "Root",
                        "Arn": "arn:aws:organizations::111111111111:root/o-
exampleorgid/r-examplerootid111",
                        "Id": "r-examplerootid111",
                        "PolicyTypes": [
                                {
                                        "Status":"ENABLED",
                                        "Type":"SERVICE_CONTROL_POLICY"
                                }
                        ]
                }
        ]
```

```
}
```

- Para obtener información sobre la API, consulte ListRoots en la Referencia de comandos de la AWS CLI.

`list-targets-for-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-targets-for-policy`.

AWS CLI

Para recuperar una lista de las raíces, unidades organizativas y cuentas a las que esté asociada una política

En el ejemplo siguiente se muestran cómo obtener una lista de las raíces, unidades organizativas y cuentas a las que está asociada una política específica:

```
aws organizations list-targets-for-policy --policy-id p-FullAWSAccess
```

En el resultado se incluye una lista de objetos asociados con información resumida sobre la raíz, las unidades organizativas y las cuentas a las que está asociada la política:

```
{
        "Targets": [
                {
                        "Arn": "arn:aws:organizations::111111111111:root/o-
exampleorgid/r-examplerootid111",
                        "Name": "Root",
                        "TargetId":"r-examplerootid111",
                        "Type":"ROOT"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/333333333333;",
                        "Name": "Developer Test Account",
                        "TargetId": "333333333333",
                        "Type": "ACCOUNT"
                },
                {
                        "Arn":"arn:aws:organizations::111111111111:ou/o-
exampleorgid/ou-examplerootid111-exampleouid111",
                        "Name":"Accounting",
```

```
                        "TargetId":"ou-examplerootid111-exampleouid111",
                        "Type":"ORGANIZATIONAL_UNIT"
                }
        ]
}
```

- Para obtener información sobre la API, consulte ListTargetsForPolicy en la Referencia de comandos de la AWS CLI.

`move-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `move-account`.

AWS CLI

Para mover una cuenta entre raíces o unidades organizativas

El siguiente ejemplo muestra cómo mover la cuenta principal de la organización de la raíz a una unidad organizativa:

```
aws organizations move-account --account-id 333333333333 --source-parent-id r-examplerootid111 --destination-parent-id ou-examplerootid111-exampleouid111
```

- Para obtener información sobre la API, consulte MoveAccount en la Referencia de comandos de la AWS CLI.

`remove-account-from-organization`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-account-from-organization`.

AWS CLI

Para eliminar una cuenta de una organización como cuenta maestra

En el siguiente ejemplo se muestra cómo eliminar una cuenta de una organización:

```
aws organizations remove-account-from-organization --account-id 333333333333
```

- Para obtener información sobre la API, consulte RemoveAccountFromOrganization en la Referencia de comandos de la AWS CLI.

update-organizational-unit

En el siguiente ejemplo de código, se muestra cómo utilizar `update-organizational-unit`.

AWS CLI

Para cambiar el nombre de una unidad organizativa

Este ejemplo muestra cómo cambiar el nombre de una unidad organizativa. En este caso, la unidad organizativa pasa a llamarse AccountingOU:

```
aws organizations update-organizational-unit --organizational-unit-id ou-examplerootid111-exampleouid111 --name AccountingOU
```

En el resultado se observa el nombre nuevo:

```
{
        "OrganizationalUnit": {
                "Id": "ou-examplerootid111-exampleouid111"
                "Name": "AccountingOU",
                "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-examplerootid111-exampleouid111""
        }
}
```

- Para obtener más información sobre la API, consulte UpdateOrganizationalUnit en la Referencia de comandos de la AWS CLI.

update-policy

En el siguiente ejemplo de código, se muestra cómo utilizar `update-policy`.

AWS CLI

Ejemplo 1: cambiar el nombre de una política

En el siguiente ejemplo de `update-policy`, se cambia el nombre de una política y se le da una nueva descripción.

```
aws organizations update-policy \
    --policy-id p-examplepolicyid111 \
```

```
    --name Renamed-Policy \
    --description "This description replaces the original."
```

El resultado muestra el nombre y la descripción nuevos.

```
{
    "Policy": {
        "Content": "{\n  \"Version\":\"2012-10-17\",\n  \"Statement\":{\n
  \"Effect\":\"Allow\",\n    \"Action\":\"ec2:*\",\n    \"Resource\":\"*\"\n
  }\n}\n",
        "PolicySummary": {
            "Id": "p-examplepolicyid111",
            "AwsManaged": false,
            "Arn":"arn:aws:organizations::111111111111:policy/o-exampleorgid/
service_control_policy/p-examplepolicyid111",
            "Description": "This description replaces the original.",
            "Name": "Renamed-Policy",
            "Type": "SERVICE_CONTROL_POLICY"
        }
    }
}
```

Ejemplo 2: reemplazar el contenido de texto JSON de una política

El siguiente ejemplo muestra cómo reemplazar el texto JSON del SCP en el ejemplo anterior por una nueva cadena de texto de política JSON que sea compatible con S3 en lugar de con EC2:

```
aws organizations update-policy \
    --policy-id p-examplepolicyid111 \
    --content "{\"Version\":\"2012-10-17\",\"Statement\":{\"Effect\":\"Allow\",
\"Action\":\"s3:*\",\"Resource\":\"*\"}}"
```

El resultado muestra el nuevo contenido:

```
{
    "Policy": {
        "Content": "{ \"Version\": \"2012-10-17\", \"Statement\": { \"Effect\":
 \"Allow\", \"Action\": \"s3:*\", \"Resource\": \"*\" } }",
        "PolicySummary": {
            "Arn": "arn:aws:organizations::111111111111:policy/o-exampleorgid/
service_control_policy/p-examplepolicyid111",
            "AwsManaged": false;
```

```
            "Description": "This description replaces the original.",
            "Id": "p-examplepolicyid111",
            "Name": "Renamed-Policy",
            "Type": "SERVICE_CONTROL_POLICY"
        }
    }
}
```

- Para obtener información sobre la API, consulte UpdatePolicy en la Referencia de comandos de la AWS CLI.

AWS Outposts Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS Outposts.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`get-outpost-instance-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-outpost-instance-types`.

AWS CLI

Para obtener los tipos de instancia en tu Outpost

En el siguiente ejemplo de `get-outpost-instance-types` se obtienen los tipos de instancia para el Outpost especificado.

```
aws outposts get-outpost-instance-types \
```

```
    --outpost-id op-0ab23c4567EXAMPLE
```

Salida:

```
{
    "InstanceTypes": [
        {
            "InstanceType": "c5d.large"
        },
        {
            "InstanceType": "i3en.24xlarge"
        },
        {
            "InstanceType": "m5d.large"
        },
        {
            "InstanceType": "r5d.large"
        }
    ],
    "OutpostId": "op-0ab23c4567EXAMPLE",
    "OutpostArn": "arn:aws:outposts:us-west-2:123456789012:outpost/
op-0ab23c4567EXAMPLE"
}
```

Para obtener más información, consulte Launch an instance on your Outpost en la Guía del usuario de Outposts de AWS.

- Para ver detalles sobre la API, consulte GetOutpostInstanceTypes en la Referencia de comandos de la AWS CLI.

`get-outpost`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-outpost`.

AWS CLI

Para obtener los detalles de Outpost

El siguiente ejemplo de `get-outpost` muestra los detalles del Outpost especificado.

```
aws outposts get-outpost \
    --outpost-id op-0ab23c4567EXAMPLE
```

Salida:

```
{
    "Outpost": {
        "OutpostId": "op-0ab23c4567EXAMPLE",
        "OwnerId": "123456789012",
        "OutpostArn": "arn:aws:outposts:us-west-2:123456789012:outpost/
op-0ab23c4567EXAMPLE",
        "SiteId": "os-0ab12c3456EXAMPLE",
        "Name": "EXAMPLE",
        "LifeCycleStatus": "ACTIVE",
        "AvailabilityZone": "us-west-2a",
        "AvailabilityZoneId": "usw2-az1",
        "Tags": {}
    }
}
```

Para obtener más información, consulte Working with Outposts en la Guía del usuario de AWS Outposts.

- Para ver detalles sobre la API, consulte GetOutpost en la Referencia de comandos de la AWS CLI.

`list-outposts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-outposts`.

AWS CLI

Para enumerar Outposts

En el siguiente ejemplo de `list-outposts`, se enumeran todos los Outposts de la cuenta de AWS.

```
aws outposts list-outposts
```

Salida:

```
{
    "Outposts": [
        {
            "OutpostId": "op-0ab23c4567EXAMPLE",
```

```
            "OwnerId": "123456789012",
            "OutpostArn": "arn:aws:outposts:us-west-2:123456789012:outpost/
op-0ab23c4567EXAMPLE",
            "SiteId": "os-0ab12c3456EXAMPLE",
            "Name": "EXAMPLE",
            "Description": "example",
            "LifeCycleStatus": "ACTIVE",
            "AvailabilityZone": "us-west-2a",
            "AvailabilityZoneId": "usw2-az1",
            "Tags": {
                "Name": "EXAMPLE"
            }
        },
        {
            "OutpostId": "op-4fe3dc21baEXAMPLE",
            "OwnerId": "123456789012",
            "OutpostArn": "arn:aws:outposts:us-west-2:123456789012:outpost/
op-4fe3dc21baEXAMPLE",
            "SiteId": "os-0ab12c3456EXAMPLE",
            "Name": "EXAMPLE2",
            "LifeCycleStatus": "ACTIVE",
            "AvailabilityZone": "us-west-2a",
            "AvailabilityZoneId": "usw2-az1",
            "Tags": {}
        }
    ]
}
```

Para obtener más información, consulte Working with Outposts en la Guía del usuario de AWS Outposts.

- Para obtener información sobre la API, consulte ListOutposts en la Referencia de comandos de la AWS CLI.

`list-sites`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-sites`.

AWS CLI

Para enumerar sitios

En el siguiente ejemplo de `list-sites`, se enumeran todos los Outposts de la cuenta de AWS.

```
aws outposts list-sites
```

Salida:

```
{
    "Sites": [
        {
            "SiteId": "os-0ab12c3456EXAMPLE",
            "AccountId": "123456789012",
            "Name": "EXAMPLE",
            "Description": "example",
            "Tags": {}
        }
    ]
}
```

Para obtener más información, consulte Working with Outposts en la Guía del usuario de AWS Outposts.

- Para obtener información sobre la API, consulte ListSites en la Referencia de comandos de la AWS CLI.

AWS Payment Cryptography Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS Payment Cryptography.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-alias`.

AWS CLI

Creación de un alias para una clave

En el siguiente ejemplo de `create-alias` se crea un alias para la clave.

```
aws payment-cryptography create-alias \
    --alias-name alias/sampleAlias1 \
    --key-arn arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h
```

Salida:

```
{
    "Alias": {
        "AliasName": "alias/sampleAlias1",
        "KeyArn": "arn:aws:payment-cryptography:us-west-2:123456789012:key/
kwapwa6qaifllw2h"
    }
}
```

Para obtener más información, consulte About aliases en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte CreateAlias en la Referencia de comandos de la AWS CLI.

`create-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-key`.

AWS CLI

Creación de una clave

El siguiente ejemplo de `create-key` genera una clave 2KEY TDES que puede usar para generar y verificar valores CVV o CVV2.

```
aws payment-cryptography create-key \
    --exportable \
    --key-
attributes KeyAlgorithm=TDES_2KEY, KeyUsage=TR31_C0_CARD_VERIFICATION_KEY,KeyClass=SYMMETRIC
```

Salida:

```
{
    "Key": {
        "CreateTimestamp": "1686800690",
        "Enabled": true,
        "Exportable": true,
        "KeyArn": "arn:aws:payment-cryptography:us-west-2:123456789012:key/
kwapwa6qaifllw2h",
        "KeyAttributes": {
            "KeyAlgorithm": "TDES_2KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
                "Decrypt": false,
                "DeriveKey": false,
                "Encrypt": false,
                "Generate": true,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": false,
                "Verify": true,
                "Wrap": false
            },
            "KeyUsage": "TR31_C0_CARD_VERIFICATION_KEY"
        },
        "KeyCheckValue": "F2E50F",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "CREATE_COMPLETE",
        "UsageStartTimestamp": "1686800690"
    }
}
```

Para obtener más información, consulte Generating keys en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte CreateKey en la Referencia de comandos de la AWS CLI.

`delete-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-alias`.

AWS CLI

Eliminación de un alias

En el siguiente ejemplo de `delete-alias`, se elimina un alias. No afecta a la clave.

```
aws payment-cryptography delete-alias \
    --alias-name alias/sampleAlias1
```

Este comando no genera ninguna salida.

Para obtener más información, consulte About aliases en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte DeleteTopic en la Referencia de comandos de la AWS CLI.

`delete-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-key`.

AWS CLI

Eliminación de una clave

En el siguiente ejemplo de `delete-key`, se programa la eliminación de una clave después de siete días, que es el período de espera predeterminado.

```
aws payment-cryptography delete-key \
    --key-identifier arn:aws:payment-cryptography:us-west-2:123456789012:key/
kwapwa6qaifllw2h
```

Salida:

```
{
    "Key": {
        "CreateTimestamp": "1686801198",
        "DeletePendingTimestamp": "1687405998",
```

```
        "Enabled": true,
        "Exportable": true,
        "KeyArn": "arn:aws:payment-cryptography:us-west-2:123456789012:key/
kwapwa6qaifllw2h",
        "KeyAttributes": {
            "KeyAlgorithm": "TDES_2KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
                "Decrypt": false,
                "DeriveKey": false,
                "Encrypt": false,
                "Generate": true,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": false,
                "Verify": true,
                "Wrap": false
            },
            "KeyUsage": "TR31_C0_CARD_VERIFICATION_KEY"
        },
        "KeyCheckValue": "F2E50F",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "DELETE_PENDING",
        "UsageStartTimestamp": "1686801190"
    }
}
```

Para obtener más información, consulte Deleting keys en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte DeleteKey en la Referencia de comandos de la AWS CLI.

`export-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `export-key`.

AWS CLI

Exportación de una clave

En el siguiente ejemplo de `export-key`, se exporta una clave.

```
aws payment-cryptography export-key \
    --export-key-identifier arn:aws:payment-cryptography:us-west-2:123456789012:key/
lco3w6agsk7zgu2l \
    --key-material '{"Tr34KeyBlock": { \
        "CertificateAuthorityPublicKeyIdentifier": "arn:aws:payment-cryptography:us-
west-2:123456789012:key/ftobshq7pvioc5fx", \
        "ExportToken": "export-token-cu4lg26ofcziixny", \
        "KeyBlockFormat": "X9_TR34_2012", \
        "WrappingKeyCertificate": file://wrapping-key-certificate.pem }}'
```

Contenido de `wrapping-key-certificate.pem`:

```
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUV2VENDQXFXZ0F3SUJBZ0lSQU1ZZS8xMXFUK2svVzlRUDJQOElV
```

Salida:

```
{
    "WrappedKey": {
        "KeyMaterial":
 "308205A106092A864886F70D010702A08205923082058E020101310D300B0609608648016503040201308203 1F
        "WrappedKeyMaterialFormat": "TR34_KEY_BLOCK"
    }
}
```

Para obtener más información, consulte Export keys en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte ExportKey en la Referencia de comandos de AWS CLI.

`get-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-alias`.

AWS CLI

Obtención de un alias

El siguiente ejemplo de `get-alias` devuelve el ARN de la clave asociada al alias.

```
aws payment-cryptography get-alias \
```

```
    --alias-name alias/sampleAlias1
```

Salida:

```
{
    "Alias": {
        "AliasName": "alias/sampleAlias1",
        "KeyArn": "arn:aws:payment-cryptography:us-west-2:123456789012:key/
kwapwa6qaifllw2h"
    }
}
```

Para obtener más información, consulte About aliases en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte GetAlias en la Referencia de comandos de AWS CLI.

get-key

En el siguiente ejemplo de código, se muestra cómo utilizar `get-key`.

AWS CLI

Obtención de los metadatos de una clave

El siguiente ejemplo de `get-key` devuelve los metadatos de la clave asociada al alias. Esta operación no devuelve ningún material criptográfico.

```
aws payment-cryptography get-key \
    --key-identifier alias/sampleAlias1
```

Salida:

```
{
    "Key": {
        "CreateTimestamp": "1686800690",
        "DeletePendingTimestamp": "1687405998",
        "Enabled": true,
        "Exportable": true,
        "KeyArn": "arn:aws:payment-cryptography:us-west-2:123456789012:key/
kwapwa6qaifllw2h",
```

```
        "KeyAttributes": {
            "KeyAlgorithm": "TDES_2KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
                "Decrypt": false,
                "DeriveKey": false,
                "Encrypt": false,
                "Generate": true,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": false,
                "Verify": true,
                "Wrap": false
            },
            "KeyUsage": "TR31_C0_CARD_VERIFICATION_KEY"
        },
        "KeyCheckValue": "F2E50F",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "DELETE_PENDING",
        "UsageStartTimestamp": "1686801190"
    }
}
```

Para obtener más información, consulte Get keys en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte GetKey en la Referencia de comandos de la AWS CLI.

`get-parameters-for-export`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-parameters-for-export`.

AWS CLI

Iniciación de un proceso de exportación

En el siguiente ejemplo de `get-parameters-for-export`, se genera un par de claves, se firma la clave y, a continuación, se devuelven el certificado y la raíz del certificado.

```
aws payment-cryptography get-parameters-for-export \
    --signing-key-algorithm RSA_2048 \
```

```
    --key-material-type TR34_KEY_BLOCK
```

Salida:

```
{
    "ExportToken": "export-token-ep5cwyzune7oya53",
    "ParametersValidUntilTimestamp": "1687415640",
    "SigningKeyAlgorithm": "RSA_2048",
    "SigningKeyCertificate":

    "MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
    VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
    b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
    BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
    MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
    VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
    b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
    YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
    21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
    rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
    Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
    nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
    FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
    NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=",
    "SigningKeyCertificateChain":
    "NIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
    VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
    b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
    BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
    MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
    VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
    b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
    YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
    21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
    rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
    Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
    nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
    FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
    NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE="
}
```

Para obtener más información, consulte Export keys en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte GetParametersForExport en la Referencia de comandos de la AWS CLI.

`get-parameters-for-import`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-parameters-for-import`.

AWS CLI

Iniciación del proceso de importación

En el siguiente ejemplo de `get-parameters-for-import`, se genera un par de claves, se firma la clave y, a continuación, se devuelven el certificado y la raíz del certificado.

```
aws payment-cryptography get-parameters-for-import \
    --key-material-type TR34_KEY_BLOCK \
    --wrapping-key-algorithm RSA_2048
```

Salida:

```
{
    "ImportToken": "import-token-qgmafpaa7nt2kfbb",
    "ParametersValidUntilTimestamp": "1687415640",
    "WrappingKeyAlgorithm": "RSA_2048",
    "WrappingKeyCertificate":
    "MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
    VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
    b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
    BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
    MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
    VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
    b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
    YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
    21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
    rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
    Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
    nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
    FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
    NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=",
    "WrappingKeyCertificateChain":
    "NIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
    VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
```

```
    b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
    BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
    MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
    VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
    b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
    YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
    21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
    rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
    Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
    nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
    FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
    NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE="
}
```

Para obtener más información, consulte Import keys en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte GetParametersForImport en la Referencia de comandos de la AWS CLI.

`get-public-key-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-public-key-certificate`.

AWS CLI

Devolución de una clave pública

El siguiente ejemplo de `get-public-key-certificate` devuelve la parte de clave pública de un par de claves.

```
aws payment-cryptography get-public-key-certificate \
    --key-identifier arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h
```

Salida:

```
{
    "KeyCertificate":
    "MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
    VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
    b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
```

```
    BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
    MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
    VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
    b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
    YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
    21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
    rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
    Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
    nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
    FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
    NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=",
    "KeyCertificateChain":
    "NIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
    VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
    b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
    BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
    MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
    VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
    b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
    YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
    21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
    rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
    Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
    nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
    FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
    NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE="
}
```

Para obtener más información, consulte Get the public key/certificate associated with a key pair en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte GetPublicKeyCertificate en la Referencia de comandos de la AWS CLI.

`import-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-key`.

AWS CLI

Importación de una clave TR-34

En el siguiente ejemplo de `import-key`, se importa una clave TR-34.

```
aws payment-cryptography import-key \
        --key-material='{ "Tr34KeyBlock": {" \
            CertificateAuthorityPublicKeyIdentifier": "arn:aws:payment-
cryptography:us-west-2:123456789012:key/rmm5wn2q564njnjm", \
            "ImportToken": "import-token-5ott6ho5nts7bbcg", \
            "KeyBlockFormat": "X9_TR34_2012", \
            "SigningKeyCertificate": file://signing-key-certificate.pem, \
            "WrappedKeyBlock": file://wrapped-key-block.pem }}'
```

Contenido de `signing-key-certificate.pem`:

```
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUV2RENDQXFTZ0F3SUJBZ0lRYWVCK25IbE1WZU1PR1ZiNjU1Q2Jz
```

Contenido de `wrapped-key-block.pem`:

```
3082059806092A864886F70D010702A0820589308205850201013 10D300B0609608648016503040201308203160 6
```

Salida:

```
{
    "Key": {
        "CreateTimestamp": "2023-06-09T16:56:27.621000-07:00",
        "Enabled": true,
        "KeyArn": "arn:aws:payment-cryptography:us-west-2:123456789012:key/
bzmvgyxdg3sktwxd",
        "KeyAttributes": {
            "KeyAlgorithm": "TDES_2KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
                "Decrypt": false,
                "DeriveKey": false,
                "Encrypt": false,
                "Generate": true,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": false,
                "Verify": true,
                "Wrap": false
            },
            "KeyUsage": "TR31_C0_CARD_VERIFICATION_KEY"
        },
```

```
        "KeyCheckValue": "D9B20E",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "KeyOrigin": "EXTERNAL",
        "KeyState": "CREATE_COMPLETE",
        "UsageStartTimestamp": "2023-06-09T16:56:27.621000-07:00"
    }
}
```

Para obtener más información, consulte Import keys en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte ImportKey en la Referencia de comandos de la AWS CLI.

`list-aliases`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-aliases`.

AWS CLI

Obtención de una lista de alias

En el siguiente ejemplo de `list-aliases`, se muestran todos los alias de su cuenta en esta región.

```
aws payment-cryptography list-aliases
```

Salida:

```
{
    "Aliases": [
        {
            "AliasName": "alias/sampleAlias1",
            "KeyArn": "arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h"
        },
        {
            "AliasName": "alias/sampleAlias2",
            "KeyArn": "arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h"
        }
    ]
```

```
}
```

Para obtener más información, consulte About aliases en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte ListAliases en la Referencia de comandos de la AWS CLI.

`list-keys`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-keys`.

AWS CLI

Obtención de la lista de claves de API

El siguiente ejemplo de `list-keys` muestra todos los alias de su cuenta en esta región.

```
aws payment-cryptography list-keys
```

Salida:

```
{
    "Keys": [
    {
        "CreateTimestamp": "1666506840",
        "Enabled": false,
        "Exportable": true,
        "KeyArn": "arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h",
        "KeyAttributes": {
            "KeyAlgorithm": "TDES_3KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
                "Decrypt": true,
                "DeriveKey": false,
                "Encrypt": true,
                "Generate": false,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": true,
                "Verify": false,
```

```
                "Wrap": true
            },
            "KeyUsage": "TR31_P1_PIN_GENERATION_KEY"
        },
        "KeyCheckValue": "369D",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "CREATE_COMPLETE",
        "UsageStopTimestamp": "1666938840"
    }
    ]
}
```

Para obtener más información, consulte List keys en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte ListKeys en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Obtención de la lista de etiquetas para una clave

En el siguiente ejemplo de `list-tags-for-resource`, se obtienen las etiquetas para una clave.

```
aws payment-cryptography list-tags-for-resource \
    --resource-arn arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h
```

Salida:

```
{
    "Tags": [
        {
            "Key": "BIN",
            "Value": "20151120"
        },
```

```
        {
            "Key": "Project",
            "Value": "Production"
        }
    ]
}
```

Para obtener más información, consulte Managing key tags with API operations en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`restore-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-key`.

AWS CLI

Restauración de una clave cuya eliminación está programada

El siguiente ejemplo de `restore-key` cancela la eliminación de una clave.

```
aws payment-cryptography restore-key \
    --key-identifier arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h
```

Salida:

```
{
    "Key": {
        "KeyArn": "arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h",
        "KeyAttributes": {
            "KeyUsage": "TR31_V2_VISA_PIN_VERIFICATION_KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyAlgorithm": "TDES_3KEY",
            "KeyModesOfUse": {
                "Encrypt": false,
                "Decrypt": false,
                "Wrap": false,
                "Unwrap": false,
```

```
                "Generate": true,
                "Sign": false,
                "Verify": true,
                "DeriveKey": false,
                "NoRestrictions": false
            }
        },
        "KeyCheckValue": "",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "Enabled": false,
        "Exportable": true,
        "KeyState": "CREATE_COMPLETE",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "CreateTimestamp": "1686800690",
        "UsageStopTimestamp": "1687405998"
    }
}
```

Para obtener más información, consulte Deleting keys en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte RestoreKey en la Referencia de comandos de la AWS CLI.

`start-key-usage`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-key-usage`.

AWS CLI

Habilitación de una clave

El siguiente ejemplo de `start-key-usage` habilita una clave para su uso.

```
aws payment-cryptography start-key-usage \
    --key-identifier arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h
```

Salida:

```
{
    "Key": {
        "CreateTimestamp": "1686800690",
```

```
        "Enabled": true,
        "Exportable": true,
        "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
alsuwfxug3pgy6xh",
        "KeyAttributes": {
            "KeyAlgorithm": "TDES_3KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
                "Decrypt": true,
                "DeriveKey": false,
                "Encrypt": true,
                "Generate": false,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": true,
                "Verify": false,
                "Wrap": true
            },
            "KeyUsage": "TR31_P1_PIN_GENERATION_KEY"
        },
        "KeyCheckValue": "369D",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "CREATE_COMPLETE",
        "UsageStartTimestamp": "1686800690"
    }
}
```

Para obtener más información, consulte Enabling and disabling keys en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte StartKeyUsage en la Referencia de comandos de la AWS CLI.

`stop-key-usage`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-key-usage`.

AWS CLI

Deshabilitación de una clave

En el siguiente ejemplo de `stop-key-usage`, se desactiva una clave.

```
aws payment-cryptography stop-key-usage \
    --key-identifier arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h
```

Salida:

```
{
    "Key": {
        "CreateTimestamp": "1686800690",
        "Enabled": true,
        "Exportable": true,
        "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
alsuwfxug3pgy6xh",
        "KeyAttributes": {
            "KeyAlgorithm": "TDES_3KEY",
            "KeyClass": "SYMMETRIC_KEY",
            "KeyModesOfUse": {
                "Decrypt": true,
                "DeriveKey": false,
                "Encrypt": true,
                "Generate": false,
                "NoRestrictions": false,
                "Sign": false,
                "Unwrap": true,
                "Verify": false,
                "Wrap": true
            },
            "KeyUsage": "TR31_P1_PIN_GENERATION_KEY"
        },
        "KeyCheckValue": "369D",
        "KeyCheckValueAlgorithm": "ANSI_X9_24",
        "KeyOrigin": "AWS_PAYMENT_CRYPTOGRAPHY",
        "KeyState": "CREATE_COMPLETE",
        "UsageStartTimestamp": "1686800690"
    }
}
```

Para obtener más información, consulte Enabling and disabling keys en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte StopKeyUsage en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Etiquetado de una clave

En el siguiente ejemplo de `tag-resource`, se etiqueta una clave.

```
aws payment-cryptography tag-resource \
    --resource-arn arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h \
    --tags Key=sampleTag,Value=sampleValue
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing key tags en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de una etiqueta en una clave

En el siguiente ejemplo de `untag-resource`, se quita la etiqueta de una clave.

```
aws payment-cryptography untag-resource \
    --resource-arn arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h \
    --tag-keys sampleTag
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing key tags en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-alias`.

AWS CLI

Actualizar un alias

En el siguiente ejemplo de `update-alias`, se asocia el alias a una clave diferente.

```
aws payment-cryptography update-alias \
    --alias-name alias/sampleAlias1 \
    --key-arn arn:aws:payment-cryptography:us-east-2:123456789012:key/
tqv5yij6wtxx64pi
```

Salida:

```
{
    "Alias": {
        "AliasName": "alias/sampleAlias1",
        "KeyArn": "arn:aws:payment-cryptography:us-west-2:123456789012:key/
tqv5yij6wtxx64pi "
    }
}
```

Para obtener más información, consulte About aliases en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte UpdateAlias en la Referencia de comandos de la AWS CLI.

Ejemplos de planos de datos de AWS Payment Cryptography que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes mediante AWS Command Line Interface con el plano de datos de AWS Payment Cryptography.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`decrypt-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `decrypt-data`.

AWS CLI

Descifrado de texto cifrado

El siguiente ejemplo de `decrypt-data` descifra los datos del texto cifrado mediante una clave simétrica. Para esta operación, la clave debe tener `KeyModesOfUse` configurado como `Decrypt` y `KeyUsage` configurado como `TR31_D0_SYMMETRIC_DATA_ENCRYPTION_KEY`.

```
aws payment-cryptography-data decrypt-data \
    --key-identifier arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h \
    --cipher-text 33612AB9D6929C3A828EB6030082B2BD \
    --decryption-attributes 'Symmetric={Mode=CBC}'
```

Salida:

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h",
    "KeyCheckValue": "71D7AE",
    "PlainText": "313233343132333431323334313233334"
}
```

Para obtener más información, consulte Decrypt data en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte DecryptData en la Referencia de comandos de AWS CLI.

`encrypt-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `encrypt-data`.

AWS CLI

Cifrado de datos

En el siguiente ejemplo de `encrypt-data` se cifran los datos en texto plano mediante una clave simétrica. Para esta operación, la clave debe tener `KeyModesOfUse` configurado como `Encrypt` y `KeyUsage` configurado como `TR31_D0_SYMMETRIC_DATA_ENCRYPTION_KEY`.

```
aws payment-cryptography-data encrypt-data \
    --key-identifier arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h \
    --plain-text 31323334313233343132333431323334 \
    --encryption-attributes 'Symmetric={Mode=CBC}'
```

Salida:

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h",
    "KeyCheckValue": "71D7AE",
    "CipherText": "33612AB9D6929C3A828EB6030082B2BD"
}
```

Para obtener más información, consulte Encrypt data en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte EncryptData en la Referencia de comandos de la AWS CLI.

`generate-card-validation-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `generate-card-validation-data`.

AWS CLI

Generación de un CVV

El siguiente ejemplo de `generate-card-validation-data` genera un CVV/CVV2.

```
aws payment-cryptography-data generate-card-validation-data \
    --key-identifier arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h \
    --primary-account-number=171234567890123 \
    --generation-attributes CardVerificationValue2={CardExpiryDate=0123}
```

Salida:

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h",
    "KeyCheckValue": "CADDA1",
    "ValidationData": "801"
}
```

Para obtener más información, consulte Generate card data en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte GenerateCardValidationData en la Referencia de comandos de la AWS CLI.

`generate-mac`

En el siguiente ejemplo de código, se muestra cómo utilizar `generate-mac`.

AWS CLI

Generación de un MAC

El siguiente ejemplo de `generate-card-validation-data` genera un código de autenticación de mensajes basado en hash (HMAC) para la autenticación de datos de tarjeta mediante el algoritmo HMAC_SHA256 y una clave de cifrado HMAC. La clave debe tener `KeyUsage` configurado en `TR31_M7_HMAC_KEY` y `KeyModesOfUse` en`Generate`.

```
aws payment-cryptography-data generate-mac \
```

```
    --key-identifier arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h \
    --message-
data "3b31303838343930303130373333934313533d323430383232363030303730303033f33" \
    --generation-attributes Algorithm=HMAC_SHA256
```

Salida:

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:123456789012:key/
kwapwa6qaifllw2h,
    "KeyCheckValue": "2976E7",
    "Mac": "ED87F26E961C6D0DDB78DA5038AA2BDDEA0DCE03E5B5E96BDDD494F4A7AA470C"
}
```

Para obtener más información, consulte Generate MAC en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte GenerateMac en la Referencia de comandos de la AWS CLI.

`generate-pin-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `generate-pin-data`.

AWS CLI

Generación de un PIN

En el siguiente ejemplo de `generate-card-validation-data`, se genera un nuevo PIN aleatorio mediante el esquema de Visa PIN.

```
aws payment-cryptography-data generate-pin-data \
    --generation-key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/37y2tsl45p5zjbh2 \
    --encryption-key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/ivi5ksfsuplneuyt \
    --primary-account-number 171234567890123 \
    --pin-block-format ISO_FORMAT_0 \
    --generation-attributes VisaPin={PinVerificationKeyIndex=1}
```

Salida:

```
{
    "GenerationKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/37y2tsl45p5zjbh2",
    "GenerationKeyCheckValue": "7F2363",
    "EncryptionKeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ivi5ksfsuplneuyt",
    "EncryptionKeyCheckValue": "7CC9E2",
    "EncryptedPinBlock": "AC17DC148BDA645E",
    "PinData": {
        "VerificationValue": "5507"
    }
}
```

Para obtener más información, consulte Generate PIN data en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte GeneratePinData en la Referencia de comandos de la AWS CLI.

`re-encrypt-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `re-encrypt-data`.

AWS CLI

Cifrado de datos por segunda vez con una clave diferente

En el siguiente ejemplo de `re-encrypt-data`, se descifra el texto cifrado con una clave simétrica AES y se vuelve a cifrar con una clave única derivada por transacción (DUKPT).

```
aws payment-cryptography-data re-encrypt-data \
    --incoming-key-identifier arn:aws:payment-cryptography:us-
west-2:111122223333:key/hyvv7ymboitd4vfy \
    --outgoing-key-identifier arn:aws:payment-cryptography:us-
west-2:111122223333:key/jl6ythkcvzesbxen \
    --cipher-
text 4D2B0BDBA192D5AEFEAA5B3EC28E4A65383C313FFA25140101560F75FE1B99F27192A90980AB9334
 \
    --incoming-encryption-
attributes "Dukpt={Mode=ECB,KeySerialNumber=0123456789111111}" \
    --outgoing-encryption-attributes '{"Symmetric": {"Mode": "ECB"}}'
```

Salida:

```
{
    "CipherText":
 "F94959DA30EEFF0C035483C6067667CF6796E3C1AD28C2B61F9CFEB772A8DD41C0D6822931E0D3B1",
    "KeyArn": "arn:aws:payment-cryptography:us-west-2:111122223333:key/
jl6ythkcvzesbxen",
    "KeyCheckValue": "2E8CD9"
}
```

Para obtener más información, consulte Encrypt and decrypt data en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte ReEncryptData en la Referencia de comandos de AWS CLI.

`translate-pin-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `translate-pin-data`.

AWS CLI

Traducción de datos PIN

En el siguiente ejemplo de `translate-pin-data`, se traduce un PIN de cifrado TDES PEK mediante un bloque de PIN ISO 0 a un bloque de PIN AES ISO 4 mediante el algoritmo DUKPT.

```
aws payment-cryptography-data translate-pin-data \
    --encrypted-pin-block "AC17DC148BDA645E" \
    --incoming-translation-
attributes=IsoFormat0='{PrimaryAccountNumber=171234567890123}' \
    --incoming-key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/ivi5ksfsuplneuyt \
    --outgoing-key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/4pmyquwjs3yj4vwe \
    --outgoing-translation-attributes
 IsoFormat4="{PrimaryAccountNumber=171234567890123}" \
    --outgoing-dukpt-attributes KeySerialNumber="FFFF9876543210E00008"
```

Salida:

```
{
```

```
    "PinBlock": "1F4209C670E49F83E75CC72E81B787D9",
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ivi5ksfsuplneuyt
    "KeyCheckValue": "7CC9E2"
}
```

Para obtener más información, consulte Translate PIN data en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte TranslatePinData en la Referencia de comandos de la AWS CLI.

`verify-auth-request-cryptogram`

En el siguiente ejemplo de código, se muestra cómo utilizar `verify-auth-request-cryptogram`.

AWS CLI

Verificación de una solicitud de autenticación

El siguiente ejemplo de `verify-auth-request-cryptogram` verifica un criptograma de solicitud de autorización (ARQC).

```
aws payment-cryptography-data verify-auth-request-cryptogram \
    --auth-request-cryptogram F6E1BD1E6037FB3E \
    --auth-response-attributes '{"ArpcMethod1": {"AuthResponseCode": "1111"}}' \
    --key-identifier arn:aws:payment-cryptography:us-west-2:111122223333:key/
pboipdfzd4mdklya \
    --major-key-derivation-mode "EMV_OPTION_A" \
    --session-key-derivation-attributes '{"EmvCommon":
 {"ApplicationTransactionCounter": "1234","PanSequenceNumber":
 "01","PrimaryAccountNumber": "471234567890123"}}' \
    --transaction-data "123456789ABCDEF"
```

Salida:

```
{
    "AuthResponseValue": "D899B8C6FBF971AA",
    "KeyArn": "arn:aws:payment-cryptography:us-west-2:111122223333:key/
pboipdfzd4mdklya",
    "KeyCheckValue": "985792"
}
```

Para obtener más información, consulte Verify auth request (ARQC) cryptogram en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte VerifyAuthRequestCryptogram en la Referencia de comandos de la AWS CLI.

`verify-card-validation-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `verify-card-validation-data`.

AWS CLI

Validación de un CVV

En el ejemplo siguiente de `verify-card-validation-data`, se valida un CVV o CVV2 para un PAN.

```
aws payment-cryptography-data verify-card-validation-data \
    --key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi \
    --primary-account-number=171234567890123 \
    --verification-attributes CardVerificationValue2={CardExpiryDate=0123} \
    --validation-data 801
```

Salida:

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
tqv5yij6wtxx64pi",
    "KeyCheckValue": "CADDA1"
}
```

Para obtener más información, consulte Verify card data en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte VerifyCardValidationData en la Referencia de comandos de la AWS CLI.

`verify-mac`

En el siguiente ejemplo de código, se muestra cómo utilizar `verify-mac`.

AWS CLI

Verificación de un MAC

El siguiente ejemplo de `verify-mac` comprueba un código de autenticación de mensajes basado en hash (HMAC) para la autenticación de datos de tarjeta mediante el algoritmo HMAC_SHA256 y una clave de cifrado HMAC.

```
aws payment-cryptography-data verify-mac \
    --key-identifier arn:aws:payment-cryptography:us-east-2:111122223333:key/
qnobl5lghrzunce6 \
    --message-
data "3b343038383439303031303733393431353d323430383232363030303730303f33" \
    --verification-attributes='Algorithm=HMAC_SHA256' \
    --mac ED87F26E961C6D0DDB78DA5038AA2BDDEA0DCE03E5B5E96BDDD494F4A7AA470C
```

Salida:

```
{
    "KeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
qnobl5lghrzunce6,
    "KeyCheckValue": "2976E7",
}
```

Para obtener más información, consulte Verify MAC en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte VerifyMac en la Referencia de comandos de la AWS CLI.

`verify-pin-data`

En el siguiente ejemplo de código, se muestra cómo utilizar `verify-pin-data`.

AWS CLI

Comprobación de un PIN

En el siguiente ejemplo de `verify-pin-data`, se valida un PIN para un PAN.

```
aws payment-cryptography-data verify-pin-data \
```

```
    --verification-key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/37y2tsl45p5zjbh2 \
    --encryption-key-identifier arn:aws:payment-cryptography:us-
east-2:111122223333:key/ivi5ksfsuplneuyt \
    --primary-account-number 171234567890123 \
    --pin-block-format ISO_FORMAT_0 \
    --verification-attributes
 VisaPin="{PinVerificationKeyIndex=1,VerificationValue=5507}" \
    --encrypted-pin-block AC17DC148BDA645E
```

Salida:

```
{
    "VerificationKeyArn": "arn:aws:payment-cryptography:us-
east-2:111122223333:key/37y2tsl45p5zjbh2",
    "VerificationKeyCheckValue": "7F2363",
    "EncryptionKeyArn": "arn:aws:payment-cryptography:us-east-2:111122223333:key/
ivi5ksfsuplneuyt",
    "EncryptionKeyCheckValue": "7CC9E2",
}
```

Para obtener más información, consulte Verify PIN data en la Guía del usuario de AWS Payment Cryptography.

- Para ver los detalles de la API, consulte VerifyPinData en la Referencia de comandos de AWS CLI.

Ejemplos de Amazon Pinpoint que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon Pinpoint.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-app`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-app`.

AWS CLI

Ejemplo 1: Creación de una aplicación

En el siguiente ejemplo de `create-app` se crea una nueva aplicación (proyecto).

```
aws pinpoint create-app \
    --create-application-request Name=ExampleCorp
```

Salida:

```
{
    "ApplicationResponse": {
        "Arn": "arn:aws:mobiletargeting:us-
west-2:AIDACKCEVSQ6C2EXAMPLE:apps/810c7aab86d42fb2b56c8c966example",
        "Id": "810c7aab86d42fb2b56c8c966example",
        "Name": "ExampleCorp",
        "tags": {}
    }
}
```

Ejemplo 2: Creación de una aplicación etiquetada

En el siguiente ejemplo de `create-app` se crea una nueva aplicación (proyecto) y asocia una etiqueta (clave y valor) a la aplicación.

```
aws pinpoint create-app \
    --create-application-request Name=ExampleCorp,tags={"Stack"="Test"}
```

Salida:

```
{
    "ApplicationResponse": {
        "Arn": "arn:aws:mobiletargeting:us-
west-2:AIDACKCEVSQ6C2EXAMPLE:apps/810c7aab86d42fb2b56c8c966example",
```

```
        "Id": "810c7aab86d42fb2b56c8c966example",
        "Name": "ExampleCorp",
        "tags": {
            "Stack": "Test"
        }
    }
}
```

- Para ver los detalles de la API, consulte CreateApp en la Referencia de comandos de la AWS CLI.

`create-sms-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-sms-template`.

AWS CLI

Permite crear una plantilla de mensaje para los mensajes que se envían a través del canal de SMS

En el siguiente ejemplo de `create-sms-template`, se crea una plantilla de mensaje SMS.

```
aws pinpoint create-sms-template \
    --template-name TestTemplate \
    --sms-template-request file://myfile.json \
    --region us-east-1
```

Contenidos de `myfile.json`:

```
{
    "Body": "hello\n how are you?\n food is good",
    "TemplateDescription": "Test SMS Template"
}
```

Salida:

```
{
    "CreateTemplateMessageBody": {
        "Arn": "arn:aws:mobiletargeting:us-east-1:AIDACKCEVSQ6C2EXAMPLE:templates/
TestTemplate/SMS",
        "Message": "Created",
```

```
        "RequestID": "8c36b17f-a0b0-400f-ac21-29e9b62a975d"
    }
}
```

Para obtener más información, consulte Amazon Pinpoint message templates en la Guía del usuario de Amazon Pinpoint.

- Para ver los detalles de la API, consulte CreateSmsTemplate en la Referencia de comandos de la AWS CLI.

`delete-app`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-app`.

AWS CLI

Eliminación de una aplicación

En el siguiente ejemplo `delete-app` se elimina una aplicación (proyecto).

```
aws pinpoint delete-app \
    --application-id 810c7aab86d42fb2b56c8c966example
```

Salida:

```
{
    "ApplicationResponse": {
        "Arn": "arn:aws:mobiletargeting:us-
west-2:AIDACKCEVSQ6C2EXAMPLE:apps/810c7aab86d42fb2b56c8c966example",
        "Id": "810c7aab86d42fb2b56c8c966example",
        "Name": "ExampleCorp",
        "tags": {}
    }
}
```

- Para ver los detalles de la API, consulte DeleteApp en la Referencia de comandos de la AWS CLI.

`get-apns-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-apns-channel`.

AWS CLI

Recuperación de información sobre el estado y la configuración del canal de APN para una aplicación

En el siguiente ejemplo de `get-apns-channel` se recupera el estado y la configuración del canal de APN de una aplicación.

```
aws pinpoint get-apns-channel \
    --application-id 9ab1068eb0a6461c86cce7f27ce0efd7 \
    --region us-east-1
```

Salida:

```
{
    "APNSChannelResponse": {
        "ApplicationId": "9ab1068eb0a6461c86cce7f27ce0efd7",
        "CreationDate": "2019-05-09T21:54:45.082Z",
        "DefaultAuthenticationMethod": "CERTIFICATE",
        "Enabled": true,
        "HasCredential": true,
        "HasTokenKey": false,
        "Id": "apns",
        "IsArchived": false,
        "LastModifiedDate": "2019-05-09T22:04:01.067Z",
        "Platform": "APNS",
        "Version": 2
    }
}
```

- Para ver los detalles de la API, consulte GetApnsChannel en la Referencia de comandos de la AWS CLI.

`get-app`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-app`.

AWS CLI

Obtención de información sobre una aplicación (proyecto)

En el siguiente ejemplo de `get-app`, se recupera información sobre una aplicación (proyecto).

```
aws pinpoint get-app \
    --application-id 810c7aab86d42fb2b56c8c966example \
    --region us-east-1
```

Salida:

```
{
    "ApplicationResponse": {
        "Arn": "arn:aws:mobiletargeting:us-
east-1:AIDACKCEVSQ6C2EXAMPLE:apps/810c7aab86d42fb2b56c8c966example",
        "Id": "810c7aab86d42fb2b56c8c966example",
        "Name": "ExampleCorp",
        "tags": {
                "Year": "2019",
                "Stack": "Production"
            }
    }
}
```

- Para ver los detalles de la API, consulte GetApp en la Referencia de comandos de la AWS CLI.

`get-apps`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-apps`.

AWS CLI

Obtención de información sobre todas las aplicaciones

En el siguiente ejemplo de `get-apps`, se recupera información sobre todas las aplicaciones (proyectos).

```
aws pinpoint get-apps
```

Salida:

```
{
    "ApplicationsResponse": {
        "Item": [
            {
```

```
                "Arn": "arn:aws:mobiletargeting:us-
west-2:AIDACKCEVSQ6C2EXAMPLE:apps/810c7aab86d42fb2b56c8c966example",
                "Id": "810c7aab86d42fb2b56c8c966example",
                "Name": "ExampleCorp",
                "tags": {
                    "Year": "2019",
                    "Stack": "Production"
                }
            },
            {
                "Arn": "arn:aws:mobiletargeting:us-
west-2:AIDACKCEVSQ6C2EXAMPLE:apps/42d8c7eb0990a57ba1d5476a3example",
                "Id": "42d8c7eb0990a57ba1d5476a3example",
                "Name": "AnyCompany",
                "tags": {}
            },
            {
                "Arn": "arn:aws:mobiletargeting:us-
west-2:AIDACKCEVSQ6C2EXAMPLE:apps/80f5c382b638ffe5ad12376bbexample",
                "Id": "80f5c382b638ffe5ad12376bbexample",
                "Name": "ExampleCorp_Test",
                "tags": {
                    "Year": "2019",
                    "Stack": "Test"
                }
            }
        ],
        "NextToken":
 "eyJDcmVhdGlvbkRhdGUiOiIyMDE5LTA3LTE2VDE0OjM4OjUzLjkwM1oiLCJBY2NvdW50SWQiOiI1MTIzOTcxODM4Nz
    }
}
```

La presencia del valor de respuesta `NextToken` indica que hay más resultados disponibles. Vuelva a ejecutar el comando e introduzca ese valor como el parámetro de entrada `NextToken`.

- Para ver los detalles de la API, consulte GetApps en la Referencia de comandos de la AWS CLI.

`get-campaign`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-campaign`.

AWS CLI

Recuperación de información sobre el estado, la configuración y otros ajustes de una campaña

El siguiente ejemplo de `get-campaign` recupera información sobre el estado, la configuración y otros ajustes para una campaña.

```
aws pinpoint get-campaign \
    --application-id 6e0b7591a90841d2b5d93fa11143e5a7 \
    --campaign-id a1e63c6cc0eb43ed826ffcc3cc90b30d \
    --region us-east-1
```

Salida:

```
{
    "CampaignResponse": {
        "AdditionalTreatments": [],
        "ApplicationId": "6e0b7591a90841d2b5d93fa11143e5a7",
        "Arn": "arn:aws:mobiletargeting:us-
east-1:AIDACKCEVSQ6C2EXAMPLE:apps/6e0b7591a90841d2b5d93fa11143e5a7/campaigns/
a1e63c6cc0eb43ed826ffcc3cc90b30d",
        "CreationDate": "2019-10-08T18:40:16.581Z",
        "Description": " ",
        "HoldoutPercent": 0,
        "Id": "a1e63c6cc0eb43ed826ffcc3cc90b30d",
        "IsPaused": false,
        "LastModifiedDate": "2019-10-08T18:40:16.581Z",
        "Limits": {
            "Daily": 0,
            "MaximumDuration": 60,
            "MessagesPerSecond": 50,
            "Total": 0
        },
        "MessageConfiguration": {
            "EmailMessage": {
                "FromAddress": "sender@example.com",
                "HtmlBody": "<!DOCTYPE html>\n  <html lang=\"en\">\n    <head>\n
 <meta http-equiv=\"Content-Type\" content=\"text/html; charset=utf-8\" />\n</head>
\n<body>Hello</body>\n</html>",
                "Title": "PinpointDemo"
            }
        },
        "Name": "MyCampaign",
```

```
        "Schedule": {
            "IsLocalTime": false,
            "StartTime": "IMMEDIATE",
            "Timezone": "utc"
        },
        "SegmentId": "b66c9e42f71444b2aa2e0ffc1df28f60",
        "SegmentVersion": 1,
        "State": {
            "CampaignStatus": "COMPLETED"
        },
        "tags": {},
        "TemplateConfiguration": {},
        "Version": 1
    }
}
```

- Para ver los detalles de la API, consulte GetCampaign en la Referencia de comandos de la AWS CLI.

`get-campaigns`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-campaigns`.

AWS CLI

Recuperación de información sobre el estado, la configuración y otros ajustes para todas las campañas asociadas a una aplicación

El siguiente ejemplo de `get-campaigns` recupera información sobre el estado, la configuración y otros ajustes para todas las campañas que están asociadas a una aplicación.

```
aws pinpoint get-campaigns \
    --application-id 6e0b7591a90841d2b5d93fa11143e5a7 \
    --region us-east-1
```

Salida:

```
{
    "CampaignsResponse": {
        "Item": [
            {
                "AdditionalTreatments": [],
```

```
                "ApplicationId": "6e0b7591a90841d2b5d93fa11143e5a7",
                "Arn": "arn:aws:mobiletargeting:us-
east-1:AIDACKCEVSQ6C2EXAMPLE:apps/6e0b7591a90841d2b5d93fa11143e5a7/
campaigns/7e1280344c8f4a9aa40a00b006fe44f1",
                "CreationDate": "2019-10-08T18:40:22.905Z",
                "Description": " ",
                "HoldoutPercent": 0,
                "Id": "7e1280344c8f4a9aa40a00b006fe44f1",
                "IsPaused": false,
                "LastModifiedDate": "2019-10-08T18:40:22.905Z",
                "Limits": {},
                "MessageConfiguration": {
                    "EmailMessage": {
                        "FromAddress": "sender@example.com",
                        "HtmlBody": "<!DOCTYPE html>\n    <html lang=\"en
\">\n    <head>\n    <meta http-equiv=\"Content-Type\" content=\"text/html;
 charset=utf-8\" />\n</head>\n<body>Hello</body>\n</html>",
                        "Title": "PInpointDemo Test"
                    }
                },
                "Name": "MyCampaign1",
                "Schedule": {
                    "IsLocalTime": false,
                    "QuietTime": {},
                    "StartTime": "IMMEDIATE",
                    "Timezone": "UTC"
                },
                "SegmentId": "b66c9e42f71444b2aa2e0ffc1df28f60",
                "SegmentVersion": 1,
                "State": {
                    "CampaignStatus": "COMPLETED"
                },
                "tags": {},
                "TemplateConfiguration": {},
                "Version": 1
            },
            {
                "AdditionalTreatments": [],
                "ApplicationId": "6e0b7591a90841d2b5d93fa11143e5a7",
                "Arn": "arn:aws:mobiletargeting:us-
east-1:AIDACKCEVSQ6C2EXAMPLE:apps/6e0b7591a90841d2b5d93fa11143e5a7/campaigns/
a1e63c6cc0eb43ed826ffcc3cc90b30d",
                "CreationDate": "2019-10-08T18:40:16.581Z",
                "Description": " ",
```

```
                "HoldoutPercent": 0,
                "Id": "a1e63c6cc0eb43ed826ffcc3cc90b30d",
                "IsPaused": false,
                "LastModifiedDate": "2019-10-08T18:40:16.581Z",
                "Limits": {
                    "Daily": 0,
                    "MaximumDuration": 60,
                    "MessagesPerSecond": 50,
                    "Total": 0
                },
                "MessageConfiguration": {
                    "EmailMessage": {
                        "FromAddress": "sender@example.com",
                        "HtmlBody": "<!DOCTYPE html>\n    <html lang=\"en
\">\n    <head>\n    <meta http-equiv=\"Content-Type\" content=\"text/html;
 charset=utf-8\" />\n</head>\n<body>Demo</body>\n</html>",
                        "Title": "PinpointDemo"
                    }
                },
                "Name": "MyCampaign2",
                "Schedule": {
                    "IsLocalTime": false,
                    "StartTime": "IMMEDIATE",
                    "Timezone": "utc"
                },
                "SegmentId": "b66c9e42f71444b2aa2e0ffc1df28f60",
                "SegmentVersion": 1,
                "State": {
                    "CampaignStatus": "COMPLETED"
                },
                "tags": {},
                "TemplateConfiguration": {},
                "Version": 1
            }
        ]
    }
}
```


- Para ver los detalles de la API, consulte GetCampaigns en la Referencia de comandos de la AWS CLI.

`get-channels`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-channels`.

AWS CLI

Recuperación de información del historial y el estado de todos los canales de una aplicación

El siguiente ejemplo de `get-channels` recupera información sobre el historial y el estado de cada canal de una aplicación.

```
aws pinpoint get-channels \
    --application-id 6e0b7591a90841d2b5d93fa11143e5a7 \
    --region us-east-1
```

Salida:

```
{
    "ChannelsResponse": {
        "Channels": {
            "GCM": {
                "ApplicationId": "6e0b7591a90841d2b5d93fa11143e5a7",
                "CreationDate": "2019-10-08T18:28:23.182Z",
                "Enabled": true,
                "HasCredential": true,
                "Id": "gcm",
                "IsArchived": false,
                "LastModifiedDate": "2019-10-08T18:28:23.182Z",
                "Version": 1
            },
            "SMS": {
                "ApplicationId": "6e0b7591a90841d2b5d93fa11143e5a7",
                "CreationDate": "2019-10-08T18:39:18.511Z",
                "Enabled": true,
                "Id": "sms",
                "IsArchived": false,
                "LastModifiedDate": "2019-10-08T18:39:18.511Z",
                "Version": 1
            },
            "EMAIL": {
                "ApplicationId": "6e0b7591a90841d2b5d93fa11143e5a7",
                "CreationDate": "2019-10-08T18:27:23.990Z",
                "Enabled": true,
```

```
                "Id": "email",
                "IsArchived": false,
                "LastModifiedDate": "2019-10-08T18:27:23.990Z",
                "Version": 1
            },
            "IN_APP": {
                "Enabled": true,
                "IsArchived": false,
                "Version": 0
            }
        }
    }
}
```

- Para ver los detalles de la API, consulte GetChannels en la Referencia de comandos de la AWS CLI.

`get-email-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-email-channel`.

AWS CLI

Recuperación de información sobre el estado y la configuración del canal de correo electrónico para una aplicación

En el siguiente ejemplo de `get-email-channel`, se recupera el estado y la configuración del canal de correo electrónico para una aplicación.

```
aws pinpoint get-email-channel \
    --application-id 6e0b7591a90841d2b5d93fa11143e5a7 \
    --region us-east-1
```

Salida:

```
{
    "EmailChannelResponse": {
        "ApplicationId": "6e0b7591a90841d2b5d93fa11143e5a7",
        "CreationDate": "2019-10-08T18:27:23.990Z",
        "Enabled": true,
        "FromAddress": "sender@example.com",
        "Id": "email",
```

```
        "Identity": "arn:aws:ses:us-east-1:AIDACKCEVSQ6C2EXAMPLE:identity/
sender@example.com",
        "IsArchived": false,
        "LastModifiedDate": "2019-10-08T18:27:23.990Z",
        "MessagesPerSecond": 1,
        "Platform": "EMAIL",
        "RoleArn": "arn:aws:iam::AIDACKCEVSQ6C2EXAMPLE:role/pinpoint-events",
        "Version": 1
    }
}
```

- Para ver los detalles de la API, consulte GetEmailChannel en la Referencia de comandos de la AWS CLI.

`get-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-endpoint`.

AWS CLI

Recuperación de información sobre la configuración y los atributos de un punto de conexión específico de una aplicación

En el siguiente ejemplo `get-endpoint` se recupera información sobre la configuración y los atributos de un punto de conexión específico de una aplicación.

```
aws pinpoint get-endpoint \
    --application-id 611e3e3cdd47474c9c1399a505665b91 \
    --endpoint-id testendpoint \
    --region us-east-1
```

Salida:

```
{
    "EndpointResponse": {
        "Address": "+11234567890",
        "ApplicationId": "611e3e3cdd47474c9c1399a505665b91",
        "Attributes": {},
        "ChannelType": "SMS",
        "CohortId": "63",
        "CreationDate": "2019-01-28T23:55:11.534Z",
```

```
        "EffectiveDate": "2021-08-06T00:04:51.763Z",
        "EndpointStatus": "ACTIVE",
        "Id": "testendpoint",
        "Location": {
            "Country": "USA"
        },
        "Metrics": {
            "SmsDelivered": 1.0
        },
        "OptOut": "ALL",
        "RequestId": "a204b1f2-7e26-48a7-9c80-b49a2143489d",
        "User": {
            "UserAttributes": {
                "Age": [
                    "24"
                ]
            },
        "UserId": "testuser"
        }
    }
}
```

- Para ver los detalles de la API, consulte GetEndpoint en la Referencia de comandos de la AWS CLI.

`get-gcm-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-gcm-channel`.

AWS CLI

Recuperación de información sobre el estado y la configuración del canal GCM para una aplicación

En el siguiente ejemplo de `get-gcm-channel`, se recupera información sobre el estado y la configuración del canal GCM para una aplicación.

```
aws pinpoint get-gcm-channel \
    --application-id 6e0b7591a90841d2b5d93fa11143e5a7 \
    --region us-east-1
```

Salida:

```
{
    "GCMChannelResponse": {
        "ApplicationId": "6e0b7591a90841d2b5d93fa11143e5a7",
        "CreationDate": "2019-10-08T18:28:23.182Z",
        "Enabled": true,
        "HasCredential": true,
        "Id": "gcm",
        "IsArchived": false,
        "LastModifiedDate": "2019-10-08T18:28:23.182Z",
        "Platform": "GCM",
        "Version": 1
    }
}
```

- Para ver los detalles de la API, consulte GetGcmChannel en la Referencia de comandos de la AWS CLI.

`get-sms-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-sms-channel`.

AWS CLI

Recuperación de información sobre el estado y la configuración del canal de SMS para una aplicación

En el siguiente ejemplo de `get-sms-channel` se recupera el estado y la configuración del canal de SMS de una aplicación.

```
aws pinpoint get-sms-channel \
    --application-id 6e0b7591a90841d2b5d93fa11143e5a7 \
    --region us-east-1
```

Salida:

```
{
    "SMSChannelResponse": {
        "ApplicationId": "6e0b7591a90841d2b5d93fa11143e5a7",
        "CreationDate": "2019-10-08T18:39:18.511Z",
        "Enabled": true,
        "Id": "sms",
```

```
        "IsArchived": false,
        "LastModifiedDate": "2019-10-08T18:39:18.511Z",
        "Platform": "SMS",
        "PromotionalMessagesPerSecond": 20,
        "TransactionalMessagesPerSecond": 20,
        "Version": 1
    }
}
```

- Para ver los detalles de la API, consulte GetSmsChannel en la Referencia de comandos de la AWS CLI.

`get-sms-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-sms-template`.

AWS CLI

Recupera el contenido y la configuración de una plantilla de mensaje para los mensajes que se envían a través del canal de SMS

El siguiente ejemplo de `get-sms-template` recupera el contenido y la configuración de una plantilla de mensaje SMS.

```
aws pinpoint get-sms-template \
    --template-name TestTemplate \
    --region us-east-1
```

Salida:

```
{
    "SMSTemplateResponse": {
        "Arn": "arn:aws:mobiletargeting:us-east-1:AIDACKCEVSQ6C2EXAMPLE:templates/
TestTemplate/SMS",
        "Body": "hello\n how are you?\n food is good",
        "CreationDate": "2023-06-20T21:37:30.124Z",
        "LastModifiedDate": "2023-06-20T21:37:30.124Z",
        "tags": {},
        "TemplateDescription": "Test SMS Template",
        "TemplateName": "TestTemplate",
        "TemplateType": "SMS",
        "Version": "1"
```

```
    }
}
```

Para obtener más información, consulte Amazon Pinpoint message templates en la Guía del usuario de Amazon Pinpoint.

- Para ver los detalles de la API, consulte GetSmsTemplate en la Referencia de comandos de la AWS CLI.

`get-voice-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-voice-channel`.

AWS CLI

Recuperación de información sobre el estado y la configuración del canal de voz para una aplicación

El siguiente ejemplo de `get-voice-channel` recupera el estado y la configuración del canal de voz de una aplicación.

```
aws pinpoint get-voice-channel \
    --application-id 6e0b7591a90841d2b5d93fa11143e5a7 \
    --region us-east-1
```

Salida:

```
{
    "VoiceChannelResponse": {
        "ApplicationId": "6e0b7591a90841d2b5d93fa11143e5a7",
        "CreationDate": "2022-04-28T00:17:03.836Z",
        "Enabled": true,
        "Id": "voice",
        "IsArchived": false,
        "LastModifiedDate": "2022-04-28T00:17:03.836Z",
        "Platform": "VOICE",
        "Version": 1
    }
}
```

- Para ver los detalles de la API, consulte GetVoiceChannel en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Pare recuperar una lista de etiquetas para un recurso

El siguiente ejemplo de `list-tags-for-resource` recupera todas las etiquetas (nombres y valores clave) asociadas al recurso especificado.

```
aws pinpoint list-tags-for-resource \
    --resource-arn arn:aws:mobiletargeting:us-
west-2:AIDACKCEVSQ6C2EXAMPLE:apps/810c7aab86d42fb2b56c8c966example
```

Salida:

```
{
    "TagsModel": {
        "tags": {
            "Year": "2019",
            "Stack": "Production"
        }
    }
}
```

Para obtener más información, consulte Etiquetado de los recursos de Amazon Pinpoint <https://docs.aws.amazon.com/pinpoint/latest/developerguide/tagging-resources.html>__ en la Guía para desarrolladores de Amazon Pinpoint.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`phone-number-validate`

En el siguiente ejemplo de código, se muestra cómo utilizar `phone-number-validate`.

AWS CLI

Recupera información sobre un número de teléfono

El siguiente `phone-number-validate` recupera información sobre un número de teléfono.

```
aws pinpoint phone-number-validate \
    --number-validate-request PhoneNumber="+12065550142" \
    --region us-east-1
```

Salida:

```
{
    "NumberValidateResponse": {
        "Carrier": "ExampleCorp Mobile",
        "City": "Seattle",
        "CleansedPhoneNumberE164": "+12065550142",
        "CleansedPhoneNumberNational": "2065550142",
        "Country": "United States",
        "CountryCodeIso2": "US",
        "CountryCodeNumeric": "1",
        "OriginalPhoneNumber": "+12065550142",
        "PhoneType": "MOBILE",
        "PhoneTypeCode": 0,
        "Timezone": "America/Los_Angeles",
        "ZipCode": "98101"
    }
}
```

Para obtener más información, consulte Canal de SMS de Amazon Pinpoint en la Guía del usuario de Amazon Pinpoint.

- Para ver los detalles de la API, consulte PhoneNumberValidate en la Referencia de comandos de la AWS CLI.

`send-messages`

En el siguiente ejemplo de código, se muestra cómo utilizar `send-messages`.

AWS CLI

Envío de un mensaje SMS mediante el punto de conexión de una aplicación

En el siguiente ejemplo de `send-messages` se envía un mensaje directo a una aplicación con un punto de conexión.

```
aws pinpoint send-messages \
    --application-id 611e3e3cdd47474c9c1399a505665b91 \
    --message-request file://myfile.json \
    --region us-west-2
```

Contenidos de `myfile.json`:

```
{
    "MessageConfiguration": {
        "SMSMessage": {
            "Body": "hello, how are you?"
        }
    },
    "Endpoints": {
        "testendpoint": {}
    }
}
```

Salida:

```
{
    "MessageResponse": {
        "ApplicationId": "611e3e3cdd47474c9c1399a505665b91",
        "EndpointResult": {
            "testendpoint": {
                "Address": "+12345678900",
                "DeliveryStatus": "SUCCESSFUL",
                "MessageId": "itnuqhai5alf1n6ahv3udc05n7hhddr6gb3lq6g0",
                "StatusCode": 200,
                "StatusMessage": "MessageId:
 itnuqhai5alf1n6ahv3udc05n7hhddr6gb3lq6g0"
            }
        },
        "RequestId": "c7e23264-04b2-4a46-b800-d24923f74753"
    }
}
```

Para obtener más información, consulte Canal de SMS de Amazon Pinpoint en la Guía del usuario de Amazon Pinpoint.

- Para ver los detalles de la API, consulte SendMessages en la Referencia de comandos de la AWS CLI.

`send-users-messages`

En el siguiente ejemplo de código, se muestra cómo utilizar `send-users-messages`.

AWS CLI

Envío de mensaje SMS a un usuario de una aplicación

El siguiente ejemplo de `send-users-messages` envía un mensaje directo a un usuario de una aplicación.

```
aws pinpoint send-users-messages \
    --application-id 611e3e3cdd47474c9c1399a505665b91 \
    --send-users-message-request file://myfile.json \
    --region us-west-2
```

Contenidos de `myfile.json`:

```
{
    "MessageConfiguration": {
        "SMSMessage": {
            "Body": "hello, how are you?"
        }
    },
    "Users": {
        "testuser": {}
    }
}
```

Salida:

```
{
    "SendUsersMessageResponse": {
        "ApplicationId": "611e3e3cdd47474c9c1399a505665b91",
        "RequestId": "e0b12cf5-2359-11e9-bb0b-d5fb91876b25",
        "Result": {
            "testuser": {
                "testuserendpoint": {
                    "DeliveryStatus": "SUCCESSFUL",
                    "MessageId": "7qu4hk5bqhda3i7i2n4pjf98qcuh8b7p45ifsmo0",
                    "StatusCode": 200,
```

```
                    "StatusMessage": "MessageId:
 7qu4hk5bqhda3i7i2n4pjf98qcuh8b7p45ifsmo0",
                    "Address": "+12345678900"
                }
            }
        }
    }
}
```

Para obtener más información, consulte Canal de SMS de Amazon Pinpoint en la Guía del usuario de Amazon Pinpoint.

- Para ver los detalles de la API, consulte SendUsersMessages en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para agregar etiquetas a un recurso

En el siguiente ejemplo, se agregan dos etiquetas (nombres y valores clave) a un recurso.

```
aws pinpoint list-tags-for-resource \
    --resource-arn arn:aws:mobiletargeting:us-
east-1:AIDACKCEVSQ6C2EXAMPLE:apps/810c7aab86d42fb2b56c8c966example \
    --tags-model tags={Stack=Production,Year=2019}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de los recursos de Amazon Pinpoint <https://docs.aws.amazon.com/pinpoint/latest/developerguide/tagging-resources.html>__ en la Guía para desarrolladores de Amazon Pinpoint.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Ejemplo 1: cómo eliminar una etiqueta de un recurso

El siguiente ejemplo de `untag-resource` elimina la etiqueta especificada (nombre y valor de clave) de un recurso.

```
aws pinpoint untag-resource \
    --resource-arn arn:aws:mobiletargeting:us-
west-2:AIDACKCEVSQ6C2EXAMPLE:apps/810c7aab86d42fb2b56c8c966example \
    --tag-keys Year
```

Este comando no genera ninguna salida.

Ejemplo 2: eliminar varias etiquetas de un recurso

El siguiente ejemplo de `untag-resource` elimina las etiquetas especificadas (nombres y valores de clave) de un recurso.

```
aws pinpoint untag-resource \
    --resource-arn arn:aws:mobiletargeting:us-
east-1:AIDACKCEVSQ6C2EXAMPLE:apps/810c7aab86d42fb2b56c8c966example \
    --tag-keys Year Stack
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de los recursos de Amazon Pinpoint <https://docs.aws.amazon.com/pinpoint/latest/developerguide/tagging-resources.html>__ en la Guía para desarrolladores de Amazon Pinpoint.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-sms-channel`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-sms-channel`.

AWS CLI

Habilitación de un canal de SMS o actualización del estado y la configuración del canal de SMS para una aplicación.

El siguiente ejemplo de `update-sms-channel` habilita un canal de SMS para un canal de SMS de una aplicación.

```
aws pinpoint update-sms-channel \
    --application-id 611e3e3cdd47474c9c1399a505665b91 \
    --sms-channel-request Enabled=true \
    --region us-west-2
```

Salida:

```
{
    "SMSChannelResponse": {
        "ApplicationId": "611e3e3cdd47474c9c1399a505665b91",
        "CreationDate": "2019-01-28T23:25:25.224Z",
        "Enabled": true,
        "Id": "sms",
        "IsArchived": false,
        "LastModifiedDate": "2023-05-18T23:22:50.977Z",
        "Platform": "SMS",
        "PromotionalMessagesPerSecond": 20,
        "TransactionalMessagesPerSecond": 20,
        "Version": 3
    }
}
```

Para obtener más información, consulte Canal de SMS de Amazon Pinpoint en la Guía del usuario de Amazon Pinpoint.

- Para ver los detalles de la API, consulte UpdateSmsChannel en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon Polly que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon Polly.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`delete-lexicon`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-lexicon`.

AWS CLI

Eliminación de un lexicón

En el siguiente ejemplo de `delete-lexicon` se elimina el lexicón especificado.

```
aws polly delete-lexicon \
    --name w3c
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de la operación DeleteLexicon en la Guía para desarrolladores de Amazon Polly.

- Para obtener información sobre la API, consulte DeleteLexicon en la Referencia de comandos de la AWS CLI.

`get-lexicon`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-lexicon`.

AWS CLI

Recuperación del contenido de un léxico

En el siguiente ejemplo de `get-lexicon` se recupera el contenido del lexicón de pronunciación especificado.

```
aws polly get-lexicon \
```

```
    --name w3c
```

Salida:

```
{
    "Lexicon": {
        "Content": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n<lexicon version=
\"1.0\" \n      xmlns=    \"http://www.w3.org/2005/01/pronunciation-lexicon
\"\n      xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\" \n
 xsi:schemaLocation=\"http://www.w3.org/2005/01/pronunciation-lexicon \n
 http://www.w3.org/TR/2007/CR-pronunciation-    lexicon-20071212/pls.xsd\"\n
   alphabet=\"ipa\" \n      xml:lang=\"en-US\">\n  <lexeme>\n    <grapheme>W3C</
grapheme>\n        <alias>World Wide Web Consortium</alias>\n  </lexeme>\n</lexicon>
\n",
        "Name": "w3c"
    },
    "LexiconAttributes": {
        "Alphabet": "ipa",
        "LanguageCode": "en-US",
        "LastModified": 1603908910.99,
        "LexiconArn": "arn:aws:polly:us-west-2:880185128111:lexicon/w3c",
        "LexemesCount": 1,
        "Size": 492
    }
}
```

Para obtener más información, consulte Uso de la operación GetLexicon en la Guía para desarrolladores de Amazon Polly.

- Para obtener información sobre la API, consulte GetLexicon en la Referencia de comandos de la AWS CLI.

`get-speech-synthesis-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-speech-synthesis-task`.

AWS CLI

Obtención de información sobre una tarea de síntesis de voz

En el siguiente ejemplo de `get-speech-synthesis-task` se recupera información sobre la tarea de síntesis de voz especificada.

```
aws polly get-speech-synthesis-task \
    --task-id 70b61c0f-57ce-4715-a247-cae8729dcce9
```

Salida:

```
{
    "SynthesisTask": {
        "TaskId": "70b61c0f-57ce-4715-a247-cae8729dcce9",
        "TaskStatus": "completed",
        "OutputUri": "https://s3.us-west-2.amazonaws.com/amzn-s3-demo-
bucket/70b61c0f-57ce-4715-a247-cae8729dcce9.mp3",
        "CreationTime": 1603911042.689,
        "RequestCharacters": 1311,
        "OutputFormat": "mp3",
        "TextType": "text",
        "VoiceId": "Joanna"
    }
}
```

Para obtener más información, consulte Creación de archivos de audio largos en la Guía para desarrolladores de Amazon Polly.

- Para obtener información sobre la API, consulte GetSpeechSynthesisTask en la Referencia de comandos de la AWS CLI.

`list-lexicons`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-lexicons`.

AWS CLI

Creación de una lista de léxicos

En el siguiente ejemplo de `list-lexicons` se enumeran sus léxicos de pronunciación.

```
aws polly list-lexicons
```

Salida:

```
{
```

```
    "Lexicons": [
        {
            "Name": "w3c",
            "Attributes": {
                "Alphabet": "ipa",
                "LanguageCode": "en-US",
                "LastModified": 1603908910.99,
                "LexiconArn": "arn:aws:polly:us-east-2:123456789012:lexicon/w3c",
                "LexemesCount": 1,
                "Size": 492
            }
        }
    ]
}
```

Para obtener más información, consulte Uso de la operación ListLexicons en la Guía para desarrolladores de Amazon Polly.

- Para obtener información sobre la API, consulte ListLexicons en la Referencia de comandos de la AWS CLI.

`list-speech-synthesis-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-speech-synthesis-tasks`.

AWS CLI

Para enumerar sus tareas de síntesis de voz

En el siguiente ejemplo de `list-speech-synthesis-tasks`, se enumeran las tareas de síntesis de voz.

```
aws polly list-speech-synthesis-tasks
```

Salida:

```
{
    "SynthesisTasks": [
        {
            "TaskId": "70b61c0f-57ce-4715-a247-cae8729dcce9",
            "TaskStatus": "completed",
```

```
            "OutputUri": "https://s3.us-west-2.amazonaws.com/amzn-s3-demo-
bucket/70b61c0f-57ce-4715-a247-cae8729dcce9.mp3",
            "CreationTime": 1603911042.689,
            "RequestCharacters": 1311,
            "OutputFormat": "mp3",
            "TextType": "text",
            "VoiceId": "Joanna"
        }
    ]
}
```

Para obtener más información, consulte Creación de archivos de audio largos en la Guía para desarrolladores de Amazon Polly.

- Para obtener información sobre la API, consulte ListSpeechSynthesisTasks en la Referencia de comandos de la AWS CLI.

`put-lexicon`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-lexicon`.

AWS CLI

Almacenamiento de un léxico

En el siguiente ejemplo de `put-lexicon` se almacena el léxico de pronunciación especificado. El archivo `example.pls` especifica un léxico compatible con PLS de W3C.

```
aws polly put-lexicon \
    --name w3c \
    --content file://example.pls
```

Contenido de `example.pls`

```
{
    <?xml version="1.0" encoding="UTF-8"?>
    <lexicon version="1.0"
        xmlns="http://www.w3.org/2005/01/pronunciation-lexicon"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://www.w3.org/2005/01/pronunciation-lexicon
            http://www.w3.org/TR/2007/CR-pronunciation-lexicon-20071212/pls.xsd"
        alphabet="ipa"
```

```
        xml:lang="en-US">
        <lexeme>
            <grapheme>W3C</grapheme>
            <alias>World Wide Web Consortium</alias>
        </lexeme>
    </lexicon>
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de la operación PutLexicon en la Guía para desarrolladores de Amazon Polly.

- Para obtener información sobre la API, consulte PutLexicon en la Referencia de comandos de la AWS CLI.

`start-speech-synthesis-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-speech-synthesis-task`.

AWS CLI

Sintetización de texto

En el siguiente ejemplo de `start-speech-synthesis-task` se sintetiza el texto en `text_file.txt` y almacena el archivo MP3 resultante en el bucket especificado.

```
aws polly start-speech-synthesis-task \
    --output-format mp3 \
    --output-s3-bucket-name amzn-s3-demo-bucket \
    --text  file://text_file.txt \
    --voice-id Joanna
```

Salida:

```
{
    "SynthesisTask": {
        "TaskId": "70b61c0f-57ce-4715-a247-cae8729dcce9",
        "TaskStatus": "scheduled",
        "OutputUri": "https://s3.us-east-2.amazonaws.com/amzn-s3-demo-
bucket/70b61c0f-57ce-4715-a247-cae8729dcce9.mp3",
```

```
        "CreationTime": 1603911042.689,
        "RequestCharacters": 1311,
        "OutputFormat": "mp3",
        "TextType": "text",
        "VoiceId": "Joanna"
    }
}
```

Para obtener más información, consulte Creación de archivos de audio largos en la Guía para desarrolladores de Amazon Polly.

- Para obtener información sobre la API, consulte StartSpeechSynthesisTask en la Referencia de comandos de la AWS CLI.

Lista de precios de AWS Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Lista de precios de AWS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`describe-services`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-services`.

AWS CLI

Para recuperar los metadatos del servicio

En este ejemplo, se recuperan los metadatos del código de servicio de Amazon EC2.

Comando:

```
aws pricing describe-services --service-code AmazonEC2 --format-version aws_v1 --
max-items 1
```

Salida:


```
{
  "Services": [
      {
          "ServiceCode": "AmazonEC2",
          "AttributeNames": [
              "volumeType",
              "maxIopsvolume",
              "instance",
              "instanceCapacity10xlarge",
              "locationType",
              "instanceFamily",
              "operatingSystem",
              "clockSpeed",
              "LeaseContractLength",
              "ecu",
              "networkPerformance",
              "instanceCapacity8xlarge",
              "group",
              "maxThroughputvolume",
              "gpuMemory",
              "ebsOptimized",
              "elasticGpuType",
              "maxVolumeSize",
              "gpu",
              "processorFeatures",
              "intelAvxAvailable",
              "instanceCapacity4xlarge",
              "servicecode",
              "groupDescription",
              "processorArchitecture",
              "physicalCores",
              "productFamily",
              "enhancedNetworkingSupported",
              "intelTurboAvailable",
              "memory",
              "dedicatedEbsThroughput",
```

```
                "vcpu",
                "OfferingClass",
                "instanceCapacityLarge",
                "capacitystatus",
                "termType",
                "storage",
                "intelAvx2Available",
                "storageMedia",
                "physicalProcessor",
                "provisioned",
                "servicename",
                "PurchaseOption",
                "instanceCapacity18xlarge",
                "instanceType",
                "tenancy",
                "usagetype",
                "normalizationSizeFactor",
                "instanceCapacity2xlarge",
                "instanceCapacity16xlarge",
                "maxIopsBurstPerformance",
                "instanceCapacity12xlarge",
                "instanceCapacity32xlarge",
                "instanceCapacityXlarge",
                "licenseModel",
                "currentGeneration",
                "preInstalledSw",
                "location",
                "instanceCapacity24xlarge",
                "instanceCapacity9xlarge",
                "instanceCapacityMedium",
                "operation"
            ]
        }
    ],
    "FormatVersion": "aws_v1"
}
```

- Para obtener información sobre la API, consulte DescribeServices en la Referencia de comandos de la AWS CLI.

`get-attribute-values`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-attribute-values`.

AWS CLI

Para recuperar una lista de valores de atributos

El siguiente ejemplo de `get-attribute-values` recupera una lista de valores disponibles para el atributo dado.

```
aws pricing get-attribute-values \
    --service-code AmazonEC2 \
    --attribute-name volumeType \
    --max-items 2
```

Salida:

```
{
    "NextToken": "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAyfQ==",
    "AttributeValues": [
        {
            "Value": "Cold HDD"
        },
        {
            "Value": "General Purpose"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetAttributeValues en la Referencia de comandos de la AWS CLI.

`get-products`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-products`.

AWS CLI

Para recuperar una lista de productos

En este ejemplo, se recupera una lista de productos que cumplen con los criterios indicados.

Comando:

```
aws pricing get-products --filters file://filters.json --format-version aws_v1 --
max-results 1 --service-code AmazonEC2
```

filters.json:

```
        [
  {
    "Type": "TERM_MATCH",
    "Field": "ServiceCode",
    "Value": "AmazonEC2"
  },
  {
    "Type": "TERM_MATCH",
    "Field": "volumeType",
    "Value": "Provisioned IOPS"
  }
]
```

Salida:

```
{
  "FormatVersion": "aws_v1",
  "NextToken": "WGDY7ko8fQXdlaUZVdasFQ==:RVSagyIFn770XQOzdUIcO9BY6ucBG9itXAZGZF/
zioUzOsUKh6PCcPWaOyPZRiMePb986TeoKYB9l55fw/
CyoMq5ymnGmT1Vj39TljbbAlhcqnVfTmPIilx8Uy5bdDaBYy/e/2Ofw9Edzsykbs8LTBuNbiDQ
+BBds5yeI9AQkUepruKk3aEahFPxJ55kx/zk",
  "PriceList": [
      "{\"product\":{\"productFamily\":\"Storage\",\"attributes\":{\"storageMedia\":
\"SSD-backed\",\"maxThroughputvolume\":\"320 MB/sec\",\"volumeType\":\"Provisioned
 IOPS\",\"maxIopsvolume\":\"20000\",\"servicecode\":\"AmazonEC2\",\"usagetype
\":\"APS1-EBS:VolumeUsage.piops\",\"locationType\":\"AWS Region\",\"location\":
\"Asia Pacific (Singapore)\",\"servicename\":\"Amazon Elastic Compute Cloud\",
\"maxVolumeSize\":\"16 TiB\",\"operation\":\"\"},\"sku\":\"3MKHN58N7RDDVGKJ\"},
\"serviceCode\":\"AmazonEC2\",\"terms\":{\"OnDemand\":{\"3MKHN58N7RDDVGKJ.JRTCKXETXF
\":{\"priceDimensions\":{\"3MKHN58N7RDDVGKJ.JRTCKXETXF.6YS6EN2CT7\":{\"unit\":\"GB-
Mo\",\"endRange\":\"Inf\",\"description\":\"$0.138 per GB-month of Provisioned
 IOPS SSD (io1)  provisioned storage - Asia Pacific (Singapore)\",\"appliesTo
\":[],\"rateCode\":\"3MKHN58N7RDDVGKJ.JRTCKXETXF.6YS6EN2CT7\",\"beginRange\":
\"0\",\"pricePerUnit\":{\"USD\":\"0.1380000000\"}}},\"sku\":\"3MKHN58N7RDDVGKJ
\",\"effectiveDate\":\"2018-08-01T00:00:00Z\",\"offerTermCode\":\"JRTCKXETXF
\",\"termAttributes\":{}}}},\"version\":\"20180808005701\",\"publicationDate\":
\"2018-08-08T00:57:01Z\"}"
```

```
  ]
}
```

- Para obtener información sobre la API, consulte GetProducts en la Referencia de comandos de la AWS CLI.

AWS Private CA Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS Private CA.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-certificate-authority-audit-report`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-certificate-authority-audit-report`.

AWS CLI

Creación de un informe de auditoría de una entidad de certificación

Con el siguiente comando `create-certificate-authority-audit-report`, se crea un informe de auditoría para la entidad de certificación privada por el ARN.

```
aws acm-pca create-certificate-authority-audit-report --certificate-
authority-arn arn:aws:acm-pca:us-east-1:accountid:certificate-
authority/12345678-1234-1234-1234-123456789012 --s3-bucket-name your-bucket-name --
audit-report-response-format JSON
```

- Para obtener información sobre la API, consulte CreateCertificateAuthorityAuditReport en la Referencia de comandos de la AWS CLI.

`create-certificate-authority`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-certificate-authority`.

AWS CLI

Creación de una entidad de certificación privada

Con el siguiente comando `create-certificate-authority`, se crea una entidad de certificación privada en la cuenta de AWS.

```
aws acm-pca create-certificate-authority --certificate-authority-configuration
 file://C:\ca_config.txt --revocation-configuration file://C:\revoke_config.txt --
certificate-authority-type "SUBORDINATE" --idempotency-token 98256344
```

- Para obtener información sobre la API, consulte CreateCertificateAuthority en la Referencia de comandos de la AWS CLI.

`delete-certificate-authority`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-certificate-authority`.

AWS CLI

Eliminación de una entidad de certificación privada

Con el siguiente comando `delete-certificate-authority`, se elimina la entidad de certificación identificada por el ARN.

```
aws acm-pca delete-certificate-authority --certificate-
authority-arn arn:aws:acm-pca:us-west-2:123456789012:certificate-
authority/12345678-1234-1234-1234-123456789012
```

- Para obtener información sobre la API, consulte DeleteCertificateAuthority en la Referencia de comandos de la AWS CLI.

`describe-certificate-authority-audit-report`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-certificate-authority-audit-report`.

AWS CLI

Descripción de un informe de auditoría de una entidad de certificación

Con el siguiente comando `describe-certificate-authority-audit-report`, se muestra información sobre el informe de auditoría especificado para la entidad de certificación identificada por el ARN.

```
aws acm-pca describe-certificate-authority-audit-report --certificate-
authority-arn arn:aws:acm-pca:us-west-2:123456789012:certificate-
authority/99999999-8888-7777-6666-555555555555 --audit-report-
id 11111111-2222-3333-4444-555555555555
```

- Para obtener información sobre la API, consulte DescribeCertificateAuthorityAuditReport en la Referencia de comandos de la AWS CLI.

`describe-certificate-authority`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-certificate-authority`.

AWS CLI

Descripción de una entidad de certificación privada

Con el siguiente comando `describe-certificate-authority`, se muestra información sobre la entidad de certificación privada identificada por el ARN.

```
aws acm-pca describe-certificate-authority --certificate-
authority-arn arn:aws:acm-pca:us-west-2:123456789012:certificate-
authority/12345678-1234-1234-1234-123456789012
```

- Para obtener información sobre la API, consulte DescribeCertificateAuthority en la Referencia de comandos de la AWS CLI.

`get-certificate-authority-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-certificate-authority-certificate`.

AWS CLI

Recuperación del certificado de una entidad de certificación (CA)

Con el siguiente comando `get-certificate-authority-certificate`, se recupera el certificado y la cadena de certificados de la entidad de certificación privada especificada por el ARN:

```
aws acm-pca get-certificate-authority-certificate --certificate-
authority-arn arn:aws:acm-pca:us-west-2:123456789012:certificate-
authority/12345678-1234-1234-1234-123456789012 --output text
```

- Para obtener información sobre la API, consulte GetCertificateAuthorityCertificate en la Referencia de comandos de la AWS CLI.

`get-certificate-authority-csr`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-certificate-authority-csr`.

AWS CLI

Recuperación de la solicitud de firma del certificado de una entidad de certificación

Con el siguiente comando `get-certificate-authority-csr`, se recupera el CSR de la entidad de certificación privada especificada por el ARN:

```
aws acm-pca get-certificate-authority-csr --certificate-
authority-arn arn:aws:acm-pca:us-west-2:123456789012:certificate-
authority/12345678-1234-1234-1234-123456789012 --output text
```

- Para obtener información sobre la API, consulte GetCertificateAuthorityCsr en la Referencia de comandos de la AWS CLI.

`get-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-certificate`.

AWS CLI

Recuperación de un certificado emitido

En el siguiente ejemplo de `get-certificate`, se recupera un certificado de la entidad de certificación privada especificada.

```
aws acm-pca get-certificate \
    --certificate-authority-arn arn:aws:acm-pca:us-west-2:123456789012:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --certificate-arn arn:aws:acm-pca:us-west-2:123456789012:certificate-authority/12345678-1234-1234-1234-123456789012/certificate/6707447683a9b7f4055627ffd55cebcc \
    --output text
```

Salida:

```
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIRAJuJ8f6ZVYL7gG/rS3qvrZMwDQYJKoZIhvcNAQELBQAw
cTELMAkGA1UEBhMCVVMxEzARBgNVBAgMCldhc2hpbmd0b24xEDAOBgNVBAcMB1Nl
    ....certificate body truncated for brevity....
tKCSglgZZrd4FdLw1EkGm+UVXnodwMtJEQyy3oTfZjURPIyyaqskTu/KSS7YDjK0
KQNy73D6LtmdOEbAyq10XiDxqY41lvKHJ1eZrPaBmYNABxU=
-----END CERTIFICATE---- -----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIRAOskdzLvcj1eShkoyEE693AwDQYJKoZIhvcNAQELBQAw
cTELMAkGA1UEBhMCVVMxEzARBgNVBAgMCldhc2hpbmd0b24xEDAOBgNVBAcMB1Nl
    ...certificate body truncated for brevity....
kdRGB6P2hpxstDOUIwAoCbhoaWwfA4ybJznf+jOQhAziNlRdKQRR8nODWpKt7H9w
dJ5nxsTk/fniJz86Ddtp6n8s82wYdkN3cVffeK72A9aTCOU=
-----END CERTIFICATE-----
```

La primera parte de la salida es el certificado en sí. La segunda parte es la cadena de certificados que se enlaza con el certificado raíz de la entidad de certificación. Tenga en cuenta que, al utilizar la opción `--output text`, se inserta un carácter TAB entre las dos partes del certificado (esa es la causa del texto con sangría). Si pretende utilizar esta salida y analizar los certificados con otras herramientas, puede que tenga que eliminar el carácter TAB para que se procese correctamente.

- Para obtener más información sobre la API, consulte GetCertificate en la Referencia de comandos de la AWS CLI.

`import-certificate-authority-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-certificate-authority-certificate`.

AWS CLI

Importación del certificado de la entidad de certificación en ACM PCA

Con el siguiente comando `import-certificate-authority-certificate`, se importa en ACM PCA el certificado de la entidad de certificación privada firmado para la entidad de certificación especificada por el ARN.

```
aws acm-pca import-certificate-authority-certificate --certificate-
authority-arn arn:aws:acm-pca:us-west-2:123456789012:certificate-
authority/12345678-1234-1234-1234-123456789012 --certificate file://C:\ca_cert.pem
 --certificate-chain file://C:\ca_cert_chain.pem
```

- Para obtener información sobre la API, consulte ImportCertificateAuthorityCertificate en la Referencia de comandos de la AWS CLI.

`issue-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `issue-certificate`.

AWS CLI

Emisión de un certificado privado

Con el siguiente comando `issue-certificate`, se utiliza la entidad de certificación privada especificada por el ARN para emitir un certificado privado.

```
aws acm-pca issue-certificate --certificate-authority-arn arn:aws:acm-pca:us-
west-2:123456789012:certificate-authority/12345678-1234-1234-1234-123456789012
 --csr file://C:\cert_1.csr --signing-algorithm "SHA256WITHRSA" --validity
 Value=365,Type="DAYS" --idempotency-token 1234
```

- Para obtener información sobre la API, consulte IssueCertificate en la Referencia de comandos de la AWS CLI.

`list-certificate-authorities`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-certificate-authorities`.

AWS CLI

Generación de una lista de las autoridades de certificación privadas

Con el siguiente comando `list-certificate-authorities`, se ofrece la siguiente información sobre todas las entidades de certificación privadas en la cuenta.

```
aws acm-pca list-certificate-authorities --max-results 10
```

- Para obtener información sobre la API, consulte ListCertificateAuthorities en la Referencia de comandos de la AWS CLI.

`list-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags`.

AWS CLI

Generación de una lista de las etiquetas de la entidad de certificación

Con el siguiente comando `list-tags`, se muestran las etiquetas asociadas a la entidad de certificación privada especificada por el ARN.

```
aws acm-pca list-tags --certificate-authority-arn arn:aws:acm-pca:us-
west-2:123456789012:certificate-authority/123455678-1234-1234-1234-123456789012 --
max-results 10
```

- Para obtener más información sobre la API, consulte ListTags en la Referencia de comandos de la AWS CLI.

`revoke-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `revoke-certificate`.

AWS CLI

Revocación de un certificado privado

Con el siguiente comando `revoke-certificate`, se revoca un certificado privado de la entidad de certificación identificada por el ARN.

```
aws acm-pca revoke-certificate --certificate-authority-arn arn:aws:acm-pca:us-west-2:1234567890:certificate-authority/12345678-1234-1234-1234-123456789012 --certificate-serial 67:07:44:76:83:a9:b7:f4:05:56:27:ff:d5:5c:eb:cc --revocation-reason "KEY_COMPROMISE"
```

- Para obtener información sobre la API, consulte RevokeCertificate en la Referencia de comandos de la AWS CLI.

`tag-certificate-authority`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-certificate-authority`.

AWS CLI

Asociación de etiquetas a una autoridad de certificación privada

Con el siguiente comando `tag-certificate-authority`, se asocian una o varias etiquetas a una entidad de certificación privada.

```
aws acm-pca tag-certificate-authority --certificate-authority-arn arn:aws:acm-pca:us-west-2:123456789012:certificate-authority/12345678-1234-1234-1234-123456789012 --tags Key=Admin,Value=Alice
```

- Para obtener información sobre la API, consulte TagCertificateAuthority en la Referencia de comandos de la AWS CLI.

`untag-certificate-authority`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-certificate-authority`.

AWS CLI

Eliminación de una o varias etiquetas de una entidad de certificación privada

Con el siguiente comando `untag-certificate-authority`, se eliminan etiquetas de la entidad de certificación privada identificada por el ARN.

```
aws acm-pca untag-certificate-authority --certificate-authority-
arn arn:aws:acm-pca:us-west-2:123456789012:certificate-
authority/12345678-1234-1234-1234-123456789012 --tags Key=Purpose,Value=Website
```

- Para obtener información sobre la API, consulte UntagCertificateAuthority en la Referencia de comandos de la AWS CLI.

`update-certificate-authority`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-certificate-authority`.

AWS CLI

Actualización de la configuración de la entidad de certificación privada

Con el siguiente comando `update-certificate-authority`, se actualiza el estado y la configuración de la entidad de certificación privada identificada por el ARN.

```
aws acm-pca update-certificate-authority --certificate-
authority-arn arn:aws:acm-pca:us-west-2:123456789012:certificate-
authority/12345678-1234-1234-1234-1232456789012 --revocation-configuration file://C:
\revoke_config.txt --status "DISABLED"
```

- Para obtener información sobre la API, consulte UpdateCertificateAuthority en la Referencia de comandos de la AWS CLI.

AWS Proton Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS Proton.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`cancel-service-instance-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-service-instance-deployment`.

AWS CLI

Para cancelar una implementación de instancia de servicio

En el siguiente ejemplo de `cancel-service-instance-deployment`, se cancela la implementación de una instancia de servicio.

```
aws proton cancel-service-instance-deployment \
    --service-instance-name "instance-one" \
    --service-name "simple-svc"
```

Salida:

```
{
    "serviceInstance": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/service-
instance/instance-one",
        "createdAt": "2021-04-02T21:29:59.962000+00:00",
        "deploymentStatus": "CANCELLING",
        "environmentName": "simple-env",
        "lastDeploymentAttemptedAt": "2021-04-02T21:45:15.406000+00:00",
        "lastDeploymentSucceededAt": "2021-04-02T21:38:00.823000+00:00",
        "name": "instance-one",
        "serviceName": "simple-svc",
        "spec": "proton: ServiceSpec\npipeline:\n
 my_sample_pipeline_optional_input: abc\n  my_sample_pipeline_required_input:
 '123'\ninstances:\n- name: my-instance\n  environment: MySimpleEnv
\n  spec:\n    my_sample_service_instance_optional_input: def\n
 my_sample_service_instance_required_input: '456'\n- name: my-other-instance\n
 environment: MySimpleEnv\n  spec:\n    my_sample_service_instance_required_input:
 '789'\n",
        "templateMajorVersion": "1",
        "templateMinorVersion": "1",
        "templateName": "svc-simple"
    }
}
```

Para obtener más información, consulte Update a service instance en la Guía del administrador de AWS Proton o Update a service instance en la Guía del usuario de AWS Proton.

- Para obtener información sobre la API, consulte CancelServiceInstanceDeployment en la Referencia de comandos de la AWS CLI.

`cancel-service-pipeline-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-service-pipeline-deployment`.

AWS CLI

Para cancelar una implementación de canalización de un servicio

En el siguiente ejemplo de `cancel-service-pipeline-deployment`, se cancela la implementación de la canalización de un servicio.

```
aws proton cancel-service-pipeline-deployment \
    --service-name "simple-svc"
```

Salida:

```
{
    "pipeline": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/pipeline",
        "createdAt": "2021-04-02T21:29:59.962000+00:00",
        "deploymentStatus": "CANCELLING",
        "lastDeploymentAttemptedAt": "2021-04-02T22:02:45.095000+00:00",
        "lastDeploymentSucceededAt": "2021-04-02T21:39:28.991000+00:00",
        "templateMajorVersion": "1",
        "templateMinorVersion": "1",
        "templateName": "svc-simple"
    }
}
```

Para obtener más información, consulte Update a service pipeline en la Guía del administrador de AWS Proton o Update a service pipeline en la Guía del usuario de AWS Proton.

- Para obtener información sobre la API, consulte CancelServicePipelineDeployment en la Referencia de comandos de la AWS CLI.

`create-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-service`.

AWS CLI

Para crear un servicio

En el siguiente ejemplo de `create-service`, se crea un servicio con una canalización de servicios.

```
aws proton create-service \
    --name "MySimpleService" \
    --template-name "fargate-service" \
    --template-major-version "1" \
    --branch-name "mainline" \
    --repository-connection-arn "arn:aws:codestar-connections:region-id:account-id:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
    --repository-id "myorg/myapp" \
    --spec file://spec.yaml
```

Contenido de `spec.yaml`:

```
proton: ServiceSpec

pipeline:
    my_sample_pipeline_required_input: "hello"
    my_sample_pipeline_optional_input: "bye"

instances:
    - name: "acme-network-dev"
        environment: "ENV_NAME"
        spec:
            my_sample_service_instance_required_input: "hi"
            my_sample_service_instance_optional_input: "ho"
```

Salida:

```
{
    "service": {
        "arn": "arn:aws:proton:region-id:123456789012:service/MySimpleService",
        "createdAt": "2020-11-18T19:50:27.460000+00:00",
        "lastModifiedAt": "2020-11-18T19:50:27.460000+00:00",
```

```
        "name": "MySimpleService",
        "repositoryConnectionArn": "arn:aws:codestar-connections:region-
id:123456789012connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "repositoryId": "myorg/myapp",
        "status": "CREATE_IN_PROGRESS",
        "templateName": "fargate-service"
    }
}
```

Para obtener más información, consulte Create a service en la Guía del administrador de AWS Proton y Create a service en la Guía del usuario de AWS Proton.

- Para obtener información sobre la API, consulte CreateService en la Referencia de comandos de la AWS CLI.

`delete-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-service`.

AWS CLI

Para eliminar un servicio

En el siguiente ejemplo de `delete-service`, se elimina un servicio.

```
aws proton delete-service \
    --name "simple-svc"
```

Salida:

```
{
    "service": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc",
        "branchName": "mainline",
        "createdAt": "2020-11-28T22:40:50.512000+00:00",
        "description": "Edit by updating description",
        "lastModifiedAt": "2020-11-29T00:30:39.248000+00:00",
        "name": "simple-svc",
        "repositoryConnectionArn": "arn:aws:codestar-connections:region-
id:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "repositoryId": "myorg/myapp",
        "status": "DELETE_IN_PROGRESS",
        "templateName": "fargate-service"
```

```
    }
}
```

Para obtener más información, consulte Delete a service en la Guía del administrador de AWS Proton.

- Para obtener información sobre la API, consulte DeleteService en la Referencia de comandos de la AWS CLI.

`get-service-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-instance`.

AWS CLI

Para obtener los detalles de la instancia de servicio

En el siguiente ejemplo de `get-service-instance`, se obtienen datos detallados de una instancia de servicio.

```
aws proton get-service-instance \
    --name "instance-one" \
    --service-name "simple-svc"
```

Salida:

```
{
    "serviceInstance": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/service-
instance/instance-one",
        "createdAt": "2020-11-28T22:40:50.512000+00:00",
        "deploymentStatus": "SUCCEEDED",
        "environmentName": "simple-env",
        "lastDeploymentAttemptedAt": "2020-11-28T22:40:50.512000+00:00",
        "lastDeploymentSucceededAt": "2020-11-28T22:40:50.512000+00:00",
        "name": "instance-one",
        "serviceName": "simple-svc",
        "spec": "proton: ServiceSpec\npipeline:\n
 my_sample_pipeline_optional_input: hello world\n
 my_sample_pipeline_required_input: pipeline up\ninstances:\n- name: instance-one\n
 environment: my-simple-env\n  spec:\n    my_sample_service_instance_optional_input:
 Ola\n    my_sample_service_instance_required_input: Ciao\n",
```

```
        "templateMajorVersion": "1",
        "templateMinorVersion": "0",
        "templateName": "svc-simple"
    }
}
```

Para obtener más información, consulte View service data en la View service data del administrador de AWS Proton o View service data en la Guía del usuario de AWS Proton.

- Para obtener información sobre la API, consulte GetServiceInstance en la Referencia de comandos de la AWS CLI.

`get-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service`.

AWS CLI

Para obtener detalles del servicio

En el siguiente ejemplo de `get-service`, se obtienen datos detallados de un servicio.

```
aws proton get-service \
    --name "simple-svc"
```

Salida:

```
{
    "service": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc",
        "branchName": "mainline",
        "createdAt": "2020-11-28T22:40:50.512000+00:00",
        "lastModifiedAt": "2020-11-28T22:44:51.207000+00:00",
        "name": "simple-svc",
        "pipeline": {
            "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/
pipeline/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "createdAt": "2020-11-28T22:40:50.512000+00:00",
            "deploymentStatus": "SUCCEEDED",
            "lastDeploymentAttemptedAt": "2020-11-28T22:40:50.512000+00:00",
            "lastDeploymentSucceededAt": "2020-11-28T22:40:50.512000+00:00",
            "spec": "proton: ServiceSpec\npipeline:\n
 my_sample_pipeline_required_input: hello\n  my_sample_pipeline_optional_input:
```

```
 bye\ninstances:\n- name: instance-svc-simple\n  environment: my-simple-
env\n  spec:\n    my_sample_service_instance_required_input: hi\n
 my_sample_service_instance_optional_input: ho\n",
            "templateMajorVersion": "1",
            "templateMinorVersion": "1",
            "templateName": "svc-simple"
        },
        "repositoryConnectionArn": "arn:aws:codestar-connections:region-
id:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "repositoryId": "myorg/myapp",
        "spec": "proton: ServiceSpec\npipeline:\n
 my_sample_pipeline_required_input: hello\n  my_sample_pipeline_optional_input:
 bye\ninstances:\n- name: instance-svc-simple\n  environment: my-simple-
env\n  spec:\n    my_sample_service_instance_required_input: hi\n
 my_sample_service_instance_optional_input: ho\n",
        "status": "ACTIVE",
        "templateName": "svc-simple"
    }
}
```

Para obtener más información, consulte View service data en la View service data del administrador de AWS Proton o View service data en la Guía del usuario de AWS Proton.

- Para obtener información sobre la API, consulte GetService en la Referencia de comandos de la AWS CLI.

`list-service-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-service-instances`.

AWS CLI

Ejemplo 1: enumerar todas las instancias de servicio

En el siguiente ejemplo de `list-service-instances`, se enumeran las instancias del servicio.

```
aws proton list-service-instances
```

Salida:

```
{
    "serviceInstances": [
        {
```

```
            "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/
service-instance/instance-one",
            "createdAt": "2020-11-28T22:40:50.512000+00:00",
            "deploymentStatus": "SUCCEEDED",
            "environmentArn": "arn:aws:proton:region-id:123456789012:environment/
simple-env",
            "lastDeploymentAttemptedAt": "2020-11-28T22:40:50.512000+00:00",
            "lastDeploymentSucceededAt": "2020-11-28T22:40:50.512000+00:00",
            "name": "instance-one",
            "serviceName": "simple-svc",
            "templateMajorVersion": "1",
            "templateMinorVersion": "0",
            "templateName": "fargate-service"
        }
    ]
}
```

Para obtener más información, consulte View service instance data en la Guía del administrador de AWS Proton o View service instance data en la Guía del usuario de AWS Proton.

Ejemplo 2: enumerar la instancia de servicio especificada

En el siguiente ejemplo de `get-service-instance`, se obtiene una instancia de servicio.

```
aws proton get-service-instance \
    --name "instance-one" \
    --service-name "simple-svc"
```

Salida:

```
{
    "serviceInstance": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/service-
instance/instance-one",
        "createdAt": "2020-11-28T22:40:50.512000+00:00",
        "deploymentStatus": "SUCCEEDED",
        "environmentName": "simple-env",
        "lastDeploymentAttemptedAt": "2020-11-28T22:40:50.512000+00:00",
        "lastDeploymentSucceededAt": "2020-11-28T22:40:50.512000+00:00",
        "name": "instance-one",
        "serviceName": "simple-svc",
        "spec": "proton: ServiceSpec\npipeline:\n
 my_sample_pipeline_optional_input: hello world\n
```

```
 my_sample_pipeline_required_input: pipeline up\ninstances:\n- name: instance-one\n
 environment: my-simple-env\n  spec:\n    my_sample_service_instance_optional_input:
 Ola\n    my_sample_service_instance_required_input: Ciao\n",
        "templateMajorVersion": "1",
        "templateMinorVersion": "0",
        "templateName": "svc-simple"
    }
}
```

Para obtener más información, consulte View service instance data en la Guía del administrador de AWS Proton o View service instance data en la Guía del usuario de AWS Proton.

- Para obtener información sobre la API, consulte ListServiceInstances en la Referencia de comandos de la AWS CLI.

`update-service-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-service-instance`.

AWS CLI

Para actualizar una instancia de servicio a una nueva versión secundaria

En el siguiente ejemplo de `update-service-instance`, se actualiza una instancia de servicio a una nueva versión secundaria de su plantilla de servicio que agrega una nueva instancia denominada my-other-instance con una nueva entrada obligatoria.

```
aws proton update-service-instance \
    --service-name "simple-svc" \
    --spec "file://service-spec.yaml " \
    --template-major-version "1" \
    --template-minor-version "1" \
    --deployment-type "MINOR_VERSION" \
    --name "instance-one"
```

Contenido de `service-spec.yaml`:

```
proton: ServiceSpec
pipeline:
    my_sample_pipeline_optional_input: "abc"
    my_sample_pipeline_required_input: "123"
instances:
```

```
    - name: "instance-one"
        environment: "simple-env"
        spec:
            my_sample_service_instance_optional_input: "def"
            my_sample_service_instance_required_input: "456"
    - name: "my-other-instance"
        environment: "simple-env"
        spec:
            my_sample_service_instance_required_input: "789"
```

Salida:

```
{
    "serviceInstance": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/service-
instance/instance-one",
        "createdAt": "2021-04-02T21:29:59.962000+00:00",
        "deploymentStatus": "IN_PROGRESS",
        "environmentName": "arn:aws:proton:region-id:123456789012:environment/
simple-env",
        "lastDeploymentAttemptedAt": "2021-04-02T21:38:00.823000+00:00",
        "lastDeploymentSucceededAt": "2021-04-02T21:29:59.962000+00:00",
        "name": "instance-one",
        "serviceName": "simple-svc",
        "templateMajorVersion": "1",
        "templateMinorVersion": "0",
        "templateName": "svc-simple"
    }
}
```

Para obtener más información, consulte Update a service instance en la Guía del administrador de AWS Proton o Update a service instance en la Guía del usuario de AWS Proton.

- Para obtener información sobre la API, consulte UpdateServiceInstance en la Referencia de comandos de la AWS CLI.

`update-service-pipeline`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-service-pipeline`.

AWS CLI

Para actualizar una canalización de servicio

En el siguiente ejemplo de `update-service-pipeline`, se actualiza a una canalización de servicio a una nueva versión secundaria de su plantilla de servicio.

```
aws proton update-service-pipeline \
    --service-name "simple-svc" \
    --spec "file://service-spec.yaml" \
    --template-major-version "1" \
    --template-minor-version "1" \
    --deployment-type "MINOR_VERSION"
```

Salida:

```
{
    "pipeline": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/pipeline/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "createdAt": "2021-04-02T21:29:59.962000+00:00",
        "deploymentStatus": "IN_PROGRESS",
        "lastDeploymentAttemptedAt": "2021-04-02T21:39:28.991000+00:00",
        "lastDeploymentSucceededAt": "2021-04-02T21:29:59.962000+00:00",
        "spec": "proton: ServiceSpec\n\npipeline:\n
 my_sample_pipeline_optional_input: \"abc\"\n  my_sample_pipeline_required_input:
 \"123\"\n\ninstances:\n  - name: \"my-instance\"\n    environment: \"MySimpleEnv
\"\n    spec:\n      my_sample_service_instance_optional_input: \"def
\"\n      my_sample_service_instance_required_input: \"456\"\n  - name:
 \"my-other-instance\"\n    environment: \"MySimpleEnv\"\n    spec:\n
 my_sample_service_instance_required_input: \"789\"\n",
        "templateMajorVersion": "1",
        "templateMinorVersion": "0",
        "templateName": "svc-simple"
    }
}
```

Para obtener más información, consulte Update a service pipeline en la Guía del administrador de AWS Proton o Update a service pipeline en la Guía del usuario de AWS Proton.

- Para obtener información sobre la API, consulte UpdateServicePipeline en la Referencia de comandos de la AWS CLI.

`update-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-service`.

AWS CLI

Para actualizar un servicio

En el siguiente ejemplo de `update-service`, se edita la descripción de un servicio.

```
aws proton update-service \
    --name "MySimpleService" \
    --description "Edit by updating description"
```

Salida:

```
{
    "service": {
        "arn": "arn:aws:proton:region-id:123456789012:service/MySimpleService",
        "branchName": "mainline",
        "createdAt": "2021-03-12T22:39:42.318000+00:00",
        "description": "Edit by updating description",
        "lastModifiedAt": "2021-03-12T22:44:21.975000+00:00",
        "name": "MySimpleService",
        "repositoryConnectionArn": "arn:aws:codestar-connections:region-
id:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "repositoryId": "myorg/myapp",
        "status": "ACTIVE",
        "templateName": "fargate-service"
    }
}
```

Para obtener más información, consulte Edit a service en la Guía del administrador de AWS Proton o Edit a service en la Guía del usuario de AWS Proton.

- Para obtener información sobre la API, consulte UpdateService en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon RDS usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon RDS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-option-to-option-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-option-to-option-group`.

AWS CLI

Para agregar una opción a un grupo de opción

El siguiente ejemplo de `add-option-to-option-group` agrega una opción a un grupo de opción especificado.

```
aws rds add-option-to-option-group \
    --option-group-name myoptiongroup \
    --options OptionName=OEM,Port=5500,DBSecurityGroupMemberships=default \
    --apply-immediately
```

Salida:

```
{
    "OptionGroup": {
        "OptionGroupName": "myoptiongroup",
        "OptionGroupDescription": "Test Option Group",
        "EngineName": "oracle-ee",
        "MajorEngineVersion": "12.1",
        "Options": [
            {
                "OptionName": "Timezone",
                "OptionDescription": "Change time zone",
                "Persistent": true,
                "Permanent": false,
                "OptionSettings": [
                    {
                        "Name": "TIME_ZONE",
                        "Value": "Australia/Sydney",
```

```
                        "DefaultValue": "UTC",
                        "Description": "Specifies the timezone the user wants to
 change the system time to",
                        "ApplyType": "DYNAMIC",
                        "DataType": "STRING",
                        "AllowedValues": "Africa/Cairo,Africa/Casablanca,Africa/
Harare,Africa/Lagos,Africa/Luanda,Africa/Monrovia,Africa/Nairobi,Africa/
Tripoli,Africa/Windhoek,America/Araguaina,America/Argentina/Buenos_Aires,America/
Asuncion,America/Bogota,America/Caracas,America/Chicago,America/Chihuahua,America/
Cuiaba,America/Denver,America/Detroit,America/Fortaleza,America/Godthab,America/
Guatemala,America/Halifax,America/Lima,America/Los_Angeles,America/Manaus,America/
Matamoros,America/Mexico_City,America/Monterrey,America/Montevideo,America/
New_York,America/Phoenix,America/Santiago,America/Sao_Paulo,America/Tijuana,America/
Toronto,Asia/Amman,Asia/Ashgabat,Asia/Baghdad,Asia/Baku,Asia/Bangkok,Asia/
Beirut,Asia/Calcutta,Asia/Damascus,Asia/Dhaka,Asia/Hong_Kong,Asia/Irkutsk,Asia/
Jakarta,Asia/Jerusalem,Asia/Kabul,Asia/Karachi,Asia/Kathmandu,Asia/Kolkata,Asia/
Krasnoyarsk,Asia/Magadan,Asia/Manila,Asia/Muscat,Asia/Novosibirsk,Asia/Rangoon,Asia/
Riyadh,Asia/Seoul,Asia/Shanghai,Asia/Singapore,Asia/Taipei,Asia/Tehran,Asia/
Tokyo,Asia/Ulaanbaatar,Asia/Vladivostok,Asia/Yakutsk,Asia/Yerevan,Atlantic/
Azores,Atlantic/Cape_Verde,Australia/Adelaide,Australia/Brisbane,Australia/
Darwin,Australia/Eucla,Australia/Hobart,Australia/Lord_Howe,Australia/
Perth,Australia/Sydney,Brazil/DeNoronha,Brazil/East,Canada/Newfoundland,Canada/
Saskatchewan,Etc/GMT-3,Europe/Amsterdam,Europe/Athens,Europe/Berlin,Europe/
Dublin,Europe/Helsinki,Europe/Kaliningrad,Europe/London,Europe/Madrid,Europe/
Moscow,Europe/Paris,Europe/Prague,Europe/Rome,Europe/Sarajevo,Pacific/Apia,Pacific/
Auckland,Pacific/Chatham,Pacific/Fiji,Pacific/Guam,Pacific/Honolulu,Pacific/
Kiritimati,Pacific/Marquesas,Pacific/Samoa,Pacific/Tongatapu,Pacific/Wake,US/
Alaska,US/Central,US/East-Indiana,US/Eastern,US/Pacific,UTC",
                        "IsModifiable": true,
                        "IsCollection": false
                    }
                ],
                "DBSecurityGroupMemberships": [],
                "VpcSecurityGroupMemberships": []
            },
            {
                "OptionName": "OEM",
                "OptionDescription": "Oracle 12c EM Express",
                "Persistent": false,
                "Permanent": false,
                "Port": 5500,
                "OptionSettings": [],
                "DBSecurityGroupMemberships": [
                    {
```

```
                    "DBSecurityGroupName": "default",
                    "Status": "authorized"
                }
            ],
            "VpcSecurityGroupMemberships": []
        }
    ],
    "AllowsVpcAndNonVpcInstanceMemberships": false,
    "OptionGroupArn": "arn:aws:rds:us-east-1:123456789012:og:myoptiongroup"
  }
}
```

Para obtener más información, consulte Agregar una opción a un grupo de opciones en la Guía del usuario de Amazon RDS.

- Para obtener detalles de la API, consulte AddOptionToOptionGroup en la Referencia de comandos de la AWS CLI.

`add-role-to-db-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-role-to-db-cluster`.

AWS CLI

Para asociar un rol de AWS Identity and Access Management (IAM) con un clúster de base de datos

El siguiente ejemplo de `add-role-to-db-cluster` asocia un rol con un clúster de base de datos.

```
aws rds add-role-to-db-cluster \
    --db-cluster-identifier mydbcluster \
    --role-arn arn:aws:iam::123456789012:role/RDSLoadFromS3
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Asociación de un rol de IAM con un clúster de base de datos Amazon Aurora MySQL en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte AddRoleToDbCluster en la Referencia de comandos de la AWS CLI.

`add-role-to-db-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-role-to-db-instance`.

AWS CLI

Para asociar un rol de AWS Identity and Access Management (IAM) con una instancia de base de datos

El siguiente ejemplo de `add-role-to-db-instance` agrega el rol a una instancia de base de datos de Oracle denominada `test-instance`.

```
aws rds add-role-to-db-instance \
    --db-instance-identifier test-instance \
    --feature-name S3_INTEGRATION \
    --role-arn arn:aws:iam::111122223333:role/rds-s3-integration-role
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Prerequisites for Amazon RDS Oracle Integration with Amazon S3 en la Guía del usuario de Amazon RDS.

- Para obtener detalles sobre la API, consulte AddRoleToDbInstance en la Referencia de comandos de la AWS CLI.

`add-source-identifier-to-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-source-identifier-to-subscription`.

AWS CLI

Para agregar un identificador de origen a una suscripción

El siguiente ejemplo de `add-source-identifier` agrega otro identificador de origen a una suscripción existente.

```
aws rds add-source-identifier-to-subscription \
    --subscription-name my-instance-events \
    --source-identifier test-instance-repl
```

Salida:

```
{
    "EventSubscription": {
        "SubscriptionCreationTime": "Tue Jul 31 23:22:01 UTC 2018",
        "CustSubscriptionId": "my-instance-events",
        "EventSubscriptionArn": "arn:aws:rds:us-east-1:123456789012:es:my-instance-
events",
        "Enabled": false,
        "Status": "modifying",
        "EventCategoriesList": [
            "backup",
            "recovery"
        ],
        "CustomerAwsId": "123456789012",
        "SnsTopicArn": "arn:aws:sns:us-east-1:123456789012:interesting-events",
        "SourceType": "db-instance",
        "SourceIdsList": [
            "test-instance",
            "test-instance-repl"
        ]
    }
}
```

- Para obtener información sobre la API, consulte AddSourceIdentifierToSubscription en la Referencia de comandos de la AWS CLI.

`add-tags-to-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-tags-to-resource`.

AWS CLI

Para agregar etiquetas a un recurso

En el siguiente ejemplo de `add-tags-to-resource` se agregan etiquetas a una base de datos de RDS.

```
aws rds add-tags-to-resource \
    --resource-name arn:aws:rds:us-east-1:123456789012:db:database-mysql \
    --tags "[{\"Key\": \"Name\",\"Value\": \"MyDatabase\"},{\"Key\": \"Environment
\",\"Value\": \"test\"}]"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de los recursos de Amazon RDS en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte AddTagsToResource en la Referencia de comandos de la AWS CLI.

`apply-pending-maintenance-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `apply-pending-maintenance-action`.

AWS CLI

Para aplicar acciones de mantenimiento pendientes

El siguiente ejemplo de `apply-pending-maintenance-action` aplica las acciones de mantenimiento pendientes para un clúster de base de datos.

```
aws rds apply-pending-maintenance-action \
    --resource-identifier arn:aws:rds:us-east-1:123456789012:cluster:my-db-cluster \
    --apply-action system-update \
    --opt-in-type immediate
```

Salida:

```
{
    "ResourcePendingMaintenanceActions": {
        "ResourceIdentifier": "arn:aws:rds:us-east-1:123456789012:cluster:my-db-
cluster",
        "PendingMaintenanceActionDetails": [
            {
                "Action": "system-update",
                "OptInStatus": "immediate",
                "CurrentApplyDate": "2021-01-23T01:07:36.100Z",
                "Description": "Upgrade to Aurora PostgreSQL 3.3.2"
            }
        ]
    }
}
```

Para obtener más información, consulte Mantenimiento de una instancia de base de datos en la Guía del usuario de Amazon RDS y Mantenimiento de un clúster de base de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte ApplyPendingMaintenanceAction en la Referencia de comandos de la AWS CLI.

`authorize-db-security-group-ingress`

En el siguiente ejemplo de código, se muestra cómo utilizar `authorize-db-security-group-ingress`.

AWS CLI

Para asociar un rol de AWS Identity and Access Management (IAM) con una instancia de base de datos

En el siguiente ejemplo de `authorize-db-security-group-ingress`, se configura el grupo de seguridad predeterminado con una regla de entrada para el rango de IP CIDR 192.0.2.0/24.

```
aws rds authorize-db-security-group-ingress \
    --db-security-group-name default \
    --cidrip 192.0.2.0/24
```

Salida:

```
{
    "DBSecurityGroup": {
        "OwnerId": "123456789012",
        "DBSecurityGroupName": "default",
        "DBSecurityGroupDescription": "default",
        "EC2SecurityGroups": [],
        "IPRanges": [
            {
                "Status": "authorizing",
                "CIDRIP": "192.0.2.0/24"
            }
        ],
        "DBSecurityGroupArn": "arn:aws:rds:us-east-1:111122223333:secgrp:default"
    }
}
```

Para obtener más información, consulte Authorizing Network Access to a DB Security Group from an IP Range en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte AuthorizeDbSecurityGroupIngress en la Referencia de comandos de la AWS CLI.

`backtrack-db-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `backtrack-db-cluster`.

AWS CLI

Para buscar datos anteriores en un clúster de base de datos de Aurora

El siguiente ejemplo de `backtrack-db-cluster` realiza una búsqueda de datos anteriores en el clúster de base de datos sample-cluster hasta el 19 de marzo de 2018 a las 10:00 horas.

```
aws rds backtrack-db-cluster --db-cluster-identifier sample-cluster --backtrack-
to 2018-03-19T10:00:00+00:00
```

Este comando genera un bloque JSON que reconoce el cambio en el recurso de RDS.

- Para obtener información sobre la API, consulte BacktrackDbCluster en la Referencia de comandos de la AWS CLI.

`cancel-export-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-export-task`.

AWS CLI

Para cancelar una exportación de instantánea a Amazon S3

El siguiente ejemplo de `cancel-export-task` cancela una tarea de exportación en curso que exporta una instantánea a Amazon S3.

```
aws rds cancel-export-task \
    --export-task-identifier my-s3-export-1
```

Salida:

```
{
```

```
    "ExportTaskIdentifier": "my-s3-export-1",
    "SourceArn": "arn:aws:rds:us-east-1:123456789012:snapshot:publisher-final-
snapshot",
    "SnapshotTime": "2019-03-24T20:01:09.815Z",
    "S3Bucket": "amzn-s3-demo-bucket",
    "S3Prefix": "",
    "IamRoleArn": "arn:aws:iam::123456789012:role/service-role/export-snap-S3-role",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/abcd0000-7bfd-4594-af38-
aabbccddeeff",
    "Status": "CANCELING",
    "PercentProgress": 0,
    "TotalExtractedDataInGB": 0
}
```

Para obtener más información, consulte Canceling a snapshot export task en la Guía del usuario de Amazon RDS o Canceling a snapshot export task en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte CancelExportTask en la Referencia de comandos de la AWS CLI.

`copy-db-cluster-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-db-cluster-parameter-group`.

AWS CLI

Para copiar un grupo de parámetros del clúster de una base de datos

En el siguiente ejemplo de `copy-db-cluster-parameter-group`, se realiza una copia de un grupo de parámetros de clúster de una base de datos.

```
aws rds copy-db-cluster-parameter-group \
    --source-db-cluster-parameter-group-identifier mydbclusterpg \
    --target-db-cluster-parameter-group-identifier mydbclusterpgcopy \
    --target-db-cluster-parameter-group-description "Copy of mydbclusterpg parameter
 group"
```

Salida:

```
{
```

```
    "DBClusterParameterGroup": {
        "DBClusterParameterGroupName": "mydbclusterpgcopy",
        "DBClusterParameterGroupArn": "arn:aws:rds:us-east-1:123456789012:cluster-
pg:mydbclusterpgcopy",
        "DBParameterGroupFamily": "aurora-mysql5.7",
        "Description": "Copy of mydbclusterpg parameter group"
    }
}
```

Para obtener más información, consulte Copying a DB Cluster Parameter Group en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte CopyDbClusterParameterGroup en la Referencia de comandos de la AWS CLI.

`copy-db-cluster-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-db-cluster-snapshot`.

AWS CLI

Para copiar una instantánea de clúster de base de datos

En el siguiente ejemplo de `copy-db-cluster-snapshot`, se crea una copia de una instantánea de un clúster de base de datos, incluidas sus etiquetas.

```
aws rds copy-db-cluster-snapshot \
    --source-db-cluster-snapshot-identifier arn:aws:rds:us-
east-1:123456789012:cluster-snapshot:rds:myaurora-2019-06-04-09-16
    --target-db-cluster-snapshot-identifier myclustersnapshotcopy \
    --copy-tags
```

Salida:

```
{
    "DBClusterSnapshot": {
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1b",
            "us-east-1e"
        ],
        "DBClusterSnapshotIdentifier": "myclustersnapshotcopy",
```

```
        "DBClusterIdentifier": "myaurora",
        "SnapshotCreateTime": "2019-06-04T09:16:42.649Z",
        "Engine": "aurora-mysql",
        "AllocatedStorage": 0,
        "Status": "available",
        "Port": 0,
        "VpcId": "vpc-6594f31c",
        "ClusterCreateTime": "2019-04-15T14:18:42.785Z",
        "MasterUsername": "myadmin",
        "EngineVersion": "5.7.mysql_aurora.2.04.2",
        "LicenseModel": "aurora-mysql",
        "SnapshotType": "manual",
        "PercentProgress": 100,
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE",
        "DBClusterSnapshotArn": "arn:aws:rds:us-east-1:123456789012:cluster-
snapshot:myclustersnapshotcopy",
        "IAMDatabaseAuthenticationEnabled": false
    }
}
```

Para obtener más información, consulte Copying a Snapshot en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte CopyDbClusterSnapshot en la Referencia de comandos de la AWS CLI.

`copy-db-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-db-parameter-group`.

AWS CLI

Para copiar un grupo de parámetros del clúster de una base de datos

En el siguiente ejemplo de `copy-db-parameter-group`, se crea un grupo de parámetros de base de datos.

```
aws rds copy-db-parameter-group \
    --source-db-parameter-group-identifier mydbpg \
    --target-db-parameter-group-identifier mydbpgcopy \
    --target-db-parameter-group-description "Copy of mydbpg parameter group"
```

Salida:

```
{
    "DBParameterGroup": {
        "DBParameterGroupName": "mydbpgcopy",
        "DBParameterGroupArn": "arn:aws:rds:us-east-1:814387698303:pg:mydbpgcopy",
        "DBParameterGroupFamily": "mysql5.7",
        "Description": "Copy of mydbpg parameter group"
    }
}
```

Para obtener más información, consulte Copying a DB Parameter Group en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte CopyDbParameterGroup en la Referencia de comandos de la AWS CLI.

`copy-db-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-db-snapshot`.

AWS CLI

Para copiar la instantánea de una base de datos

El siguiente ejemplo de `copy-db-snapshot` crea la copia de una instantánea de una base de datos.

```
aws rds copy-db-snapshot \
    --source-db-snapshot-identifier rds:database-mysql-2019-06-06-08-38
    --target-db-snapshot-identifier mydbsnapshotcopy
```

Salida:

```
{
    "DBSnapshot": {
        "VpcId": "vpc-6594f31c",
        "Status": "creating",
        "Encrypted": true,
        "SourceDBSnapshotIdentifier": "arn:aws:rds:us-
east-1:123456789012:snapshot:rds:database-mysql-2019-06-06-08-38",
```

```
        "MasterUsername": "admin",
        "Iops": 1000,
        "Port": 3306,
        "LicenseModel": "general-public-license",
        "DBSnapshotArn": "arn:aws:rds:us-
east-1:123456789012:snapshot:mydbsnapshotcopy",
        "EngineVersion": "5.6.40",
        "OptionGroupName": "default:mysql-5-6",
        "ProcessorFeatures": [],
        "Engine": "mysql",
        "StorageType": "io1",
        "DbiResourceId": "db-ZI7UJ5BLKMBYFGX7FDENCKADC4",
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE",
        "SnapshotType": "manual",
        "IAMDatabaseAuthenticationEnabled": false,
        "SourceRegion": "us-east-1",
        "DBInstanceIdentifier": "database-mysql",
        "InstanceCreateTime": "2019-04-30T15:45:53.663Z",
        "AvailabilityZone": "us-east-1f",
        "PercentProgress": 0,
        "AllocatedStorage": 100,
        "DBSnapshotIdentifier": "mydbsnapshotcopy"
    }
}
```

Para obtener más información, consulte Copying a Snapshot en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte CopyDbSnapshot en la Referencia de comandos de la AWS CLI.

`copy-option-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-option-group`.

AWS CLI

Para copiar un grupo de opciones

En el siguiente ejemplo de `copy-option-group`, se realiza una copia de un grupo de opciones.

```
aws rds copy-option-group \
    --source-option-group-identifier myoptiongroup \
```

```
    --target-option-group-identifier new-option-group \
    --target-option-group-description "My option group copy"
```

Salida:

```
{
    "OptionGroup": {
        "Options": [],
        "OptionGroupName": "new-option-group",
        "MajorEngineVersion": "11.2",
        "OptionGroupDescription": "My option group copy",
        "AllowsVpcAndNonVpcInstanceMemberships": true,
        "EngineName": "oracle-ee",
        "OptionGroupArn": "arn:aws:rds:us-east-1:123456789012:og:new-option-group"
    }
}
```

Para obtener más información, consulte Copia de un grupo de opciones en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte CopyOptionGroup en la Referencia de comandos de la AWS CLI.

`create-blue-green-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-blue-green-deployment`.

AWS CLI

Ejemplo 1: crear una implementación azul/verde para un RDS en una instancia de base de datos de MySQL DB

En el siguiente ejemplo de `create-blue-green-deployment`, se crea una implementación azul/verde para una instancia de base de datos de MySQL.

```
aws rds create-blue-green-deployment \
    --blue-green-deployment-name bgd-cli-test-instance \
    --source arn:aws:rds:us-east-1:123456789012:db:my-db-instance \
    --target-engine-version 8.0 \
    --target-db-parameter-group-name mysql-80-group
```

Salida:

```
{
    "BlueGreenDeployment": {
        "BlueGreenDeploymentIdentifier": "bgd-v53303651eexfake",
        "BlueGreenDeploymentName": "bgd-cli-test-instance",
        "Source": "arn:aws:rds:us-east-1:123456789012:db:my-db-instance",
        "SwitchoverDetails": [
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-1"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-2"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-3"
            }
        ],
        "Tasks": [
            {
                "Name": "CREATING_READ_REPLICA_OF_SOURCE",
                "Status": "PENDING"
            },
            {
                "Name": "DB_ENGINE_VERSION_UPGRADE",
                "Status": "PENDING"
            },
            {
                "Name": "CONFIGURE_BACKUPS",
                "Status": "PENDING"
            },
            {
                "Name": "CREATING_TOPOLOGY_OF_SOURCE",
                "Status": "PENDING"
            }
        ],
        "Status": "PROVISIONING",
```

```
        "CreateTime": "2022-02-25T21:18:51.183000+00:00"
    }
}
```

Para obtener más información, consulte Creación de una implementación azul/verde en la Guía del usuario de Amazon RDS.

Ejemplo 2: crear una implementación azul/verde para un clúster de base de datos en Aurora MySQL

En el siguiente ejemplo de `create-blue-green-deployment`, se crea una implementación azul/verde para un clúster de base de datos de Aurora MySQL.

```
aws rds create-blue-green-deployment \
    --blue-green-deployment-name my-blue-green-deployment \
    --source arn:aws:rds:us-east-1:123456789012:cluster:my-aurora-mysql-cluster \
    --target-engine-version 8.0 \
    --target-db-cluster-parameter-group-name ams-80-binlog-enabled \
    --target-db-parameter-group-name mysql-80-cluster-group
```

Salida:

```
{
      "BlueGreenDeployment": {
        "BlueGreenDeploymentIdentifier": "bgd-wi89nwzglccsfake",
        "BlueGreenDeploymentName": "my-blue-green-deployment",
        "Source": "arn:aws:rds:us-east-1:123456789012:cluster:my-aurora-mysql-
cluster",
        "SwitchoverDetails": [
          {
            "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster:my-aurora-
mysql-cluster",
            "Status": "PROVISIONING"
          },
          {
            "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-aurora-mysql-
cluster-1",
            "Status": "PROVISIONING"
          },
          {
            "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-aurora-mysql-
cluster-2",
```

```
            "Status": "PROVISIONING"
          },
          {
            "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-aurora-mysql-
cluster-3",
            "Status": "PROVISIONING"
          },
          {
            "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster-endpoint:my-
excluded-member-endpoint",
            "Status": "PROVISIONING"
          },
          {
            "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster-endpoint:my-
reader-endpoint",
            "Status": "PROVISIONING"
          }
        ],
        "Tasks": [
          {
            "Name": "CREATING_READ_REPLICA_OF_SOURCE",
            "Status": "PENDING"
          },
          {
            "Name": "DB_ENGINE_VERSION_UPGRADE",
            "Status": "PENDING"
          },
          {
            "Name": "CREATE_DB_INSTANCES_FOR_CLUSTER",
            "Status": "PENDING"
          },
          {
            "Name": "CREATE_CUSTOM_ENDPOINTS",
            "Status": "PENDING"
          }
        ],
        "Status": "PROVISIONING",
        "CreateTime": "2022-02-25T21:12:00.288000+00:00"
      }
}
```

Para obtener más información, consulte Creación de una implementación azul/verde en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte CreateBlueGreenDeployment en la Referencia de comandos de la AWS CLI.

`create-db-cluster-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-cluster-endpoint`.

AWS CLI

Para crear un punto de conexión de clúster de base de datos personalizado

El siguiente ejemplo de `create-db-cluster-endpoint` crea un punto de conexión de clúster de base de datos personalizado y lo asocia a un clúster de base de datos Aurora especificado.

```
aws rds create-db-cluster-endpoint \
    --db-cluster-endpoint-identifier mycustomendpoint \
    --endpoint-type reader \
    --db-cluster-identifier mydbcluster \
    --static-members dbinstance1 dbinstance2
```

Salida:

```
{
    "DBClusterEndpointIdentifier": "mycustomendpoint",
    "DBClusterIdentifier": "mydbcluster",
    "DBClusterEndpointResourceIdentifier": "cluster-endpoint-ANPAJ4AE5446DAEXAMPLE",
    "Endpoint": "mycustomendpoint.cluster-custom-cnpexample.us-
east-1.rds.amazonaws.com",
    "Status": "creating",
    "EndpointType": "CUSTOM",
    "CustomEndpointType": "READER",
    "StaticMembers": [
        "dbinstance1",
        "dbinstance2"
    ],
    "ExcludedMembers": [],
    "DBClusterEndpointArn": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:mycustomendpoint"
}
```

Para obtener más información, consulte Amazon Aurora Connection Management en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte CreateDbClusterEndpoint en la Referencia de comandos de la AWS CLI.

`create-db-cluster-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-cluster-parameter-group`.

AWS CLI

Para crear un grupo de parámetros de clúster de base de datos

En el siguiente ejemplo de `create-db-cluster-parameter-group`, se crea un grupo de parámetros de clúster de base de datos.

```
aws rds create-db-cluster-parameter-group \
    --db-cluster-parameter-group-name mydbclusterparametergroup \
    --db-parameter-group-family aurora5.6 \
    --description "My new cluster parameter group"
```

Salida:

```
{
    "DBClusterParameterGroup": {
        "DBClusterParameterGroupName": "mydbclusterparametergroup",
        "DBParameterGroupFamily": "aurora5.6",
        "Description": "My new cluster parameter group",
        "DBClusterParameterGroupArn": "arn:aws:rds:us-east-1:123456789012:cluster-
pg:mydbclusterparametergroup"
    }
}
```

Para obtener más información, consulte Creating a DB Cluster Parameter Group en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte CreateDbClusterParameterGroup en la Referencia de comandos de la AWS CLI.

`create-db-cluster-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-cluster-snapshot`.

AWS CLI

Para crear una instantánea de clúster de base de datos

En el siguiente ejemplo de `create-db-cluster-snapshot`, se crea una instantánea de clúster de base de datos.

```
aws rds create-db-cluster-snapshot \
    --db-cluster-identifier mydbcluster \
    --db-cluster-snapshot-identifier mydbclustersnapshot
```

Salida:

```
{
    "DBClusterSnapshot": {
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1b",
            "us-east-1e"
        ],
        "DBClusterSnapshotIdentifier": "mydbclustersnapshot",
        "DBClusterIdentifier": "mydbcluster",
        "SnapshotCreateTime": "2019-06-18T21:21:00.469Z",
        "Engine": "aurora-mysql",
        "AllocatedStorage": 1,
        "Status": "creating",
        "Port": 0,
        "VpcId": "vpc-6594f31c",
        "ClusterCreateTime": "2019-04-15T14:18:42.785Z",
        "MasterUsername": "myadmin",
        "EngineVersion": "5.7.mysql_aurora.2.04.2",
        "LicenseModel": "aurora-mysql",
        "SnapshotType": "manual",
        "PercentProgress": 0,
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE",
        "DBClusterSnapshotArn": "arn:aws:rds:us-east-1:123456789012:cluster-
snapshot:mydbclustersnapshot",
        "IAMDatabaseAuthenticationEnabled": false
    }
}
```

Para obtener más información, consulte Creación de una instantánea de clúster de base de datos en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte CreateDbClusterSnapshot en la Referencia de comandos de la AWS CLI.

`create-db-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-cluster`.

AWS CLI

Ejemplo 1: crear un clúster de base de datos compatible con MySQL 5.7

En el siguiente ejemplo de `create-db-cluster`, se crea un clúster de base de datos compatible con MySQL 5.7 con la versión predeterminada del motor. Reemplace la contraseña de muestra `secret99` con una contraseña segura. Cuando usa la consola para crear un clúster de base de datos, Amazon RDS crea automáticamente la instancia de base de datos de escritura para el clúster de base de datos. Sin embargo, cuando usa la CLI de AWS para crear un clúster de base de datos, debe crear expresamente la instancia de base de datos escritura para su clúster de base de datos mediante el comando de la CLI `create-db-instance` AWS.

```
aws rds create-db-cluster \
    --db-cluster-identifier sample-cluster \
    --engine aurora-mysql \
    --engine-version 5.7 \
    --master-username admin \
    --master-user-password secret99 \
    --db-subnet-group-name default \
    --vpc-security-group-ids sg-0b9130572daf3dc16
```

Salida:

```
{
    "DBCluster": {
        "DBSubnetGroup": "default",
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-0b9130572daf3dc16",
                "Status": "active"
            }
```

```
        ],
        "AllocatedStorage": 1,
        "AssociatedRoles": [],
        "PreferredBackupWindow": "09:12-09:42",
        "ClusterCreateTime": "2023-02-27T23:21:33.048Z",
        "DeletionProtection": false,
        "IAMDatabaseAuthenticationEnabled": false,
        "ReadReplicaIdentifiers": [],
        "EngineMode": "provisioned",
        "Engine": "aurora-mysql",
        "StorageEncrypted": false,
        "MultiAZ": false,
        "PreferredMaintenanceWindow": "mon:04:31-mon:05:01",
        "HttpEndpointEnabled": false,
        "BackupRetentionPeriod": 1,
        "DbClusterResourceId": "cluster-ANPAJ4AE5446DAEXAMPLE",
        "DBClusterIdentifier": "sample-cluster",
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1b",
            "us-east-1e"
        ],
        "MasterUsername": "master",
        "EngineVersion": "5.7.mysql_aurora.2.11.1",
        "DBClusterArn": "arn:aws:rds:us-east-1:123456789012:cluster:sample-cluster",
        "DBClusterMembers": [],
        "Port": 3306,
        "Status": "creating",
        "Endpoint": "sample-cluster.cluster-cnpexample.us-east-1.rds.amazonaws.com",
        "DBClusterParameterGroup": "default.aurora-mysql5.7",
        "HostedZoneId": "Z2R2ITUGPM61AM",
        "ReaderEndpoint": "sample-cluster.cluster-ro-cnpexample.us-
east-1.rds.amazonaws.com",
        "CopyTagsToSnapshot": false
    }
}
```

Ejemplo 2: crear un clúster de base de datos compatible con PostgreSQL

En el siguiente ejemplo de `create-db-cluster`, se crea un clúster de base de datos compatible con PostgreSQL con la versión predeterminada del motor. Reemplace la contraseña de ejemplo `secret99` con una contraseña segura. Cuando usa la consola para crear un clúster de base de datos, Amazon RDS crea automáticamente la instancia de base de datos de escritura

para el clúster de base de datos. Sin embargo, cuando usa la CLI de AWS para crear un clúster de base de datos, debe crear expresamente la instancia de base de datos escritura para su clúster de base de datos mediante el comando de la CLI `create-db-instance` AWS.

```
aws rds create-db-cluster \
    --db-cluster-identifier sample-pg-cluster \
    --engine aurora-postgresql \
    --master-username master \
    --master-user-password secret99 \
    --db-subnet-group-name default \
    --vpc-security-group-ids sg-0b9130572daf3dc16
```

Salida:

```
{
    "DBCluster": {
        "Endpoint": "sample-pg-cluster.cluster-cnpexample.us-
east-1.rds.amazonaws.com",
        "HttpEndpointEnabled": false,
        "DBClusterMembers": [],
        "EngineMode": "provisioned",
        "CopyTagsToSnapshot": false,
        "HostedZoneId": "Z2R2ITUGPM61AM",
        "IAMDatabaseAuthenticationEnabled": false,
        "AllocatedStorage": 1,
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-0b9130572daf3dc16",
                "Status": "active"
            }
        ],
        "DeletionProtection": false,
        "StorageEncrypted": false,
        "BackupRetentionPeriod": 1,
        "PreferredBackupWindow": "09:56-10:26",
        "ClusterCreateTime": "2023-02-27T23:26:08.371Z",
        "DBClusterParameterGroup": "default.aurora-postgresql13",
        "EngineVersion": "13.7",
        "Engine": "aurora-postgresql",
        "Status": "creating",
        "DBClusterIdentifier": "sample-pg-cluster",
        "MultiAZ": false,
        "Port": 5432,
```

```
        "DBClusterArn": "arn:aws:rds:us-east-1:123456789012:cluster:sample-pg-
cluster",
        "AssociatedRoles": [],
        "DbClusterResourceId": "cluster-ANPAJ4AE5446DAEXAMPLE",
        "PreferredMaintenanceWindow": "wed:03:33-wed:04:03",
        "ReaderEndpoint": "sample-pg-cluster.cluster-ro-cnpexample.us-
east-1.rds.amazonaws.com",
        "MasterUsername": "master",
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1b",
            "us-east-1c"
        ],
        "ReadReplicaIdentifiers": [],
        "DBSubnetGroup": "default"
    }
}
```

Para obtener más información, consulte Creación de un clúster de base de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte CreateDbCluster en la Referencia de comandos de la AWS CLI.

`create-db-instance-read-replica`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-instance-read-replica`.

AWS CLI

Para crear una réplica de lectura de una instancia de base de datos

En este ejemplo, se crea una réplica de lectura de una instancia de base de datos existente denominada `test-instance`. La réplica de lectura denominada `test-instance-repl`.

```
aws rds create-db-instance-read-replica \
    --db-instance-identifier test-instance-repl \
    --source-db-instance-identifier test-instance
```

Salida:

```
{
    "DBInstance": {
        "IAMDatabaseAuthenticationEnabled": false,
        "MonitoringInterval": 0,
        "DBInstanceArn": "arn:aws:rds:us-east-1:123456789012:db:test-instance-repl",
        "ReadReplicaSourceDBInstanceIdentifier": "test-instance",
        "DBInstanceIdentifier": "test-instance-repl",
        ...some output truncated...
    }
}
```

- Para obtener información sobre la API, consulte CreateDbInstanceReadReplica en la Referencia de comandos de la AWS CLI.

`create-db-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-instance`.

AWS CLI

Creación de una instancia de base de datos

En el siguiente ejemplo `create-db-instance`, se utilizan las opciones necesarias para lanzar una nueva instancia de base de datos.

```
aws rds create-db-instance \
    --db-instance-identifier test-mysql-instance \
    --db-instance-class db.t3.micro \
    --engine mysql \
    --master-username admin \
    --master-user-password secret99 \
    --allocated-storage 20
```

Salida:

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "test-mysql-instance",
        "DBInstanceClass": "db.t3.micro",
        "Engine": "mysql",
        "DBInstanceStatus": "creating",
        "MasterUsername": "admin",
```

```
        "AllocatedStorage": 20,
        "PreferredBackupWindow": "12:55-13:25",
        "BackupRetentionPeriod": 1,
        "DBSecurityGroups": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-12345abc",
                "Status": "active"
            }
        ],
        "DBParameterGroups": [
            {
                "DBParameterGroupName": "default.mysql5.7",
                "ParameterApplyStatus": "in-sync"
            }
        ],
        "DBSubnetGroup": {
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-2ff2ff2f",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-########",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2c"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-########",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2d"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-########",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2a"
                    },
                    "SubnetStatus": "Active"
                },
                {
```

```
                    "SubnetIdentifier": "subnet-########",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2b"
                    },
                    "SubnetStatus": "Active"
                }
            ]
        },
        "PreferredMaintenanceWindow": "sun:08:07-sun:08:37",
        "PendingModifiedValues": {
            "MasterUserPassword": "****"
        },
        "MultiAZ": false,
        "EngineVersion": "5.7.22",
        "AutoMinorVersionUpgrade": true,
        "ReadReplicaDBInstanceIdentifiers": [],
        "LicenseModel": "general-public-license",
        "OptionGroupMemberships": [
            {
                "OptionGroupName": "default:mysql-5-7",
                "Status": "in-sync"
            }
        ],
        "PubliclyAccessible": true,
        "StorageType": "gp2",
        "DbInstancePort": 0,
        "StorageEncrypted": false,
        "DbiResourceId": "db-5555EXAMPLE44444444EXAMPLE",
        "CACertificateIdentifier": "rds-ca-2019",
        "DomainMemberships": [],
        "CopyTagsToSnapshot": false,
        "MonitoringInterval": 0,
        "DBInstanceArn": "arn:aws:rds:us-west-2:123456789012:db:test-mysql-
instance",
        "IAMDatabaseAuthenticationEnabled": false,
        "PerformanceInsightsEnabled": false,
        "DeletionProtection": false,
        "AssociatedRoles": []
    }
}
```

Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte CreateDBInstance en la Referencia de comandos de la AWS CLI.

`create-db-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-parameter-group`.

AWS CLI

Creación de un grupo de parámetros de base de datos

En el siguiente ejemplo `create-db-parameter-group`, se crea un grupo de parámetros de base de datos.

```
aws rds create-db-parameter-group \
    --db-parameter-group-name mydbparametergroup \
    --db-parameter-group-family MySQL5.6 \
    --description "My new parameter group"
```

Salida:

```
{
    "DBParameterGroup": {
        "DBParameterGroupName": "mydbparametergroup",
        "DBParameterGroupFamily": "mysql5.6",
        "Description": "My new parameter group",
        "DBParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:pg:mydbparametergroup"
    }
}
```

Para obtener más información, consulte Creación de un grupo de parámetros de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte CreateDBParameterGroup en la Referencia de comandos de la AWS CLI.

`create-db-proxy-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-proxy-endpoint`.

AWS CLI

Para crear un punto de conexión de proxy de base de datos para una base de datos de RDS

En el siguiente ejemplo de `create-db-proxy-endpoint`, se crea un punto de conexión de proxy de base de datos.

```
aws rds create-db-proxy-endpoint \
    --db-proxy-name proxyExample \
    --db-proxy-endpoint-name "proxyep1" \
    --vpc-subnet-ids subnetgroup1 subnetgroup2
```

Salida:

```
{
"DBProxyEndpoint": {
        "DBProxyEndpointName": "proxyep1",
        "DBProxyEndpointArn": "arn:aws:rds:us-east-1:123456789012:db-proxy-
endpoint:prx-endpoint-0123a01b12345c0ab",
        "DBProxyName": "proxyExample",
        "Status": "creating",
        "VpcId": "vpc-1234567",
        "VpcSecurityGroupIds": [
            "sg-1234",
            "sg-5678"
        ],
        "VpcSubnetIds": [
            "subnetgroup1",
            "subnetgroup2"
        ],
        "Endpoint": "proxyep1.endpoint.proxy-ab0cd1efghij.us-
east-1.rds.amazonaws.com",
        "CreatedDate": "2023-04-05T16:09:33.452000+00:00",
        "TargetRole": "READ_WRITE",
        "IsDefault": false
    }
}
```

Para obtener más información, consulte Creating a proxy endpoint en la Guía del usuario de Amazon RDS y Creating a proxy endpoint en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte CreateDbProxyEndpoint en la Referencia de comandos de la AWS CLI.

create-db-proxy

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-proxy`.

AWS CLI

Para crear un proxy de base de datos para una base de datos de RDS

En el siguiente ejemplo de `create-db-proxy`, se crea un proxy de base de datos.

```
aws rds create-db-proxy \
    --db-proxy-name proxyExample \
    --engine-family MYSQL \
    --auth
 Description="proxydescription1",AuthScheme="SECRETS",SecretArn="arn:aws:secretsmanager:us-
west-2:123456789123:secret:secretName-1234f",IAMAuth="DISABLED",ClientPasswordAuthType="MYSQ
 \
    --role-arn arn:aws:iam::123456789123:role/ProxyRole \
    --vpc-subnet-ids subnetgroup1 subnetgroup2
```

Salida:

```
{
"DBProxy": {
        "DBProxyName": "proxyExample",
        "DBProxyArn": "arn:aws:rds:us-east-1:123456789012:db-
proxy:prx-0123a01b12345c0ab",
        "EngineFamily": "MYSQL",
        "VpcId": "vpc-1234567",
        "VpcSecuritytGroupIds": [
            "sg-1234",
            "sg-5678",
            "sg-9101"
        ],
        "VpcSubnetIds": [
            "subnetgroup1",
            "subnetgroup2"
        ],
        "Auth": "[
            {
                "Description": "proxydescription1",
                "AuthScheme": "SECRETS",
                "SecretArn": "arn:aws:secretsmanager:us-
west-2:123456789123:secret:proxysecret1-Abcd1e",
```

```
                "IAMAuth": "DISABLED"
            }
        ]",
        "RoleArn": "arn:aws:iam::12345678912:role/ProxyRole",
        "Endpoint": "proxyExample.proxy-ab0cd1efghij.us-east-1.rds.amazonaws.com",
        "RequireTLS": false,
        "IdleClientTimeout": 1800,
        "DebuggingLogging": false,
        "CreatedDate": "2023-04-05T16:09:33.452000+00:00",
        "UpdatedDate": "2023-04-13T01:49:38.568000+00:00"
    }
}
```

Para obtener más información, consulte Creación de un RDS Proxy en la Guía del usuario de Amazon RDS y Creación de un RDS Proxy en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte CreateDbProxy en la Referencia de comandos de la AWS CLI.

`create-db-security-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-security-group`.

AWS CLI

Para crear un grupo de seguridad de base de datos de Amazon RDS

El siguiente comando `create-db-security-group` crea un nuevo grupo de seguridad de base de datos de Amazon RDS:

```
aws rds create-db-security-group --db-security-group-name mysecgroup --db-security-group-description "My Test Security Group"
```

En el ejemplo, el nuevo grupo de seguridad de base de datos recibe el nombre `mysecgroup` y tiene una descripción.

Salida:

```
{
    "DBSecurityGroup": {
        "OwnerId": "123456789012",
        "DBSecurityGroupName": "mysecgroup",
```

```
        "DBSecurityGroupDescription": "My Test Security Group",
        "VpcId": "vpc-a1b2c3d4",
        "EC2SecurityGroups": [],
        "IPRanges": [],
        "DBSecurityGroupArn": "arn:aws:rds:us-west-2:123456789012:secgrp:mysecgroup"
    }
}
```

- Para obtener información sobre la API, consulte CreateDbSecurityGroup en la Referencia de comandos de la AWS CLI.

`create-db-shard-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-shard-group`.

AWS CLI

Ejemplo 1: crear un clúster de base de datos principal en Aurora PostgreSQL

En el siguiente ejemplo de `create-db-cluster`, se crea un clúster de base de datos principal de SQL en Aurora PostgreSQL que es compatible con Aurora sin servidor versión 2 y Aurora Limitless Database.

```
aws rds create-db-cluster \
    --db-cluster-identifier my-sv2-cluster \
    --engine aurora-postgresql \
    --engine-version 15.2-limitless \
    --storage-type aurora-iopt1 \
    --serverless-v2-scaling-configuration MinCapacity=2,MaxCapacity=16 \
    --enable-limitless-database \
    --master-username myuser \
    --master-user-password mypassword \
    --enable-cloudwatch-logs-exports postgresql
```

Salida:

```
{
    "DBCluster": {
        "AllocatedStorage": 1,
        "AvailabilityZones": [
            "us-east-2b",
            "us-east-2c",
```

```
            "us-east-2a"
        ],
        "BackupRetentionPeriod": 1,
        "DBClusterIdentifier": "my-sv2-cluster",
        "DBClusterParameterGroup": "default.aurora-postgresql15",
        "DBSubnetGroup": "default",
        "Status": "creating",
        "Endpoint": "my-sv2-cluster.cluster-cekycexample.us-
east-2.rds.amazonaws.com",
        "ReaderEndpoint": "my-sv2-cluster.cluster-ro-cekycexample.us-
east-2.rds.amazonaws.com",
        "MultiAZ": false,
        "Engine": "aurora-postgresql",
        "EngineVersion": "15.2-limitless",
        "Port": 5432,
        "MasterUsername": "myuser",
        "PreferredBackupWindow": "06:05-06:35",
        "PreferredMaintenanceWindow": "mon:08:25-mon:08:55",
        "ReadReplicaIdentifiers": [],
        "DBClusterMembers": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-########",
                "Status": "active"
            }
        ],
        "HostedZoneId": "Z2XHWR1EXAMPLE",
        "StorageEncrypted": false,
        "DbClusterResourceId": "cluster-XYEDT6ML6FHIXH4Q2J1EXAMPLE",
        "DBClusterArn": "arn:aws:rds:us-east-2:123456789012:cluster:my-sv2-cluster",
        "AssociatedRoles": [],
        "IAMDatabaseAuthenticationEnabled": false,
        "ClusterCreateTime": "2024-02-19T16:24:07.771000+00:00",
        "EnabledCloudwatchLogsExports": [
            "postgresql"
        ],
        "EngineMode": "provisioned",
        "DeletionProtection": false,
        "HttpEndpointEnabled": false,
        "CopyTagsToSnapshot": false,
        "CrossAccountClone": false,
        "DomainMemberships": [],
        "TagList": [],
        "StorageType": "aurora-iopt1",
```

```
        "AutoMinorVersionUpgrade": true,
        "ServerlessV2ScalingConfiguration": {
            "MinCapacity": 2.0,
            "MaxCapacity": 16.0
        },
        "NetworkType": "IPV4",
        "IOOptimizedNextAllowedModificationTime":
 "2024-03-21T16:24:07.781000+00:00",
        "LimitlessDatabase": {
            "Status": "not-in-use",
            "MinRequiredACU": 96.0
        }
    }
}
```

Ejemplo 2: crear la instancia de base de datos principal (de escritura)

En el siguiente ejemplo de `create-db-instance`, se crea una instancia de base de datos principal (de escritura) en Aurora sin servidor versión 2. Cuando usa la consola para crear un clúster de base de datos, Amazon RDS crea automáticamente la instancia de base de datos de escritura para el clúster de base de datos. Sin embargo, cuando usa la CLI de AWS para crear un clúster de base de datos, debe crear expresamente la instancia de base de datos escritura para su clúster de base de datos mediante el comando de la CLI `create-db-instance` AWS.

```
aws rds create-db-instance \
    --db-instance-identifier my-sv2-instance \
    --db-cluster-identifier my-sv2-cluster \
    --engine aurora-postgresql \
    --db-instance-class db.serverless
```

Salida:

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "my-sv2-instance",
        "DBInstanceClass": "db.serverless",
        "Engine": "aurora-postgresql",
        "DBInstanceStatus": "creating",
        "MasterUsername": "myuser",
        "AllocatedStorage": 1,
        "PreferredBackupWindow": "06:05-06:35",
        "BackupRetentionPeriod": 1,
```

```
        "DBSecurityGroups": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-########",
                "Status": "active"
            }
        ],
        "DBParameterGroups": [
            {
                "DBParameterGroupName": "default.aurora-postgresql15",
                "ParameterApplyStatus": "in-sync"
            }
        ],
        "DBSubnetGroup": {
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-########",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-########",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-2c"
                    },
                    "SubnetOutpost": {},
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-########",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-2a"
                    },
                    "SubnetOutpost": {},
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-########",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-2b"
                    },
                    "SubnetOutpost": {},
                    "SubnetStatus": "Active"
                }
            ]
```

```
        },
        "PreferredMaintenanceWindow": "fri:09:01-fri:09:31",
        "PendingModifiedValues": {
            "PendingCloudwatchLogsExports": {
                "LogTypesToEnable": [
                    "postgresql"
                ]
            }
        },
        "MultiAZ": false,
        "EngineVersion": "15.2-limitless",
        "AutoMinorVersionUpgrade": true,
        "ReadReplicaDBInstanceIdentifiers": [],
        "LicenseModel": "postgresql-license",
        "OptionGroupMemberships": [
            {
                "OptionGroupName": "default:aurora-postgresql-15",
                "Status": "in-sync"
            }
        ],
        "PubliclyAccessible": false,
        "StorageType": "aurora-iopt1",
        "DbInstancePort": 0,
        "DBClusterIdentifier": "my-sv2-cluster",
        "StorageEncrypted": false,
        "DbiResourceId": "db-BIQTE3B3K3RM7M74SK5EXAMPLE",
        "CACertificateIdentifier": "rds-ca-rsa2048-g1",
        "DomainMemberships": [],
        "CopyTagsToSnapshot": false,
        "MonitoringInterval": 0,
        "PromotionTier": 1,
        "DBInstanceArn": "arn:aws:rds:us-east-2:123456789012:db:my-sv2-instance",
        "IAMDatabaseAuthenticationEnabled": false,
        "PerformanceInsightsEnabled": false,
        "DeletionProtection": false,
        "AssociatedRoles": [],
        "TagList": [],
        "CustomerOwnedIpEnabled": false,
        "BackupTarget": "region",
        "NetworkType": "IPV4",
        "StorageThroughput": 0,
        "CertificateDetails": {
            "CAIdentifier": "rds-ca-rsa2048-g1"
        },
```

```
        "DedicatedLogVolume": false
    }
}
```

Ejemplo 3: crear el grupo de partición de base de datos

En el siguiente ejemplo de `create-db-shard-group`, se crea un grupo de partición de base de datos en el clúster de base de datos principal de Aurora PostgreSQL.

```
aws rds create-db-shard-group \
    --db-shard-group-identifier my-db-shard-group \
    --db-cluster-identifier my-sv2-cluster \
    --max-acu 768
```

Salida:

```
{
    "DBShardGroupResourceId": "shardgroup-a6e3a0226aa243e2ac6c7a1234567890",
    "DBShardGroupIdentifier": "my-db-shard-group",
    "DBClusterIdentifier": "my-sv2-cluster",
    "MaxACU": 768.0,
    "ComputeRedundancy": 0,
    "Status": "creating",
    "PubliclyAccessible": false,
    "Endpoint": "my-sv2-cluster.limitless-cekycexample.us-east-2.rds.amazonaws.com"
}
```

Para obtener más información, consulte Uso de Aurora Serverless v2 en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte CreateDbShardGroup en la Referencia de comandos de la AWS CLI.

`create-db-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-snapshot`.

AWS CLI

Creación de una instantánea de base de datos

En el siguiente ejemplo `create-db-snapshot`, se crea una instantánea de base de datos.

```
aws rds create-db-snapshot \
    --db-instance-identifier database-mysql \
    --db-snapshot-identifier mydbsnapshot
```

Salida:

```
{
    "DBSnapshot": {
        "DBSnapshotIdentifier": "mydbsnapshot",
        "DBInstanceIdentifier": "database-mysql",
        "Engine": "mysql",
        "AllocatedStorage": 100,
        "Status": "creating",
        "Port": 3306,
        "AvailabilityZone": "us-east-1b",
        "VpcId": "vpc-6594f31c",
        "InstanceCreateTime": "2019-04-30T15:45:53.663Z",
        "MasterUsername": "admin",
        "EngineVersion": "5.6.40",
        "LicenseModel": "general-public-license",
        "SnapshotType": "manual",
        "Iops": 1000,
        "OptionGroupName": "default:mysql-5-6",
        "PercentProgress": 0,
        "StorageType": "io1",
        "Encrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE",
        "DBSnapshotArn": "arn:aws:rds:us-east-1:123456789012:snapshot:mydbsnapshot",
        "IAMDatabaseAuthenticationEnabled": false,
        "ProcessorFeatures": [],
        "DbiResourceId": "db-AKIAIOSFODNN7EXAMPLE"
    }
}
```

Para obtener más información, consulte Creación de una instantánea de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte CreateDBSnapshot en la Referencia de comandos de la AWS CLI.

`create-db-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-db-subnet-group`.

AWS CLI

Para crear un grupo de subredes de base de datos

En el siguiente ejemplo de `create-db-subnet-group`, se crea un grupo de subredes de base de datos denominado `mysubnetgroup` utilizando las subredes existentes.

```
aws rds create-db-subnet-group \
    --db-subnet-group-name mysubnetgroup \
    --db-subnet-group-description "test DB subnet group" \
    --subnet-ids
 '["subnet-0a1dc4e1a6f123456","subnet-070dd7ecb3aaaaaaa","subnet-00f5b198bc0abcdef"]'
```

Salida:

```
{
    "DBSubnetGroup": {
        "DBSubnetGroupName": "mysubnetgroup",
        "DBSubnetGroupDescription": "test DB subnet group",
        "VpcId": "vpc-0f08e7610a1b2c3d4",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-070dd7ecb3aaaaaaa",
                "SubnetAvailabilityZone": {
                    "Name": "us-west-2b"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-00f5b198bc0abcdef",
                "SubnetAvailabilityZone": {
                    "Name": "us-west-2d"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-0a1dc4e1a6f123456",
                "SubnetAvailabilityZone": {
```

```
                    "Name": "us-west-2b"
                },
                "SubnetStatus": "Active"
            }
        ],
        "DBSubnetGroupArn": "arn:aws:rds:us-
west-2:0123456789012:subgrp:mysubnetgroup"
    }
}
```

Para obtener más información, consulte Creación de una instancia de base de datos en una VPC en la Guía del usuario de Amazon RDS.

- Para obtener detalles sobre la API, consulte CreateDbSubnetGroup en la Referencia de comandos de la AWS CLI.

`create-event-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-event-subscription`.

AWS CLI

Para crear una suscripción de evento

En el siguiente ejemplo de `create-event-subscription`, se crea una suscripción para eventos de copia de seguridad y recuperación de instancias de base de datos en la cuenta de AWS actual. Las notificaciones se envían a un tema de Amazon Simple Notification Service, especificado por `--sns-topic-arn`.

```
aws rds create-event-subscription \
    --subscription-name my-instance-events \
    --source-type db-instance \
    --event-categories '["backup","recovery"]' \
    --sns-topic-arn arn:aws:sns:us-east-1:123456789012:interesting-events
```

Salida:

```
{
    "EventSubscription": {
        "Status": "creating",
        "CustSubscriptionId": "my-instance-events",
```

```
        "SubscriptionCreationTime": "Tue Jul 31 23:22:01 UTC 2018",
        "EventCategoriesList": [
            "backup",
            "recovery"
        ],
        "SnsTopicArn": "arn:aws:sns:us-east-1:123456789012:interesting-events",
        "CustomerAwsId": "123456789012",
        "EventSubscriptionArn": "arn:aws:rds:us-east-1:123456789012:es:my-instance-
events",
        "SourceType": "db-instance",
        "Enabled": true
    }
}
```

- Para obtener detalles sobre la API, consulte CreateEventSubscription en la Referencia de comandos de la AWS CLI.

`create-global-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-global-cluster`.

AWS CLI

Para crear un clúster de base de datos global

En el siguiente ejemplo de `create-global-cluster`, se crea un nuevo clúster de base de datos global compatible con Aurora MySQL.

```
aws rds create-global-cluster \
    --global-cluster-identifier myglobalcluster \
    --engine aurora-mysql
```

Salida:

```
{
    "GlobalCluster": {
        "GlobalClusterIdentifier": "myglobalcluster",
        "GlobalClusterResourceId": "cluster-f0e523bfe07aabb",
        "GlobalClusterArn": "arn:aws:rds::123456789012:global-
cluster:myglobalcluster",
        "Status": "available",
        "Engine": "aurora-mysql",
```

```
        "EngineVersion": "5.7.mysql_aurora.2.07.2",
        "StorageEncrypted": false,
        "DeletionProtection": false,
        "GlobalClusterMembers": []
    }
}
```

Para obtener más información, consulte Creating an Aurora global database en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte CreateGlobalCluster en la Referencia de comandos de la AWS CLI.

`create-option-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-option-group`.

AWS CLI

Para crear un grupo de opción de Amazon RDS

El siguiente comando `create-option-group` crea un nuevo grupo de opciones de Amazon RDS para la versión de `Oracle Enterprise Edition 11.2`, is named ``MyOptionGroup e incluye una descripción.

```
aws rds create-option-group \
    --option-group-name MyOptionGroup \
    --engine-name oracle-ee \
    --major-engine-version 11.2 \
    --option-group-description "Oracle Database Manager Database Control"
```

Salida:

```
{
    "OptionGroup": {
        "OptionGroupName": "myoptiongroup",
        "OptionGroupDescription": "Oracle Database Manager Database Control",
        "EngineName": "oracle-ee",
        "MajorEngineVersion": "11.2",
        "Options": [],
        "AllowsVpcAndNonVpcInstanceMemberships": true,
        "OptionGroupArn": "arn:aws:rds:us-west-2:123456789012:og:myoptiongroup"
```

```
    }
}
```

- Para obtener información sobre la API, consulte CreateOptionGroup en la Referencia de comandos de la AWS CLI.

`delete-blue-green-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-blue-green-deployment`.

AWS CLI

Ejemplo 1: eliminar recursos en un entorno verde de una instancia de base de datos de RDS para MySQL

El siguiente ejemplo de `delete-blue-green-deployment` elimina los recursos de un entorno verde para un RDS de una instancia de base de datos en MySQL.

```
aws rds delete-blue-green-deployment \
    --blue-green-deployment-identifier bgd-v53303651eexfake \
    --delete-target
```

Salida:

```
{
    "BlueGreenDeployment": {
        "BlueGreenDeploymentIdentifier": "bgd-v53303651eexfake",
        "BlueGreenDeploymentName": "bgd-cli-test-instance",
        "Source": "arn:aws:rds:us-east-1:123456789012:db:my-db-instance",
        "Target": "arn:aws:rds:us-east-1:123456789012:db:my-db-instance-green-
rkfbpe",
        "SwitchoverDetails": [
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-green-rkfbpe",
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-1",
```

```
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-1-green-j382ha",
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-2",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-2-green-ejv4ao",
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-3",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-3-green-vlpz3t",
                "Status": "AVAILABLE"
            }
        ],
        "Tasks": [
            {
                "Name": "CREATING_READ_REPLICA_OF_SOURCE",
                "Status": "COMPLETED"
            },
            {
                "Name": "DB_ENGINE_VERSION_UPGRADE",
                "Status": "COMPLETED"
            },
            {
                "Name": "CONFIGURE_BACKUPS",
                "Status": "COMPLETED"
            },
            {
                "Name": "CREATING_TOPOLOGY_OF_SOURCE",
                "Status": "COMPLETED"
            }
        ],
        "Status": "DELETING",
        "CreateTime": "2022-02-25T21:18:51.183000+00:00",
        "DeleteTime": "2022-02-25T22:25:31.331000+00:00"
    }
}
```

Para obtener más información, consulte Eliminación de una implementación azul/verde en la Guía del usuario de Amazon RDS.

Ejemplo 2: eliminar recursos en un entorno verde de un clúster de base de datos de Aurora MySQL

El siguiente ejemplo de `delete-blue-green-deployment` elimina los recursos de un entorno verde para un clúster de base de datos en Aurora MySQL.

```
aws rds delete-blue-green-deployment \
    --blue-green-deployment-identifier bgd-wi89nwzglccsfake \
    --delete-target
```

Salida:

```
{
    "BlueGreenDeployment": {
        "BlueGreenDeploymentIdentifier": "bgd-wi89nwzglccsfake",
        "BlueGreenDeploymentName": "my-blue-green-deployment",
        "Source": "arn:aws:rds:us-east-1:123456789012:cluster:my-aurora-mysql-
cluster",
        "Target": "arn:aws:rds:us-east-1:123456789012:cluster:my-aurora-mysql-
cluster-green-3rnukl",
        "SwitchoverDetails": [
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster:my-
aurora-mysql-cluster",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:cluster:my-
aurora-mysql-cluster-green-3rnukl",
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-aurora-
mysql-cluster-1",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-aurora-
mysql-cluster-1-green-gpmaxf",
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-aurora-
mysql-cluster-2",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-aurora-
mysql-cluster-2-green-j2oajq",
```

```
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-aurora-
mysql-cluster-3",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-aurora-
mysql-cluster-3-green-mkxies",
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-excluded-member-endpoint",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-excluded-member-endpoint-green-4sqjrq",
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-reader-endpoint",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-reader-endpoint-green-gwwzlg",
                "Status": "AVAILABLE"
            }
        ],
        "Tasks": [
            {
                "Name": "CREATING_READ_REPLICA_OF_SOURCE",
                "Status": "COMPLETED"
            },
            {
                "Name": "DB_ENGINE_VERSION_UPGRADE",
                "Status": "COMPLETED"
            },
            {
                "Name": "CREATE_DB_INSTANCES_FOR_CLUSTER",
                "Status": "COMPLETED"
            },
            {
                "Name": "CREATE_CUSTOM_ENDPOINTS",
                "Status": "COMPLETED"
            }
        ],
        "Status": "DELETING",
        "CreateTime": "2022-02-25T21:12:00.288000+00:00",
```

```
        "DeleteTime": "2022-02-25T22:29:11.336000+00:00"
    }
}
```

Para obtener más información, consulte Eliminación de una implementación azul/verde en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DeleteBlueGreenDeployment en la Referencia de comandos de la AWS CLI.

`delete-db-cluster-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-cluster-endpoint`.

AWS CLI

Para eliminar un punto de conexión de clúster de base de datos personalizado

En el siguiente ejemplo de `delete-db-cluster-endpoint` se elimina el punto de conexión de clúster de base de datos personalizado especificado.

```
aws rds delete-db-cluster-endpoint \
    --db-cluster-endpoint-identifier mycustomendpoint
```

Salida:

```
{
    "DBClusterEndpointIdentifier": "mycustomendpoint",
    "DBClusterIdentifier": "mydbcluster",
    "DBClusterEndpointResourceIdentifier": "cluster-endpoint-ANPAJ4AE5446DAEXAMPLE",
    "Endpoint": "mycustomendpoint.cluster-custom-cnpexample.us-
east-1.rds.amazonaws.com",
    "Status": "deleting",
    "EndpointType": "CUSTOM",
    "CustomEndpointType": "READER",
    "StaticMembers": [
        "dbinstance1",
        "dbinstance2",
        "dbinstance3"
    ],
    "ExcludedMembers": [],
```

```
    "DBClusterEndpointArn": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:mycustomendpoint"
}
```

Para obtener más información, consulte Amazon Aurora Connection Management en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DeleteDbClusterEndpoint en la Referencia de comandos de la AWS CLI.

`delete-db-cluster-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-cluster-parameter-group`.

AWS CLI

Para eliminar un grupo de parámetros de clúster de base de datos

En el siguiente ejemplo de `delete-db-cluster-parameter-group`, se elimina el grupo de parámetros de clúster de base de datos especificado.

```
aws rds delete-db-cluster-parameter-group \
    --db-cluster-parameter-group-name mydbclusterparametergroup
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with DB Parameter Groups and DB Cluster Parameter Groups en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte DeleteDbClusterParameterGroup en la Referencia de comandos de la AWS CLI.

`delete-db-cluster-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-cluster-snapshot`.

AWS CLI

Para eliminar una instantánea de clúster de base de datos

En el siguiente ejemplo de `delete-db-cluster-snapshot`, se elimina la instantánea del clúster de base de datos especificada.

```
aws rds delete-db-cluster-snapshot \
    --db-cluster-snapshot-identifier mydbclustersnapshot
```

Salida:

```
{
    "DBClusterSnapshot": {
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1b",
            "us-east-1e"
        ],
        "DBClusterSnapshotIdentifier": "mydbclustersnapshot",
        "DBClusterIdentifier": "mydbcluster",
        "SnapshotCreateTime": "2019-06-18T21:21:00.469Z",
        "Engine": "aurora-mysql",
        "AllocatedStorage": 0,
        "Status": "available",
        "Port": 0,
        "VpcId": "vpc-6594f31c",
        "ClusterCreateTime": "2019-04-15T14:18:42.785Z",
        "MasterUsername": "myadmin",
        "EngineVersion": "5.7.mysql_aurora.2.04.2",
        "LicenseModel": "aurora-mysql",
        "SnapshotType": "manual",
        "PercentProgress": 100,
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE",
        "DBClusterSnapshotArn": "arn:aws:rds:us-east-1:123456789012:cluster-
snapshot:mydbclustersnapshot",
        "IAMDatabaseAuthenticationEnabled": false
    }
}
```

Para obtener más información, consulte Deleting a Snapshot en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte DeleteDbClusterSnapshot en la Referencia de comandos de la AWS CLI.

`delete-db-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-cluster`.

AWS CLI

Ejemplo 1: eliminar una instancia de base de datos en un clúster de base de datos

En el siguiente ejemplo de `delete-db-instance`, se elimina la instancia de base de datos final de un clúster de base de datos. No puede eliminar un clúster de base de datos si contiene instancias de base de datos que no están en el estado de eliminación. No puede tomar una instantánea final al eliminar una instancia de base de datos de un clúster de base de datos.

```
aws rds delete-db-instance \
    --db-instance-identifier database-3
```

Salida:

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "database-3",
        "DBInstanceClass": "db.r4.large",
        "Engine": "aurora-postgresql",
        "DBInstanceStatus": "deleting",

    ...output omitted...

    }
}
```

Para obtener más información, consulte Deleting a DB Instance in an Aurora DB Cluster en la Guía del usuario de Amazon Aurora.

Ejemplo 2: eliminar un clúster de una base de datos

En el siguiente ejemplo de `delete-db-cluster`, se elimina el clúster de base de datos denominado `mycluster` y se toma una instantánea final con el nombre `mycluster-final-snapshot`. El estado del clúster de base de datos está disponible mientras se realiza la instantánea. Para seguir el progreso de la eliminación, utilice el comando de CLI `describe-db-clusters`.

```
aws rds delete-db-cluster \
```

```
    --db-cluster-identifier mycluster \
    --no-skip-final-snapshot \
    --final-db-snapshot-identifier mycluster-final-snapshot
```

Salida:

```
{
    "DBCluster": {
        "AllocatedStorage": 20,
        "AvailabilityZones": [
            "eu-central-1b",
            "eu-central-1c",
            "eu-central-1a"
        ],
        "BackupRetentionPeriod": 7,
        "DBClusterIdentifier": "mycluster",
        "DBClusterParameterGroup": "default.aurora-postgresql10",
        "DBSubnetGroup": "default-vpc-aa11bb22",
        "Status": "available",

    ...output omitted...

    }
}
```

Para obtener más información, consulte Aurora Clusters with a Single DB Instance en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte DeleteDbCluster en la Referencia de comandos de la AWS CLI.

`delete-db-instance-automated-backup`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-instance-automated-backup`.

AWS CLI

Para eliminar una copia de seguridad automatizada replicada de una región

En el siguiente ejemplo de `delete-db-instance-automated-backup`, se elimina la copia de seguridad automatizada con el ARN (Amazon Resource Name) especificado.

```
aws rds delete-db-instance-automated-backup \
    --db-instance-automated-backups-arn "arn:aws:rds:us-west-2:123456789012:auto-backup:ab-jkib2gfq5rv7replzadausbrktni2bn4example"
```

Salida:

```
{
    "DBInstanceAutomatedBackup": {
        "DBInstanceArn": "arn:aws:rds:us-east-1:123456789012:db:new-orcl-db",
        "DbiResourceId": "db-JKIB2GFQ5RV7REPLZA4EXAMPLE",
        "Region": "us-east-1",
        "DBInstanceIdentifier": "new-orcl-db",
        "RestoreWindow": {},
        "AllocatedStorage": 20,
        "Status": "deleting",
        "Port": 1521,
        "AvailabilityZone": "us-east-1b",
        "VpcId": "vpc-########",
        "InstanceCreateTime": "2020-12-04T15:28:31Z",
        "MasterUsername": "admin",
        "Engine": "oracle-se2",
        "EngineVersion": "12.1.0.2.v21",
        "LicenseModel": "bring-your-own-license",
        "OptionGroupName": "default:oracle-se2-12-1",
        "Encrypted": false,
        "StorageType": "gp2",
        "IAMDatabaseAuthenticationEnabled": false,
        "BackupRetentionPeriod": 7,
        "DBInstanceAutomatedBackupsArn": "arn:aws:rds:us-west-2:123456789012:auto-backup:ab-jkib2gfq5rv7replzadausbrktni2bn4example"
    }
}
```

Para obtener más información, consulte Deleting replicated backups en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DeleteDbInstanceAutomatedBackup en la Referencia de comandos de la AWS CLI.

`delete-db-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-instance`.

AWS CLI

Para eliminar una instancia de base de datos

En el siguiente ejemplo `delete-db-instance`, se elimina la instancia de base de datos especificada tras crear una instantánea de base de datos final denominada `test-instance-final-snap`.

```
aws rds delete-db-instance \
    --db-instance-identifier test-instance \
    --final-db-snapshot-identifier test-instance-final-snap
```

Salida:

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "test-instance",
        "DBInstanceStatus": "deleting",
        ...some output truncated...
    }
}
```

- Para obtener información sobre la API, consulte DeleteDBInstance en la Referencia de comandos de la AWS CLI.

`delete-db-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-parameter-group`.

AWS CLI

Eliminación de un grupo de parámetros de base de datos

En el siguiente ejemplo `command`, se elimina un grupo de parámetros de base de datos.

```
aws rds delete-db-parameter-group \
    --db-parameter-group-name mydbparametergroup
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Trabajo con los grupos de parámetros de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DeleteDBParameterGroup en la Referencia de comandos de la AWS CLI.

`delete-db-proxy-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-proxy-endpoint`.

AWS CLI

Para eliminar un punto de conexión de proxy de base de datos para una base de datos de RDS

En el siguiente ejemplo de `delete-db-proxy-endpoint`, se elimina un punto de conexión de proxy de base de datos de la base de datos de destino.

```
aws rds delete-db-proxy-endpoint \
    --db-proxy-endpoint-name proxyEP1
```

Salida:

```
{
"DBProxyEndpoint":
    {
        "DBProxyEndpointName": "proxyEP1",
        "DBProxyEndpointArn": "arn:aws:rds:us-east-1:123456789012:db-proxy-
endpoint:prx-endpoint-0123a01b12345c0ab",
        "DBProxyName": "proxyExample",
        "Status": "deleting",
        "VpcId": "vpc-1234567",
        "VpcSecurityGroupIds": [
            "sg-1234",
            "sg-5678"
        ],
        "VpcSubnetIds": [
            "subnetgroup1",
            "subnetgroup2"
        ],
        "Endpoint": "proxyEP1.endpoint.proxy-ab0cd1efghij.us-
east-1.rds.amazonaws.com",
        "CreatedDate": "2023-04-13T01:49:38.568000+00:00",
        "TargetRole": "READ_ONLY",
        "IsDefault": false
    }
```

```
}
```

Para obtener más información, consulte Deleting a proxy endpoint en la Guía del usuario de Amazon RDS y Deleting a proxy endpoint en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DeleteDbProxyEndpoint en la Referencia de comandos de la AWS CLI.

`delete-db-proxy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-proxy`.

AWS CLI

Para eliminar un proxy de base de datos para una base de datos de RDS

En el siguiente ejemplo de `delete-db-proxy` se elimina un proxy de base de datos.

```
aws rds delete-db-proxy \
    --db-proxy-name proxyExample
```

Salida:

```
{
        "DBProxy":
        {
            "DBProxyName": "proxyExample",
            "DBProxyArn": "arn:aws:rds:us-east-1:123456789012:db-
proxy:prx-0123a01b12345c0ab",
            "Status": "deleting",
            "EngineFamily": "PostgreSQL",
            "VpcId": "vpc-1234567",
            "VpcSecurityGroupIds": [
                "sg-1234",
                "sg-5678"
            ],
            "VpcSubnetIds": [
                "subnetgroup1",
                "subnetgroup2"
            ],
            "Auth": "[
                {
                "Description": "proxydescription`"
```

```
                "AuthScheme": "SECRETS",
                "SecretArn": "arn:aws:secretsmanager:us-
west-2:123456789123:secret:proxysecret1-Abcd1e",
                "IAMAuth": "DISABLED"
                } ],
            "RoleArn": "arn:aws:iam::12345678912:role/ProxyPostgreSQLRole",
            "Endpoint": "proxyExample.proxy-ab0cd1efghij.us-
east-1.rds.amazonaws.com",
            "RequireTLS": false,
            "IdleClientTimeout": 1800,
            "DebuggingLogging": false,
        "CreatedDate": "2023-04-05T16:09:33.452000+00:00",
        "UpdatedDate": "2023-04-13T01:49:38.568000+00:00"
    }
}
```

Para obtener más información, consulte Eliminación de un RDS Proxy en la Guía del usuario de Amazon RDS y Eliminación de un RDS Proxy en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DeleteDbProxy en la Referencia de comandos de AWS CLI.

`delete-db-security-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-security-group`.

AWS CLI

Para eliminar un grupo de seguridad de la base de datos

En el siguiente ejemplo de `delete-db-security-group`, se elimina un grupo de seguridad denominado `mysecuritygroup`.

```
aws rds delete-db-security-group \
    --db-security-group-name mysecuritygroup
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with DB security groups (EC2-Classic platform) en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DeleteDbSecurityGroup en la Referencia de comandos de la AWS CLI.

delete-db-shard-group

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-shard-group`.

AWS CLI

Ejemplo 1: eliminar un grupo de partición de base de datos sin éxito

El siguiente ejemplo de `delete-db-shard-group` muestra el error que se produce cuando se intenta eliminar un grupo de partición de base de datos antes de eliminar todas las bases de datos y los esquemas.

```
aws rds delete-db-shard-group \
    --db-shard-group-identifier limitless-test-shard-grp
```

Salida:

```
An error occurred (InvalidDBShardGroupState) when calling the DeleteDBShardGroup
 operation: Unable to delete the DB shard group limitless-test-db-shard-group.
Delete all of your Limitless Database databases and schemas, then try again.
```

Ejemplo 2: eliminar un grupo de partición de base de datos correctamente

En el siguiente ejemplo de `delete-db-shard-group`, se elimina un grupo de partición de base de datos después de haber eliminado todas las bases de datos y los esquemas, incluido el esquema `public`.

```
aws rds delete-db-shard-group \
    --db-shard-group-identifier limitless-test-shard-grp
```

Salida:

```
{
    "DBShardGroupResourceId": "shardgroup-7bb446329da94788b3f957746example",
    "DBShardGroupIdentifier": "limitless-test-shard-grp",
    "DBClusterIdentifier": "limitless-test-cluster",
    "MaxACU": 768.0,
    "ComputeRedundancy": 0,
    "Status": "deleting",
    "PubliclyAccessible": true,
    "Endpoint": "limitless-test-cluster.limitless-cekycexample.us-
east-2.rds.amazonaws.com"
```

```
}
```

Para obtener más información, consulte Eliminación de clústeres e instancias de base de datos de Aurora en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DeleteDbShardGroup en la Referencia de comandos de la AWS CLI.

`delete-db-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-snapshot`.

AWS CLI

Para eliminar una instantánea de base de datos

En el siguiente ejemplo de `delete-db-snapshot`, se elimina una instantánea de base de datos especificada.

```
aws rds delete-db-snapshot \
    --db-snapshot-identifier mydbsnapshot
```

Salida:

```
{
    "DBSnapshot": {
        "DBSnapshotIdentifier": "mydbsnapshot",
        "DBInstanceIdentifier": "database-mysql",
        "SnapshotCreateTime": "2019-06-18T22:08:40.702Z",
        "Engine": "mysql",
        "AllocatedStorage": 100,
        "Status": "deleted",
        "Port": 3306,
        "AvailabilityZone": "us-east-1b",
        "VpcId": "vpc-6594f31c",
        "InstanceCreateTime": "2019-04-30T15:45:53.663Z",
        "MasterUsername": "admin",
        "EngineVersion": "5.6.40",
        "LicenseModel": "general-public-license",
        "SnapshotType": "manual",
        "Iops": 1000,
        "OptionGroupName": "default:mysql-5-6",
```

```
        "PercentProgress": 100,
        "StorageType": "io1",
        "Encrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE",
        "DBSnapshotArn": "arn:aws:rds:us-east-1:123456789012:snapshot:mydbsnapshot",
        "IAMDatabaseAuthenticationEnabled": false,
        "ProcessorFeatures": [],
        "DbiResourceId": "db-AKIAIOSFODNN7EXAMPLE"
    }
}
```

Para obtener más información, consulte Deleting a Snapshot en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DeleteDbSnapshot en la Referencia de comandos de la AWS CLI.

`delete-db-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-db-subnet-group`.

AWS CLI

Para eliminar un grupo de subred de base de datos

En el siguiente ejemplo de `delete-db-subnet-group`, se elimina el grupo de subred de base de datos llamado `mysubnetgroup`.

```
aws rds delete-db-subnet-group --db-subnet-group-name mysubnetgroup
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with a DB instance in a VPC en la Guía del usuario de Amazon RDS.

- Para obtener detalles sobre la API, consulte DeleteDbSubnetGroup en la Referencia de comandos de la AWS CLI.

`delete-event-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-event-subscription`.

AWS CLI

Para eliminar la suscripción a un evento

En el siguiente ejemplo de `delete-event-subscription`, se elimina la suscripción a un evento especificado.

```
aws rds delete-event-subscription --subscription-name my-instance-events
```

Salida:

```
{
    "EventSubscription": {
        "EventSubscriptionArn": "arn:aws:rds:us-east-1:123456789012:es:my-instance-
events",
        "CustomerAwsId": "123456789012",
        "Enabled": false,
        "SourceIdsList": [
            "test-instance"
        ],
        "SourceType": "db-instance",
        "EventCategoriesList": [
            "backup",
            "recovery"
        ],
        "SubscriptionCreationTime": "2018-07-31 23:22:01.893",
        "CustSubscriptionId": "my-instance-events",
        "SnsTopicArn": "arn:aws:sns:us-east-1:123456789012:interesting-events",
        "Status": "deleting"
    }
}
```

- Para obtener información sobre la API, consulte DeleteEventSubscription en la Referencia de comandos de la AWS CLI.

`delete-global-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-global-cluster`.

AWS CLI

Para eliminar un clúster de base de datos global

En el siguiente ejemplo de `delete-global-cluster`, se elimina un nuevo clúster de base de datos global compatible con Aurora MySQL. El resultado muestra el clúster que va a eliminar, pero los comandos `describe-global-clusters` posteriores no generan una lista de ese clúster de base de datos.

```
aws rds delete-global-cluster \
    --global-cluster-identifier myglobalcluster
```

Salida:

```
{
    "GlobalCluster": {
        "GlobalClusterIdentifier": "myglobalcluster",
        "GlobalClusterResourceId": "cluster-f0e523bfe07aabb",
        "GlobalClusterArn": "arn:aws:rds::123456789012:global-
cluster:myglobalcluster",
        "Status": "available",
        "Engine": "aurora-mysql",
        "EngineVersion": "5.7.mysql_aurora.2.07.2",
        "StorageEncrypted": false,
        "DeletionProtection": false,
        "GlobalClusterMembers": []
    }
}
```

Para obtener más información, consulte Eliminación de una base de datos global de Amazon Aurora en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DeleteGlobalCluster en la Referencia de comandos de la AWS CLI.

`delete-option-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-option-group`.

AWS CLI

Para eliminar un grupo de opciones

En el siguiente ejemplo de `delete-option-group`, se elimina el grupo de opciones especificado.

```
aws rds delete-option-group \
    --option-group-name myoptiongroup
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de un grupo de opciones en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DeleteOptionGroup en la Referencia de comandos de la AWS CLI.

`deregister-db-proxy-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-db-proxy-targets`.

AWS CLI

Para anular el registro de un destino proxy de base de datos del grupo de destino de la base de datos

En el siguiente ejemplo de `deregister-db-proxy-targets`, se elimina la asociación entre el proxy `proxyExample` y su destino.

```
aws rds deregister-db-proxy-targets \
    --db-proxy-name proxyExample \
    --db-instance-identifiers database-1
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de un RDS Proxy en la Guía del usuario de Amazon RDS y Eliminación de un RDS Proxy en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DeregisterDbProxyTargets en la Referencia de comandos de la AWS CLI.

`describe-account-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-account-attributes`.

AWS CLI

Descripción de atributos de cuenta

En el siguiente ejemplo `describe-account-attributes`, se recuperan los atributos de la cuenta actual de AWS.

```
aws rds describe-account-attributes
```

Salida:

```
{
    "AccountQuotas": [
        {
            "Max": 40,
            "Used": 4,
            "AccountQuotaName": "DBInstances"
        },
        {
            "Max": 40,
            "Used": 0,
            "AccountQuotaName": "ReservedDBInstances"
        },
        {
            "Max": 100000,
            "Used": 40,
            "AccountQuotaName": "AllocatedStorage"
        },
        {
            "Max": 25,
            "Used": 0,
            "AccountQuotaName": "DBSecurityGroups"
        },
        {
            "Max": 20,
            "Used": 0,
            "AccountQuotaName": "AuthorizationsPerDBSecurityGroup"
        },
        {
            "Max": 50,
            "Used": 1,
            "AccountQuotaName": "DBParameterGroups"
        },
        {
            "Max": 100,
            "Used": 3,
            "AccountQuotaName": "ManualSnapshots"
```

```
        },
        {
            "Max": 20,
            "Used": 0,
            "AccountQuotaName": "EventSubscriptions"
        },
        {
            "Max": 50,
            "Used": 1,
            "AccountQuotaName": "DBSubnetGroups"
        },
        {
            "Max": 20,
            "Used": 1,
            "AccountQuotaName": "OptionGroups"
        },
        {
            "Max": 20,
            "Used": 6,
            "AccountQuotaName": "SubnetsPerDBSubnetGroup"
        },
        {
            "Max": 5,
            "Used": 0,
            "AccountQuotaName": "ReadReplicasPerMaster"
        },
        {
            "Max": 40,
            "Used": 1,
            "AccountQuotaName": "DBClusters"
        },
        {
            "Max": 50,
            "Used": 0,
            "AccountQuotaName": "DBClusterParameterGroups"
        },
        {
            "Max": 5,
            "Used": 0,
            "AccountQuotaName": "DBClusterRoles"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeAccountAttributes en la Referencia de comandos de la AWS CLI.

`describe-blue-green-deployments`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-blue-green-deployments`.

AWS CLI

Ejemplo 1: describir una implementación azul/verde de una instancia de base de datos de RDS una vez finalizada la creación

En el siguiente ejemplo de `describe-blue-green-deployment`, se recuperan los detalles de una implementación azul/verde una vez que se completa la creación.

```
aws rds describe-blue-green-deployments \
    --blue-green-deployment-identifier bgd-v53303651eexfake
```

Salida:

```
{
    "BlueGreenDeployments": [
        {
            "BlueGreenDeploymentIdentifier": "bgd-v53303651eexfake",
            "BlueGreenDeploymentName": "bgd-cli-test-instance",
            "Source": "arn:aws:rds:us-east-1:123456789012:db:my-db-instance",
            "Target": "arn:aws:rds:us-east-1:123456789012:db:my-db-instance-green-
rkfbpe",
            "SwitchoverDetails": [
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-green-rkfbpe",
                    "Status": "AVAILABLE"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-1",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-1-green-j382ha",
```

```
                    "Status": "AVAILABLE"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-2",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-2-green-ejv4ao",
                    "Status": "AVAILABLE"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-3",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-3-green-vlpz3t",
                    "Status": "AVAILABLE"
                }
            ],
            "Tasks": [
                {
                    "Name": "CREATING_READ_REPLICA_OF_SOURCE",
                    "Status": "COMPLETED"
                },
                {
                    "Name": "DB_ENGINE_VERSION_UPGRADE",
                    "Status": "COMPLETED"
                },
                {
                    "Name": "CONFIGURE_BACKUPS",
                    "Status": "COMPLETED"
                },
                {
                    "Name": "CREATING_TOPOLOGY_OF_SOURCE",
                    "Status": "COMPLETED"
                }
            ],
            "Status": "AVAILABLE",
            "CreateTime": "2022-02-25T21:18:51.183000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Visualización de una implementación azul/verde en la Guía del usuario de Amazon RDS.

Ejemplo 2: describir una implementación azul/verde para un clúster de base de datos en Aurora MySQL

En el siguiente ejemplo de `describe-blue-green-deployment`, se recuperan los detalles de una implementación azul/verde.

```
aws rds describe-blue-green-deployments \
    --blue-green-deployment-identifier bgd-wi89nwzglccsfake
```

Salida:

```
{
    "BlueGreenDeployments": [
        {
            "BlueGreenDeploymentIdentifier": "bgd-wi89nwzglccsfake",
            "BlueGreenDeploymentName": "my-blue-green-deployment",
            "Source": "arn:aws:rds:us-east-1:123456789012:cluster:my-aurora-mysql-
cluster",
            "Target": "arn:aws:rds:us-east-1:123456789012:cluster:my-aurora-mysql-
cluster-green-3rnukl",
            "SwitchoverDetails": [
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster:my-
aurora-mysql-cluster",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:cluster:my-
aurora-mysql-cluster-green-3rnukl",
                    "Status": "AVAILABLE"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-1",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-1-green-gpmaxf",
                    "Status": "AVAILABLE"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-2",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-2-green-j2oajq",
                    "Status": "AVAILABLE"
                },
                {
```

```
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-3",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-3-green-mkxies",
                    "Status": "AVAILABLE"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-excluded-member-endpoint",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-excluded-member-endpoint-green-4sqjrq",
                    "Status": "AVAILABLE"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-reader-endpoint",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-reader-endpoint-green-gwwzlg",
                    "Status": "AVAILABLE"
                }
            ],
            "Tasks": [
                {
                    "Name": "CREATING_READ_REPLICA_OF_SOURCE",
                    "Status": "COMPLETED"
                },
                {
                    "Name": "DB_ENGINE_VERSION_UPGRADE",
                    "Status": "COMPLETED"
                },
                {
                    "Name": "CREATE_DB_INSTANCES_FOR_CLUSTER",
                    "Status": "COMPLETED"
                },
                {
                    "Name": "CREATE_CUSTOM_ENDPOINTS",
                    "Status": "COMPLETED"
                }
            ],
            "Status": "AVAILABLE",
            "CreateTime": "2022-02-25T21:12:00.288000+00:00"
        }
    ]
```

```
}
```

Para obtener más información, consulte Visualización de una implementación azul/verde en la Guía del usuario de Amazon Aurora.

Ejemplo 3: describir una implementación azul/verde para un clúster de Aurora MySQL después de una transición

En el siguiente ejemplo de `describe-blue-green-deployment`, se recuperan los detalles sobre una implementación azul/verde después de que el entorno verde se haya convertido en el entorno de producción.

```
aws rds describe-blue-green-deployments \
    --blue-green-deployment-identifier bgd-wi89nwzglccsfake
```

Salida:

```
{
    "BlueGreenDeployments": [
        {
            "BlueGreenDeploymentIdentifier": "bgd-wi89nwzglccsfake",
            "BlueGreenDeploymentName": "my-blue-green-deployment",
            "Source": "arn:aws:rds:us-east-1:123456789012:cluster:my-aurora-mysql-
cluster-old1",
            "Target": "arn:aws:rds:us-east-1:123456789012:cluster:my-aurora-mysql-
cluster",
            "SwitchoverDetails": [
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster:my-
aurora-mysql-cluster-old1",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:cluster:my-
aurora-mysql-cluster",
                    "Status": "SWITCHOVER_COMPLETED"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-1-old1",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-1",
                    "Status": "SWITCHOVER_COMPLETED"
                },
                {
```

```
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-2-old1",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-2",
                    "Status": "SWITCHOVER_COMPLETED"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-3-old1",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-3",
                    "Status": "SWITCHOVER_COMPLETED"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-excluded-member-endpoint-old1",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-excluded-member-endpoint",
                    "Status": "SWITCHOVER_COMPLETED"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-reader-endpoint-old1",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-reader-endpoint",
                    "Status": "SWITCHOVER_COMPLETED"
                }
            ],
            "Tasks": [
                {
                    "Name": "CREATING_READ_REPLICA_OF_SOURCE",
                    "Status": "COMPLETED"
                },
                {
                    "Name": "DB_ENGINE_VERSION_UPGRADE",
                    "Status": "COMPLETED"
                },
                {
                    "Name": "CREATE_DB_INSTANCES_FOR_CLUSTER",
                    "Status": "COMPLETED"
                },
                {
                    "Name": "CREATE_CUSTOM_ENDPOINTS",
                    "Status": "COMPLETED"
```

```
                }
            ],
            "Status": "SWITCHOVER_COMPLETED",
            "CreateTime": "2022-02-25T22:38:49.522000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Visualización de una implementación azul/verde en la Guía del usuario de Amazon Aurora.

Ejemplo 4: describir una implementación azul/verde combinada

En el siguiente ejemplo de `describe-blue-green-deployment`, se recuperan los detalles de una implementación azul/verde combinada.

```
aws rds describe-blue-green-deployments
```

Salida:

```
{
    "BlueGreenDeployments": [
        {
            "BlueGreenDeploymentIdentifier": "bgd-wi89nwzgfakelccs",
            "BlueGreenDeploymentName": "my-blue-green-deployment",
            "Source": "arn:aws:rds:us-east-1:123456789012:cluster:my-aurora-mysql-
cluster",
            "Target": "arn:aws:rds:us-east-1:123456789012:cluster:my-aurora-mysql-
cluster-green-3rnukl",
            "SwitchoverDetails": [
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster:my-
aurora-mysql-cluster",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:cluster:my-
aurora-mysql-cluster-green-3rnukl",
                    "Status": "AVAILABLE"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-1",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-1-green-gpmaxf",
                    "Status": "AVAILABLE"
```

```
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-2",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-2-green-j2oajq",
                    "Status": "AVAILABLE"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-3",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-
aurora-mysql-cluster-3-green-mkxies",
                    "Status": "AVAILABLE"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-excluded-member-endpoint",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-excluded-member-endpoint-green-4sqjrq",
                    "Status": "AVAILABLE"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-reader-endpoint",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-reader-endpoint-green-gwwzlg",
                    "Status": "AVAILABLE"
                }
            ],
            "Tasks": [
                {
                    "Name": "CREATING_READ_REPLICA_OF_SOURCE",
                    "Status": "COMPLETED"
                },
                {
                    "Name": "DB_ENGINE_VERSION_UPGRADE",
                    "Status": "COMPLETED"
                },
                {
                    "Name": "CREATE_DB_INSTANCES_FOR_CLUSTER",
                    "Status": "COMPLETED"
                },
                {
```

```
                    "Name": "CREATE_CUSTOM_ENDPOINTS",
                    "Status": "COMPLETED"
                }
            ],
            "Status": "AVAILABLE",
            "CreateTime": "2022-02-25T21:12:00.288000+00:00"
        },
        {
            "BlueGreenDeploymentIdentifier": "bgd-v5330365fake1eex",
            "BlueGreenDeploymentName": "bgd-cli-test-instance",
            "Source": "arn:aws:rds:us-east-1:123456789012:db:my-db-instance-old1",
            "Target": "arn:aws:rds:us-east-1:123456789012:db:my-db-instance",
            "SwitchoverDetails": [
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-old1",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance",
                    "Status": "SWITCHOVER_COMPLETED"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-1-old1",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-1",
                    "Status": "SWITCHOVER_COMPLETED"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-2-old1",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-2",
                    "Status": "SWITCHOVER_COMPLETED"
                },
                {
                    "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-3-old1",
                    "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-3",
                    "Status": "SWITCHOVER_COMPLETED"
                }
            ],
            "Tasks": [
                {
```

```
                    "Name": "CREATING_READ_REPLICA_OF_SOURCE",
                    "Status": "COMPLETED"
                },
                {
                    "Name": "DB_ENGINE_VERSION_UPGRADE",
                    "Status": "COMPLETED"
                },
                {
                    "Name": "CONFIGURE_BACKUPS",
                    "Status": "COMPLETED"
                },
                {
                    "Name": "CREATING_TOPOLOGY_OF_SOURCE",
                    "Status": "COMPLETED"
                }
            ],
            "Status": "SWITCHOVER_COMPLETED",
            "CreateTime": "2022-02-25T22:33:22.225000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Visualización de una implementación azul/verde en la Guía del usuario de Amazon RDS y Visualización de una implementación azul/verde en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DescribeBlueGreenDeployments en la Referencia de comandos de la AWS CLI.

`describe-certificates`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-certificates`.

AWS CLI

Para describir certificados

En el siguiente ejemplo de `describe-certificates`, se recuperan los detalles del certificado asociado a la región predeterminada del usuario.

```
aws rds describe-certificates
```

Salida:


```
{
    "Certificates": [
        {
            "CertificateIdentifier": "rds-ca-ecc384-g1",
            "CertificateType": "CA",
            "Thumbprint": "2ee3dcc06e50192559b13929e73484354f23387d",
            "ValidFrom": "2021-05-24T22:06:59+00:00",
            "ValidTill": "2121-05-24T23:06:59+00:00",
            "CertificateArn": "arn:aws:rds:us-west-2::cert:rds-ca-ecc384-g1",
            "CustomerOverride": false
        },
        {
            "CertificateIdentifier": "rds-ca-rsa4096-g1",
            "CertificateType": "CA",
            "Thumbprint": "19da4f2af579a8ae1f6a0fa77aa5befd874b4cab",
            "ValidFrom": "2021-05-24T22:03:20+00:00",
            "ValidTill": "2121-05-24T23:03:20+00:00",
            "CertificateArn": "arn:aws:rds:us-west-2::cert:rds-ca-rsa4096-g1",
            "CustomerOverride": false
        },
        {
            "CertificateIdentifier": "rds-ca-rsa2048-g1",
            "CertificateType": "CA",
            "Thumbprint": "7c40cb42714b6fdb2b296f9bbd0e8bb364436a76",
            "ValidFrom": "2021-05-24T21:59:00+00:00",
            "ValidTill": "2061-05-24T22:59:00+00:00",
            "CertificateArn": "arn:aws:rds:us-west-2::cert:rds-ca-rsa2048-g1",
            "CustomerOverride": true,
            "CustomerOverrideValidTill": "2061-05-24T22:59:00+00:00"
        },
        {
            "CertificateIdentifier": "rds-ca-2019",
            "CertificateType": "CA",
            "Thumbprint": "d40ddb29e3750dffa671c3140bbf5f478d1c8096",
            "ValidFrom": "2019-08-22T17:08:50+00:00",
            "ValidTill": "2024-08-22T17:08:50+00:00",
            "CertificateArn": "arn:aws:rds:us-west-2::cert:rds-ca-2019",
            "CustomerOverride": false
        }
    ],
    "DefaultCertificateForNewLaunches": "rds-ca-rsa2048-g1"
```

```
}
```

Para obtener más información, consulte Uso de SSL/TLS para cifrar una conexión a una instancia de base de datos en la Guía del usuario de Amazon RDS y Uso de SSL/TLS para cifrar una conexión a un clúster de base de datos en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte DescribeCertificates en la Referencia de comandos de la AWS CLI.

`describe-db-cluster-backtracks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-cluster-backtracks`.

AWS CLI

Para describir las búsquedas de datos anteriores en un clúster de base de datos

En el siguiente ejemplo de `describe-db-cluster-backtracks` se recuperan los detalles sobre el clúster de base de datos especificado.

```
aws rds describe-db-cluster-backtracks \
    --db-cluster-identifier mydbcluster
```

Salida:

```
{
    "DBClusterBacktracks": [
        {
            "DBClusterIdentifier": "mydbcluster",
            "BacktrackIdentifier": "2f5f5294-0dd2-44c9-9f50-EXAMPLE",
            "BacktrackTo": "2021-02-12T04:59:22Z",
            "BacktrackedFrom": "2021-02-12T14:37:31.640Z",
            "BacktrackRequestCreationTime": "2021-02-12T14:36:18.819Z",
            "Status": "COMPLETED"
        },
        {
            "DBClusterIdentifier": "mydbcluster",
            "BacktrackIdentifier": "3c7a6421-af2a-4ea3-ae95-EXAMPLE",
            "BacktrackTo": "2021-02-11T22:53:46Z",
            "BacktrackedFrom": "2021-02-12T00:09:27.006Z",
            "BacktrackRequestCreationTime": "2021-02-12T00:07:53.487Z",
            "Status": "COMPLETED"
```

```
        }
    ]
}
```

Para obtener más información, consulte Búsqueda de datos anteriores de un clúster de base de datos de Aurora en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DescribeDbClusterBacktracks en la Referencia de comandos de la AWS CLI.

`describe-db-cluster-endpoints`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-cluster-endpoints`.

AWS CLI

Ejemplo 1: describir los puntos de conexión de un clúster de base de datos

En el siguiente ejemplo de `describe-db-cluster-endpoints`, se recuperan los detalles de los puntos de conexión de su clúster de base de datos. Los tipos más comunes de clústeres de Aurora tienen dos puntos de conexión. Un punto de conexión tiene un tipo `WRITER`. Puede utilizar este punto de conexión para todas las instrucciones SQL. El otro punto de conexión tiene el tipo `READER`. Puede usar este punto de conexión solo para SELECT y otras instrucciones SQL de solo lectura.

```
aws rds describe-db-cluster-endpoints
```

Salida:

```
{
    "DBClusterEndpoints": [
        {
            "DBClusterIdentifier": "my-database-1",
            "Endpoint": "my-database-1.cluster-cnpexample.us-
east-1.rds.amazonaws.com",
            "Status": "creating",
            "EndpointType": "WRITER"
        },
        {
            "DBClusterIdentifier": "my-database-1",
            "Endpoint": "my-database-1.cluster-ro-cnpexample.us-
east-1.rds.amazonaws.com",
```

```
            "Status": "creating",
            "EndpointType": "READER"
        },
        {
            "DBClusterIdentifier": "mydbcluster",
            "Endpoint": "mydbcluster.cluster-cnpexamle.us-east-1.rds.amazonaws.com",
            "Status": "available",
            "EndpointType": "WRITER"
        },
        {
            "DBClusterIdentifier": "mydbcluster",
            "Endpoint": "mydbcluster.cluster-ro-cnpexample.us-
east-1.rds.amazonaws.com",
            "Status": "available",
            "EndpointType": "READER"
        }
    ]
}
```

Ejemplo 2: describir los puntos de conexión de un clúster de base de datos de un solo clúster de base de datos

En el siguiente ejemplo de `describe-db-cluster-endpoints`, se recuperan los detalles de los puntos de conexión del clúster de base de datos de un solo clúster de base de datos especificado. Los clústeres Aurora sin servidor solo tienen un punto de conexión con un tipo de `WRITER`.

```
aws rds describe-db-cluster-endpoints \
    --db-cluster-identifier serverless-cluster
```

Salida:

```
{
    "DBClusterEndpoints": [
        {
            "Status": "available",
            "Endpoint": "serverless-cluster.cluster-cnpexample.us-
east-1.rds.amazonaws.com",
            "DBClusterIdentifier": "serverless-cluster",
            "EndpointType": "WRITER"
        }
    ]
```

```
}
```

Para obtener más información, consulte Amazon Aurora Connection Management en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DescribeDbClusterEndpoints en la Referencia de comandos de la AWS CLI.

`describe-db-cluster-parameter-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-cluster-parameter-groups`.

AWS CLI

Para describir los grupos de parámetro de un clúster de base de datos

En el siguiente ejemplo de `describe-db-cluster-parameter-groups`, se recuperan los detalles de los grupos de parámetros de su clúster de base de datos.

```
aws rds describe-db-cluster-parameter-groups
```

Salida:

```
{
    "DBClusterParameterGroups": [
        {
            "DBClusterParameterGroupName": "default.aurora-mysql5.7",
            "DBParameterGroupFamily": "aurora-mysql5.7",
            "Description": "Default cluster parameter group for aurora-mysql5.7",
            "DBClusterParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:cluster-pg:default.aurora-mysql5.7"
        },
        {
            "DBClusterParameterGroupName": "default.aurora-postgresql9.6",
            "DBParameterGroupFamily": "aurora-postgresql9.6",
            "Description": "Default cluster parameter group for aurora-
postgresql9.6",
            "DBClusterParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:cluster-pg:default.aurora-postgresql9.6"
        },
        {
```

```
            "DBClusterParameterGroupName": "default.aurora5.6",
            "DBParameterGroupFamily": "aurora5.6",
            "Description": "Default cluster parameter group for aurora5.6",
            "DBClusterParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:cluster-pg:default.aurora5.6"
        },
        {
            "DBClusterParameterGroupName": "mydbclusterpg",
            "DBParameterGroupFamily": "aurora-mysql5.7",
            "Description": "My DB cluster parameter group",
            "DBClusterParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:cluster-pg:mydbclusterpg"
        },
        {
            "DBClusterParameterGroupName": "mydbclusterpgcopy",
            "DBParameterGroupFamily": "aurora-mysql5.7",
            "Description": "Copy of mydbclusterpg parameter group",
            "DBClusterParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:cluster-pg:mydbclusterpgcopy"
        }
    ]
}
```

Para obtener más información, consulte Working with DB Parameter Groups and DB Cluster Parameter Groups en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte DescribeDbClusterParameterGroups en la Referencia de comandos de la AWS CLI.

`describe-db-cluster-parameters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-cluster-parameters`.

AWS CLI

Ejemplo 1: describir los parámetros de un grupo de parámetros de clúster de base de datos

En el siguiente ejemplo de `describe-db-cluster-parameters`, se recuperan los detalles sobre los parámetros en un grupo de parámetros de clúster de base de datos.

```
aws rds describe-db-cluster-parameters \
    --db-cluster-parameter-group-name mydbclusterpg
```

Salida:

```
{
    "Parameters": [
        {
            "ParameterName": "allow-suspicious-udfs",
            "Description": "Controls whether user-defined functions that have only
 an xxx symbol for the main function can be loaded",
            "Source": "engine-default",
            "ApplyType": "static",
            "DataType": "boolean",
            "AllowedValues": "0,1",
            "IsModifiable": false,
            "ApplyMethod": "pending-reboot",
            "SupportedEngineModes": [
                "provisioned"
            ]
        },
        {
            "ParameterName": "aurora_lab_mode",
            "ParameterValue": "0",
            "Description": "Enables new features in the Aurora engine.",
            "Source": "engine-default",
            "ApplyType": "static",
            "DataType": "boolean",
            "AllowedValues": "0,1",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot",
            "SupportedEngineModes": [
                "provisioned"
            ]
        },
        ...some output truncated...
    ]
}
```

Ejemplo 2: generar una lista solo de nombres de parámetros de un grupo de parámetros de clúster de base de datos

En el siguiente ejemplo de `describe-db-cluster-parameters`, se recuperan solo los nombres de los parámetros en un grupo de parámetros de clúster de base de datos.

```
aws rds describe-db-cluster-parameters \
```

```
    --db-cluster-parameter-group-name default.aurora-mysql5.7 \
    --query 'Parameters[].{ParameterName:ParameterName}'
```

Salida:

```
[
    {
        "ParameterName": "allow-suspicious-udfs"
    },
    {
        "ParameterName": "aurora_binlog_read_buffer_size"
    },
    {
        "ParameterName": "aurora_binlog_replication_max_yield_seconds"
    },
    {
        "ParameterName": "aurora_binlog_use_large_read_buffer"
    },
    {
        "ParameterName": "aurora_lab_mode"
    },

    ...some output truncated...
    }
]
```

Ejemplo 3: describir solo los parámetros modificables de un grupo de parámetros de clúster de base de datos

En el siguiente ejemplo de `describe-db-cluster-parameters`, se recuperan solo los nombres de los parámetros que se pueden modificar en un grupo de parámetros de clúster de base de datos.

```
aws rds describe-db-cluster-parameters \
    --db-cluster-parameter-group-name default.aurora-mysql5.7 \
    --query 'Parameters[].{ParameterName:ParameterName,IsModifiable:IsModifiable} |
 [?IsModifiable == `true`]'
```

Salida:

```
[
    {
```

```
        "ParameterName": "aurora_binlog_read_buffer_size",
        "IsModifiable": true
    },
    {
        "ParameterName": "aurora_binlog_replication_max_yield_seconds",
        "IsModifiable": true
    },
    {
        "ParameterName": "aurora_binlog_use_large_read_buffer",
        "IsModifiable": true
    },
    {
        "ParameterName": "aurora_lab_mode",
        "IsModifiable": true
    },

    ...some output truncated...
    }
]
```

Ejemplo 4: describir solo los parámetros booleanos modificables de un grupo de parámetros de clúster de base de datos

En el siguiente ejemplo de `describe-db-cluster-parameters`, se recuperan solo los nombres de los parámetros que se pueden modificar en un grupo de parámetros de clúster de base de datos y que tienen un tipo de datos booleano.

```
aws rds describe-db-cluster-parameters \
    --db-cluster-parameter-group-name default.aurora-mysql5.7 \
    --query 'Parameters[].
{ParameterName:ParameterName,DataType:DataType,IsModifiable:IsModifiable} | [?
DataType == `boolean`] | [?IsModifiable == `true`]'
```

Salida:

```
[
    {
        "DataType": "boolean",
        "ParameterName": "aurora_binlog_use_large_read_buffer",
        "IsModifiable": true
    },
    {
```

```
        "DataType": "boolean",
        "ParameterName": "aurora_lab_mode",
        "IsModifiable": true
    },
    {
        "DataType": "boolean",
        "ParameterName": "autocommit",
        "IsModifiable": true
    },
    {
        "DataType": "boolean",
        "ParameterName": "automatic_sp_privileges",
        "IsModifiable": true
    },
    ...some output truncated...
    }
]
```

Para obtener más información, consulte Working with DB Parameter Groups and DB Cluster Parameter Groups en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte DescribeDbClusterParameters en la Referencia de comandos de la AWS CLI.

`describe-db-cluster-snapshot-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-cluster-snapshot-attributes`.

AWS CLI

Para describir los nombres y valores de los atributos de una instantánea de clúster de base de datos

En el siguiente ejemplo de `describe-db-cluster-snapshot-attributes`, se recuperan detalles de los nombres y valores de los atributos de la instantánea del clúster de base de datos especificado.

```
aws rds describe-db-cluster-snapshot-attributes \
    --db-cluster-snapshot-identifier myclustersnapshot
```

Salida:

```
{
    "DBClusterSnapshotAttributesResult": {
        "DBClusterSnapshotIdentifier": "myclustersnapshot",
        "DBClusterSnapshotAttributes": [
            {
                "AttributeName": "restore",
                "AttributeValues": [
                    "123456789012"
                ]
            }
        ]
    }
}
```

Para obtener más información, consulte Sharing a DB Cluster Snapshot en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte DescribeDbClusterSnapshotAttributes en la Referencia de comandos de la AWS CLI.

`describe-db-cluster-snapshots`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-cluster-snapshots`.

AWS CLI

Para describir una instantánea de clúster de base de datos para un clúster de base de datos

En el siguiente ejemplo de `describe-db-cluster-snapshots`, se recuperan los detalles de las instantáneas del clúster de base de datos para el clúster de base de datos especificado.

```
aws rds describe-db-cluster-snapshots \
    --db-cluster-identifier mydbcluster
```

Salida:

```
{
    "DBClusterSnapshots": [
        {
            "AvailabilityZones": [
                "us-east-1a",
                "us-east-1b",
```

```
                "us-east-1e"
            ],
            "DBClusterSnapshotIdentifier": "myclustersnapshotcopy",
            "DBClusterIdentifier": "mydbcluster",
            "SnapshotCreateTime": "2019-06-04T09:16:42.649Z",
            "Engine": "aurora-mysql",
            "AllocatedStorage": 0,
            "Status": "available",
            "Port": 0,
            "VpcId": "vpc-6594f31c",
            "ClusterCreateTime": "2019-04-15T14:18:42.785Z",
            "MasterUsername": "myadmin",
            "EngineVersion": "5.7.mysql_aurora.2.04.2",
            "LicenseModel": "aurora-mysql",
            "SnapshotType": "manual",
            "PercentProgress": 100,
            "StorageEncrypted": true,
            "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/
AKIAIOSFODNN7EXAMPLE",
            "DBClusterSnapshotArn": "arn:aws:rds:us-east-1:814387698303:cluster-
snapshot:myclustersnapshotcopy",
            "IAMDatabaseAuthenticationEnabled": false
        },
        {
            "AvailabilityZones": [
                "us-east-1a",
                "us-east-1b",
                "us-east-1e"
            ],
            "DBClusterSnapshotIdentifier": "rds:mydbcluster-2019-06-20-09-16",
            "DBClusterIdentifier": "mydbcluster",
            "SnapshotCreateTime": "2019-06-20T09:16:26.569Z",
            "Engine": "aurora-mysql",
            "AllocatedStorage": 0,
            "Status": "available",
            "Port": 0,
            "VpcId": "vpc-6594f31c",
            "ClusterCreateTime": "2019-04-15T14:18:42.785Z",
            "MasterUsername": "myadmin",
            "EngineVersion": "5.7.mysql_aurora.2.04.2",
            "LicenseModel": "aurora-mysql",
            "SnapshotType": "automated",
            "PercentProgress": 100,
            "StorageEncrypted": true,
```

```
            "KmsKeyId": "arn:aws:kms:us-east-1:814387698303:key/
AKIAIOSFODNN7EXAMPLE",
            "DBClusterSnapshotArn": "arn:aws:rds:us-east-1:123456789012:cluster-
snapshot:rds:mydbcluster-2019-06-20-09-16",
            "IAMDatabaseAuthenticationEnabled": false
        }
    ]
}
```

Para obtener más información, consulte Creación de una instantánea de clúster de base de datos en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte DescribeDbClusterSnapshots en la Referencia de comandos de la AWS CLI.

`describe-db-clusters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-clusters`.

AWS CLI

Ejemplo 1: describir un clúster de base de datos

En el siguiente ejemplo de `describe-db-clusters` se recuperan los detalles sobre el clúster de base de datos especificado.

```
aws rds describe-db-clusters \
    --db-cluster-identifier mydbcluster
```

Salida:

```
{
    "DBClusters": [
        {
            "AllocatedStorage": 1,
            "AvailabilityZones": [
                "us-east-1a",
                "us-east-1b",
                "us-east-1e"
            ],
            "BackupRetentionPeriod": 1,
            "DatabaseName": "mydbcluster",
            "DBClusterIdentifier": "mydbcluster",
```

```
            "DBClusterParameterGroup": "default.aurora-mysql5.7",
            "DBSubnetGroup": "default",
            "Status": "available",
            "EarliestRestorableTime": "2019-06-19T09:16:28.210Z",
            "Endpoint": "mydbcluster.cluster-cnpexample.us-
east-1.rds.amazonaws.com",
            "ReaderEndpoint": "mydbcluster.cluster-ro-cnpexample.us-
east-1.rds.amazonaws.com",
            "MultiAZ": true,
            "Engine": "aurora-mysql",
            "EngineVersion": "5.7.mysql_aurora.2.04.2",
            "LatestRestorableTime": "2019-06-20T22:38:14.908Z",
            "Port": 3306,
            "MasterUsername": "myadmin",
            "PreferredBackupWindow": "09:09-09:39",
            "PreferredMaintenanceWindow": "sat:04:09-sat:04:39",
            "ReadReplicaIdentifiers": [],
            "DBClusterMembers": [
                {
                    "DBInstanceIdentifier": "dbinstance3",
                    "IsClusterWriter": false,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "PromotionTier": 1
                },
                {
                    "DBInstanceIdentifier": "dbinstance1",
                    "IsClusterWriter": false,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "PromotionTier": 1
                },
                {
                    "DBInstanceIdentifier": "dbinstance2",
                    "IsClusterWriter": false,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "PromotionTier": 1
                },
                {
                    "DBInstanceIdentifier": "mydbcluster",
                    "IsClusterWriter": false,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "PromotionTier": 1
                },
                {
                    "DBInstanceIdentifier": "mydbcluster-us-east-1b",
```

```
                    "IsClusterWriter": false,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "PromotionTier": 1
                },
                {
                    "DBInstanceIdentifier": "mydbcluster",
                    "IsClusterWriter": true,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "PromotionTier": 1
                }
            ],
            "VpcSecurityGroups": [
                {
                    "VpcSecurityGroupId": "sg-0b9130572daf3dc16",
                    "Status": "active"
                }
            ],
            "HostedZoneId": "Z2R2ITUGPM61AM",
            "StorageEncrypted": true,
            "KmsKeyId": "arn:aws:kms:us-east-1:814387698303:key/
AKIAIOSFODNN7EXAMPLE",
            "DbClusterResourceId": "cluster-AKIAIOSFODNN7EXAMPLE",
            "DBClusterArn": "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster",
            "AssociatedRoles": [],
            "IAMDatabaseAuthenticationEnabled": false,
            "ClusterCreateTime": "2019-04-15T14:18:42.785Z",
            "EngineMode": "provisioned",
            "DeletionProtection": false,
            "HttpEndpointEnabled": false
        }
    ]
}
```

Ejemplo 2: generar una lista de determinados atributos de todos los clústeres de bases de datos

El siguiente ejemplo de `describe-db-clusters` recupera solo los atributos `DBClusterIdentifier`, `Endpoint` y `ReaderEndpoint` de todos los clústeres de base de datos de la región AWS actual.

```
aws rds describe-db-clusters \
    --query 'DBClusters[].
{DBClusterIdentifier:DBClusterIdentifier,Endpoint:Endpoint,ReaderEndpoint:ReaderEndpoint}'
```

Salida:

```
[
    {
        "Endpoint": "cluster-57-2020-05-01-2270.cluster-cnpexample.us-
east-1.rds.amazonaws.com",
        "ReaderEndpoint": "cluster-57-2020-05-01-2270.cluster-ro-cnpexample.us-
east-1.rds.amazonaws.com",
        "DBClusterIdentifier": "cluster-57-2020-05-01-2270"
    },
    {
        "Endpoint": "cluster-57-2020-05-01-4615.cluster-cnpexample.us-
east-1.rds.amazonaws.com",
        "ReaderEndpoint": "cluster-57-2020-05-01-4615.cluster-ro-cnpexample.us-
east-1.rds.amazonaws.com",
        "DBClusterIdentifier": "cluster-57-2020-05-01-4615"
    },
    {
        "Endpoint": "pg2-cluster.cluster-cnpexample.us-east-1.rds.amazonaws.com",
        "ReaderEndpoint": "pg2-cluster.cluster-ro-cnpexample.us-
east-1.rds.amazonaws.com",
        "DBClusterIdentifier": "pg2-cluster"
    },
    ...output omitted...
    }
]
```

Ejemplo 3: generar una lista de los clústeres de bases de datos con un atributo específico

El siguiente ejemplo de `describe-db-clusters` recupera solo los atributos `DBClusterIdentifier` y `Engine` de los clústeres de base de datos que utilicen el motor de base de datos `aurora-postgresql`.

```
aws rds describe-db-clusters \
    --query 'DBClusters[].{DBClusterIdentifier:DBClusterIdentifier,Engine:Engine} |
 [?Engine == `aurora-postgresql`]'
```

Salida:

```
[
    {
        "Engine": "aurora-postgresql",
```

```
        "DBClusterIdentifier": "pg2-cluster"
    }
]
```

Para obtener más información, consulte la sección sobre Clústeres de base de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte DescribeDbClusters en la Referencia de comandos de la AWS CLI.

`describe-db-engine-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-engine-versions`.

AWS CLI

Descripción de las versiones del motor de base de datos para el motor de base de datos MySQL

El siguiente ejemplo `describe-db-engine-versions` se muestran detalles sobre cada una de las versiones del motor de base de datos especificado.

```
aws rds describe-db-engine-versions \
    --engine mysql
```

Salida:

```
{
    "DBEngineVersions": [
        {
            "Engine": "mysql",
            "EngineVersion": "5.5.46",
            "DBParameterGroupFamily": "mysql5.5",
            "DBEngineDescription": "MySQL Community Edition",
            "DBEngineVersionDescription": "MySQL 5.5.46",
            "ValidUpgradeTarget": [
                {
                    "Engine": "mysql",
                    "EngineVersion": "5.5.53",
                    "Description": "MySQL 5.5.53",
                    "AutoUpgrade": false,
                    "IsMajorVersionUpgrade": false
                },
```

```
            {
                "Engine": "mysql",
                "EngineVersion": "5.5.54",
                "Description": "MySQL 5.5.54",
                "AutoUpgrade": false,
                "IsMajorVersionUpgrade": false
            },
            {
                "Engine": "mysql",
                "EngineVersion": "5.5.57",
                "Description": "MySQL 5.5.57",
                "AutoUpgrade": false,
                "IsMajorVersionUpgrade": false
            },
            ...some output truncated...
        ]
    }
```

Para obtener más información acerca de Amazon RDS, consulte ¿Qué es Amazon Relational Database Service (Amazon RDS)? en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeDBEngineVersions en la Referencia de comandos de la AWS CLI.

`describe-db-instance-automated-backups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-instance-automated-backups`.

AWS CLI

Para describir las copias de seguridad automatizadas de una instancia de base de datos

En el ejemplo siguiente de `describe-db-instance-automated-backups`, se muestran los detalles sobre las copias de seguridad automatizadas para la instancia de base de datos especificada. Los detalles incluyen copias de seguridad automatizadas replicadas en otras regiones de AWS.

```
aws rds describe-db-instance-automated-backups \
    --db-instance-identifier new-orcl-db
```

Salida:

```
{
    "DBInstanceAutomatedBackups": [
        {
            "DBInstanceArn": "arn:aws:rds:us-east-1:123456789012:db:new-orcl-db",
            "DbiResourceId": "db-JKIB2GFQ5RV7REPLZA4EXAMPLE",
            "Region": "us-east-1",
            "DBInstanceIdentifier": "new-orcl-db",
            "RestoreWindow": {
                "EarliestTime": "2020-12-07T21:05:20.939Z",
                "LatestTime": "2020-12-07T21:05:20.939Z"
            },
            "AllocatedStorage": 20,
            "Status": "replicating",
            "Port": 1521,
            "InstanceCreateTime": "2020-12-04T15:28:31Z",
            "MasterUsername": "admin",
            "Engine": "oracle-se2",
            "EngineVersion": "12.1.0.2.v21",
            "LicenseModel": "bring-your-own-license",
            "OptionGroupName": "default:oracle-se2-12-1",
            "Encrypted": false,
            "StorageType": "gp2",
            "IAMDatabaseAuthenticationEnabled": false,
            "BackupRetentionPeriod": 14,
            "DBInstanceAutomatedBackupsArn": "arn:aws:rds:us-
west-2:123456789012:auto-backup:ab-jkib2gfq5rv7replzadausbrktni2bn4example"
        }
    ]
}
```

Para obtener más información, consulte Finding information about replicated backups en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeDbInstanceAutomatedBackups en la Referencia de comandos de la AWS CLI.

`describe-db-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-instances`.

AWS CLI

Descripción de una instancia de base de datos

En el siguiente ejemplo de `describe-db-instances`, se recuperan los detalles sobre la instancia de base de datos especificada.

```
aws rds describe-db-instances \
    --db-instance-identifier mydbinstancecf
```

Salida:

```
{
    "DBInstances": [
        {
            "DBInstanceIdentifier": "mydbinstancecf",
            "DBInstanceClass": "db.t3.small",
            "Engine": "mysql",
            "DBInstanceStatus": "available",
            "MasterUsername": "masterawsuser",
            "Endpoint": {
                "Address": "mydbinstancecf.abcexample.us-east-1.rds.amazonaws.com",
                "Port": 3306,
                "HostedZoneId": "Z2R2ITUGPM61AM"
            },
            ...some output truncated...
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeDBInstances en la Referencia de comandos de la AWS CLI.

`describe-db-log-files`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-log-files`.

AWS CLI

Para describir los archivos de registro de una instancia de base de datos

En el siguiente ejemplo de `describe-db-log-files`, se recuperan los detalles sobre los archivos de registro para la instancia de base de datos especificada.

```
aws rds describe-db-log-files -\
```

```
    -db-instance-identifier test-instance
```

Salida:

```
{
    "DescribeDBLogFiles": [
        {
            "Size": 0,
            "LastWritten": 1533060000000,
            "LogFileName": "error/mysql-error-running.log"
        },
        {
            "Size": 2683,
            "LastWritten": 1532994300000,
            "LogFileName": "error/mysql-error-running.log.0"
        },
        {
            "Size": 107,
            "LastWritten": 1533057300000,
            "LogFileName": "error/mysql-error-running.log.18"
        },
        {
            "Size": 13105,
            "LastWritten": 1532991000000,
            "LogFileName": "error/mysql-error-running.log.23"
        },
        {
            "Size": 0,
            "LastWritten": 1533061200000,
            "LogFileName": "error/mysql-error.log"
        },
        {
            "Size": 3519,
            "LastWritten": 1532989252000,
            "LogFileName": "mysqlUpgrade"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeDbLogFiles en la Referencia de comandos de la AWS CLI.

`describe-db-parameter-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-parameter-groups`.

AWS CLI

Descripción del grupo de parámetros de base de datos

En el siguiente ejemplo `describe-db-parameter-groups`, se recuperan los detalles sobre los grupos de parámetros de base de datos.

```
aws rds describe-db-parameter-groups
```

Salida:

```
{
    "DBParameterGroups": [
        {
            "DBParameterGroupName": "default.aurora-mysql5.7",
            "DBParameterGroupFamily": "aurora-mysql5.7",
            "Description": "Default parameter group for aurora-mysql5.7",
            "DBParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:pg:default.aurora-mysql5.7"
        },
        {
            "DBParameterGroupName": "default.aurora-postgresql9.6",
            "DBParameterGroupFamily": "aurora-postgresql9.6",
            "Description": "Default parameter group for aurora-postgresql9.6",
            "DBParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:pg:default.aurora-postgresql9.6"
        },
        {
            "DBParameterGroupName": "default.aurora5.6",
            "DBParameterGroupFamily": "aurora5.6",
            "Description": "Default parameter group for aurora5.6",
            "DBParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:pg:default.aurora5.6"
        },
        {
            "DBParameterGroupName": "default.mariadb10.1",
            "DBParameterGroupFamily": "mariadb10.1",
            "Description": "Default parameter group for mariadb10.1",
```

```
            "DBParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:pg:default.mariadb10.1"
        },
        ...some output truncated...
    ]
}
```

Para obtener más información, consulte Trabajo con los grupos de parámetros de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeDBParameterGroups en la Referencia de comandos de la AWS CLI.

`describe-db-parameters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-parameters`.

AWS CLI

Descripción de los parámetros de un grupo de parámetros de base de datos

En el siguiente ejemplo `describe-db-parameters`, se recuperan los detalles del grupo de parámetros de base de datos especificado.

```
aws rds describe-db-parameters \
    --db-parameter-group-name mydbpg
```

Salida:

```
{
    "Parameters": [
        {
            "ParameterName": "allow-suspicious-udfs",
            "Description": "Controls whether user-defined functions that have only
 an xxx symbol for the main function can be loaded",
            "Source": "engine-default",
            "ApplyType": "static",
            "DataType": "boolean",
            "AllowedValues": "0,1",
            "IsModifiable": false,
            "ApplyMethod": "pending-reboot"
        },
        {
```

```
            "ParameterName": "auto_generate_certs",
            "Description": "Controls whether the server autogenerates SSL key and
 certificate files in the data directory, if they do not already exist.",
            "Source": "engine-default",
            "ApplyType": "static",
            "DataType": "boolean",
            "AllowedValues": "0,1",
            "IsModifiable": false,
            "ApplyMethod": "pending-reboot"
        },
        ...some output truncated...
    ]
}
```

Para obtener más información, consulte Trabajo con los grupos de parámetros de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeDBParameters en la Referencia de comandos de la AWS CLI.

`describe-db-proxies`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-proxies`.

AWS CLI

Para describir un proxy de base de datos para una base de datos de RDS

El siguiente ejemplo de `describe-db-proxies` proporciona información sobre proxies de base de datos.

```
aws rds describe-db-proxies
```

Salida:

```
{
    "DBProxies": [
        {
            "DBProxyName": "proxyExample1",
            "DBProxyArn": "arn:aws:rds:us-east-1:123456789012:db-
proxy:prx-0123a01b12345c0ab",
            "Status": "available",
            "EngineFamily": "PostgreSQL",
```

```
            "VpcId": "vpc-1234567",
            "VpcSecurityGroupIds": [
                "sg-1234"
            ],
            "VpcSubnetIds": [
                "subnetgroup1",
                "subnetgroup2"
            ],
            "Auth": "[
                {
                    "Description": "proxydescription1"
                    "AuthScheme": "SECRETS",
                    "SecretArn": "arn:aws:secretsmanager:us-
west-2:123456789123:secret:secretName-1234f",
                    "IAMAuth": "DISABLED"
                }
            ]",
            "RoleArn": "arn:aws:iam::12345678912??:role/ProxyPostgreSQLRole",
            "Endpoint": "proxyExample1.proxy-ab0cd1efghij.us-
east-1.rds.amazonaws.com",
            "RequireTLS": false,
            "IdleClientTimeout": 1800,
            "DebuggingLogging": false,
            "CreatedDate": "2023-04-05T16:09:33.452000+00:00",
            "UpdatedDate": "2023-04-13T01:49:38.568000+00:00"
        },
        {
            "DBProxyName": "proxyExample2",
            "DBProxyArn": "arn:aws:rds:us-east-1:123456789012:db-
proxy:prx-1234a12b23456c1ab",
            "Status": "available",
            "EngineFamily": "PostgreSQL",
            "VpcId": "sg-1234567",
            "VpcSecurityGroupIds": [
                "sg-1234"
            ],
            "VpcSubnetIds": [
                "subnetgroup1",
                "subnetgroup2"
            ],
            "Auth": "[
                {
                    "Description": "proxydescription2"
                    "AuthScheme": "SECRETS",
```

```
                    "SecretArn": "aarn:aws:secretsmanager:us-
west-2:123456789123:secret:secretName-1234f",
                    "IAMAuth": "DISABLED"
                }
            ]",
            "RoleArn": "arn:aws:iam::12345678912:role/ProxyPostgreSQLRole",
            "Endpoint": "proxyExample2.proxy-ab0cd1efghij.us-
east-1.rds.amazonaws.com",
            "RequireTLS": false,
            "IdleClientTimeout": 1800,
            "DebuggingLogging": false,
            "CreatedDate": "2022-01-05T16:19:33.452000+00:00",
            "UpdatedDate": "2023-04-13T01:49:38.568000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Ver un RDS Proxy en la Guía del usuario de Amazon RDS y Ver un RDS Proxy en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DescribeDbProxies en la Referencia de comandos de la AWS CLI.

`describe-db-proxy-endpoints`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-proxy-endpoints`.

AWS CLI

Para describir los puntos de conexión de un proxy de base de datos

El siguiente ejemplo de `describe-db-proxy-endpoints` proporciona información sobre puntos de conexión de proxies de base de datos.

```
aws rds describe-db-proxy-endpoints
```

Salida:

```
{
    "DBProxyEndpoints": [
        {
            "DBProxyEndpointName": "proxyEndpoint1",
```

```
            "DBProxyEndpointArn": "arn:aws:rds:us-east-1:123456789012:db-proxy-
endpoint:prx-endpoint-0123a01b12345c0ab",
            "DBProxyName": "proxyExample",
            "Status": "available",
            "VpcId": "vpc-1234567",
            "VpcSecurityGroupIds": [
                "sg-1234"
            ],
            "VpcSubnetIds": [
                "subnetgroup1",
                "subnetgroup2"
            ],
            "Endpoint": "proxyEndpoint1.endpoint.proxy-ab0cd1efghij.us-
east-1.rds.amazonaws.com",
            "CreatedDate": "2023-04-05T16:09:33.452000+00:00",
            "TargetRole": "READ_WRITE",
            "IsDefault": false
        },
        {
            "DBProxyEndpointName": "proxyEndpoint2",
            "DBProxyEndpointArn": "arn:aws:rds:us-east-1:123456789012:db-proxy-
endpoint:prx-endpoint-4567a01b12345c0ab",
            "DBProxyName": "proxyExample2",
            "Status": "available",
            "VpcId": "vpc1234567",
            "VpcSecurityGroupIds": [
                "sg-5678"
            ],
            "VpcSubnetIds": [
                "subnetgroup1",
                "subnetgroup2"
            ],
            "Endpoint": "proxyEndpoint2.endpoint.proxy-cd1ef2klmnop.us-
east-1.rds.amazonaws.com",
            "CreatedDate": "2023-04-05T16:09:33.452000+00:00",
            "TargetRole": "READ_WRITE",
            "IsDefault": false
        }
    ]
}
```

Para obtener más información, consulte Viewing a proxy endpoint en la Guía del usuario de Amazon RDS y Viewing a proxy endpoint en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DescribeDbProxyEndpoints en la Referencia de comandos de la AWS CLI.

`describe-db-proxy-target-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-proxy-target-groups`.

AWS CLI

Para describir los puntos de conexión de un proxy de base de datos

El siguiente ejemplo de `describe-db-proxy-target-groups` proporciona información sobre grupos de destino de proxy de base de datos.

```
aws rds describe-db-proxy-target-groups \
    --db-proxy-name proxyExample
```

Salida:

```
{
"TargetGroups":
    {
        "DBProxyName": "proxyExample",
        "TargetGroupName": "default",
        "TargetGroupArn": "arn:aws:rds:us-east-1:123456789012:target-group:prx-
tg-0123a01b12345c0ab",
        "IsDefault": true,
        "Status": "available",
        "ConnectionPoolConfig": {
            "MaxConnectionsPercent": 100,
            "MaxIdleConnectionsPercent": 50,
            "ConnectionBorrowTimeout": 120,
            "SessionPinningFilters": []
        },
        "CreatedDate": "2023-05-02T18:41:19.495000+00:00",
        "UpdatedDate": "2023-05-02T18:41:21.762000+00:00"
    }
}
```

Para obtener más información, consulte Ver un RDS Proxy en la Guía del usuario de Amazon RDS y Ver un RDS Proxy en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DescribeDbProxyTargetGroups en la Referencia de comandos de la AWS CLI.

`describe-db-proxy-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-proxy-targets`.

AWS CLI

Para describir los objetivos de un proxy de base de datos

El siguiente ejemplo de `describe-db-proxy-targets` proporciona información sobre destinos de proxy de base de datos.

```
aws rds describe-db-proxy-targets \
    --db-proxy-name proxyExample
```

Salida:

```
{
    "Targets": [
        {
            "Endpoint": "database1.ab0cd1efghij.us-east-1.rds.amazonaws.com",
            "TrackedClusterId": "database1",
            "RdsResourceId": "database1-instance-1",
            "Port": 3306,
            "Type": "RDS_INSTANCE",
            "Role": "READ_WRITE",
            "TargetHealth": {
                "State": "UNAVAILABLE",
                "Reason": "PENDING_PROXY_CAPACITY",
                "Description": "DBProxy Target is waiting for proxy to scale to
 desired capacity"
            }
        }
    ]
}
```

Para obtener más información, consulte Ver un RDS Proxy en la Guía del usuario de Amazon RDS y Ver un RDS Proxy en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DescribeDbProxyTargets en la Referencia de comandos de la AWS CLI.

`describe-db-recommendations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-recommendations`.

AWS CLI

Ejemplo 1: generar listas de todas las recomendaciones de bases de datos

En el siguiente ejemplo de `describe-db-recommendations`, se generan listas de todas las recomendaciones de bases de datos de su cuenta de AWS.

```
aws rds describe-db-recommendations
```

Salida:

```
{
    "DBRecommendations": [
        {
            "RecommendationId": "12ab3cde-f456-7g8h-9012-i3j45678k9lm",
            "TypeId": "config_recommendation::old_minor_version",
            "Severity": "informational",
            "ResourceArn": "arn:aws:rds:us-west-2:111122223333:db:database-1",
            "Status": "active",
            "CreatedTime": "2024-02-21T23:14:19.292000+00:00",
            "UpdatedTime": "2024-02-21T23:14:19+00:00",
            "Detection": "**[resource-name]** is not running the latest minor DB
 engine version",
            "Recommendation": "Upgrade to latest engine version",
            "Description": "Your database resources aren't running the latest minor
 DB engine version. The latest minor version contains the latest security fixes and
 other improvements.",
            "RecommendedActions": [
                {
                    "ActionId": "12ab34c5de6fg7h89i0jk1lm234n5678",
                    "Operation": "modifyDbInstance",
                    "Parameters": [
                        {
                            "Key": "EngineVersion",
                            "Value": "5.7.44"
```

```
                        },
                        {
                            "Key": "DBInstanceIdentifier",
                            "Value": "database-1"
                        }
                    ],
                    "ApplyModes": [
                        "immediately",
                        "next-maintenance-window"
                    ],
                    "Status": "ready",
                    "ContextAttributes": [
                        {
                            "Key": "Recommended value",
                            "Value": "5.7.44"
                        },
                        {
                            "Key": "Current engine version",
                            "Value": "5.7.42"
                        }
                    ]
                }
            ],
            "Category": "security",
            "Source": "RDS",
            "TypeDetection": "**[resource-count] resources** are not running the
 latest minor DB engine version",
            "TypeRecommendation": "Upgrade to latest engine version",
            "Impact": "Reduced database performance and data security at risk",
            "AdditionalInfo": "We recommend that you maintain your database with the
 latest DB engine minor version as this version includes the latest security and
 functionality fixes. The DB engine minor version upgrades contain only the changes
 which are backward-compatible with earlier minor versions of the same major version
 of the DB engine.",
            "Links": [
                {
                    "Text": "Upgrading an RDS DB instance engine version",
                    "Url": "https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/
USER_UpgradeDBInstance.Upgrading.html"
                },
                {
                    "Text": "Using Amazon RDS Blue/Green Deployments for database
 updates for Amazon Aurora",
```

```
                    "Url": "https://docs.aws.amazon.com/AmazonRDS/latest/
AuroraUserGuide/blue-green-deployments.html"
                },
                {
                    "Text": "Using Amazon RDS Blue/Green Deployments for database
 updates for Amazon RDS",
                    "Url": "https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/
blue-green-deployments.html"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Recomendaciones para Amazon RDS en la Guía del usuario de Amazon RDS y Recomendaciones para Amazon Aurora en la Guía del usuario de Amazon Aurora.

Ejemplo 2: generar listas de las recomendaciones de bases de datos de alta gravedad

En el siguiente ejemplo de `describe-db-recommendations`, se generan listas de las recomendaciones de bases de datos de alta gravedad en su cuenta de AWS.

```
aws rds describe-db-recommendations \
    --filters Name=severity,Values=high
```

Salida:

```
{
    "DBRecommendations": [
        {
            "RecommendationId": "12ab3cde-f456-7g8h-9012-i3j45678k9lm",
            "TypeId": "config_recommendation::rds_extended_support",
            "Severity": "high",
            "ResourceArn": "arn:aws:rds:us-west-2:111122223333:db:database-1",
            "Status": "active",
            "CreatedTime": "2024-02-21T23:14:19.392000+00:00",
            "UpdatedTime": "2024-02-21T23:14:19+00:00",
            "Detection": "Your databases will be auto-enrolled to RDS Extended
 Support on February 29",
            "Recommendation": "Upgrade your major version before February 29, 2024
 to avoid additional charges",
```

```
            "Description": "Your PostgreSQL 11 and MySQL 5.7 databases will be
 automatically enrolled into RDS Extended Support on February 29, 2024. To avoid
 the increase in charges due to RDS Extended Support, we recommend upgrading your
 databases to a newer major engine version before February 29, 2024.\nTo learn more
 about the RDS Extended Support pricing, refer to the pricing page.",
            "RecommendedActions": [
                {
                    "ActionId": "12ab34c5de6fg7h89i0jk1lm234n5678",
                    "Parameters": [],
                    "ApplyModes": [
                        "manual"
                    ],
                    "Status": "ready",
                    "ContextAttributes": []
                }
            ],
            "Category": "cost optimization",
            "Source": "RDS",
            "TypeDetection": "Your database will be auto-enrolled to RDS Extended
 Support on February 29",
            "TypeRecommendation": "Upgrade your major version before February 29,
 2024 to avoid additional charges",
            "Impact": "Increase in charges due to RDS Extended Support",
            "AdditionalInfo": "With Amazon RDS Extended Support, you can continue
 running your database on a major engine version past the RDS end of standard
 support date for an additional cost. This paid feature gives you more time to
 upgrade to a supported major engine version.\nDuring Extended Support, Amazon RDS
 will supply critical CVE patches and bug fixes.",
            "Links": [
                {
                    "Text": "Amazon RDS Extended Support pricing for RDS for MySQL",
                    "Url": "https://aws.amazon.com/rds/mysql/pricing/"
                },
                {
                    "Text": "Amazon RDS Extended Support for RDS for MySQL and
 PostgreSQL databases",
                    "Url": "https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/
extended-support.html"
                },
                {
                    "Text": "Amazon RDS Extended Support pricing for Amazon Aurora
 PostgreSQL",
                    "Url": "https://aws.amazon.com/rds/aurora/pricing/"
                },
```

```
                {
                    "Text": "Amazon RDS Extended Support for Aurora PostgreSQL
 databases",
                    "Url": "https://docs.aws.amazon.com/AmazonRDS/latest/
AuroraUserGuide/extended-support.html"
                },
                {
                    "Text": "Amazon RDS Extended Support pricing for RDS for
 PostgreSQL",
                    "Url": "https://aws.amazon.com/rds/postgresql/pricing/"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Viewing and responding to Amazon RDS recommendations en la Guía del usuario de Amazon RDS y Viewing and responding to Amazon RDS recommendations en la Guía del usuario de Amazon Aurora.

Ejemplo 3: generar listas de las recomendaciones de base de datos para una instancia de base de datos específica

El siguiente ejemplo de `describe-db-recommendations` genera listas de todas las recomendaciones de base de datos para una instancia de base de datos específica.

```
aws rds describe-db-recommendations \
    --filters Name=dbi-resource-id,Values=database-1
```

Salida:

```
{
    "DBRecommendations": [
        {
            "RecommendationId": "12ab3cde-f456-7g8h-9012-i3j45678k9lm",
            "TypeId": "config_recommendation::old_minor_version",
            "Severity": "informational",
            "ResourceArn": "arn:aws:rds:us-west-2:111122223333:db:database-1",
            "Status": "active",
            "CreatedTime": "2024-02-21T23:14:19.292000+00:00",
            "UpdatedTime": "2024-02-21T23:14:19+00:00",
```

```
            "Detection": "**[resource-name]** is not running the latest minor DB
engine version",
            "Recommendation": "Upgrade to latest engine version",
            "Description": "Your database resources aren't running the latest minor
DB engine version. The latest minor version contains the latest security fixes and
other improvements.",
            "RecommendedActions": [
                {
                    "ActionId": "12ab34c5de6fg7h89i0jk1lm234n5678",
                    "Operation": "modifyDbInstance",
                    "Parameters": [
                        {
                            "Key": "EngineVersion",
                            "Value": "5.7.44"
                        },
                        {
                            "Key": "DBInstanceIdentifier",
                            "Value": "database-1"
                        }
                    ],
                    "ApplyModes": [
                        "immediately",
                        "next-maintenance-window"
                    ],
                    "Status": "ready",
                    "ContextAttributes": [
                        {
                            "Key": "Recommended value",
                            "Value": "5.7.44"
                        },
                        {
                            "Key": "Current engine version",
                            "Value": "5.7.42"
                        }
                    ]
                }
            ],
            "Category": "security",
            "Source": "RDS",
            "TypeDetection": "**[resource-count] resources** are not running the
latest minor DB engine version",
            "TypeRecommendation": "Upgrade to latest engine version",
            "Impact": "Reduced database performance and data security at risk",
```

```
            "AdditionalInfo": "We recommend that you maintain your database with the
 latest DB engine minor version as this version includes the latest security and
 functionality fixes. The DB engine minor version upgrades contain only the changes
 which are backward-compatible with earlier minor versions of the same major version
 of the DB engine.",
            "Links": [
                {
                    "Text": "Upgrading an RDS DB instance engine version",
                    "Url": "https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/
USER_UpgradeDBInstance.Upgrading.html"
                },
                {
                    "Text": "Using Amazon RDS Blue/Green Deployments for database
 updates for Amazon Aurora",
                    "Url": "https://docs.aws.amazon.com/AmazonRDS/latest/
AuroraUserGuide/blue-green-deployments.html"
                },
                {
                    "Text": "Using Amazon RDS Blue/Green Deployments for database
 updates for Amazon RDS",
                    "Url": "https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/
blue-green-deployments.html"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Viewing and responding to Amazon RDS recommendations en la Guía del usuario de Amazon RDS y Viewing and responding to Amazon RDS recommendations en la Guía del usuario de Amazon Aurora.

Ejemplo 4: generar listas de todas las recomendaciones de bases de datos activas

En el siguiente ejemplo de `describe-db-recommendations`, se generan listas de todas las recomendaciones de bases de datos activas de su cuenta de AWS.

```
aws rds describe-db-recommendations \
    --filters Name=status,Values=active
```

Salida:

```
{
```

```
   "DBRecommendations": [
       {
           "RecommendationId": "12ab3cde-f456-7g8h-9012-i3j45678k9lm",
           "TypeId": "config_recommendation::old_minor_version",
           "Severity": "informational",
           "ResourceArn": "arn:aws:rds:us-west-2:111122223333:db:database-1",
           "Status": "active",
           "CreatedTime": "2024-02-21T23:14:19.292000+00:00",
           "UpdatedTime": "2024-02-21T23:14:19+00:00",
           "Detection": "**[resource-name]** is not running the latest minor DB
engine version",
           "Recommendation": "Upgrade to latest engine version",
           "Description": "Your database resources aren't running the latest minor
DB engine version. The latest minor version contains the latest security fixes and
other improvements.",
           "RecommendedActions": [
               {
                   "ActionId": "12ab34c5de6fg7h89i0jk1lm234n5678",
                   "Operation": "modifyDbInstance",
                   "Parameters": [
                       {
                           "Key": "EngineVersion",
                           "Value": "5.7.44"
                       },
                       {
                           "Key": "DBInstanceIdentifier",
                           "Value": "database-1"
                       }
                   ],
                   "ApplyModes": [
                       "immediately",
                       "next-maintenance-window"
                   ],
                   "Status": "ready",
                   "ContextAttributes": [
                       {
                           "Key": "Recommended value",
                           "Value": "5.7.44"
                       },
                       {
                           "Key": "Current engine version",
                           "Value": "5.7.42"
                       }
                   ]
```

```
                }
            ],
            "Category": "security",
            "Source": "RDS",
            "TypeDetection": "**[resource-count] resources** are not running the
 latest minor DB engine version",
            "TypeRecommendation": "Upgrade to latest engine version",
            "Impact": "Reduced database performance and data security at risk",
            "AdditionalInfo": "We recommend that you maintain your database with the
 latest DB engine minor version as this version includes the latest security and
 functionality fixes. The DB engine minor version upgrades contain only the changes
 which are backward-compatible with earlier minor versions of the same major version
 of the DB engine.",
            "Links": [
                {
                    "Text": "Upgrading an RDS DB instance engine version",
                    "Url": "https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/
USER_UpgradeDBInstance.Upgrading.html"
                },
                {
                    "Text": "Using Amazon RDS Blue/Green Deployments for database
 updates for Amazon Aurora",
                    "Url": "https://docs.aws.amazon.com/AmazonRDS/latest/
AuroraUserGuide/blue-green-deployments.html"
                },
                {
                    "Text": "Using Amazon RDS Blue/Green Deployments for database
 updates for Amazon RDS",
                    "Url": "https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/
blue-green-deployments.html"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Viewing and responding to Amazon RDS recommendations en la Guía del usuario de Amazon RDS y Viewing and responding to Amazon RDS recommendations en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DescribeDbRecommendations en la Referencia de comandos de la AWS CLI.

`describe-db-security-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-security-groups`.

AWS CLI

Para generar listas de los grupos de seguridad de bases de datos

En el siguiente ejemplo de `describe-db-security-groups`, se generan listas de grupos de seguridad de base de datos.

```
aws rds describe-db-security-groups
```

Salida:

```
{
    "DBSecurityGroups": [
        {
            "OwnerId": "123456789012",
            "DBSecurityGroupName": "default",
            "DBSecurityGroupDescription": "default",
            "EC2SecurityGroups": [],
            "IPRanges": [],
            "DBSecurityGroupArn": "arn:aws:rds:us-
west-1:111122223333:secgrp:default"
        },
        {
            "OwnerId": "123456789012",
            "DBSecurityGroupName": "mysecgroup",
            "DBSecurityGroupDescription": "My Test Security Group",
            "VpcId": "vpc-1234567f",
            "EC2SecurityGroups": [],
            "IPRanges": [],
            "DBSecurityGroupArn": "arn:aws:rds:us-
west-1:111122223333:secgrp:mysecgroup"
        }
    ]
}
```

Para obtener más información, consulte Listing Available DB Security Groups en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeDbSecurityGroups en la Referencia de comandos de la AWS CLI.

`describe-db-shard-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-shard-groups`.

AWS CLI

Ejemplo 1: describir los grupos de partición de base de datos

En el siguiente ejemplo de `describe-db-shard-groups`, se recuperan los detalles sobre los grupos de partición de base de datos.

```
aws rds describe-db-shard-groups
```

Salida:

```
{
    "DBShardGroups": [
        {
            "DBShardGroupResourceId": "shardgroup-7bb446329da94788b3f957746example",
            "DBShardGroupIdentifier": "limitless-test-shard-grp",
            "DBClusterIdentifier": "limitless-test-cluster",
            "MaxACU": 768.0,
            "ComputeRedundancy": 0,
            "Status": "available",
            "PubliclyAccessible": true,
            "Endpoint": "limitless-test-cluster.limitless-cekycexample.us-
east-2.rds.amazonaws.com"
        },
        {
            "DBShardGroupResourceId": "shardgroup-a6e3a0226aa243e2ac6c7a1234567890",
            "DBShardGroupIdentifier": "my-db-shard-group",
            "DBClusterIdentifier": "my-sv2-cluster",
            "MaxACU": 768.0,
            "ComputeRedundancy": 0,
            "Status": "available",
            "PubliclyAccessible": false,
            "Endpoint": "my-sv2-cluster.limitless-cekycexample.us-
east-2.rds.amazonaws.com"
        }
```

```
    ]
}
```

Para obtener más información, consulte la sección sobre Clústeres de base de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DescribeDbShardGroups en la Referencia de comandos de la AWS CLI.

`describe-db-snapshot-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-snapshot-attributes`.

AWS CLI

Para describir los nombres y valores de los atributos de una instantánea de base de datos

En el siguiente ejemplo de `describe-db-snapshot-attributes`, se describen los nombres y los valores de los atributos de una instantánea de base de datos.

```
aws rds describe-db-snapshot-attributes \
    --db-snapshot-identifier mydbsnapshot
```

Salida:

```
{
    "DBSnapshotAttributesResult": {
        "DBSnapshotIdentifier": "mydbsnapshot",
        "DBSnapshotAttributes": [
            {
                "AttributeName": "restore",
                "AttributeValues": [
                    "123456789012",
                    "210987654321"
                ]
            }
        ]
    }
}
```

Para obtener más información, consulte Uso compartido de una instantánea en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeDbSnapshotAttributes en la Referencia de comandos de la AWS CLI.

`describe-db-snapshots`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-snapshots`.

AWS CLI

Ejemplo 1: Descripción de una instantánea de base de datos para una instancia de base de datos

En el siguiente ejemplo `describe-db-snapshots`, se recuperan los detalles de una instantánea de base de datos de una instancia de base de datos.

```
aws rds describe-db-snapshots \
    --db-snapshot-identifier mydbsnapshot
```

Salida:

```
{
    "DBSnapshots": [
        {
            "DBSnapshotIdentifier": "mydbsnapshot",
            "DBInstanceIdentifier": "mysqldb",
            "SnapshotCreateTime": "2018-02-08T22:28:08.598Z",
            "Engine": "mysql",
            "AllocatedStorage": 20,
            "Status": "available",
            "Port": 3306,
            "AvailabilityZone": "us-east-1f",
            "VpcId": "vpc-6594f31c",
            "InstanceCreateTime": "2018-02-08T22:24:55.973Z",
            "MasterUsername": "mysqladmin",
            "EngineVersion": "5.6.37",
            "LicenseModel": "general-public-license",
            "SnapshotType": "manual",
            "OptionGroupName": "default:mysql-5-6",
            "PercentProgress": 100,
            "StorageType": "gp2",
```

```
            "Encrypted": false,
            "DBSnapshotArn": "arn:aws:rds:us-
east-1:123456789012:snapshot:mydbsnapshot",
            "IAMDatabaseAuthenticationEnabled": false,
            "ProcessorFeatures": [],
            "DbiResourceId": "db-AKIAIOSFODNN7EXAMPLE"
        }
    ]
}
```

Para obtener más información, consulte Creación de una instantánea de base de datos en la Guía del usuario de Amazon RDS.

Ejemplo 2: Búsqueda del número de instantáneas manuales realizadas

En el siguiente ejemplo de `describe-db-snapshots` se utiliza el operador `length` como opción `--query` para devolver el número de instantáneas manuales que se han realizado en una región concreta de AWS.

```
aws rds describe-db-snapshots \
    --snapshot-type manual \
    --query "length(*[].{DBSnapshots:SnapshotType})" \
    --region eu-central-1
```

Salida:

```
35
```

Para obtener más información, consulte Creación de una instantánea de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeDBSnapshots en la Referencia de comandos de la AWS CLI.

`describe-db-subnet-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-db-subnet-groups`.

AWS CLI

Para describir un grupo de subred de base de datos

En el siguiente ejemplo de `describe-db-subnet-groups`, se recuperan los detalles del grupo de subred de base de datos especificado.

```
aws rds describe-db-subnet-groups
```

Salida:

```
{
    "DBSubnetGroups": [
        {
            "DBSubnetGroupName": "mydbsubnetgroup",
            "DBSubnetGroupDescription": "My DB Subnet Group",
            "VpcId": "vpc-971c12ee",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-d8c8e7f4",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1a"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-718fdc7d",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1f"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-cbc8e7e7",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1a"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-0ccde220",
                    "SubnetAvailabilityZone": {
                        "Name": "us-east-1a"
                    },
                    "SubnetStatus": "Active"
                }
```

```
            ],
            "DBSubnetGroupArn": "arn:aws:rds:us-
east-1:123456789012:subgrp:mydbsubnetgroup"
        }
    ]
}
```

Para obtener más información, consulte Amazon Virtual Private Cloud VPCs and Amazon RDS en la Guía del usuario de Amazon RDS.

- Para obtener detalles sobre la API, consulte DescribeDbSubnetGroups en la Referencia de comandos de la AWS CLI.

`describe-engine-default-cluster-parameters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-engine-default-cluster-parameters`.

AWS CLI

Para describir la información de parámetro del sistema y del motor predeterminado para el motor de una base de datos de Aurora

En el siguiente ejemplo de `describe-engine-default-cluster-parameters`, se recuperan los detalles del motor predeterminado y la información de los parámetros del sistema para los clústeres de bases de datos Aurora compatibles con MySQL 5.7.

```
aws rds describe-engine-default-cluster-parameters \
    --db-parameter-group-family aurora-mysql5.7
```

Salida:

```
{
    "EngineDefaults": {
        "Parameters": [
            {
                "ParameterName": "aurora_load_from_s3_role",
                "Description": "IAM role ARN used to load data from AWS S3",
                "Source": "engine-default",
                "ApplyType": "dynamic",
                "DataType": "string",
                "IsModifiable": true,
```

```
                "SupportedEngineModes": [
                    "provisioned"
                ]
            },
            ...some output truncated...
        ]
    }
}
```

Para obtener más información, consulte Working with DB Parameter Groups and DB Cluster Parameter Groups en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DescribeEngineDefaultClusterParameters en la Referencia de comandos de la AWS CLI.

`describe-engine-default-parameters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-engine-default-parameters`.

AWS CLI

Para describir la información de motor predeterminado y la información de los parámetros del sistema para el motor de una base de datos

En el siguiente ejemplo de `describe-engine-default-parameters`, se recuperan los detalles del motor predeterminado y la información de los parámetros del sistema para las instancias de base de datos MySQL 5.7.

```
aws rds describe-engine-default-parameters \
    --db-parameter-group-family mysql5.7
```

Salida:

```
{
    "EngineDefaults": {
        "Parameters": [
            {
                "ParameterName": "allow-suspicious-udfs",
                "Description": "Controls whether user-defined functions that have
 only an xxx symbol for the main function can be loaded",
                "Source": "engine-default",
```

```
                "ApplyType": "static",
                "DataType": "boolean",
                "AllowedValues": "0,1",
                "IsModifiable": false
            },
            ...some output truncated...
        ]
    }
}
```

Para obtener más información, consulte Trabajo con los grupos de parámetros de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeEngineDefaultParameters en la Referencia de comandos de la AWS CLI.

`describe-event-categories`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-event-categories`.

AWS CLI

Para describir las categorías de eventos

El siguiente ejemplo de `describe-event-categories` recupera detalles sobre las categorías de eventos para todos los orígenes de eventos disponibles.

```
aws rds describe-event-categories
```

Salida:

```
{
    "EventCategoriesMapList": [
        {
            "SourceType": "db-instance",
            "EventCategories": [
                "deletion",
                "read replica",
                "failover",
                "restoration",
                "maintenance",
                "low storage",
                "configuration change",
```

```
                "backup",
                "creation",
                "availability",
                "recovery",
                "failure",
                "backtrack",
                "notification"
            ]
        },
        {
            "SourceType": "db-security-group",
            "EventCategories": [
                "configuration change",
                "failure"
            ]
        },
        {
            "SourceType": "db-parameter-group",
            "EventCategories": [
                "configuration change"
            ]
        },
        {
            "SourceType": "db-snapshot",
            "EventCategories": [
                "deletion",
                "creation",
                "restoration",
                "notification"
            ]
        },
        {
            "SourceType": "db-cluster",
            "EventCategories": [
                "failover",
                "failure",
                "notification"
            ]
        },
        {
            "SourceType": "db-cluster-snapshot",
            "EventCategories": [
                "backup"
            ]
```

```
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeEventCategories en la Referencia de comandos de la AWS CLI.

`describe-event-subscriptions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-event-subscriptions`.

AWS CLI

Para describir suscripciones a eventos

En este ejemplo se describen todas las suscripciones a eventos de Amazon RDS para la cuenta de AWS actual.

```
aws rds describe-event-subscriptions
```

Salida:

```
{
    "EventSubscriptionsList": [
        {
            "EventCategoriesList": [
                "backup",
                "recovery"
            ],
            "Enabled": true,
            "EventSubscriptionArn": "arn:aws:rds:us-east-1:123456789012:es:my-
instance-events",
            "Status": "creating",
            "SourceType": "db-instance",
            "CustomerAwsId": "123456789012",
            "SubscriptionCreationTime": "2018-07-31 23:22:01.893",
            "CustSubscriptionId": "my-instance-events",
            "SnsTopicArn": "arn:aws:sns:us-east-1:123456789012:interesting-events"
        },
        ...some output truncated...
    ]
}
```

- Para obtener información sobre la API, consulte DescribeEventSubscriptions en la Referencia de comandos de la AWS CLI.

`describe-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-events`.

AWS CLI

Para describir eventos

En el siguiente ejemplo de `describe-events`, se recuperan los detalles de los eventos que se han producido para la instancia de base de datos especificada.

```
aws rds describe-events \
    --source-identifier test-instance \
    --source-type db-instance
```

Salida:

```
{
    "Events": [
        {
            "SourceType": "db-instance",
            "SourceIdentifier": "test-instance",
            "EventCategories": [
                "backup"
            ],
            "Message": "Backing up DB instance",
            "Date": "2018-07-31T23:09:23.983Z",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:db:test-instance"
        },
        {
            "SourceType": "db-instance",
            "SourceIdentifier": "test-instance",
            "EventCategories": [
                "backup"
            ],
            "Message": "Finished DB Instance backup",
            "Date": "2018-07-31T23:15:13.049Z",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:db:test-instance"
        }
```

```
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeEvents en la Referencia de comandos de la AWS CLI.

`describe-export-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-export-tasks`.

AWS CLI

Para describir las tareas de exportación de instantáneas

El siguiente ejemplo de `describe-export-tasks` devuelve información sobre las exportaciones de instantáneas a Amazon S3.

```
aws rds describe-export-tasks
```

Salida:

```
{
    "ExportTasks": [
        {
            "ExportTaskIdentifier": "test-snapshot-export",
            "SourceArn": "arn:aws:rds:us-west-2:123456789012:snapshot:test-
snapshot",
            "SnapshotTime": "2020-03-02T18:26:28.163Z",
            "TaskStartTime": "2020-03-02T18:57:56.896Z",
            "TaskEndTime": "2020-03-02T19:10:31.985Z",
            "S3Bucket": "amzn-s3-demo-bucket",
            "S3Prefix": "",
            "IamRoleArn": "arn:aws:iam::123456789012:role/service-role/ExportRole",
            "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/
abcd0000-7fca-4128-82f2-aabbccddeeff",
            "Status": "COMPLETE",
            "PercentProgress": 100,
            "TotalExtractedDataInGB": 0
        },
        {
            "ExportTaskIdentifier": "my-s3-export",
```

```
            "SourceArn": "arn:aws:rds:us-west-2:123456789012:snapshot:db5-snapshot-
test",
            "SnapshotTime": "2020-03-27T20:48:42.023Z",
            "S3Bucket": "amzn-s3-demo-bucket",
            "S3Prefix": "",
            "IamRoleArn": "arn:aws:iam::123456789012:role/service-role/ExportRole",
            "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/
abcd0000-7fca-4128-82f2-aabbccddeeff",
            "Status": "STARTING",
            "PercentProgress": 0,
            "TotalExtractedDataInGB": 0
        }
    ]
}
```

Para obtener más información, consulte Monitoreo de las exportaciones de instantáneas en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeExportTasks en la Referencia de comandos de la AWS CLI.

`describe-global-clusters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-global-clusters`.

AWS CLI

Para describir los clústeres de bases de datos globales

El siguiente ejemplo de `describe-global-clusters` genera una lista de los clústeres de bases de datos globales de Aurora en la región de AWS actual.

```
aws rds describe-global-clusters
```

Salida:

```
{
    "GlobalClusters": [
        {
            "GlobalClusterIdentifier": "myglobalcluster",
            "GlobalClusterResourceId": "cluster-f5982077e3b5aabb",
            "GlobalClusterArn": "arn:aws:rds::123456789012:global-
cluster:myglobalcluster",
```

```
            "Status": "available",
            "Engine": "aurora-mysql",
            "EngineVersion": "5.7.mysql_aurora.2.07.2",
            "StorageEncrypted": false,
            "DeletionProtection": false,
            "GlobalClusterMembers": []
        }
    ]
}
```

Para obtener más información, consulte Administración de una base de datos global de Amazon Aurora en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DescribeGlobalClusters en la Referencia de comandos de la AWS CLI.

`describe-option-group-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-option-group-options`.

AWS CLI

Para describir todas las opciones disponibles

El siguiente ejemplo de `describe-option-group-options` genera listas de las dos opciones para una instancia de Oracle Database 19c.

```
aws rds describe-option-group-options \
    --engine-name oracle-ee \
    --major-engine-version 19 \
    --max-items 2
```

Salida:

```
{
    "OptionGroupOptions": [
        {
            "Name": "APEX",
            "Description": "Oracle Application Express Runtime Environment",
            "EngineName": "oracle-ee",
            "MajorEngineVersion": "19",
            "MinimumRequiredMinorEngineVersion": "0.0.0.ru-2019-07.rur-2019-07.r1",
```

```
            "PortRequired": false,
            "OptionsDependedOn": [],
            "OptionsConflictsWith": [],
            "Persistent": false,
            "Permanent": false,
            "RequiresAutoMinorEngineVersionUpgrade": false,
            "VpcOnly": false,
            "SupportsOptionVersionDowngrade": false,
            "OptionGroupOptionSettings": [],
            "OptionGroupOptionVersions": [
                {
                    "Version": "19.1.v1",
                    "IsDefault": true
                },
                {
                    "Version": "19.2.v1",
                    "IsDefault": false
                }
            ]
        },
        {
            "Name": "APEX-DEV",
            "Description": "Oracle Application Express Development Environment",
            "EngineName": "oracle-ee",
            "MajorEngineVersion": "19",
            "MinimumRequiredMinorEngineVersion": "0.0.0.ru-2019-07.rur-2019-07.r1",
            "PortRequired": false,
            "OptionsDependedOn": [
                "APEX"
            ],
            "OptionsConflictsWith": [],
            "Persistent": false,
            "Permanent": false,
            "RequiresAutoMinorEngineVersionUpgrade": false,
            "VpcOnly": false,
            "OptionGroupOptionSettings": []
        }
    ],
    "NextToken": "eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAyfQ=="
}
```


Para obtener más información, consulte Descripción de opciones y configuración de opciones para un grupo de opciones en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeOptionGroupOptions en la Referencia de comandos de la AWS CLI.

`describe-option-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-option-groups`.

AWS CLI

Para describir los grupos de opción disponibles

El siguiente ejemplo de `describe-option-groups` genera listas de los grupos de opciones para una instancia de Oracle Database 19c.

```
aws rds describe-option-groups \
    --engine-name oracle-ee \
    --major-engine-version 19
```

Salida:

```
{
    "OptionGroupsList": [
        {
            "OptionGroupName": "default:oracle-ee-19",
            "OptionGroupDescription": "Default option group for oracle-ee 19",
            "EngineName": "oracle-ee",
            "MajorEngineVersion": "19",
            "Options": [],
            "AllowsVpcAndNonVpcInstanceMemberships": true,
            "OptionGroupArn": "arn:aws:rds:us-west-1:111122223333:og:default:oracle-
ee-19"
        }
    ]
}
```

Para obtener más información, consulte Descripción de opciones y configuración de opciones para un grupo de opciones en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeOptionGroups en la Referencia de comandos de la AWS CLI.

describe-orderable-db-instance-options

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-orderable-db-instance-options`.

AWS CLI

Descripción de las opciones de instancias de base de datos ordenables

En el siguiente ejemplo `describe-orderable-db-instance-options`, se recuperan detalles sobre las opciones ordenables de una instancia de base de datos que ejecuta el motor de base de datos MySQL.

```
aws rds describe-orderable-db-instance-options \
    --engine mysql
```

Salida:

```
{
    "OrderableDBInstanceOptions": [
        {
            "MinStorageSize": 5,
            "ReadReplicaCapable": true,
            "MaxStorageSize": 6144,
            "AvailabilityZones": [
                {
                    "Name": "us-east-1a"
                },
                {
                    "Name": "us-east-1b"
                },
                {
                    "Name": "us-east-1c"
                },
                {
                    "Name": "us-east-1d"
                }
            ],
            "SupportsIops": false,
            "AvailableProcessorFeatures": [],
            "MultiAZCapable": true,
            "DBInstanceClass": "db.m1.large",
            "Vpc": true,
```

```
            "StorageType": "gp2",
            "LicenseModel": "general-public-license",
            "EngineVersion": "5.5.46",
            "SupportsStorageEncryption": false,
            "SupportsEnhancedMonitoring": true,
            "Engine": "mysql",
            "SupportsIAMDatabaseAuthentication": false,
            "SupportsPerformanceInsights": false
        }
    ]
    ...some output truncated...
}
```

- Para obtener información sobre la API, consulte DescribeOrderableDBInstanceOptions en la Referencia de comandos de la AWS CLI.

`describe-pending-maintenance-actions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-pending-maintenance-actions`.

AWS CLI

Para generar listas de los recursos con al menos una acción de mantenimiento pendiente

El siguiente ejemplo de `describe-pending-maintenance-actions` genera listas de las acciones de mantenimiento pendientes para una instancia de base de datos.

```
aws rds describe-pending-maintenance-actions
```

Salida:

```
{
    "PendingMaintenanceActions": [
        {
            "ResourceIdentifier": "arn:aws:rds:us-
west-2:123456789012:cluster:global-db1-cl1",
            "PendingMaintenanceActionDetails": [
                {
                    "Action": "system-update",
                    "Description": "Upgrade to Aurora PostgreSQL 2.4.2"
                }
```

```
            ]
        }
    ]
}
```

Para obtener más información, consulte Mantenimiento de una instancia de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener detalles sobre la API, consulte DescribePendingMaintenanceActions en la Referencia de comandos de la AWS CLI.

`describe-reserved-db-instances-offerings`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-reserved-db-instances-offerings`.

AWS CLI

Para describir ofertas de instancias reservadas de bases de datos

El siguiente ejemplo de `describe-reserved-db-instances-offerings` recupera detalles sobre las opciones de instancias de base de datos reservadas para `oracle`.

```
aws rds describe-reserved-db-instances-offerings \
    --product-description oracle
```

Salida:

```
{
    "ReservedDBInstancesOfferings": [
        {
            "CurrencyCode": "USD",
            "UsagePrice": 0.0,
            "ProductDescription": "oracle-se2(li)",
            "ReservedDBInstancesOfferingId": "005bdee3-9ef4-4182-aa0c-58ef7cb6c2f8",
            "MultiAZ": true,
            "DBInstanceClass": "db.m4.xlarge",
            "OfferingType": "Partial Upfront",
            "RecurringCharges": [
                {
                    "RecurringChargeAmount": 0.594,
                    "RecurringChargeFrequency": "Hourly"
```

```
                }
            ],
            "FixedPrice": 4089.0,
            "Duration": 31536000
        },
    ...some output truncated...
}
```

- Para obtener información sobre la API, consulte DescribeReservedDbInstancesOfferings en la Referencia de comandos de la AWS CLI.

`describe-reserved-db-instances`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-reserved-db-instances`.

AWS CLI

Para describir instancias de bases de datos reservadas

En el siguiente ejemplo de `describe-reserved-db-instances`, se recuperan los detalles sobre cualquier instancia de base de datos reservada de la cuenta de AWS actual.

```
aws rds describe-reserved-db-instances
```

Salida:

```
{
    "ReservedDBInstances": [
        {
            "ReservedDBInstanceId": "myreservedinstance",
            "ReservedDBInstancesOfferingId": "12ab34cd-59af-4b2c-a660-1abcdef23456",
            "DBInstanceClass": "db.t3.micro",
            "StartTime": "2020-06-01T13:44:21.436Z",
            "Duration": 31536000,
            "FixedPrice": 0.0,
            "UsagePrice": 0.0,
            "CurrencyCode": "USD",
            "DBInstanceCount": 1,
            "ProductDescription": "sqlserver-ex(li)",
            "OfferingType": "No Upfront",
            "MultiAZ": false,
            "State": "payment-pending",
```

```
            "RecurringCharges": [
                {
                    "RecurringChargeAmount": 0.014,
                    "RecurringChargeFrequency": "Hourly"
                }
            ],
            "ReservedDBInstanceArn": "arn:aws:rds:us-
west-2:123456789012:ri:myreservedinstance",
            "LeaseId": "a1b2c3d4-6b69-4a59-be89-5e11aa446666"
        }
    ]
}
```

Para obtener más información, consulte la sección sobre Instancias de base de datos reservadas para Amazon RDS en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeReservedDbInstances en la Referencia de comandos de la AWS CLI.

`describe-source-regions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-source-regions`.

AWS CLI

Para describir las regiones de origen

El siguiente ejemplo de `describe-source-regions` recupera detalles sobre todas las regiones AWS de origen. También muestra que las copias de seguridad automatizadas se pueden replicar solo desde el Oeste de EE. UU. (Oregón) a la región de AWS de destino, Este de EE. UU. (Norte de Virginia).

```
aws rds describe-source-regions \
    --region us-east-1
```

Salida:

```
{
    "SourceRegions": [
        {
            "RegionName": "af-south-1",
            "Endpoint": "https://rds.af-south-1.amazonaws.com",
```

```
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": false
        },
        {
            "RegionName": "ap-east-1",
            "Endpoint": "https://rds.ap-east-1.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": false
        },
        {
            "RegionName": "ap-northeast-1",
            "Endpoint": "https://rds.ap-northeast-1.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": true
        },
        {
            "RegionName": "ap-northeast-2",
            "Endpoint": "https://rds.ap-northeast-2.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": true
        },
        {
            "RegionName": "ap-northeast-3",
            "Endpoint": "https://rds.ap-northeast-3.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": false
        },
        {
            "RegionName": "ap-south-1",
            "Endpoint": "https://rds.ap-south-1.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": true
        },
        {
            "RegionName": "ap-southeast-1",
            "Endpoint": "https://rds.ap-southeast-1.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": true
        },
        {
            "RegionName": "ap-southeast-2",
            "Endpoint": "https://rds.ap-southeast-2.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": true
```

```
        },
        {
            "RegionName": "ap-southeast-3",
            "Endpoint": "https://rds.ap-southeast-3.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": false
        },
        {
            "RegionName": "ca-central-1",
            "Endpoint": "https://rds.ca-central-1.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": true
        },
        {
            "RegionName": "eu-north-1",
            "Endpoint": "https://rds.eu-north-1.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": true
        },
        {
            "RegionName": "eu-south-1",
            "Endpoint": "https://rds.eu-south-1.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": false
        },
        {
            "RegionName": "eu-west-1",
            "Endpoint": "https://rds.eu-west-1.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": true
        },
        {
            "RegionName": "eu-west-2",
            "Endpoint": "https://rds.eu-west-2.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": true
        },
        {
            "RegionName": "eu-west-3",
            "Endpoint": "https://rds.eu-west-3.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": true
        },
        {
```

```
            "RegionName": "me-central-1",
             "Endpoint": "https://rds.me-central-1.amazonaws.com",
             "Status": "available",
             "SupportsDBInstanceAutomatedBackupsReplication": false
        },
        {
            "RegionName": "me-south-1",
            "Endpoint": "https://rds.me-south-1.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": false
        },
        {
            "RegionName": "sa-east-1",
            "Endpoint": "https://rds.sa-east-1.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": true
        },
        {
            "RegionName": "us-east-2",
            "Endpoint": "https://rds.us-east-2.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": true
        },
        {
            "RegionName": "us-west-1",
            "Endpoint": "https://rds.us-west-1.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": true
        },
        {
            "RegionName": "us-west-2",
           "Endpoint": "https://rds.us-west-2.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": true
        }
    ]
}
```

Para obtener más información, consulte Búsqueda de información sobre las copias de seguridad replicadas en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeSourceRegions en la Referencia de comandos de la AWS CLI.

describe-valid-db-instance-modifications

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-valid-db-instance-modifications`.

AWS CLI

Para describir las modificaciones válidas de una instancia de base de datos

En el siguiente ejemplo de `describe-valid-db-instance-modifications`, se recuperan los detalles sobre las modificaciones válidas de la instancia de base de datos especificada.

```
aws rds describe-valid-db-instance-modifications \
    --db-instance-identifier test-instance
```

Salida:

```
{
    "ValidDBInstanceModificationsMessage": {
        "ValidProcessorFeatures": [],
        "Storage": [
            {
                "StorageSize": [
                    {
                        "Step": 1,
                        "To": 20,
                        "From": 20
                    },
                    {
                        "Step": 1,
                        "To": 6144,
                        "From": 22
                    }
                ],
                "ProvisionedIops": [
                    {
                        "Step": 1,
                        "To": 0,
                        "From": 0
                    }
                ],
                "IopsToStorageRatio": [
                    {
```

```
                    "To": 0.0,
                    "From": 0.0
                }
            ],
            "StorageType": "gp2"
        },
        {
            "StorageSize": [
                {
                    "Step": 1,
                    "To": 6144,
                    "From": 100
                }
            ],
            "ProvisionedIops": [
                {
                    "Step": 1,
                    "To": 40000,
                    "From": 1000
                }
            ],
            "IopsToStorageRatio": [
                {
                    "To": 50.0,
                    "From": 1.0
                }
            ],
            "StorageType": "io1"
        },
        {
            "StorageSize": [
                {
                    "Step": 1,
                    "To": 20,
                    "From": 20
                },
                {
                    "Step": 1,
                    "To": 3072,
                    "From": 22
                }
            ],
            "ProvisionedIops": [
                {
```

```
                        "Step": 1,
                        "To": 0,
                        "From": 0
                    }
                ],
                "IopsToStorageRatio": [
                    {
                        "To": 0.0,
                        "From": 0.0
                    }
                ],
                "StorageType": "magnetic"
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte DescribeValidDbInstanceModifications en la Referencia de comandos de la AWS CLI.

`download-db-log-file-portion`

En el siguiente ejemplo de código, se muestra cómo utilizar `download-db-log-file-portion`.

AWS CLI

Ejemplo 1: descarga de la última parte de un archivo de registro de base de datos

El siguiente ejemplo de `download-db-log-file-portion` descarga solo la parte más reciente del archivo de registro y la guarda en un archivo local denominado `tail.txt`.

```
aws rds download-db-log-file-portion \
    --db-instance-identifier test-instance \
    --log-file-name log.txt \
    --output text > tail.txt
```

El archivo guardado puede contener líneas en blanco. Aparecen al final de cada parte del archivo de registro durante la descarga.

Ejemplo 2: descarga de un archivo de registro de base de datos completo

En el siguiente ejemplo de `download-db-log-file-portion`, se descarga el archivo de registro completo mediante el parámetro `--starting-token 0` y se guarda el resultado en un archivo local denominado `full.txt`.

```
aws rds download-db-log-file-portion \
    --db-instance-identifier test-instance \
    --log-file-name log.txt \
    --starting-token 0 \
    --output text > full.txt
```

El archivo guardado puede contener líneas en blanco. Aparecen al final de cada parte del archivo de registro durante la descarga.

- Para obtener información sobre la API, consulte DownloadDbLogFilePortion en la Referencia de comandos de la AWS CLI.

`generate-auth-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `generate-auth-token`.

AWS CLI

Para generar un token de autenticación

El siguiente ejemplo de `generate-db-auth-token` genera un token de autenticación para usarlo con la autenticación de la base de datos de IAM.

```
aws rds generate-db-auth-token \
    --hostname aurmysql-test.cdgmuqiadpid.us-west-2.rds.amazonaws.com \
    --port 3306 \
    --region us-east-1 \
    --username jane_doe
```

Salida:

```
aurmysql-test.cdgmuqiadpid.us-west-2.rds.amazonaws.com:3306/?
Action=connect&DBUser=jane_doe&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIESZCNJ3OEXAMPLE%2F20180731%2Fus-east-1%2Frds-db%2Faws4_request&X-
Amz-Date=20180731T235209Z&X-Amz-Expires=900&X-Amz-SignedHeaders=host&X-Amz-
Signature=5a8753ebEXAMPLEa2c724e5667797EXAMPLE9d6ec6e3f427191fa41aeEXAMPLE
```

- Para obtener información sobre la API, consulte GenerateAuthToken en la Referencia de comandos de la AWS CLI.

`generate-db-auth-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `generate-db-auth-token`.

AWS CLI

Para generar un token de autenticación de IAM

El siguiente ejemplo de `generate-db-auth-token` genera un token de autenticación de IAM para conectarse a una base de datos.

```
aws rds generate-db-auth-token \
    --hostname mydb.123456789012.us-east-1.rds.amazonaws.com \
    --port 3306 \
    --region us-east-1 \
    --username db_user
```

Salida:

```
mydb.123456789012.us-east-1.rds.amazonaws.com:3306/?
Action=connect&DBUser=db_user&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIEXAMPLE%2Fus-east-1%2Frds-db%2Faws4_request&X-Amz-
Date=20210123T011543Z&X-Amz-Expires=900&X-Amz-SignedHeaders=host&X-Amz-
Signature=88987EXAMPLE1EXAMPLE2EXAMPLE3EXAMPLE4EXAMPLE5EXAMPLE6
```

Para obtener más información, consulte Conexión a la instancia con la autenticación de IAM en la Guía del usuario de Amazon RDS y Conexión a la instancia con la autenticación de IAM en la Guía del usuario de Amazon Aurora.

- Para obtener más información sobre la API, consulte GenerateDbAuthToken en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para generar listas de etiquetas de un recurso en Amazon RDS

En el siguiente ejemplo de `list-tags-for-resource`, se generan listas de todas las etiquetas de una instancia de base de datos.

```
aws rds list-tags-for-resource \
    --resource-name arn:aws:rds:us-east-1:123456789012:db:orcl1
```

Salida:

```
{
    "TagList": [
        {
            "Key": "Environment",
            "Value": "test"
        },
        {
            "Key": "Name",
            "Value": "MyDatabase"
        }
    ]
}
```

Para obtener más información, consulte Etiquetado de los recursos de Amazon RDS en la Guía del usuario de Amazon RDS.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`modify-certificates`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-certificates`.

AWS CLI

Para anular temporalmente el certificado SSL/TLS predeterminado del sistema para las nuevas instancias de base de datos

El siguiente ejemplo de `modify-certificates` anula temporalmente el certificado SSL/TLS predeterminado del sistema para las nuevas instancias de la base de datos.

```
aws rds modify-certificates \
    --certificate-identifier rds-ca-2019
```

Salida:

```
{
    "Certificate": {
        "CertificateIdentifier": "rds-ca-2019",
        "CertificateType": "CA",
        "Thumbprint": "EXAMPLE123456789012",
        "ValidFrom": "2019-09-19T18:16:53Z",
        "ValidTill": "2024-08-22T17:08:50Z",
        "CertificateArn": "arn:aws:rds:us-east-1::cert:rds-ca-2019",
        "CustomerOverride": true,
        "CustomerOverrideValidTill": "2024-08-22T17:08:50Z"
    }
}
```

Para obtener más información, consulte Rotar certificados SSL/TLS en la Guía del usuario de Amazon RDS y Rotar certificados SSL/TLS en la Guía del usuario de Amazon Aurora.

- Para obtener más información sobre la API, consulte ModifyCertificates en la Referencia de comandos de la AWS CLI.

`modify-current-db-cluster-capacity`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-current-db-cluster-capacity`.

AWS CLI

Para escalar la capacidad de un clúster de base de datos Aurora sin servidor

En el siguiente ejemplo de `modify-current-db-cluster-capacity` se escala la capacidad de un clúster de base de datos Aurora sin servidor a 8.

```
aws rds modify-current-db-cluster-capacity \
    --db-cluster-identifier mydbcluster \
    --capacity 8
```

Salida:

```
{
    "DBClusterIdentifier": "mydbcluster",
    "PendingCapacity": 8,
    "CurrentCapacity": 1,
    "SecondsBeforeTimeout": 300,
    "TimeoutAction": "ForceApplyCapacityChange"
}
```

Para obtener más información, consulte Escalado manual de la capacidad del clúster de bases de datos de Aurora sin servidor, versión 1 en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte ModifyCurrentDbClusterCapacity en la Referencia de comandos de la AWS CLI.

`modify-db-cluster-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-cluster-endpoint`.

AWS CLI

Para modificar un punto de conexión de clúster de base de datos personalizado

En el siguiente ejemplo de `modify-db-cluster-endpoint`, se modifica el punto de conexión de clúster de base de datos personalizado especificado.

```
aws rds modify-db-cluster-endpoint \
    --db-cluster-endpoint-identifier mycustomendpoint \
    --static-members dbinstance1 dbinstance2 dbinstance3
```

Salida:

```
{
    "DBClusterEndpointIdentifier": "mycustomendpoint",
    "DBClusterIdentifier": "mydbcluster",
    "DBClusterEndpointResourceIdentifier": "cluster-endpoint-ANPAJ4AE5446DAEXAMPLE",
    "Endpoint": "mycustomendpoint.cluster-custom-cnpexample.us-
east-1.rds.amazonaws.com",
    "Status": "modifying",
    "EndpointType": "CUSTOM",
    "CustomEndpointType": "READER",
    "StaticMembers": [
```

```
        "dbinstance1",
        "dbinstance2",
        "dbinstance3"
    ],
    "ExcludedMembers": [],
    "DBClusterEndpointArn": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:mycustomendpoint"
}
```

Para obtener más información, consulte Amazon Aurora Connection Management en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte ModifyDbClusterEndpoint en la Referencia de comandos de la AWS CLI.

`modify-db-cluster-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-cluster-parameter-group`.

AWS CLI

Para modificar parámetros de un grupo de parámetros de clúster de base de datos

En el siguiente ejemplo de `modify-db-cluster-parameter-group`, se modifican los valores de los parámetros en un grupo de parámetros de clúster de base de datos.

```
aws rds modify-db-cluster-parameter-group \
    --db-cluster-parameter-group-name mydbclusterpg \
    --
parameters "ParameterName=server_audit_logging,ParameterValue=1,ApplyMethod=immediate"
 \

  "ParameterName=server_audit_logs_upload,ParameterValue=1,ApplyMethod=immediate"
```

Salida:

```
{
    "DBClusterParameterGroupName": "mydbclusterpg"
}
```

Para obtener más información, consulte Working with DB Parameter Groups and DB Cluster Parameter Groups en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte ModifyDbClusterParameterGroup en la Referencia de comandos de la AWS CLI.

`modify-db-cluster-snapshot-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-cluster-snapshot-attribute`.

AWS CLI

Para modificar un atributo de la instantánea del clúster de base de datos

En el siguiente ejemplo de `modify-db-cluster-snapshot-attribute`, se realizan cambios en el atributo de la instantánea del clúster de base de datos especificado.

```
aws rds modify-db-cluster-snapshot-attribute \
    --db-cluster-snapshot-identifier myclustersnapshot \
    --attribute-name restore \
    --values-to-add 123456789012
```

Salida:

```
{
    "DBClusterSnapshotAttributesResult": {
        "DBClusterSnapshotIdentifier": "myclustersnapshot",
        "DBClusterSnapshotAttributes": [
            {
                "AttributeName": "restore",
                "AttributeValues": [
                    "123456789012"
                ]
            }
        ]
    }
}
```

Para obtener más información, consulte Restauración de una instantánea de clúster de base de datos en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte ModifyDbClusterSnapshotAttribute en la Referencia de comandos de la AWS CLI.

`modify-db-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-cluster`.

AWS CLI

Ejemplo 1: modificar el clúster de una base de datos

El siguiente ejemplo de `modify-db-cluster` cambia la contraseña del usuario maestro del clúster de base de datos denominado `cluster-2` y establece el período de retención de la copia de seguridad en 14 días. El parámetro `--apply-immediately` hace que los cambios se produzcan de inmediato, en lugar de esperar hasta el siguiente período de mantenimiento.

```
aws rds modify-db-cluster \
    --db-cluster-identifier cluster-2 \
    --backup-retention-period 14 \
    --master-user-password newpassword99 \
    --apply-immediately
```

Salida:

```
{
    "DBCluster": {
        "AllocatedStorage": 1,
        "AvailabilityZones": [
            "eu-central-1b",
            "eu-central-1c",
            "eu-central-1a"
        ],
        "BackupRetentionPeriod": 14,
        "DatabaseName": "",
        "DBClusterIdentifier": "cluster-2",
        "DBClusterParameterGroup": "default.aurora5.6",
        "DBSubnetGroup": "default-vpc-2305ca49",
        "Status": "available",
        "EarliestRestorableTime": "2020-06-03T02:07:29.637Z",
        "Endpoint": "cluster-2.cluster-############.eu-central-1.rds.amazonaws.com",
        "ReaderEndpoint": "cluster-2.cluster-ro-############.eu-
central-1.rds.amazonaws.com",
```

```
        "MultiAZ": false,
        "Engine": "aurora",
        "EngineVersion": "5.6.10a",
        "LatestRestorableTime": "2020-06-04T15:11:25.748Z",
        "Port": 3306,
        "MasterUsername": "admin",
        "PreferredBackupWindow": "01:55-02:25",
        "PreferredMaintenanceWindow": "thu:21:14-thu:21:44",
        "ReadReplicaIdentifiers": [],
        "DBClusterMembers": [
            {
                "DBInstanceIdentifier": "cluster-2-instance-1",
                "IsClusterWriter": true,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
            }
        ],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-20a5c047",
                "Status": "active"
            }
        ],
        "HostedZoneId": "Z1RLNU0EXAMPLE",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:eu-central-1:123456789012:key/
d1bd7c8f-5cdb-49ca-8a62-a1b2c3d4e5f6",
        "DbClusterResourceId": "cluster-AGJ7XI77XVIS6FUXHU1EXAMPLE",
        "DBClusterArn": "arn:aws:rds:eu-central-1:123456789012:cluster:cluster-2",
        "AssociatedRoles": [],
        "IAMDatabaseAuthenticationEnabled": false,
        "ClusterCreateTime": "2020-04-03T14:44:02.764Z",
        "EngineMode": "provisioned",
        "DeletionProtection": false,
        "HttpEndpointEnabled": false,
        "CopyTagsToSnapshot": true,
        "CrossAccountClone": false,
        "DomainMemberships": []
    }
}
```

Para obtener más información, consulte Modificación de un clúster de base de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora.

Ejemplo 2: asociar un grupo de seguridad VPC con un clúster de base de datos

El siguiente ejemplo de `modify-db-instance` asocia un grupo de seguridad de VPC específico y elimina los grupos de seguridad de base de datos de un clúster de base de datos:

```
aws rds modify-db-cluster \
    --db-cluster-identifier dbName \
    --vpc-security-group-ids sg-ID
```

Salida:

```
{
    "DBCluster": {
        "AllocatedStorage": 1,
        "AvailabilityZones": [
            "us-west-2c",
            "us-west-2b",
            "us-west-2a"
        ],
        "BackupRetentionPeriod": 1,
        "DBClusterIdentifier": "dbName",
        "DBClusterParameterGroup": "default.aurora-mysql8.0",
        "DBSubnetGroup": "default",
        "Status": "available",
        "EarliestRestorableTime": "2024-02-15T01:12:13.966000+00:00",
        "Endpoint": "dbName.cluster-abcdefghji.us-west-2.rds.amazonaws.com",
        "ReaderEndpoint": "dbName.cluster-ro-abcdefghji.us-
west-2.rds.amazonaws.com",
        "MultiAZ": false,
        "Engine": "aurora-mysql",
        "EngineVersion": "8.0.mysql_aurora.3.04.1",
        "LatestRestorableTime": "2024-02-15T02:25:33.696000+00:00",
        "Port": 3306,
        "MasterUsername": "admin",
        "PreferredBackupWindow": "10:59-11:29",
        "PreferredMaintenanceWindow": "thu:08:54-thu:09:24",
        "ReadReplicaIdentifiers": [],
        "DBClusterMembers": [
            {
                "DBInstanceIdentifier": "dbName-instance-1",
                "IsClusterWriter": true,
                "DBClusterParameterGroupStatus": "in-sync",
                "PromotionTier": 1
```

```
            }
        ],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-ID",
                "Status": "active"
            }
        ],
        ...output omitted...
    }
}
```

Para obtener más información, consulte Control de acceso con grupos de seguridad en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte ModifyDbCluster en la Referencia de comandos de la AWS CLI.

`modify-db-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-instance`.

AWS CLI

Ejemplo 1: modificar una instancia de base de datos

En el siguiente ejemplo de `modify-db-instance` se asocia un grupo de opciones y un grupo de parámetros a una instancia de base de datos de Microsoft SQL Server compatible. El parámetro `--apply-immediately` hace que los grupos de opciones y parámetros se asocien de inmediato, en lugar de esperar hasta el siguiente período de mantenimiento.

```
aws rds modify-db-instance \
    --db-instance-identifier database-2 \
    --option-group-name test-se-2017 \
    --db-parameter-group-name test-sqlserver-se-2017 \
    --apply-immediately
```

Salida:

```
{
    "DBInstance": {
```

```
        "DBInstanceIdentifier": "database-2",
        "DBInstanceClass": "db.r4.large",
        "Engine": "sqlserver-se",
        "DBInstanceStatus": "available",

        ...output omitted...

        "DBParameterGroups": [
            {
                "DBParameterGroupName": "test-sqlserver-se-2017",
                "ParameterApplyStatus": "applying"
            }
        ],
        "AvailabilityZone": "us-west-2d",

        ...output omitted...

        "MultiAZ": true,
        "EngineVersion": "14.00.3281.6.v1",
        "AutoMinorVersionUpgrade": false,
        "ReadReplicaDBInstanceIdentifiers": [],
        "LicenseModel": "license-included",
        "OptionGroupMemberships": [
            {
                "OptionGroupName": "test-se-2017",
                "Status": "pending-apply"
            }
        ],
        "CharacterSetName": "SQL_Latin1_General_CP1_CI_AS",
        "SecondaryAvailabilityZone": "us-west-2c",
        "PubliclyAccessible": true,
        "StorageType": "gp2",

        ...output omitted...

        "DeletionProtection": false,
        "AssociatedRoles": [],
        "MaxAllocatedStorage": 1000
    }
}
```

Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS en la Guía del usuario de Amazon RDS.

Ejemplo 2: asociar un grupo de seguridad VPC con una instancia de base de datos

El siguiente ejemplo de `modify-db-instance` asocia un grupo de seguridad de VPC específico y elimina los grupos de seguridad de base de datos de una instancia de base de datos:

```
aws rds modify-db-instance \
    --db-instance-identifier dbName \
    --vpc-security-group-ids sg-ID
```

Salida:

```
{
"DBInstance": {
    "DBInstanceIdentifier": "dbName",
    "DBInstanceClass": "db.t3.micro",
    "Engine": "mysql",
    "DBInstanceStatus": "available",
    "MasterUsername": "admin",
    "Endpoint": {
        "Address": "dbName.abcdefghijk.us-west-2.rds.amazonaws.com",
        "Port": 3306,
        "HostedZoneId": "ABCDEFGHIJK1234"
    },
    "AllocatedStorage": 20,
    "InstanceCreateTime": "2024-02-15T00:37:58.793000+00:00",
    "PreferredBackupWindow": "11:57-12:27",
    "BackupRetentionPeriod": 7,
    "DBSecurityGroups": [],
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-ID",
            "Status": "active"
        }
    ],
    ... output omitted ...
    "MultiAZ": false,
    "EngineVersion": "8.0.35",
    "AutoMinorVersionUpgrade": true,
    "ReadReplicaDBInstanceIdentifiers": [],
    "LicenseModel": "general-public-license",

    ... output ommited ...
    }
```

```
}
```

Para obtener más información, consulte Control de acceso con grupos de seguridad en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte ModifyDBInstance en la Referencia de comandos de la AWS CLI.

`modify-db-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-parameter-group`.

AWS CLI

Modificación de un grupo de parámetros de base de datos

En el siguiente ejemplo `modify-db-parameter-group`, se cambia el valor del parámetro `clr enabled` en un grupo de parámetros de base de datos. El parámetro `--apply-immediately` hace que el grupo de parámetros de la base de datos se modifique de inmediato, en lugar de esperar hasta el siguiente período de mantenimiento.

```
aws rds modify-db-parameter-group \
    --db-parameter-group-name test-sqlserver-se-2017 \
    --parameters "ParameterName='clr
 enabled',ParameterValue=1,ApplyMethod=immediate"
```

Salida:

```
{
    "DBParameterGroupName": "test-sqlserver-se-2017"
}
```

Para obtener más información, consulte Modificación de parámetros de un grupo de parámetros de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte ModifyDBParameterGroup en la Referencia de comandos de la AWS CLI.

`modify-db-proxy-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-proxy-endpoint`.

AWS CLI

Para modificar un punto de conexión de proxy de base de datos para una base de datos de RDS

El siguiente ejemplo de `modify-db-proxy-endpoint` modifica un punto de conexión de proxy de base de datos `proxyEndpoint` para establecer el tiempo de espera de lectura en 65 segundos.

```
aws rds modify-db-proxy-endpoint \
    --db-proxy-endpoint-name proxyEndpoint \
    --cli-read-timeout 65
```

Salida:

```
{
"DBProxyEndpoint":
    {
        "DBProxyEndpointName": "proxyEndpoint",
        "DBProxyEndpointArn": "arn:aws:rds:us-east-1:123456789012:db-proxy-
endpoint:prx-endpoint-0123a01b12345c0ab",
        "DBProxyName": "proxyExample",
        "Status": "available",
        "VpcId": "vpc-1234567",
        "VpcSecurityGroupIds": [
            "sg-1234"
        ],
        "VpcSubnetIds": [
            "subnetgroup1",
            "subnetgroup2"
        ],
        "Endpoint": "proxyEndpoint.endpoint.proxyExample-ab0cd1efghij.us-
east-1.rds.amazonaws.com",
        "CreatedDate": "2023-04-05T16:09:33.452000+00:00",
        "TargetRole": "READ_WRITE",
        "IsDefault": "false"
    }
}
```

Para obtener más información, consulte Modificación de un punto de conexión de proxy en la Guía del usuario de Amazon RDS y Viewing a proxy endpoint en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte ModifyDbProxyEndpoint en la Referencia de comandos de la AWS CLI.

`modify-db-proxy-target-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-proxy-target-group`.

AWS CLI

Para modificar los puntos de conexión de un proxy de base de datos

El siguiente ejemplo de `modify-db-proxy-target-group` modifica un grupo de destino de proxy de base de datos para establecer el número máximo de conexiones en un 80 % y el máximo de conexiones inactivas en un 10 %.

```
aws rds modify-db-proxy-target-group \
    --target-group-name default \
    --db-proxy-name proxyExample \
    --connection-pool-config MaxConnectionsPercent=80,MaxIdleConnectionsPercent=10
```

Salida:

```
{
"DBProxyTargetGroup":
    {
        "DBProxyName": "proxyExample",
        "TargetGroupName": "default",
        "TargetGroupArn": "arn:aws:rds:us-east-1:123456789012:target-group:prx-
tg-0123a01b12345c0ab",
        "IsDefault": true,
        "Status": "available",
        "ConnectionPoolConfig": {
            "MaxConnectionsPercent": 80,
            "MaxIdleConnectionsPercent": 10,
            "ConnectionBorrowTimeout": 120,
            "SessionPinningFilters": []
        },
        "CreatedDate": "2023-05-02T18:41:19.495000+00:00",
        "UpdatedDate": "2023-05-02T18:41:21.762000+00:00"
    }
}
```

Para obtener más información, consulte Modificación de RDS Proxy en la Guía del usuario de Amazon RDS y Modificación de RDS Proxy en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte ModifyDbProxyTargetGroup en la Referencia de comandos de la AWS CLI.

`modify-db-proxy`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-proxy`.

AWS CLI

Para modificar un proxy de base de datos para una base de datos de RDS

El siguiente ejemplo de `modify-db-proxy` modifica un proxy de base de datos denominado `proxyExample` para que requiera SSL para sus conexiones.

```
aws rds modify-db-proxy \
    --db-proxy-name proxyExample \
    --require-tls
```

Salida:

```
{
"DBProxy":
    {
        "DBProxyName": "proxyExample",
        "DBProxyArn": "arn:aws:rds:us-east-1:123456789012:db-
proxy:prx-0123a01b12345c0ab",
        "Status": "modifying"
        "EngineFamily": "PostgreSQL",
        "VpcId": "sg-1234567",
        "VpcSecurityGroupIds": [
            "sg-1234"
        ],
        "VpcSubnetIds": [
            "subnetgroup1",
            "subnetgroup2"
        ],
        "Auth": "[
            {
                "Description": "proxydescription1",
                "AuthScheme": "SECRETS",
```

```
                "SecretArn": "arn:aws:secretsmanager:us-
west-2:123456789123:secret:proxysecret1-Abcd1e",
                "IAMAuth": "DISABLED"
            }
        ]",
        "RoleArn": "arn:aws:iam::12345678912:role/ProxyPostgreSQLRole",
        "Endpoint": "proxyExample.proxy-ab0cd1efghij.us-east-1.rds.amazonaws.com",
        "RequireTLS": true,
        "IdleClientTimeout": 1800,
        "DebuggingLogging": false,
        "CreatedDate": "2023-04-05T16:09:33.452000+00:00",
        "UpdatedDate": "2023-04-13T01:49:38.568000+00:00"
    }
}
```

Para obtener más información, consulte Modificación de RDS Proxy en la Guía del usuario de Amazon RDS y Creación de un RDS Proxy en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte ModifyDbProxy en la Referencia de comandos de la AWS CLI.

`modify-db-shard-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-shard-group`.

AWS CLI

Ejemplo 1: modificar un grupo de partición de base de datos

El siguiente ejemplo de `modify-db-shard-group` cambia la capacidad máxima de un grupo de partición de base de datos.

```
aws rds modify-db-shard-group \
    --db-shard-group-identifier my-db-shard-group \
    --max-acu 1000
```

Salida:

```
{
    "DBShardGroups": [
        {
            "DBShardGroupResourceId": "shardgroup-a6e3a0226aa243e2ac6c7a1234567890",
```

```
            "DBShardGroupIdentifier": "my-db-shard-group",
            "DBClusterIdentifier": "my-sv2-cluster",
            "MaxACU": 768.0,
            "ComputeRedundancy": 0,
            "Status": "available",
            "PubliclyAccessible": false,
            "Endpoint": "my-sv2-cluster.limitless-cekycexample.us-
east-2.rds.amazonaws.com"
        }
    ]
}
```

Para obtener más información, consulte la sección sobre Clústeres de base de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora.

Ejemplo 2: describir sus grupos de partición de base de datos

En el siguiente ejemplo de `describe-db-shard-groups`, se recuperan los detalles sobre los grupos de partición de base de datos después de ejecutar `modify-db-shard-group`. La capacidad máxima del grupo de partición de base de datos `my-db-shard-group` es ahora de 1000 unidades de capacidad de Aurora (ACU).

```
aws rds describe-db-shard-groups
```

Salida:

```
{
    "DBShardGroups": [
        {
            "DBShardGroupResourceId": "shardgroup-7bb446329da94788b3f957746example",
            "DBShardGroupIdentifier": "limitless-test-shard-grp",
            "DBClusterIdentifier": "limitless-test-cluster",
            "MaxACU": 768.0,
            "ComputeRedundancy": 0,
            "Status": "available",
            "PubliclyAccessible": true,
            "Endpoint": "limitless-test-cluster.limitless-cekycexample.us-
east-2.rds.amazonaws.com"
        },
        {
            "DBShardGroupResourceId": "shardgroup-a6e3a0226aa243e2ac6c7a1234567890",
            "DBShardGroupIdentifier": "my-db-shard-group",
```

```
            "DBClusterIdentifier": "my-sv2-cluster",
            "MaxACU": 1000.0,
            "ComputeRedundancy": 0,
            "Status": "available",
            "PubliclyAccessible": false,
            "Endpoint": "my-sv2-cluster.limitless-cekycexample.us-
east-2.rds.amazonaws.com"
        }
    ]
}
```

Para obtener más información, consulte la sección sobre Clústeres de base de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte ModifyDbShardGroup en la Referencia de comandos de la AWS CLI.

`modify-db-snapshot-attribute`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-snapshot-attribute`.

AWS CLI

Ejemplo 1: habilitar dos cuentas de AWS para que restauren una instantánea de base de datos

El siguiente ejemplo de `modify-db-snapshot-attribute` da permiso a dos cuentas de AWS, con los identificadores `111122223333` y `444455556666`, para restaurar la instantánea de base de datos denominada `mydbsnapshot`.

```
aws rds modify-db-snapshot-attribute \
    --db-snapshot-identifier mydbsnapshot \
    --attribute-name restore \
    --values-to-add {"111122223333","444455556666"}
```

Salida:

```
{
    "DBSnapshotAttributesResult": {
        "DBSnapshotIdentifier": "mydbsnapshot",
        "DBSnapshotAttributes": [
            {
                "AttributeName": "restore",
```

```
                "AttributeValues": [
                    "111122223333",
                    "444455556666"
                ]
            }
        ]
    }
}
```

Para obtener más información, consulte Uso compartido de una instantánea en la Guía del usuario de Amazon RDS.

Ejemplo 2: evitar que una cuenta de AWS restaure una instantánea de base de datos

El siguiente ejemplo de `modify-db-snapshot-attribute` elimina el permiso de una cuenta de AWS concreta para restaurar la instantánea de base de datos denominada `mydbsnapshot`. Al especificar una sola cuenta, el identificador de la cuenta no puede estar entre comillas o corchetes.

```
aws rds modify-db-snapshot-attribute \
    --db-snapshot-identifier mydbsnapshot \
    --attribute-name restore \
    --values-to-remove 444455556666
```

Salida:

```
{
    "DBSnapshotAttributesResult": {
        "DBSnapshotIdentifier": "mydbsnapshot",
        "DBSnapshotAttributes": [
            {
                "AttributeName": "restore",
                "AttributeValues": [
                    "111122223333"
                ]
            }
        ]
    }
}
```

Para obtener más información, consulte Uso compartido de una instantánea en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte ModifyDbSnapshotAttribute en la Referencia de comandos de la AWS CLI.

`modify-db-snapshot-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-snapshot-attributes`.

AWS CLI

Para modificar un atributo de la instantánea de una base de datos

El siguiente ejemplo de `modify-db-snapshot-attribute` permite a dos identificadores de cuenta de AWS, `111122223333` y `444455556666`, restaurar la instantánea de base de datos denominada `mydbsnapshot`.

```
aws rds modify-db-snapshot-attribute \
    --db-snapshot-identifier mydbsnapshot \
    --attribute-name restore \
    --values-to-add '["111122223333","444455556666"]'
```

Salida:

```
{
    "DBSnapshotAttributesResult": {
        "DBSnapshotIdentifier": "mydbsnapshot",
        "DBSnapshotAttributes": [
            {
                "AttributeName": "restore",
                "AttributeValues": [
                    "111122223333",
                    "444455556666"
                ]
            }
        ]
    }
}
```

Para obtener más información, consulte Uso compartido de una instantánea en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte ModifyDbSnapshotAttributes en la Referencia de comandos de la AWS CLI.

`modify-db-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-snapshot`.

AWS CLI

Para modificar una instantánea de base de datos

En el siguiente ejemplo de `modify-db-snapshot` se actualiza una instantánea de PostgreSQL 10.6 denominada `db5-snapshot-upg-test` a PostgreSQL 11.7. La nueva versión del motor de base de datos se muestra cuando la instantánea ha terminado de actualizarse y su estado está disponible.

```
aws rds modify-db-snapshot \
    --db-snapshot-identifier db5-snapshot-upg-test \
    --engine-version 11.7
```

Salida:

```
{
    "DBSnapshot": {
        "DBSnapshotIdentifier": "db5-snapshot-upg-test",
        "DBInstanceIdentifier": "database-5",
        "SnapshotCreateTime": "2020-03-27T20:49:17.092Z",
        "Engine": "postgres",
        "AllocatedStorage": 20,
        "Status": "upgrading",
        "Port": 5432,
        "AvailabilityZone": "us-west-2a",
        "VpcId": "vpc-2ff27557",
        "InstanceCreateTime": "2020-03-27T19:59:04.735Z",
        "MasterUsername": "postgres",
        "EngineVersion": "10.6",
        "LicenseModel": "postgresql-license",
        "SnapshotType": "manual",
        "OptionGroupName": "default:postgres-11",
        "PercentProgress": 100,
        "StorageType": "gp2",
        "Encrypted": false,
        "DBSnapshotArn": "arn:aws:rds:us-west-2:123456789012:snapshot:db5-snapshot-
upg-test",
        "IAMDatabaseAuthenticationEnabled": false,
        "ProcessorFeatures": [],
```

```
        "DbiResourceId": "db-GJMF75LM42IL6BTFRE4UZJ5YM4"
    }
}
```

Para obtener más información, consulte Upgrading a PostgreSQL DB Snapshot en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte ModifyDbSnapshot en la Referencia de comandos de la AWS CLI.

`modify-db-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-db-subnet-group`.

AWS CLI

Para modificar un grupo de subred de base de datos

El siguiente ejemplo de `modify-db-subnet-group` agrega una subred con el ID `subnet-08e41f9e230222222` al grupo de subredes de base de datos denominado `mysubnetgroup`. Para mantener las subredes existentes en el grupo de subredes, incluya sus ID como valores en la opción `--subnet-ids`. Asegúrese de tener subredes con, al menos, dos zonas de disponibilidad distintas en el grupo de subred de base de datos.

```
aws rds modify-db-subnet-group \
    --db-subnet-group-name mysubnetgroup \
    --subnet-ids
 '["subnet-0a1dc4e1a6f123456","subnet-070dd7ecb3aaaaaaa","subnet-00f5b198bc0abcdef","subnet-
```

Salida:

```
{
    "DBSubnetGroup": {
        "DBSubnetGroupName": "mysubnetgroup",
        "DBSubnetGroupDescription": "test DB subnet group",
        "VpcId": "vpc-0f08e7610a1b2c3d4",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-08e41f9e230222222",
                "SubnetAvailabilityZone": {
                    "Name": "us-west-2a"
```

```
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-070dd7ecb3aaaaaaa",
                "SubnetAvailabilityZone": {
                    "Name": "us-west-2b"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-00f5b198bc0abcdef",
                "SubnetAvailabilityZone": {
                    "Name": "us-west-2d"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-0a1dc4e1a6f123456",
                "SubnetAvailabilityZone": {
                    "Name": "us-west-2b"
                },
                "SubnetStatus": "Active"
            }
        ],
        "DBSubnetGroupArn": "arn:aws:rds:us-
west-2:534026745191:subgrp:mysubnetgroup"
    }
}
```

Para obtener más información, consulte Paso 3: Crear un grupo de subredes de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener detalles sobre la API, consulte ModifyDbSubnetGroup en la Referencia de comandos de la AWS CLI.

`modify-event-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-event-subscription`.

AWS CLI

Para modificar una suscripción a un evento

El siguiente ejemplo de `modify-event-subscription` deshabilita la suscripción al evento especificada, de modo que ya no publique notificaciones en el tema especificado de Amazon Simple Notification Service.

```
aws rds modify-event-subscription \
    --subscription-name my-instance-events \
    --no-enabled
```

Salida:

```
{
    "EventSubscription": {
        "EventCategoriesList": [
            "backup",
            "recovery"
        ],
        "CustomerAwsId": "123456789012",
        "SourceType": "db-instance",
        "SubscriptionCreationTime": "Tue Jul 31 23:22:01 UTC 2018",
        "EventSubscriptionArn": "arn:aws:rds:us-east-1:123456789012:es:my-instance-
events",
        "SnsTopicArn": "arn:aws:sns:us-east-1:123456789012:interesting-events",
        "CustSubscriptionId": "my-instance-events",
        "Status": "modifying",
        "Enabled": false
    }
}
```

- Para obtener información sobre la API, consulte ModifyEventSubscription en la Referencia de comandos de la AWS CLI.

`modify-global-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-global-cluster`.

AWS CLI

Para modificar un clúster de base de datos global

En el siguiente ejemplo de `modify-global-cluster`, se habilita la protección contra la eliminación de un clúster de base de datos global compatible con Aurora MySQL.

```
aws rds modify-global-cluster \
    --global-cluster-identifier myglobalcluster \
    --deletion-protection
```

Salida:

```
{
    "GlobalCluster": {
        "GlobalClusterIdentifier": "myglobalcluster",
        "GlobalClusterResourceId": "cluster-f0e523bfe07aabb",
        "GlobalClusterArn": "arn:aws:rds::123456789012:global-
cluster:myglobalcluster",
        "Status": "available",
        "Engine": "aurora-mysql",
        "EngineVersion": "5.7.mysql_aurora.2.07.2",
        "StorageEncrypted": false,
        "DeletionProtection": true,
        "GlobalClusterMembers": []
    }
}
```

Para obtener más información, consulte Administración de una base de datos global de Amazon Aurora en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte ModifyGlobalCluster en la Referencia de comandos de la AWS CLI.

`promote-read-replica-db-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `promote-read-replica-db-cluster`.

AWS CLI

Para promocionar una réplica de lectura del clúster de base de datos

En el siguiente ejemplo de `promote-read-replica-db-cluster`, se promociona que la réplica de lectura especificada sea un clúster de base de datos independiente.

```
aws rds promote-read-replica-db-cluster \
    --db-cluster-identifier mydbcluster-1
```

Salida:

```
{
    "DBCluster": {
        "AllocatedStorage": 1,
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1b",
            "us-east-1c"
        ],
        "BackupRetentionPeriod": 1,
        "DatabaseName": "",
        "DBClusterIdentifier": "mydbcluster-1",
        ...some output truncated...
    }
}
```

Para obtener más información, consulte Promoting a read replica to be a DB cluster en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte PromoteReadReplicaDbCluster en la Referencia de comandos de la AWS CLI.

`promote-read-replica`

En el siguiente ejemplo de código, se muestra cómo utilizar `promote-read-replica`.

AWS CLI

Para promocionar una réplica de lectura

En el siguiente ejemplo de `promote-read-replica`, se promociona que la réplica de lectura especificada sea una instancia de base de datos independiente.

```
aws rds promote-read-replica \
    --db-instance-identifier test-instance-repl
```

Salida:

```
{
    "DBInstance": {
        "DBInstanceArn": "arn:aws:rds:us-east-1:123456789012:db:test-instance-repl",
```

```
        "StorageType": "standard",
        "ReadReplicaSourceDBInstanceIdentifier": "test-instance",
        "DBInstanceStatus": "modifying",
        ...some output truncated...
    }
}
```

- Para obtener información acerca de la API, consulte PromoteReadReplica en la Referencia de comandos de la AWS CLI.

`purchase-reserved-db-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `purchase-reserved-db-instance`.

AWS CLI

Para adquirir una oferta de instancia de base de datos reservada

En el ejemplo siguiente de `purchase-reserved-db-instances-offering`, se adquiere una oferta de instancia de base de datos reservada. `reserved-db-instances-offering-id` debe ser un identificador de oferta válido, tal como lo devuelve el comando `describe-reserved-db-instances-offering`.

aws rds purchase-reserved-db-instances-offering --reserved-db-instances-offering-id 438012d3-4a52-4cc7-b2e3-8dff72e0e706

- Para obtener información sobre la API, consulte PurchaseReservedDbInstance en la Referencia de comandos de la AWS CLI.

`purchase-reserved-db-instances-offerings`

En el siguiente ejemplo de código, se muestra cómo utilizar `purchase-reserved-db-instances-offerings`.

AWS CLI

Ejemplo 1: buscar una instancia de base de datos reservada y comprarla

En el siguiente ejemplo de `describe-reserved-db-instances-offerings`, se generan listas de las instancias de base de datos MySQL reservadas disponibles con la clase de instancia db.t2.micro y una duración de un año. El ID de oferta es obligatorio para comprar una instancia de base de datos reservada.

```
aws rds describe-reserved-db-instances-offerings \
    --product-description mysql \
    --db-instance-class db.t2.micro \
    --duration 1
```

Salida:

```
{
    "ReservedDBInstancesOfferings": [
        {
            "ReservedDBInstancesOfferingId": "8ba30be1-b9ec-447f-8f23-6114e3f4c7b4",
            "DBInstanceClass": "db.t2.micro",
            "Duration": 31536000,
            "FixedPrice": 51.0,
            "UsagePrice": 0.0,
            "CurrencyCode": "USD",
            "ProductDescription": "mysql",
            "OfferingType": "Partial Upfront",
            "MultiAZ": false,
            "RecurringCharges": [
                {
                    "RecurringChargeAmount": 0.006,
                    "RecurringChargeFrequency": "Hourly"
                }
            ]
        },
    ... some output truncated ...
    ]
}
```

Para obtener más información, consulte la sección sobre Instancias de base de datos reservadas para Amazon RDS en la Guía del usuario de Amazon RDS.

Ejemplo 2: adquirir una instancia de base de datos reservada

El siguiente ejemplo de `purchase-reserved-db-instances-offering` muestra cómo comprar la oferta de instancia de base de datos reservada del ejemplo anterior.

aws rds purchase-reserved-db-instances-offering --reserved-db-instances-offering-id 8ba30be1-b9ec-447f-8f23-6114e3f4c7b4

Salida:

```
{
    "ReservedDBInstance": {
        "ReservedDBInstanceId": "ri-2020-06-29-16-54-57-670",
        "ReservedDBInstancesOfferingId": "8ba30be1-b9ec-447f-8f23-6114e3f4c7b4",
        "DBInstanceClass": "db.t2.micro",
        "StartTime": "2020-06-29T16:54:57.670Z",
        "Duration": 31536000,
        "FixedPrice": 51.0,
        "UsagePrice": 0.0,
        "CurrencyCode": "USD",
        "DBInstanceCount": 1,
        "ProductDescription": "mysql",
        "OfferingType": "Partial Upfront",
        "MultiAZ": false,
        "State": "payment-pending",
        "RecurringCharges": [
            {
                "RecurringChargeAmount": 0.006,
                "RecurringChargeFrequency": "Hourly"
            }
        ],
        "ReservedDBInstanceArn": "arn:aws:rds:us-
west-2:123456789012:ri:ri-2020-06-29-16-54-57-670"
    }
}
```

Para obtener más información, consulte la sección sobre Instancias de base de datos reservadas para Amazon RDS en la Guía del usuario de Amazon RDS.

- Para obtener más información sobre la API, consulte PurchaseReservedDbInstancesOfferings en la Referencia de comandos de la AWS CLI.

`reboot-db-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `reboot-db-instance`.

AWS CLI

Reinicio de una instancia de base de datos

En el siguiente ejemplo `reboot-db-instance`, se inicia un reinicio de la instancia de base de datos especificada.

```
aws rds reboot-db-instance \
    --db-instance-identifier test-mysql-instance
```

Salida:

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "test-mysql-instance",
        "DBInstanceClass": "db.t3.micro",
        "Engine": "mysql",
        "DBInstanceStatus": "rebooting",
        "MasterUsername": "admin",
        "Endpoint": {
            "Address": "test-mysql-instance.############.us-
west-2.rds.amazonaws.com",
            "Port": 3306,
            "HostedZoneId": "Z1PVIF0EXAMPLE"
        },

    ... output omitted...

    }
}
```

Para obtener más información, consulte Reinicio de una instancia de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte RebootDBInstance en la Referencia de comandos de la AWS CLI.

`reboot-db-shard-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `reboot-db-shard-group`.

AWS CLI

Ejemplo 1: reiniciar un grupo de partición de base de datos

En el siguiente ejemplo de `reboot-db-shard-group`, se reinicia un grupo de partición de base de datos.

```
aws rds reboot-db-shard-group \
```

```
    --db-shard-group-identifier my-db-shard-group
```

Salida:

```
{
    "DBShardGroups": [
        {
            "DBShardGroupResourceId": "shardgroup-a6e3a0226aa243e2ac6c7a1234567890",
            "DBShardGroupIdentifier": "my-db-shard-group",
            "DBClusterIdentifier": "my-sv2-cluster",
            "MaxACU": 1000.0,
            "ComputeRedundancy": 0,
            "Status": "available",
            "PubliclyAccessible": false,
            "Endpoint": "my-sv2-cluster.limitless-cekycexample.us-
east-2.rds.amazonaws.com"
        }
    ]
}
```

Para obtener más información, consulte Reinicio de un clúster de base de datos de Amazon Aurora o de una instancia de base de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora.

Ejemplo 2: describir sus grupos de partición de base de datos

En el siguiente ejemplo de `describe-db-shard-groups`, se recuperan los detalles sobre los grupos de partición de base de datos después de ejecutar `reboot-db-shard-group`. El grupo de partición de base de datos `my-db-shard-group` se está reiniciando ahora.

```
aws rds describe-db-shard-groups
```

Salida:

```
{
    "DBShardGroups": [
        {
            "DBShardGroupResourceId": "shardgroup-7bb446329da94788b3f957746example",
            "DBShardGroupIdentifier": "limitless-test-shard-grp",
            "DBClusterIdentifier": "limitless-test-cluster",
            "MaxACU": 768.0,
            "ComputeRedundancy": 0,
```

```
            "Status": "available",
            "PubliclyAccessible": true,
            "Endpoint": "limitless-test-cluster.limitless-cekycexample.us-
east-2.rds.amazonaws.com"
        },
        {
            "DBShardGroupResourceId": "shardgroup-a6e3a0226aa243e2ac6c7a1234567890",
            "DBShardGroupIdentifier": "my-db-shard-group",
            "DBClusterIdentifier": "my-sv2-cluster",
            "MaxACU": 1000.0,
            "ComputeRedundancy": 0,
            "Status": "rebooting",
            "PubliclyAccessible": false,
            "Endpoint": "my-sv2-cluster.limitless-cekycexample.us-
east-2.rds.amazonaws.com"
        }
    ]
}
```

Para obtener más información, consulte Reinicio de un clúster de base de datos de Amazon Aurora o de una instancia de base de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora.

- Para obtener más información sobre la API, consulte RebootDbShardGroup en la Referencia de comandos de la AWS CLI.

`register-db-proxy-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-db-proxy-targets`.

AWS CLI

Para registrar un proxy de base de datos con una base de datos

En el siguiente ejemplo de `register-db-proxy-targets`, se crea la asociación entre una base de datos y un proxy.

```
aws rds register-db-proxy-targets \
    --db-proxy-name proxyExample \
    --db-cluster-identifiers database-5
```

Salida:

```
{
    "DBProxyTargets": [
        {
            "RdsResourceId": "database-5",
            "Port": 3306,
            "Type": "TRACKED_CLUSTER",
            "TargetHealth": {
                "State": "REGISTERING"
            }
        },
        {
            "Endpoint": "database-5instance-1.ab0cd1efghij.us-
east-1.rds.amazonaws.com",
            "RdsResourceId": "database-5",
            "Port": 3306,
            "Type": "RDS_INSTANCE",
            "TargetHealth": {
                "State": "REGISTERING"
            }
        }
    ]
}
```

Para obtener más información, consulte Creación de un RDS Proxy en la Guía del usuario de Amazon RDS y Creación de un RDS Proxy en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte RegisterDbProxyTargets en la Referencia de comandos de la AWS CLI.

`remove-from-global-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-from-global-cluster`.

AWS CLI

Para separar un clúster secundario de Aurora de un clúster de base de datos global de Aurora

El siguiente ejemplo de `remove-from-global-cluster` separa un clúster secundario de Aurora de un clúster de base de datos global de Aurora. El clúster pasa de ser de solo lectura a un clúster independiente con capacidad de lectura y escritura.

```
aws rds remove-from-global-cluster \
```

```
    --region us-west-2 \
    --global-cluster-identifier myglobalcluster \
    --db-cluster-identifier arn:aws:rds:us-west-2:123456789012:cluster:DB-1
```

Salida:

```
{
    "GlobalCluster": {
        "GlobalClusterIdentifier": "myglobalcluster",
        "GlobalClusterResourceId": "cluster-abc123def456gh",
        "GlobalClusterArn": "arn:aws:rds::123456789012:global-
cluster:myglobalcluster",
        "Status": "available",
        "Engine": "aurora-postgresql",
        "EngineVersion": "10.11",
        "StorageEncrypted": true,
        "DeletionProtection": false,
        "GlobalClusterMembers": [
            {
                "DBClusterArn": "arn:aws:rds:us-east-1:123456789012:cluster:js-
global-cluster",
                "Readers": [
                    "arn:aws:rds:us-west-2:123456789012:cluster:DB-1"
                ],
                "IsWriter": true
            },
            {
                "DBClusterArn": "arn:aws:rds:us-west-2:123456789012:cluster:DB-1",
                "Readers": [],
                "IsWriter": false,
                "GlobalWriteForwardingStatus": "disabled"
            }
        ]
    }
}
```

Para obtener más información, consulte Eliminación de un clúster de una base de datos global de Amazon Aurora en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte RemoveFromGlobalCluster en la Referencia de comandos de la AWS CLI.

`remove-option-from-option-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-option-from-option-group`.

AWS CLI

Para eliminar una opción de un grupo de opciones

En el ejemplo siguiente `remove-option-from-option-group` se elimina la opción `OEM` de `myoptiongroup`.

```
aws rds remove-option-from-option-group \
    --option-group-name myoptiongroup \
    --options OEM \
    --apply-immediately
```

Salida:

```
{
    "OptionGroup": {
        "OptionGroupName": "myoptiongroup",
        "OptionGroupDescription": "Test",
        "EngineName": "oracle-ee",
        "MajorEngineVersion": "19",
        "Options": [],
        "AllowsVpcAndNonVpcInstanceMemberships": true,
        "OptionGroupArn": "arn:aws:rds:us-east-1:123456789012:og:myoptiongroup"
    }
}
```

Para obtener más información, consulte Quitar una opción de un grupo de opciones en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte RemoveOptionFromOptionGroup en la Referencia de comandos de la AWS CLI.

`remove-role-from-db-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-role-from-db-cluster`.

AWS CLI

Para desasociar un rol de AWS Identity and Access Management (IAM) de un clúster de base de datos

En el siguiente ejemplo de `remove-role-from-db-cluster`, se quita un rol de un clúster de base de datos.

```
aws rds remove-role-from-db-cluster \
    --db-cluster-identifier mydbcluster \
    --role-arn arn:aws:iam::123456789012:role/RDSLoadFromS3
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Asociación de un rol de IAM con un clúster de base de datos Amazon Aurora MySQL en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte RemoveRoleFromDbCluster en la Referencia de comandos de la AWS CLI.

`remove-role-from-db-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-role-from-db-instance`.

AWS CLI

Para desasociar un rol de AWS Identity and Access Management (IAM) de una instancia de base de datos

El siguiente ejemplo de `remove-role-from-db-instance` elimina el rol denominado `rds-s3-integration-role` de una instancia de base de datos de Oracle denominada `test-instance`.

```
aws rds remove-role-from-db-instance \
    --db-instance-identifier test-instance \
    --feature-name S3_INTEGRATION \
    --role-arn arn:aws:iam::111122223333:role/rds-s3-integration-role
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Desactivación de la integración de RDS for SQL Server con S3 en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte RemoveRoleFromDbInstance en la Referencia de comandos de la AWS CLI.

`remove-source-identifier-from-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-source-identifier-from-subscription`.

AWS CLI

Para quitar un identificador de origen de una suscripción

En el siguiente ejemplo de `remove-source-identifier`, se elimina el identificador de origen especificado de una suscripción existente.

```
aws rds remove-source-identifier-from-subscription \
    --subscription-name my-instance-events \
    --source-identifier test-instance-repl
```

Salida:

```
{
    "EventSubscription": {
        "EventSubscriptionArn": "arn:aws:rds:us-east-1:123456789012:es:my-instance-
events",
        "SubscriptionCreationTime": "Tue Jul 31 23:22:01 UTC 2018",
        "EventCategoriesList": [
            "backup",
            "recovery"
        ],
        "SnsTopicArn": "arn:aws:sns:us-east-1:123456789012:interesting-events",
        "Status": "modifying",
        "CustSubscriptionId": "my-instance-events",
        "CustomerAwsId": "123456789012",
        "SourceIdsList": [
            "test-instance"
        ],
        "SourceType": "db-instance",
        "Enabled": false
    }
}
```

- Para obtener información sobre la API, consulte RemoveSourceIdentifierFromSubscription en la Referencia de comandos de la AWS CLI.

`remove-tags-from-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-tags-from-resource`.

AWS CLI

Para eliminar etiquetas de un recurso

En el siguiente ejemplo de `remove-tags-from-resource`, se eliminan las etiquetas de un recurso.

```
aws rds remove-tags-from-resource \
    --resource-name arn:aws:rds:us-east-1:123456789012:db:mydbinstance \
    --tag-keys Name Environment
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de los recursos de Amazon RDS en la Guía del usuario de Amazon RDS y Etiquetado de los recursos de Amazon RDS en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte RemoveTagsFromResource en la Referencia de comandos de la AWS CLI.

`reset-db-cluster-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-db-cluster-parameter-group`.

AWS CLI

Ejemplo 1: restablecimiento de todos los parámetros a sus valores predeterminados

El siguiente ejemplo de `reset-db-cluster-parameter-group` restablece todos los valores de los parámetros de un grupo de parámetros de clúster de base de datos creado por el cliente a sus valores predeterminados.

```
aws rds reset-db-cluster-parameter-group \
    --db-cluster-parameter-group-name mydbclpg \
```

```
    --reset-all-parameters
```

Salida:

```
{
    "DBClusterParameterGroupName": "mydbclpg"
}
```

Para obtener más información, consulte Working with DB Parameter Groups and DB Cluster Parameter Groups en la Guía del usuario de Amazon Aurora.

Ejemplo 2: restablecer los parámetros específicos a sus valores predeterminados

El siguiente ejemplo de `reset-db-cluster-parameter-group` restablece todos los valores de los parámetros de unos parámetros especificados a sus valores predeterminados en un grupo de parámetros de clúster de base de datos creado por el cliente.

```
aws rds reset-db-cluster-parameter-group \
    --db-cluster-parameter-group-name mydbclpgy \
    --parameters "ParameterName=max_connections,ApplyMethod=immediate" \
                 "ParameterName=max_allowed_packet,ApplyMethod=immediate"
```

Salida:

```
{
    "DBClusterParameterGroupName": "mydbclpg"
}
```

Para obtener más información, consulte Working with DB Parameter Groups and DB Cluster Parameter Groups en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte ResetDbClusterParameterGroup en la Referencia de comandos de la AWS CLI.

`reset-db-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-db-parameter-group`.

AWS CLI

Ejemplo 1: restablecimiento de todos los parámetros a sus valores predeterminados

El siguiente ejemplo de `reset-db-parameter-group` restablece todos los valores de los parámetros de un grupo de parámetros de base de datos creado por el cliente a sus valores predeterminados.

```
aws rds reset-db-parameter-group \
    --db-parameter-group-name mypg \
    --reset-all-parameters
```

Salida:

```
{
    "DBParameterGroupName": "mypg"
}
```

Para obtener más información, consulte Working with DB parameter groups en la Guía del usuario de Amazon RDS y Working with DB parameter groups and DB cluster parameter groups en la Guía del usuario de Amazon Aurora.

Ejemplo 2: restablecer los parámetros específicos a sus valores predeterminados

El siguiente ejemplo de `reset-db-parameter-group` restablece todos los valores de los parámetros de unos parámetros específicos a sus valores predeterminados en un grupo de parámetros de base de datos creado por el cliente.

```
aws rds reset-db-parameter-group \
    --db-parameter-group-name mypg \
    --parameters "ParameterName=max_connections,ApplyMethod=immediate" \
                 "ParameterName=max_allowed_packet,ApplyMethod=immediate"
```

Salida:

```
{
    "DBParameterGroupName": "mypg"
}
```

Para obtener más información, consulte Working with DB parameter groups en la Guía del usuario de Amazon RDS y Working with DB parameter groups and DB cluster parameter groups en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte ResetDbParameterGroup en la Referencia de comandos de la AWS CLI.

`restore-db-cluster-from-s3`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-db-cluster-from-s3`.

AWS CLI

Para restaurar un clúster de base de datos de Amazon Aurora desde Amazon S3

El siguiente ejemplo de `restore-db-cluster-from-s3` restaura un clúster de base de datos compatible con Amazon Aurora MySQL versión 5.7 a partir de un archivo de copia de seguridad de base de datos de MySQL 5.7 en Amazon S3.

```
aws rds restore-db-cluster-from-s3 \
    --db-cluster-identifier cluster-s3-restore \
    --engine aurora-mysql \
    --master-username admin \
    --master-user-password mypassword \
    --s3-bucket-name amzn-s3-demo-bucket \
    --s3-prefix test-backup \
    --s3-ingestion-role-arn arn:aws:iam::123456789012:role/service-role/TestBackup \
    --source-engine mysql \
    --source-engine-version 5.7.28
```

Salida:

```
{
    "DBCluster": {
        "AllocatedStorage": 1,
        "AvailabilityZones": [
            "us-west-2c",
            "us-west-2a",
            "us-west-2b"
        ],
        "BackupRetentionPeriod": 1,
        "DBClusterIdentifier": "cluster-s3-restore",
        "DBClusterParameterGroup": "default.aurora-mysql5.7",
        "DBSubnetGroup": "default",
        "Status": "creating",
        "Endpoint": "cluster-s3-restore.cluster-co3xyzabc123.us-
west-2.rds.amazonaws.com",
        "ReaderEndpoint": "cluster-s3-restore.cluster-ro-co3xyzabc123.us-
west-2.rds.amazonaws.com",
```

```
        "MultiAZ": false,
        "Engine": "aurora-mysql",
        "EngineVersion": "5.7.12",
        "Port": 3306,
        "MasterUsername": "admin",
        "PreferredBackupWindow": "11:15-11:45",
        "PreferredMaintenanceWindow": "thu:12:19-thu:12:49",
        "ReadReplicaIdentifiers": [],
        "DBClusterMembers": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-########",
                "Status": "active"
            }
        ],
        "HostedZoneId": "Z1PVIF0EXAMPLE",
        "StorageEncrypted": false,
        "DbClusterResourceId": "cluster-SU5THYQQHOWCXZZDGXREXAMPLE",
        "DBClusterArn": "arn:aws:rds:us-west-2:123456789012:cluster:cluster-s3-
restore",
        "AssociatedRoles": [],
        "IAMDatabaseAuthenticationEnabled": false,
        "ClusterCreateTime": "2020-07-27T14:22:08.095Z",
        "EngineMode": "provisioned",
        "DeletionProtection": false,
        "HttpEndpointEnabled": false,
        "CopyTagsToSnapshot": false,
        "CrossAccountClone": false,
        "DomainMemberships": []
    }
}
```

Para obtener más información, consulte Migrating Data from MySQL by Using an Amazon S3 Bucket en la Guía del usuario de Amazon Aurora.

- Para obtener detalles de la API, consulte RestoreDbClusterFromS3 en la Referencia de comandos de la AWS CLI.

`restore-db-cluster-from-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-db-cluster-from-snapshot`.

AWS CLI

Para para restaurar un clúster de base de datos desde una instantánea

A continuación, `restore-db-cluster-from-snapshot` restaura un clúster de base de datos Aurora PostgreSQL compatible con la versión 10.7 de PostgreSQL a partir de una instantánea de clúster de base de datos denominada `test-instance-snapshot`.

```
aws rds restore-db-cluster-from-snapshot \
    --db-cluster-identifier newdbcluster \
    --snapshot-identifier test-instance-snapshot \
    --engine aurora-postgresql \
    --engine-version 10.7
```

Salida:

```
{
    "DBCluster": {
        "AllocatedStorage": 1,
        "AvailabilityZones": [
            "us-west-2c",
            "us-west-2a",
            "us-west-2b"
        ],
        "BackupRetentionPeriod": 7,
        "DatabaseName": "",
        "DBClusterIdentifier": "newdbcluster",
        "DBClusterParameterGroup": "default.aurora-postgresql10",
        "DBSubnetGroup": "default",
        "Status": "creating",
        "Endpoint": "newdbcluster.cluster-############.us-west-2.rds.amazonaws.com",
        "ReaderEndpoint": "newdbcluster.cluster-ro-############.us-
west-2.rds.amazonaws.com",
        "MultiAZ": false,
        "Engine": "aurora-postgresql",
        "EngineVersion": "10.7",
        "Port": 5432,
        "MasterUsername": "postgres",
        "PreferredBackupWindow": "09:33-10:03",
        "PreferredMaintenanceWindow": "sun:12:22-sun:12:52",
        "ReadReplicaIdentifiers": [],
        "DBClusterMembers": [],
        "VpcSecurityGroups": [
```

```
            {
                "VpcSecurityGroupId": "sg-########",
                "Status": "active"
            }
        ],
        "HostedZoneId": "Z1PVIF0EXAMPLE",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/287364e4-33e3-4755-a3b0-
a1b2c3d4e5f6",
        "DbClusterResourceId": "cluster-5DSB5IFQDDUVAWOUWM1EXAMPLE",
        "DBClusterArn": "arn:aws:rds:us-west-2:123456789012:cluster:newdbcluster",
        "AssociatedRoles": [],
        "IAMDatabaseAuthenticationEnabled": false,
        "ClusterCreateTime": "2020-06-05T15:06:58.634Z",
        "EngineMode": "provisioned",
        "DeletionProtection": false,
        "HttpEndpointEnabled": false,
        "CopyTagsToSnapshot": false,
        "CrossAccountClone": false,
        "DomainMemberships": []
    }
}
```

Para obtener más información, consulte Restauración de una instantánea de clúster de base de datos en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte RestoreDbClusterFromSnapshot en la Referencia de comandos de la AWS CLI.

`restore-db-cluster-to-point-in-time`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-db-cluster-to-point-in-time`.

AWS CLI

Para restaurar un clúster de bases de datos a un momento indicado

En el siguiente ejemplo de `restore-db-cluster-to-point-in-time`, se restaura el clúster de base de datos denominado `database-4` al último momento posible. Si se usa `copy-on-write` como tipo de restauración, se restaura el nuevo clúster de base de datos como un clon del clúster de base de datos de origen.

```
aws rds restore-db-cluster-to-point-in-time \
    --source-db-cluster-identifier database-4 \
    --db-cluster-identifier sample-cluster-clone \
    --restore-type copy-on-write \
    --use-latest-restorable-time
```

Salida:

```
{
    "DBCluster": {
        "AllocatedStorage": 1,
        "AvailabilityZones": [
            "us-west-2c",
            "us-west-2a",
            "us-west-2b"
        ],
        "BackupRetentionPeriod": 7,
        "DatabaseName": "",
        "DBClusterIdentifier": "sample-cluster-clone",
        "DBClusterParameterGroup": "default.aurora-postgresql10",
        "DBSubnetGroup": "default",
        "Status": "creating",
        "Endpoint": "sample-cluster-clone.cluster-############.us-
west-2.rds.amazonaws.com",
        "ReaderEndpoint": "sample-cluster-clone.cluster-ro-############.us-
west-2.rds.amazonaws.com",
        "MultiAZ": false,
        "Engine": "aurora-postgresql",
        "EngineVersion": "10.7",
        "Port": 5432,
        "MasterUsername": "postgres",
        "PreferredBackupWindow": "09:33-10:03",
        "PreferredMaintenanceWindow": "sun:12:22-sun:12:52",
        "ReadReplicaIdentifiers": [],
        "DBClusterMembers": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-########",
                "Status": "active"
            }
        ],
        "HostedZoneId": "Z1PVIF0EXAMPLE",
        "StorageEncrypted": true,
```

```
        "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/287364e4-33e3-4755-a3b0-
a1b2c3d4e5f6",
        "DbClusterResourceId": "cluster-BIZ77GDSA2XBSTNPFW1EXAMPLE",
        "DBClusterArn": "arn:aws:rds:us-west-2:123456789012:cluster:sample-cluster-
clone",
        "AssociatedRoles": [],
        "IAMDatabaseAuthenticationEnabled": false,
        "CloneGroupId": "8d19331a-099a-45a4-b4aa-11aa22bb33cc44dd",
        "ClusterCreateTime": "2020-03-10T19:57:38.967Z",
        "EngineMode": "provisioned",
        "DeletionProtection": false,
        "HttpEndpointEnabled": false,
        "CopyTagsToSnapshot": false,
        "CrossAccountClone": false
    }
}
```

Para obtener más información, consulte Restauración de un clúster de base de dato a un momento indicado en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte RestoreDbClusterToPointInTime en la Referencia de comandos de la AWS CLI.

`restore-db-instance-from-db-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-db-instance-from-db-snapshot`.

AWS CLI

Para restaurar una instancia de base de datos a partir de una instantánea de base de datos

El siguiente ejemplo de `restore-db-instance-from-db-snapshot` crea una nueva instancia de base de datos denominada `db7-new-instance` con la clase de instancia de base de datos `db.t3.small` de la instantánea de base de datos especificada. La instancia de base de datos de origen de la que se tomó la instantánea utiliza una clase de instancia de base de datos obsoleta, por lo que no se puede actualizar.

```
aws rds restore-db-instance-from-db-snapshot \
    --db-instance-identifier db7-new-instance \
    --db-snapshot-identifier db7-test-snapshot \
    --db-instance-class db.t3.small
```

Salida:

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "db7-new-instance",
        "DBInstanceClass": "db.t3.small",
        "Engine": "mysql",
        "DBInstanceStatus": "creating",

        ...output omitted...

        "PreferredMaintenanceWindow": "mon:07:37-mon:08:07",
        "PendingModifiedValues": {},
        "MultiAZ": false,
        "EngineVersion": "5.7.22",
        "AutoMinorVersionUpgrade": true,
        "ReadReplicaDBInstanceIdentifiers": [],
        "LicenseModel": "general-public-license",

        ...output omitted...

        "DBInstanceArn": "arn:aws:rds:us-west-2:123456789012:db:db7-new-instance",
        "IAMDatabaseAuthenticationEnabled": false,
        "PerformanceInsightsEnabled": false,
        "DeletionProtection": false,
        "AssociatedRoles": []
    }
}
```

Para obtener más información, consulte Restoring from a DB Snapshot en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte RestoreDbInstanceFromDbSnapshot en la Referencia de comandos de la AWS CLI.

`restore-db-instance-from-s3`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-db-instance-from-s3`.

AWS CLI

Para restaurar una instancia de base de datos a partir de una copia de seguridad en Amazon S3

En el siguiente ejemplo de `restore-db-instance-from-s3`, se crea una nueva instancia de base de datos con el nombre `restored-test-instance` de una copia de seguridad existente en el bucket de S3 `my-backups`.

```
aws rds restore-db-instance-from-s3 \
    --db-instance-identifier restored-test-instance \
    --allocated-storage 250 --db-instance-class db.m4.large --engine mysql \
    --master-username master --master-user-password secret99 \
    --s3-bucket-name my-backups --s3-ingestion-role-
arn arn:aws:iam::123456789012:role/my-role \
    --source-engine mysql --source-engine-version 5.6.27
```

- Para obtener detalles de la API, consulte RestoreDbInstanceFromS3 en la Referencia de comandos de la AWS CLI.

`restore-db-instance-to-point-in-time`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-db-instance-to-point-in-time`.

AWS CLI

Ejemplo 1: restaurar una instancia de base de datos a un momento en el tiempo

En el siguiente ejemplo de `restore-db-instance-to-point-in-time`, se restaura `test-instance` a una nueva instancia de base de datos denominada `restored-test-instance`, en la hora especificada.

```
aws rds restore-db-instance-to-point-in-time \
    --source-db-instance-identifier test-instance \
    --target-db-instance restored-test-instance \
    --restore-time 2018-07-30T23:45:00.000Z
```

Salida:

```
{
    "DBInstance": {
        "AllocatedStorage": 20,
        "DBInstanceArn": "arn:aws:rds:us-east-1:123456789012:db:restored-test-
instance",
        "DBInstanceStatus": "creating",
```

```
        "DBInstanceIdentifier": "restored-test-instance",
        ...some output omitted...
    }
}
```

Para obtener más información, consulte Restauración de una instancia de base de datos a un momento especificado en la Guía del usuario de Amazon RDS.

Ejemplo 2: restaurar una instancia de base de datos a un tiempo especificado desde una copia de seguridad replicada

El siguiente ejemplo de `restore-db-instance-to-point-in-time` restaura una instancia de base de datos de Oracle a la hora especificada a partir de una copia de seguridad automatizada replicada.

```
aws rds restore-db-instance-to-point-in-time \
    --source-db-instance-automated-backups-arn "arn:aws:rds:us-
west-2:123456789012:auto-backup:ab-jkib2gfq5rv7replzadausbrktni2bn4example" \
    --target-db-instance-identifier myorclinstance-from-replicated-backup \
    --restore-time 2020-12-08T18:45:00.000Z
```

Salida:

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "myorclinstance-from-replicated-backup",
        "DBInstanceClass": "db.t3.micro",
        "Engine": "oracle-se2",
        "DBInstanceStatus": "creating",
        "MasterUsername": "admin",
        "DBName": "ORCL",
        "AllocatedStorage": 20,
        "PreferredBackupWindow": "07:45-08:15",
        "BackupRetentionPeriod": 14,
        ... some output omitted ...
        "DbiResourceId": "db-KGLXG75BGVIWKQT7NQ4EXAMPLE",
        "CACertificateIdentifier": "rds-ca-2019",
        "DomainMemberships": [],
        "CopyTagsToSnapshot": false,
        "MonitoringInterval": 0,
        "DBInstanceArn": "arn:aws:rds:us-west-2:123456789012:db:myorclinstance-from-
replicated-backup",
```

```
        "IAMDatabaseAuthenticationEnabled": false,
        "PerformanceInsightsEnabled": false,
        "DeletionProtection": false,
        "AssociatedRoles": [],
        "TagList": []
    }
}
```

Para obtener más información, consulte Restoring to a specified time from a replicated backup en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte RestoreDbInstanceToPointInTime en la Referencia de comandos de la AWS CLI.

`start-activity-stream`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-activity-stream`.

AWS CLI

Para iniciar un flujo de actividad de la base de datos

En el siguiente ejemplo de `start-activity-stream`, se inicia un flujo de actividad asíncrona para supervisar un clúster de Aurora denominado my-pg-cluster.

```
aws rds start-activity-stream \
    --region us-east-1 \
    --mode async \
    --kms-key-id arn:aws:kms:us-east-1:1234567890123:key/a12c345d-6ef7-890g-
h123-456i789jk0l1 \
    --resource-arn arn:aws:rds:us-east-1:1234567890123:cluster:my-pg-cluster \
    --apply-immediately
```

Salida:

```
{
    "KmsKeyId": "arn:aws:kms:us-east-1:1234567890123:key/a12c345d-6ef7-890g-
h123-456i789jk0l1",
    "KinesisStreamName": "aws-rds-das-cluster-0ABCDEFGHI1JKLM2NOPQ3R4S",
    "Status": "starting",
    "Mode": "async",
    "ApplyImmediately": true
```

```
}
```

Para obtener más información, consulte Inicio de una secuencia de actividades de la base de datos en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte StartActivityStream en la Referencia de comandos de la AWS CLI.

`start-db-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-db-cluster`.

AWS CLI

Para iniciar un clúster de base de datos

El siguiente ejemplo de `start-db-cluster` inicia un clúster de base de datos y sus instancias de base de datos.

```
aws rds start-db-cluster \
    --db-cluster-identifier mydbcluster
```

Salida:

```
{
    "DBCluster": {
        "AllocatedStorage": 1,
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1e",
            "us-east-1b"
        ],
        "BackupRetentionPeriod": 1,
        "DatabaseName": "mydb",
        "DBClusterIdentifier": "mydbcluster",
        ...some output truncated...
    }
}
```

Para obtener más información, consulte Detención e inicio de un clúster de bases de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora.

- Para obtener detalles sobre la API, consulte StartDbCluster en la Referencia de comandos de la AWS CLI.

`start-db-instance-automated-backups-replication`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-db-instance-automated-backups-replication`.

AWS CLI

Para habilitar copias de seguridad automatizadas entre regiones

El siguiente ejemplo de `start-db-instance-automated-backups-replication` replica las copias de seguridad automatizadas desde una instancia de base de datos en el Este de EE. UU. (Norte de Virginia) hasta el Oeste de EE. UU. (Oregón). El período de retención de la copia de seguridad es de 14 días.

```
aws rds start-db-instance-automated-backups-replication \
    --region us-west-2 \
    --source-db-instance-arn "arn:aws:rds:us-east-1:123456789012:db:new-orcl-db" \
    --backup-retention-period 14
```

Salida:

```
{
    "DBInstanceAutomatedBackup": {
        "DBInstanceArn": "arn:aws:rds:us-east-1:123456789012:db:new-orcl-db",
        "DbiResourceId": "db-JKIB2GFQ5RV7REPLZA4EXAMPLE",
        "Region": "us-east-1",
        "DBInstanceIdentifier": "new-orcl-db",
        "RestoreWindow": {},
        "AllocatedStorage": 20,
        "Status": "pending",
        "Port": 1521,
        "InstanceCreateTime": "2020-12-04T15:28:31Z",
        "MasterUsername": "admin",
        "Engine": "oracle-se2",
        "EngineVersion": "12.1.0.2.v21",
        "LicenseModel": "bring-your-own-license",
        "OptionGroupName": "default:oracle-se2-12-1",
        "Encrypted": false,
```

```
        "StorageType": "gp2",
        "IAMDatabaseAuthenticationEnabled": false,
        "BackupRetentionPeriod": 14,
        "DBInstanceAutomatedBackupsArn": "arn:aws:rds:us-west-2:123456789012:auto-
backup:ab-jkib2gfq5rv7replzadausbrktni2bn4example"
    }
}
```

Para obtener más información, consulte Habilitación de copias de seguridad automatizadas entre regiones en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte StartDbInstanceAutomatedBackupsReplication en la Referencia de comandos de la AWS CLI.

`start-db-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-db-instance`.

AWS CLI

Para iniciar una instancia de base de datos

En el siguiente ejemplo de `start-db-instance`, se inicia una instancia de base de datos especificada.

```
aws rds start-db-instance \
    --db-instance-identifier test-instance
```

Salida:

```
{
    "DBInstance": {
        "DBInstanceStatus": "starting",
        ...some output truncated...
    }
}
```

- Para obtener información sobre la API, consulte StartDbInstance en la Referencia de comandos de la AWS CLI.

`start-export-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-export-task`.

AWS CLI

Para exportar una instantánea a Amazon S3

El siguiente ejemplo de `start-export-task` exporta una instantánea de base de datos denominada `db5-snapshot-test` al bucket de Amazon S3 denominado `amzn-s3-demo-bucket`.

```
aws rds start-export-task \
    --export-task-identifier my-s3-export \
    --source-arn arn:aws:rds:us-west-2:123456789012:snapshot:db5-snapshot-test \
    --s3-bucket-name amzn-s3-demo-bucket \
    --iam-role-arn arn:aws:iam::123456789012:role/service-role/ExportRole \
    --kms-key-id arn:aws:kms:us-west-2:123456789012:key/abcd0000-7fca-4128-82f2-
aabbccddeeff
```

Salida:

```
{
    "ExportTaskIdentifier": "my-s3-export",
    "SourceArn": "arn:aws:rds:us-west-2:123456789012:snapshot:db5-snapshot-test",
    "SnapshotTime": "2020-03-27T20:48:42.023Z",
    "S3Bucket": "amzn-s3-demo-bucket",
    "IamRoleArn": "arn:aws:iam::123456789012:role/service-role/ExportRole",
    "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/abcd0000-7fca-4128-82f2-
aabbccddeeff",
    "Status": "STARTING",
    "PercentProgress": 0,
    "TotalExtractedDataInGB": 0
}
```

Para obtener más información, consulte Exportación de una instantánea de base de datos a un bucket de Amazon S3 en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte StartExportTask en la Referencia de comandos de la AWS CLI.

stop-activity-stream

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-activity-stream`.

AWS CLI

Para detener un flujo de actividades de la base de datos

En el siguiente ejemplo de `stop-activity-stream`, se detiene un flujo de actividad en un clúster de Aurora denominado my-pg-cluster.

```
aws rds stop-activity-stream \
    --region us-east-1 \
    --resource-arn arn:aws:rds:us-east-1:1234567890123:cluster:my-pg-cluster \
    --apply-immediately
```

Salida:

```
{
    "KmsKeyId": "arn:aws:kms:us-east-1:1234567890123:key/a12c345d-6ef7-890g-
h123-456i789jk0l1",
    "KinesisStreamName": "aws-rds-das-cluster-0ABCDEFGHI1JKLM2NOPQ3R4S",
    "Status": "stopping"
}
```

Para obtener más información, consulte Detención de un flujo de actividad en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte StopActivityStream en la Referencia de comandos de la AWS CLI.

stop-db-cluster

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-db-cluster`.

AWS CLI

Para detener un clúster de base de datos

El siguiente ejemplo de `stop-db-cluster` detiene un clúster de base de datos y sus instancias de base de datos.

```
aws rds stop-db-cluster \
    --db-cluster-identifier mydbcluster
```

Salida:

```
{
    "DBCluster": {
        "AllocatedStorage": 1,
        "AvailabilityZones": [
            "us-east-1a",
            "us-east-1e",
            "us-east-1b"
        ],
        "BackupRetentionPeriod": 1,
        "DatabaseName": "mydb",
        "DBClusterIdentifier": "mydbcluster",
        ...some output truncated...
    }
}
```

Para obtener más información, consulte Detención e inicio de un clúster de bases de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte StopDbCluster en la Referencia de comandos de la AWS CLI.

`stop-db-instance-automated-backups-replication`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-db-instance-automated-backups-replication`.

AWS CLI

Para dejar de replicar las copias de seguridad automatizadas

El siguiente `stop-db-instance-automated-backups-replication` finaliza la replicación de copias de seguridad automatizadas en la región del Oeste de EE. UU. (Oregón). Las copias de seguridad replicadas se conservan de acuerdo con el período de retención de copias de seguridad establecido.

```
aws rds stop-db-instance-automated-backups-replication \
```

```
    --region us-west-2 \
    --source-db-instance-arn "arn:aws:rds:us-east-1:123456789012:db:new-orcl-db"
```

Salida:

```
{
    "DBInstanceAutomatedBackup": {
        "DBInstanceArn": "arn:aws:rds:us-east-1:123456789012:db:new-orcl-db",
        "DbiResourceId": "db-JKIB2GFQ5RV7REPLZA4EXAMPLE",
        "Region": "us-east-1",
        "DBInstanceIdentifier": "new-orcl-db",
        "RestoreWindow": {
            "EarliestTime": "2020-12-04T23:13:21.030Z",
            "LatestTime": "2020-12-07T19:59:57Z"
        },
        "AllocatedStorage": 20,
        "Status": "replicating",
        "Port": 1521,
        "InstanceCreateTime": "2020-12-04T15:28:31Z",
        "MasterUsername": "admin",
        "Engine": "oracle-se2",
        "EngineVersion": "12.1.0.2.v21",
        "LicenseModel": "bring-your-own-license",
        "OptionGroupName": "default:oracle-se2-12-1",
        "Encrypted": false,
        "StorageType": "gp2",
        "IAMDatabaseAuthenticationEnabled": false,
        "BackupRetentionPeriod": 7,
        "DBInstanceAutomatedBackupsArn": "arn:aws:rds:us-west-2:123456789012:auto-
backup:ab-jkib2gfq5rv7replzadausbrktni2bn4example"
    }
}
```

Para obtener más información, consulte Detención de la replicación de la copia de seguridad automatizada en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte StopDbInstanceAutomatedBackupsReplication en la Referencia de comandos de la AWS CLI.

`stop-db-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-db-instance`.

AWS CLI

Para detener una instancia de base de datos

En el siguiente ejemplo de `stop-db-instance`, se detiene una instancia de base de datos especificada.

```
aws rds stop-db-instance \
    --db-instance-identifier test-instance
```

Salida:

```
{
    "DBInstance": {
        "DBInstanceStatus": "stopping",
        ...some output truncated...
    }
}
```

- Para obtener información sobre la API, consulte StopDbInstance en la Referencia de comandos de la AWS CLI.

`switchover-blue-green-deployment`

En el siguiente ejemplo de código, se muestra cómo utilizar `switchover-blue-green-deployment`.

AWS CLI

Ejemplo 1: cambiar una implementación azul/verde por una instancia de base de datos de RDS

En el siguiente ejemplo de `switchover-blue-green-deployment`, se promueve que el entorno verde especificado sea el nuevo entorno de producción.

```
aws rds switchover-blue-green-deployment \
    --blue-green-deployment-identifier bgd-wi89nwzglccsfake \
    --switchover-timeout 300
```

Salida:

```
{
```

```
    "BlueGreenDeployment": {
        "BlueGreenDeploymentIdentifier": "bgd-v53303651eexfake",
        "BlueGreenDeploymentName": "bgd-cli-test-instance",
        "Source": "arn:aws:rds:us-east-1:123456789012:db:my-db-instance",
        "Target": "arn:aws:rds:us-east-1:123456789012:db:my-db-instance-green-
blhi1e",
        "SwitchoverDetails": [
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-green-blhi1e",
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-1",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-1-green-k5fv7u",
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-2",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-2-green-ggsh8m",
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-3",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-db-
instance-replica-3-green-o2vwm0",
                "Status": "AVAILABLE"
            }
        ],
        "Tasks": [
            {
                "Name": "CREATING_READ_REPLICA_OF_SOURCE",
                "Status": "COMPLETED"
            },
            {
                "Name": "DB_ENGINE_VERSION_UPGRADE",
                "Status": "COMPLETED"
```

```
            },
            {
                "Name": "CONFIGURE_BACKUPS",
                "Status": "COMPLETED"
            },
            {
                "Name": "CREATING_TOPOLOGY_OF_SOURCE",
                "Status": "COMPLETED"
            }
        ],
        "Status": "SWITCHOVER_IN_PROGRESS",
        "CreateTime": "2022-02-25T22:33:22.225000+00:00"
    }
}
```

Para obtener más información, consulte Cambio de una implementación azul/verde en la Guía del usuario de Amazon RDS.

Ejemplo 2: promocionar una implementación azul/verde para un clúster de base de datos en Aurora MySQL

En el siguiente ejemplo de `switchover-blue-green-deployment`, se promueve que el entorno verde especificado sea el nuevo entorno de producción.

```
aws rds switchover-blue-green-deployment \
    --blue-green-deployment-identifier bgd-wi89nwzglccsfake \
    --switchover-timeout 300
```

Salida:

```
{
    "BlueGreenDeployment": {
        "BlueGreenDeploymentIdentifier": "bgd-wi89nwzglccsfake",
        "BlueGreenDeploymentName": "my-blue-green-deployment",
        "Source": "arn:aws:rds:us-east-1:123456789012:cluster:my-aurora-mysql-
cluster",
        "Target": "arn:aws:rds:us-east-1:123456789012:cluster:my-aurora-mysql-
cluster-green-3ud8z6",
        "SwitchoverDetails": [
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster:my-
aurora-mysql-cluster",
```

```
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:cluster:my-
aurora-mysql-cluster-green-3ud8z6",
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-aurora-
mysql-cluster-1",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-aurora-
mysql-cluster-1-green-bvxc73",
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-aurora-
mysql-cluster-2",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-aurora-
mysql-cluster-2-green-7wc4ie",
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:db:my-aurora-
mysql-cluster-3",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:db:my-aurora-
mysql-cluster-3-green-p4xxkz",
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-excluded-member-endpoint",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-excluded-member-endpoint-green-np1ikl",
                "Status": "AVAILABLE"
            },
            {
                "SourceMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-reader-endpoint",
                "TargetMember": "arn:aws:rds:us-east-1:123456789012:cluster-
endpoint:my-reader-endpoint-green-miszlf",
                "Status": "AVAILABLE"
            }
        ],
        "Tasks": [
            {
                "Name": "CREATING_READ_REPLICA_OF_SOURCE",
                "Status": "COMPLETED"
```

```
            },
            {
                "Name": "DB_ENGINE_VERSION_UPGRADE",
                "Status": "COMPLETED"
            },
            {
                "Name": "CREATE_DB_INSTANCES_FOR_CLUSTER",
                "Status": "COMPLETED"
            },
            {
                "Name": "CREATE_CUSTOM_ENDPOINTS",
                "Status": "COMPLETED"
            }
        ],
        "Status": "SWITCHOVER_IN_PROGRESS",
        "CreateTime": "2022-02-25T22:38:49.522000+00:00"
    }
}
```

Para obtener más información, consulte Cambio de una implementación azul/verde en la Guía del usuario de Amazon Aurora.

- Para obtener más información sobre la API, consulte SwitchoverBlueGreenDeployment en la Referencia de comandos de la AWS CLI.

Ejemplos de servicio de datos de Amazon RDS que utilizan la AWS CLI

Los siguientes ejemplos de código muestran cómo realizar acciones e implementar escenarios comunes utilizando el AWS Command Line Interface con Amazon RDS Data Service.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`batch-execute-statement`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-execute-statement`.

AWS CLI

Para ejecutar una instrucción SQL por lotes

El siguiente ejemplo de `batch-execute-statement` ejecuta una instrucción SQL por lotes en una matriz de datos con un conjunto de parámetros.

```
aws rds-data batch-execute-statement \
    --resource-arn "arn:aws:rds:us-west-2:123456789012:cluster:mydbcluster" \
    --database "mydb" \
    --secret-arn "arn:aws:secretsmanager:us-west-2:123456789012:secret:mysecret" \
    --sql "insert into mytable values (:id, :val)" \
    --parameter-sets "[[{\"name\": \"id\", \"value\": {\"longValue\": 1}},{\"name\":
 \"val\", \"value\": {\"stringValue\": \"ValueOne\"}}],
        [{\"name\": \"id\", \"value\": {\"longValue\": 2}},{\"name\": \"val\",
 \"value\": {\"stringValue\": \"ValueTwo\"}}],
        [{\"name\": \"id\", \"value\": {\"longValue\": 3}},{\"name\": \"val\",
 \"value\": {\"stringValue\": \"ValueThree\"}}]]"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte la sección de Uso de la API de datos de RDS en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte BatchExecuteStatement en la Referencia de la API de AWS CLI.

`begin-transaction`

En el siguiente ejemplo de código, se muestra cómo utilizar `begin-transaction`.

AWS CLI

Para iniciar una transacción SQL

En el ejemplo siguiente de `begin-transaction` se inicia una transacción SQL.

```
aws rds-data begin-transaction \
    --resource-arn "arn:aws:rds:us-west-2:123456789012:cluster:mydbcluster" \
    --database "mydb" \
    --secret-arn "arn:aws:secretsmanager:us-west-2:123456789012:secret:mysecret"
```

Salida:

```
{
    "transactionId": "ABC1234567890xyz"
}
```

Para obtener más información, consulte la sección de Uso de la API de datos de RDS en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte BeginTransaction en la Referencia de comandos de la AWS CLI.

`commit-transaction`

En el siguiente ejemplo de código, se muestra cómo utilizar `commit-transaction`.

AWS CLI

Para confirmar una transacción SQL

El siguiente ejemplo de `commit-transaction` finaliza la transacción de SQL especificada y confirma los cambios que haya realizado como parte de ella.

```
aws rds-data commit-transaction \
    --resource-arn "arn:aws:rds:us-west-2:123456789012:cluster:mydbcluster" \
    --secret-arn "arn:aws:secretsmanager:us-west-2:123456789012:secret:mysecret" \
    --transaction-id "ABC1234567890xyz"
```

Salida:

```
{
    "transactionStatus": "Transaction Committed"
}
```

Para obtener más información, consulte la sección de Uso de la API de datos de RDS en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte CommitTransaction en la Referencia de comandos de la AWS CLI.

`execute-statement`

En el siguiente ejemplo de código, se muestra cómo utilizar `execute-statement`.

AWS CLI

Ejemplo 1: Ejecución de una instrucción SQL que forma parte de una transacción

En el siguiente ejemplo de `execute-statement` se ejecuta una instrucción SQL que forma parte de una transacción.

```
aws rds-data execute-statement \
    --resource-arn "arn:aws:rds:us-west-2:123456789012:cluster:mydbcluster" \
    --database "mydb" \
    --secret-arn "arn:aws:secretsmanager:us-west-2:123456789012:secret:mysecret" \
    --sql "update mytable set quantity=5 where id=201" \
    --transaction-id "ABC1234567890xyz"
```

Salida:

```
{
    "numberOfRecordsUpdated": 1
}
```

Ejemplo 2: Ejecución de una instrucción SQL con parámetros

En el siguiente ejemplo de `execute-statement` se ejecuta una instrucción SQL con parámetros.

```
aws rds-data execute-statement \
    --resource-arn "arn:aws:rds:us-east-1:123456789012:cluster:mydbcluster" \
    --database "mydb" \
    --secret-arn "arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret" \
    --sql "insert into mytable values (:id, :val)" \
    --parameters "[{\"name\": \"id\", \"value\": {\"longValue\": 1}},{\"name\":
 \"val\", \"value\": {\"stringValue\": \"value1\"}}]"
```

Salida:

```
{
    "numberOfRecordsUpdated": 1
}
```

Para obtener más información, consulte la sección de Uso de la API de datos para Aurora Serverless en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte ExecuteStatement en la Referencia de comandos de la AWS CLI.

`rollback-transaction`

En el siguiente ejemplo de código, se muestra cómo utilizar `rollback-transaction`.

AWS CLI

Restauración de una transacción SQL

El siguiente ejemplo de `rollback-transaction` revierte la transacción SQL especificada.

```
aws rds-data rollback-transaction \
    --resource-arn "arn:aws:rds:us-west-2:123456789012:cluster:mydbcluster" \
    --secret-arn "arn:aws:secretsmanager:us-west-2:123456789012:secret:mysecret" \
    --transaction-id "ABC1234567890xyz"
```

Salida:

```
{
    "transactionStatus": "Rollback Complete"
}
```

Para obtener más información, consulte la sección de Uso de la API de datos de RDS en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte RollbackTransaction en la Referencia de comandos de la AWS CLI.

Ejemplos de información de rendimiento de Amazon RDS que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes utilizando la AWS Command Line Interface con Información de rendimiento de Amazon RDS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-performance-analysis-report`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-performance-analysis-report`.

AWS CLI

Creación de un informe de análisis de rendimiento

En el siguiente ejemplo de `create-performance-analysis-report`, se crea un informe de análisis de rendimiento con la hora de inicio `1682969503` y la hora de finalización `1682979503` para la base de datos `db-abcdefg123456789`.

```
aws pi create-performance-analysis-report \
    --service-type RDS \
    --identifier db-abcdefg123456789 \
    --start-time 1682969503 \
    --end-time 1682979503
```

Salida:

```
{
    "AnalysisReportId": "report-0234d3ed98e28fb17"
}
```

Para obtener más información sobre la creación de informes de análisis de rendimiento, consulte Creación de un informe de análisis de rendimiento en Información de rendimiento en la Guía del usuario de Amazon RDS y Creación de un informe de análisis de rendimiento en Información de rendimiento en la Guía del usuario de Amazon Aurora.

- Para obtener más información sobre la API, consulte CreatePerformanceAnalysisReport en la Referencia de comandos de la AWS CLI.

`delete-performance-analysis-report`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-performance-analysis-report`.

AWS CLI

Eliminación de un informe de análisis de rendimiento

El siguiente ejemplo de `delete-performance-analysis-report`, se elimina el informe de análisis de rendimiento con el ID de informe `report-0d99cc91c4422ee61`.

```
aws pi delete-performance-analysis-report \
    --service-type RDS \
    --identifier db-abcdefg123456789 \
    --analysis-report-id report-0d99cc91c4422ee61
```

Este comando no genera ninguna salida.

Para obtener más información sobre la eliminación de informes de análisis de rendimiento, consulte Eliminación de un informe de análisis de rendimiento en Información de rendimiento en la Guía del usuario de Amazon RDS y Eliminación de un informe de análisis de rendimiento en Información de rendimiento en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DeletePerformanceAnalysisReport en la Referencia de comandos de la AWS CLI.

describe-dimension-keys

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-dimension-keys`.

AWS CLI

Ejemplo 1: Para describir las claves de dimensión

En este ejemplo se solicitan los nombres de todos los eventos de espera. Los datos se resumen por nombre del evento y los valores agregados de esos eventos durante el período de tiempo especificado.

Comando:

```
aws pi describe-dimension-keys --service-type RDS --identifier db-
LKCGOBK26374TPTDFXOIWVCPPM --start-time 1527026400 --end-time 1527080400 --
metric db.load.avg --group-by '{"Group":"db.wait_event"}'
```

Salida:

```
{
    "AlignedEndTime": 1.5270804E9,
    "AlignedStartTime": 1.5270264E9,
    "Keys": [
        {
            "Dimensions": {"db.wait_event.name": "wait/synch/mutex/innodb/
aurora_lock_thread_slot_futex"},
            "Total": 0.05906906851195666
        },
        {
            "Dimensions": {"db.wait_event.name": "wait/io/aurora_redo_log_flush"},
            "Total": 0.015824722186149193
        },
        {
            "Dimensions": {"db.wait_event.name": "CPU"},
            "Total": 0.008014396230265477
        },
        {
            "Dimensions": {"db.wait_event.name": "wait/io/
aurora_respond_to_client"},
            "Total": 0.0036361612526204477
        },
        {
```

```
            "Dimensions": {"db.wait_event.name": "wait/io/table/sql/handler"},
            "Total": 0.0019108398419382965
        },
        {
            "Dimensions": {"db.wait_event.name": "wait/synch/cond/mysys/
my_thread_var::suspend"},
            "Total": 8.533847837782684E-4
        },
        {
            "Dimensions": {"db.wait_event.name": "wait/io/file/csv/data"},
            "Total": 6.864181956477376E-4
        },
        {
            "Dimensions": {"db.wait_event.name": "Unknown"},
            "Total": 3.895887056379051E-4
        },
        {
            "Dimensions": {"db.wait_event.name": "wait/synch/mutex/sql/
FILE_AS_TABLE::LOCK_shim_lists"},
            "Total": 3.710368625122906E-5
        },
        {
            "Dimensions": {"db.wait_event.name": "wait/lock/table/sql/handler"},
            "Total": 0
        }
    ]
}
```

Ejemplo 2: Para encontrar el ID de SQL de las instrucciones que más contribuyen a la carga de la base de datos

La siguiente `describe-dimension-keys` solicita la instrucción SQL y el ID de SQL para las 10 instrucciones que más han contribuido a la carga de la base de datos.

```
aws pi describe-dimension-keys \
    --service-type RDS \
    --identifier db-abcdefg123456789 \
    --start-time 2023-05-01T00:00:00Z \
    --end-time 2023-05-01T01:00:00Z \
    --metric db.load.avg \
    --group-by '{"Group": "db.sql", "Dimensions": ["db.sql.id",
 "db.sql.statement"],"Limit": 10}'
```

Salida:

```
{
    "AlignedEndTime": 1.5270804E9,
    "AlignedStartTime": 1.5270264E9,
    "Identifier": "db-abcdefg123456789",
    "MetricList": [
        {
            "Keys": [
                {
                    "Dimensions": {"db.sql.id": "AKIAIOSFODNN7EXAMPLE",
 "db.sql.statement": "SELECT * FROM customers WHERE customer_id = 123"},
                    "Total": 25.5,"Partitions": [12.3, 13.2]
                }
            ]
        }
    ]
}
```

Para obtener más información sobre las dimensiones en Información de rendimiento, consulte Carga de la base de datos en la Guía del usuario de Amazon RDS y Carga de la base de datos en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte DescribeDimensionKeys en la Referencia de comandos de la AWS CLI.

`get-dimension-key-details`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-dimension-key-details`.

AWS CLI

Obtención de detalles de un grupo de dimensiones específico para una instancia de base de datos

En el siguiente ejemplo de `get-dimension-key-details`, se recupera el texto completo de una instrucción SQL para una instancia de base de datos `db-10BCD2EFGHIJ3KL4M5NO6PQRS5`. El `--group` es `db.sql` y el `--group-identifier` es `db.sql.id`. En este ejemplo, `example-sql-id` representa un ID de SQL recuperado mediante las operaciones `get-resource-metrics` o `describe-dimension-keys`. En este ejemplo, los detalles de las

dimensiones están disponibles. Por lo tanto, Performance Insights recupera el texto completo de la instrucción SQL, sin truncarlo.

```
aws pi get-dimension-key-details \
    --service-type RDS \
    --identifier db-10BCD2EFGHIJ3KL4M5NO6PQRS5 \
    --group db.sql \
    --group-identifier example-sql-id \
    --requested-dimensions statement
```

Salida:

```
{
    "Dimensions":[
        {
            "Value": "SELECT e.last_name, d.department_name FROM employees e,
 departments d WHERE e.department_id=d.department_id",
            "Dimension": "db.sql.statement",
            "Status": "AVAILABLE"
        },
    ...
    ]
}
```

Para obtener más información sobre las dimensiones en Información de rendimiento, consulte Carga de la base de datos en la Guía del usuario de Amazon RDS y Carga de la base de datos en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte GetDimensionKeyDetails en la Referencia de comandos de la AWS CLI.

`get-performance-analysis-report`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-performance-analysis-report`.

AWS CLI

Obtención de un informe de análisis de rendimiento

En el ejemplo de `get-performance-analysis-report` siguiente se obtiene el informe de análisis de rendimiento para la base de datos `db-abcdefg123456789` con el ID de informe

`report-0d99cc91c4422ee61`. La respuesta proporciona el estado del informe, el identificador, los detalles del tiempo y la información.

```
aws pi get-performance-analysis-report \
    --service-type RDS \
    --identifier db-abcdefg123456789 \
    --analysis-report-id report-0d99cc91c4422ee61
```

Salida:

```
{
    "AnalysisReport": {
        "Status": "Succeeded",
        "ServiceType": "RDS",
        "Identifier": "db-abcdefg123456789",
        "StartTime": 1680583486.584,
        "AnalysisReportId": "report-0d99cc91c4422ee61",
        "EndTime": 1680587086.584,
        "CreateTime": 1680587087.139,
        "Insights": [
            ... (Condensed for space)
       ]
    }
}
```

Para obtener más información sobre los informes de análisis de rendimiento, consulte Análisis del rendimiento de la base de datos durante un periodo de tiempo en la Guía del usuario de Amazon RDS y Análisis del rendimiento de la base de datos durante un periodo de tiempo en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte GetPerformanceAnalysisReport en la Referencia de comandos de la AWS CLI.

`get-resource-metadata`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource-metadata`.

AWS CLI

Obtención de metadatos de recursos para una base de datos

En el ejemplo de `get-resource-metadata` siguiente se obtienen los metadatos de recursos de la base de datos `db-abcdefg123456789`. La respuesta muestra que las estadísticas de resumen SQL están habilitadas.

```
aws pi get-resource-metadata \
    --service-type RDS \
    --identifier db-abcdefg123456789
```

Salida:

```
{
    "Identifier": "db-abcdefg123456789",
    "Features":{
        "SQL_DIGEST_STATISTICS":{
            "Status": "ENABLED"
        }
    }
}
```

Para obtener más información sobre las estadísticas de SQL para Información de rendimiento, consulte Estadísticas de SQL para Información de rendimiento en la Guía del usuario de Amazon RDS y Estadísticas de SQL para Información de rendimiento en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte GetResourceMetadata en la Referencia de comandos de la AWS CLI.

`get-resource-metrics`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource-metrics`.

AWS CLI

Para obtener métricas de recursos

En este ejemplo, se solicitan puntos de datos para el grupo de dimensiones db.wait_event y para la dimensión db.wait_event.name dentro de ese grupo. En la respuesta, los puntos de datos relevantes se agrupan por la dimensión solicitada (db.wait_event.name).

Comando:

```
aws pi get-resource-metrics --service-type RDS --identifier db-
LKCGOBK26374TPTDFXOIWVCPPM --start-time 1527026400 --end-time 1527080400 --period-
in-seconds 300 --metric db.load.avg --metric-queries file://metric-queries.json
```

Los argumentos de `--metric-queries` se almacenan en el archivo JSON `metric-queries.json`: A continuación, se muestra el contenido de ese archivo:

```
[
    {
        "Metric": "db.load.avg",
        "GroupBy": {
            "Group":"db.wait_event"
        }
    }
]
```

Salida:

```
{
    "AlignedEndTime": 1.5270804E9,
    "AlignedStartTime": 1.5270264E9,
    "Identifier": "db-LKCGOBK26374TPTDFXOIWVCPPM",
    "MetricList": [
        {
            "Key": {
                "Metric": "db.load.avg"
            },
            "DataPoints": [
                {
                    "Timestamp": 1527026700.0,
                    "Value": 1.3533333333333333
                },
                {
                    "Timestamp": 1527027000.0,
                    "Value": 0.88
                },
                <...remaining output omitted...>
            ]
        },
        {
            "Key": {
                "Metric": "db.load.avg",
```

```
                "Dimensions": {
                    "db.wait_event.name": "wait/synch/mutex/innodb/
aurora_lock_thread_slot_futex"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": 1527026700.0,
                    "Value": 0.8566666666666667
                },
                {
                    "Timestamp": 1527027000.0,
                    "Value": 0.8633333333333333
                },
                <...remaining output omitted...>
            ],
        },
            <...remaining output omitted...>
    ]
}
```

- Para obtener información sobre la API, consulte GetResourceMetrics en la Referencia de comandos de la AWS CLI.

`list-available-resource-dimensions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-available-resource-dimensions`.

AWS CLI

Muestra de las dimensiones que se pueden consultar para un tipo de métrica en una instancia de base de datos

El ejemplo de `list-available-resource-dimensions` siguiente muestra las métricas de `db.load` que puede consultar para la base de datos `db-abcdefg123456789`.

```
aws pi list-available-resource-dimensions \
    --service-type RDS \
    --identifier db-abcdefg123456789 \
    --metrics db.load
```

Salida:

```
{
    "MetricDimensions": [
        {
            "Metric": "db.load",
            "Groups": [
                {
                    "Group": "db.user",
                    "Dimensions": [
                        {
                            "Identifier": "db.user.id"
                        },
                        {
                            "Identifier": "db.user.name"
                        }
                    ]
                },
                {
                    "Group": "db.sql_tokenized",
                    "Dimensions": [
                        {
                            "Identifier": "db.sql_tokenized.id"
                        },
                        {
                            "Identifier": "db.sql_tokenized.db_id"
                        },
                        {
                            "Identifier": "db.sql_tokenized.statement"
                        }
                    ]
                },
                ...
            ]
        }
    ]
}
```

Para obtener más información sobre las dimensiones en Información de rendimiento, consulte Carga de la base de datos en la Guía del usuario de Amazon RDS y Carga de la base de datos en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte ListAvailableResourceDimensions en la Referencia de comandos de la AWS CLI.

`list-available-resource-metrics`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-available-resource-metrics`.

AWS CLI

Muestra de las métricas que se pueden consultar para un tipo de métrica en una instancia de base de datos

El ejemplo de `list-available-resource-metrics` siguiente muestra las métricas de `db.load` que puede consultar para la base de datos `db-abcdefg123456789`.

```
aws pi list-available-resource-metrics \
    --service-type RDS \
    --identifier db-abcdefg123456789 \
    --metric-types "os" "db"
```

Salida:

```
{
    "Metrics": [
        {
            "Description": "The number of virtual CPUs for the DB instance",
            "Metric": "os.general.numVCPUs",
            "Unit": "vCPUs"
        },
        ......,
        {
            "Description": "Time spent reading data file blocks by backends in this
 instance",
            "Metric": "db.IO.read_latency",
            "Unit": "Milliseconds per block"
        },
        ......
    ]
}
```

Para obtener más información sobre las métricas en Información de rendimiento, consulte Carga de la base de datos en la Guía del usuario de Amazon RDS y Carga de la base de datos en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte ListAvailableResourceMetrics en la Referencia de comandos de la AWS CLI.

`list-performance-analysis-reports`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-performance-analysis-reports`.

AWS CLI

Muestra de los informes de análisis de rendimiento de una base de datos

En el ejemplo de `list-performance-analysis-reports` siguiente se muestran los informes de análisis de rendimiento para la base de datos `db-abcdefg123456789`. La respuesta enumera todos los informes con el ID del informe, el estado y los detalles del período de tiempo.

```
aws pi list-performance-analysis-reports \
    --service-type RDS \
    --identifier db-abcdefg123456789
```

Salida:

```
{
    "AnalysisReports": [
        {
            "Status": "Succeeded",
            "EndTime": 1680587086.584,
            "CreateTime": 1680587087.139,
            "StartTime": 1680583486.584,
            "AnalysisReportId": "report-0d99cc91c4422ee61"
        },
        {
            "Status": "Succeeded",
            "EndTime": 1681491137.914,
            "CreateTime": 1681491145.973,
            "StartTime": 1681487537.914,
            "AnalysisReportId": "report-002633115cc002233"
        },
```

```
        {
            "Status": "Succeeded",
            "EndTime": 1681493499.849,
            "CreateTime": 1681493507.762,
            "StartTime": 1681489899.849,
            "AnalysisReportId": "report-043b1e006b47246f9"
        },
        {
            "Status": "InProgress",
            "EndTime": 1682979503.0,
            "CreateTime": 1682979618.994,
            "StartTime": 1682969503.0,
            "AnalysisReportId": "report-01ad15f9b88bcbd56"
        }
    ]
}
```

Para obtener más información sobre los informes de análisis de rendimiento, consulte Análisis del rendimiento de la base de datos durante un periodo de tiempo en la Guía del usuario de Amazon RDS y Análisis del rendimiento de la base de datos durante un periodo de tiempo en la Guía del usuario de Amazon Aurora.

- Para obtener información sobre la API, consulte ListPerformanceAnalysisReports en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Muestra de las etiquetas de un informe de análisis de rendimiento

El ejemplo de `list-tags-for-resource` siguiente muestra las etiquetas de un informe de análisis de rendimiento con el ID de informe `report-0d99cc91c4422ee61`.

```
aws pi list-tags-for-resource \
    --service-type RDS \
    --resource-arn arn:aws:pi:us-west-2:123456789012:perf-reports/RDS/db-abcdefg123456789/report-0d99cc91c4422ee61
```

Salida:

```
{
    "Tags": [
        {
            "Value": "test-tag",
            "Key": "name"
        }
    ]
}
```

Para obtener más información sobre el etiquetado de informes de análisis de rendimiento, consulte Agregación de etiquetas a un informe de análisis de rendimiento en Información de rendimiento en la Guía del usuario de Amazon RDS y Agregación de etiquetas a un informe de análisis de rendimiento en Información de rendimiento en la Guía del usuario de Amazon Aurora.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Agregación de una etiqueta a un informe de análisis de rendimiento

El ejemplo de `tag-resource` siguiente agrega la clave de etiqueta `name` con el valor de etiqueta `test-tag` a un informe de análisis de rendimiento con el ID de informe `report-0d99cc91c4422ee61`.

```
aws pi tag-resource \
    --service-type RDS \
    --resource-arn arn:aws:pi:us-west-2:123456789012:perf-reports/RDS/db-abcdefg123456789/report-0d99cc91c4422ee61 \
    --tags Key=name,Value=test-tag
```

Este comando no genera ninguna salida.

Para obtener más información sobre el etiquetado de informes de análisis de rendimiento, consulte Agregación de etiquetas a un informe de análisis de rendimiento en Información de rendimiento en la Guía del usuario de Amazon RDS y Agregación de etiquetas a un informe de análisis de rendimiento en Información de rendimiento en la Guía del usuario de Amazon Aurora.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Eliminación de una etiqueta para un informe de análisis de rendimiento

El ejemplo de `untag-resource` siguiente elimina la etiqueta `name` de un informe de análisis de rendimiento con el ID de informe `report-0d99cc91c4422ee61`.

```
aws pi untag-resource \
    --service-type RDS \
    --resource-arn arn:aws:pi:us-west-2:123456789012:perf-reports/RDS/db-abcdefg123456789/report-0d99cc91c4422ee61 \
    --tag-keys name
```

Este comando no genera ninguna salida.

Para obtener más información sobre el etiquetado de informes de análisis de rendimiento, consulte Agregación de etiquetas a un informe de análisis de rendimiento en Información de rendimiento en la Guía del usuario de Amazon RDS y Agregación de etiquetas a un informe de análisis de rendimiento en Información de rendimiento en la Guía del usuario de Amazon Aurora.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon Redshift que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon Redshift.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`accept-reserved-node-exchange`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-reserved-node-exchange`.

AWS CLI

Para aceptar un intercambio de nodos reservados

El siguiente ejemplo de `accept-reserved-node-exchange` aceptará el intercambio de un nodo reservado de DC1 por un nodo reservado de DC2.

```
aws redshift accept-reserved-node-exchange /
    --reserved-node-id 12345678-12ab-12a1-1a2a-12ab-12a12EXAMPLE /
    --target-reserved-node-offering-id 12345678-12ab-12a1-1a2a-12ab-12a12EXAMPLE
```

Salida:

```
{
    "ExchangedReservedNode": {
        "ReservedNodeId": "12345678-12ab-12a1-1a2a-12ab-12a12EXAMPLE",
        "ReservedNodeOfferingId": "12345678-12ab-12a1-1a2a-12ab-12a12EXAMPLE",
        "NodeType": "dc2.large",
        "StartTime": "2019-12-06T21:17:26Z",
        "Duration": 31536000,
        "FixedPrice": 0.0,
        "UsagePrice": 0.0,
        "CurrencyCode": "USD",
        "NodeCount": 1,
        "State": "exchanging",
        "OfferingType": "All Upfront",
        "RecurringCharges": [
            {
                "RecurringChargeAmount": 0.0,
                "RecurringChargeFrequency": "Hourly"
            }
        ],
        "ReservedNodeOfferingType": "Regular"
```

```
    }
}
```

Para obtener más información, consulte Upgrading Reserved Nodes With the AWS CLI en la Guía de administración del clúster de Amazon Redshift.

- Para obtener información sobre la API, consulte AcceptReservedNodeExchange en la Referencia de comandos de la AWS CLI.

`authorize-cluster-security-group-ingress`

En el siguiente ejemplo de código, se muestra cómo utilizar `authorize-cluster-security-group-ingress`.

AWS CLI

Autorización del acceso a un grupo de seguridad de EC2. Este ejemplo autoriza el acceso a un grupo de seguridad de Amazon EC2. Comando:

```
aws redshift authorize-cluster-security-group-ingress --cluster-security-group-name
 mysecuritygroup --ec2-security-group-name myec2securitygroup --ec2-security-group-
owner-id 123445677890
```

Autorización del acceso a un rango de CIDR. Este ejemplo autoriza el acceso a un rango de CIDR. Comando:

```
aws redshift authorize-cluster-security-group-ingress --cluster-security-group-name
 mysecuritygroup --cidrip 192.168.100.100/32
```

- Para obtener información sobre la API, consulte AuthorizeClusterSecurityGroupIngress en la Referencia de comandos de la AWS CLI.

`authorize-snapshot-access`

En el siguiente ejemplo de código, se muestra cómo utilizar `authorize-snapshot-access`.

AWS CLI

Autorizar una cuenta de AWS para restaurar una instantánea. Este ejemplo autoriza a la cuenta de AWS `444455556666` a restaurar la instantánea `my-snapshot-id`. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift authorize-snapshot-access --snapshot-id my-snapshot-id --account-with-
restore-access 444455556666
```

Resultado:

```
{
   "Snapshot": {
      "Status": "available",
      "SnapshotCreateTime": "2013-07-17T22:04:18.947Z",
      "EstimatedSecondsToCompletion": 0,
      "AvailabilityZone": "us-east-1a",
      "ClusterVersion": "1.0",
      "MasterUsername": "adminuser",
      "Encrypted": false,
      "OwnerAccount": "111122223333",
      "BackupProgressInMegabytes": 11.0,
      "ElapsedTimeInSeconds": 0,
      "DBName": "dev",
      "CurrentBackupRateInMegabytesPerSecond: 0.1534,
      "ClusterCreateTime": "2013-01-22T21:59:29.559Z",
      "ActualIncrementalBackupSizeInMegabytes"; 11.0,
      "SnapshotType": "manual",
      "NodeType": "dw.hs1.xlarge",
      "ClusterIdentifier": "mycluster",
      "TotalBackupSizeInMegabytes": 20.0,
      "Port": 5439,
      "NumberOfNodes": 2,
      "SnapshotIdentifier": "my-snapshot-id"
   }
}
```

- Para obtener información sobre la API, consulte AuthorizeSnapshotAccess en la Referencia de comandos de la AWS CLI.

`batch-delete-cluster-snapshots`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-delete-cluster-snapshots`.

AWS CLI

Para eliminar un conjunto de instantáneas del clúster

En el siguiente ejemplo de `batch-delete-cluster-snapshots`, se elimina un conjunto de instantáneas del clúster manual.

```
aws redshift batch-delete-cluster-snapshots \
        --
identifiers SnapshotIdentifier=mycluster-2019-11-06-14-12 SnapshotIdentifier=mycluster-2019-
```

Salida:

```
{
    "Resources": [
        "mycluster-2019-11-06-14-12",
        "mycluster-2019-11-06-14-20"
    ]
}
```

Para obtener más información, consulte Amazon Redshift Snapshots en la Guía de administración de clúster de Amazon Redshift.

- Para obtener información sobre la API, consulte BatchDeleteClusterSnapshots en la Referencia de comandos de la AWS CLI.

`batch-modify-cluster-snapshots`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-modify-cluster-snapshots`.

AWS CLI

Para modificar un conjunto de instantáneas del clúster

En el siguiente ejemplo de `batch-modify-cluster-snapshots`, se modifica la configuración de un conjunto de instantáneas del clúster.

```
aws redshift batch-modify-cluster-snapshots \
    --snapshot-identifier-list mycluster-2019-11-06-16-31 mycluster-2019-11-06-16-32
 \
    --manual-snapshot-retention-period 30
```

Salida:

```
{
```

```
    "Resources": [
        "mycluster-2019-11-06-16-31",
        "mycluster-2019-11-06-16-32"
    ],
    "Errors": [],
    "ResponseMetadata": {
        "RequestId": "12345678-12ab-12a1-1a2a-12ab-12a12EXAMPLE",
        "HTTPStatusCode": 200,
        "HTTPHeaders": {
                "x-amzn-requestid": "12345678-12ab-12a1-1a2a-12ab-12a12EXAMPLE,
                "content-type": "text/xml",
                "content-length": "480",
                "date": "Sat, 07 Dec 2019 00:36:09 GMT",
                "connection": "keep-alive"
        },
        "RetryAttempts": 0
    }
}
```

Para obtener más información, consulte Amazon Redshift Snapshots en la Guía de administración de clúster de Amazon Redshift.

- Para obtener información sobre la API, consulte BatchModifyClusterSnapshots en la Referencia de comandos de la AWS CLI.

`cancel-resize`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-resize`.

AWS CLI

Para cancelar el cambio de tamaño de un clúster

El siguiente ejemplo de `cancel-resize` cancela una operación de cambio de tamaño clásica de un clúster.

```
aws redshift cancel-resize \
    --cluster-identifier mycluster
```

Salida:

```
{
```

```
    "TargetNodeType": "dc2.large",
    "TargetNumberOfNodes": 2,
    "TargetClusterType": "multi-node",
    "Status": "CANCELLING",
    "ResizeType": "ClassicResize",
    "TargetEncryptionType": "NONE"
}
```

Para obtener más información, consulte Resizing Clusters in Amazon Redshift en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte CancelResize en la Referencia de comandos de la AWS CLI.

`copy-cluster-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-cluster-snapshot`.

AWS CLI

Obtener una descripción de todas las versiones del clúster. Este ejemplo proporciona una descripción de todas las versiones del clúster. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift copy-cluster-snapshot --source-snapshot-identifier
 cm:examplecluster-2013-01-22-19-27-58 --target-snapshot-identifier my-saved-
snapshot-copy
```

Resultado:

```
{
   "Snapshot": {
      "Status": "available",
      "SnapshotCreateTime": "2013-01-22T19:27:58.931Z",
      "AvailabilityZone": "us-east-1c",
      "ClusterVersion": "1.0",
      "MasterUsername": "adminuser",
      "DBName": "dev",
      "ClusterCreateTime": "2013-01-22T19:23:59.368Z",
      "SnapshotType": "manual",
      "NodeType": "dw.hs1.xlarge",
```

```
      "ClusterIdentifier": "examplecluster",
      "Port": 5439,
      "NumberOfNodes": "2",
      "SnapshotIdentifier": "my-saved-snapshot-copy"
   },
   "ResponseMetadata": {
      "RequestId": "3b279691-64e3-11e2-bec0-17624ad140dd"
   }
}
```

- Para obtener información sobre la API, consulte AWS CLICopyClusterSnapshot en la Referencia de comandos de la .

`create-cluster-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-cluster-parameter-group`.

AWS CLI

Crear un grupo de parámetros de clúster. Este ejemplo crea un nuevo grupo de parámetros del clúster. Comando:

```
aws redshift create-cluster-parameter-group --parameter-group-name
 myclusterparametergroup --parameter-group-family redshift-1.0 --description "My
 first cluster parameter group"
```

Resultado:

```
{
   "ClusterParameterGroup": {
      "ParameterGroupFamily": "redshift-1.0",
      "Description": "My first cluster parameter group",
      "ParameterGroupName": "myclusterparametergroup"
   },
   "ResponseMetadata": {
      "RequestId": "739448f0-64cc-11e2-8f7d-3b939af52818"
   }
}
```

- Para obtener información sobre la API, consulte CreateClusterParameterGroup en la Referencia de comandos de la AWS CLI.

`create-cluster-security-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-cluster-security-group`.

AWS CLI

Creación de un grupo de seguridad de clúster. Este ejemplo crea un nuevo grupo de seguridad de clúster. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift create-cluster-security-group --cluster-security-group-name
 mysecuritygroup --description "This is my cluster security group"
```

Resultado:

```
{
   "create_cluster_security_group_response": {
      "create_cluster_security_group_result": {
         "cluster_security_group": {
            "description": "This is my cluster security group",
            "owner_id": "300454760768",
            "cluster_security_group_name": "mysecuritygroup",
            "ec2_security_groups": \[],
            "ip_ranges": \[]
         }
      },
      "response_metadata": {
         "request_id": "5df486a0-343a-11e2-b0d8-d15d0ef48549"
      }
   }
}
```

También puede obtener la misma información en formato de texto mediante la opción `--output text`. Comando:

`--output text` option.Command:

option.Command:

```
aws redshift create-cluster-security-group --cluster-security-group-name
 mysecuritygroup --description "This is my cluster security group" --output text
```

Resultado:

```
This is my cluster security group   300454760768    mysecuritygroup
a0c0bfab-343a-11e2-95d2-c3dc9fe8ab57
```

- Para obtener información sobre la API, consulte CreateClusterSecurityGroup en la Referencia de comandos de la AWS CLI.

`create-cluster-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-cluster-snapshot`.

AWS CLI

Crea un clúster desde una instantánea. Este ejemplo crea una nueva instantánea del clúster. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift create-cluster-snapshot --cluster-identifier mycluster --snapshot-
identifier my-snapshot-id
```

Resultado:

```
{
   "Snapshot": {
      "Status": "creating",
      "SnapshotCreateTime": "2013-01-22T22:20:33.548Z",
      "AvailabilityZone": "us-east-1a",
      "ClusterVersion": "1.0",
      "MasterUsername": "adminuser",
      "DBName": "dev",
      "ClusterCreateTime": "2013-01-22T21:59:29.559Z",
      "SnapshotType": "manual",
      "NodeType": "dw.hs1.xlarge",
      "ClusterIdentifier": "mycluster",
      "Port": 5439,
      "NumberOfNodes": "2",
      "SnapshotIdentifier": "my-snapshot-id"
   },
   "ResponseMetadata": {
      "RequestId": "f024d1a5-64e1-11e2-88c5-53eb05787dfb"
   }
}
```

- Para obtener información sobre la API, consulte CreateClusterSnapshot en la Referencia de comandos de la AWS CLI.

`create-cluster-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-cluster-subnet-group`.

AWS CLI

Crear un grupo de subred del clúster. Este ejemplo crea un nuevo grupo de subred del clúster. Comando:

```
aws redshift create-cluster-subnet-group --cluster-subnet-group-name mysubnetgroup
 --description "My subnet group" --subnet-ids subnet-763fdd1c
```

Resultado:

```
{
   "ClusterSubnetGroup": {
      "Subnets": [
         {
            "SubnetStatus": "Active",
            "SubnetIdentifier": "subnet-763fdd1c",
            "SubnetAvailabilityZone": {
               "Name": "us-east-1a"
            }
         } ],
      "VpcId": "vpc-7e3fdd14",
      "SubnetGroupStatus": "Complete",
      "Description": "My subnet group",
      "ClusterSubnetGroupName": "mysubnetgroup"
   },
   "ResponseMetadata": {
      "RequestId": "500b8ce2-698f-11e2-9790-fd67517fb6fd"
   }
}
```

- Para obtener información sobre la API, consulte CreateClusterSubnetGroup en la Referencia de comandos de la AWS CLI.

`create-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-cluster`.

AWS CLI

Crear un clúster con parámetros mínimos En este ejemplo, se crea un clúster con el conjunto mínimo de parámetros. De forma predeterminada, la salida es en JSON format.Command:

```
aws redshift create-cluster --node-type dw.hs1.xlarge --number-of-nodes 2 --master-
username adminuser --master-user-password TopSecret1 --cluster-identifier mycluster
```

Resultado:

```
{
   "Cluster": {
      "NodeType": "dw.hs1.xlarge",
      "ClusterVersion": "1.0",
      "PubliclyAccessible": "true",
      "MasterUsername": "adminuser",
      "ClusterParameterGroups": [
         {
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "default.redshift-1.0"
         } ],
      "ClusterSecurityGroups": [
         {
            "Status": "active",
            "ClusterSecurityGroupName": "default"
         } ],
      "AllowVersionUpgrade": true,
      "VpcSecurityGroups": \[],
      "PreferredMaintenanceWindow": "sat:03:30-sat:04:00",
      "AutomatedSnapshotRetentionPeriod": 1,
      "ClusterStatus": "creating",
      "ClusterIdentifier": "mycluster",
      "DBName": "dev",
      "NumberOfNodes": 2,
      "PendingModifiedValues": {
         "MasterUserPassword": "\****"
      }
   },
   "ResponseMetadata": {
```

```
        "RequestId": "7cf4bcfc-64dd-11e2-bea9-49e0ce183f07"
    }
}
```

- Para obtener información sobre la API, consulte CreateCluster en la Referencia de comandos de la AWS CLI.

`create-event-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-event-subscription`.

AWS CLI

Para crear una suscripción de notificaciones de un evento

El siguiente ejemplo de `create-event-subscription` crea una suscripción de notificación al evento.

```
aws redshift create-event-subscription \
    --subscription-name mysubscription \
    --sns-topic-arn arn:aws:sns:us-west-2:123456789012:MySNStopic \
    --source-type cluster \
    --source-ids mycluster
```

Salida:

```
{
        "EventSubscription": {
        "CustomerAwsId": "123456789012",
        "CustSubscriptionId": "mysubscription",
        "SnsTopicArn": "arn:aws:sns:us-west-2:123456789012:MySNStopic",
        "Status": "active",
        "SubscriptionCreationTime": "2019-12-09T20:05:19.365Z",
        "SourceType": "cluster",
        "SourceIdsList": [
            "mycluster"
        ],
        "EventCategoriesList": [],
        "Severity": "INFO",
        "Enabled": true,
        "Tags": []
```

```
    }
}
```

Para obtener más información, consulte Subscribing to Amazon Redshift Event Notifications en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener detalles sobre la API, consulte CreateEventSubscription en la Referencia de comandos de la AWS CLI.

`create-hsm-client-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-hsm-client-certificate`.

AWS CLI

Para crear un certificado de cliente del HSM

El siguiente ejemplo de `create-hsm-client-certificate` genera un certificado de cliente de HSM que puede utilizar un clúster para conectarse a un HSM.

```
aws redshift create-hsm-client-certificate \
    --hsm-client-certificate-identifier myhsmclientcert
```

Salida:

```
{
    "HsmClientCertificate": {
        "HsmClientCertificateIdentifier": "myhsmclientcert",
        "HsmClientCertificatePublicKey": "-----BEGIN CERTIFICATE-----
        MIICiEXAMPLECQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
        VVMxCzAJBgNVBAgTEXAMPLEwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
        b24xFDASBgNVBAsTC0lBTSBDb25EXAMPLEIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
        BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb2EXAMPLETEwNDI1MjA0NTIxWhcN
        MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBEXAMPLEMRAwDgYD
        EXAMPLETZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
        b2xlMRIwEAEXAMPLEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
        YXpvbi5jb20wgZ8wDQYJKEXAMPLEAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
        21uUSfwfEvySWtC2XADZ4nB+BLYgVIk6EXAMPLE3G93vUEIO3IyNoH/f0wYK8m9T
        rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugEXAMPLEzZswY6786m86gpE
        Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEEXAMPLEEAtCu4
        nUhVVxYUEXAMPLEh8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
```

```
        FFBjvSfpJIlJ00zbhNYS5f6GEXAMPLEl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
        NYiytVbZPQUQ5Yaxu2jXnimvw3rEXAMPLE=-----END CERTIFICATE-----\n",
    "Tags": []
    }
}
```

Para obtener más información, consulte Amazon Redshift API Permissions Reference en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte CreateHsmClientCertificate en la Referencia de comandos de la AWS CLI.

`create-hsm-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-hsm-configuration`.

AWS CLI

Para crear una configuración del HSM

El siguiente ejemplo de `create-hsm-configuration` crea una configuración del HSM que contiene la información requerida por un clúster para almacenar y utilizar las claves de cifrado de base de datos en un módulo de seguridad de hardware (HSM).

```
aws redshift create-hsm-configuration /
    --hsm-configuration-identifier myhsmconnection
    --description "My HSM connection"
    --hsm-ip-address 192.0.2.09
    --hsm-partition-name myhsmpartition /
    --hsm-partition-password A1b2c3d4 /
    --hsm-server-public-certificate myhsmclientcert
```

Salida:

```
{
    "HsmConfiguration": {
        "HsmConfigurationIdentifier": "myhsmconnection",
        "Description": "My HSM connection",
        "HsmIpAddress": "192.0.2.09",
        "HsmPartitionName": "myhsmpartition",
        "Tags": []
```

```
    }
}
```

- Para obtener información sobre la API, consulte CreateHsmConfiguration en la Referencia de comandos de la AWS CLI.

`create-snapshot-copy-grant`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-snapshot-copy-grant`.

AWS CLI

Para crear una autorización de copia de instantáneas

En el siguiente ejemplo de `create-snapshot-copy-grant`, se crea una concesión de copia de instantáneas y cifra las instantáneas copiadas en una región de AWS de destino.

```
aws redshift create-snapshot-copy-grant \
    --snapshot-copy-grant-name mysnapshotcopygrantname
```

Salida:

```
{
    "SnapshotCopyGrant": {
        "SnapshotCopyGrantName": "mysnapshotcopygrantname",
        "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/
bPxRfih3yCo8nvbEXAMPLEKEY",
        "Tags": []
    }
}
```

Para obtener más información, consulte Cifrado de la base de datos de Amazon Redshift en la Guía de administración de Amazon Redshift.

- Para obtener información sobre la API, consulte CreateSnapshotCopyGrant en la Referencia de comandos de la AWS CLI.

`create-snapshot-schedule`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-snapshot-schedule`.

AWS CLI

Para crear una programación de instantáneas

En el siguiente ejemplo de `create-snapshot-schedule`, se crea una programación de instantáneas con la descripción especificada y una frecuencia de cada 12 horas.

```
aws redshift create-snapshot-schedule \
    --schedule-definitions "rate(12 hours)" \
    --schedule-identifier mysnapshotschedule \
    --schedule-description "My schedule description"
```

Salida:

```
{
    "ScheduleDefinitions": [
        "rate(12 hours)"
    ],
    "ScheduleIdentifier": "mysnapshotschedule",
    "ScheduleDescription": "My schedule description",
    "Tags": []
}
```

Para obtener más información, consulte Programación de instantáneas automatizadas en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte CreateSnapshotSchedule en la Referencia de comandos de la AWS CLI.

`create-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-tags`.

AWS CLI

Para crear etiquetas para un clúster

En el siguiente ejemplo de `create-tags`, se agrega el par clave/valor de etiqueta especificado al clúster especificado.

```
aws redshift create-tags \
```

```
    --resource-name arn:aws:redshift:us-west-2:123456789012:cluster:mycluster \
    --tags "Key"="mytags","Value"="tag1"
```

Este comando no produce ninguna salida.

Para obtener más información, consulte Etiquetado de recursos en Amazon Redshift en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte CreateTags en la Referencia de comandos de la AWS CLI.

`delete-cluster-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-cluster-parameter-group`.

AWS CLI

Eliminar un grupo de parámetros de clúster. Este ejemplo elimina un grupo de parámetros del clúster. Comando:

```
aws redshift delete-cluster-parameter-group --parameter-group-name
 myclusterparametergroup
```

- Para obtener información sobre la API, consulte DeleteClusterParameterGroup en la Referencia de comandos de la AWS CLI.

`delete-cluster-security-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-cluster-security-group`.

AWS CLI

Eliminar un grupo de seguridad del clúster. Este ejemplo elimina un grupo de seguridad del clúster. Comando:

```
aws redshift delete-cluster-security-group --cluster-security-group-name
 mysecuritygroup
```

- Para obtener información sobre la API, consulte DeleteClusterSecurityGroup en la Referencia de comandos de la AWS CLI.

`delete-cluster-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-cluster-snapshot`.

AWS CLI

Eliminación de una instantánea de clúster En este ejemplo se elimina una instantánea de clúster. Comando:

```
aws redshift delete-cluster-snapshot --snapshot-identifier my-snapshot-id
```

- Para obtener información sobre la API, consulte DeleteClusterSnapshot en la Referencia de comandos de la AWS CLI.

`delete-cluster-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-cluster-subnet-group`.

AWS CLI

Eliminar un grupo de subred del clúster. Este ejemplo elimina un grupo de subred del clúster. Comando:

```
aws redshift delete-cluster-subnet-group --cluster-subnet-group-name mysubnetgroup
```

Resultado:

```
{
   "ResponseMetadata": {
      "RequestId": "253fbffd-6993-11e2-bc3a-47431073908a"
   }
}
```

- Para obtener información sobre la API, consulte DeleteClusterSubnetGroup en la Referencia de comandos de la AWS CLI.

`delete-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-cluster`.

AWS CLI

Eliminación de un clúster sin una instantánea final del clúster En este ejemplo, se elimina un clúster y se fuerza la eliminación de los datos, por lo que no se crea una instantánea final del clúster. Comando:

```
aws redshift delete-cluster --cluster-identifier mycluster --skip-final-cluster-
snapshot
```

Eliminación de un clúster, lo que permite obtener una instantánea final del clúster En este ejemplo se elimina un clúster, pero especifica una instantánea final del clúster. Comando:

```
aws redshift delete-cluster --cluster-identifier mycluster --final-cluster-snapshot-
identifier myfinalsnapshot
```

- Para obtener información sobre la API, consulte DeleteCluster en la Referencia de comandos de la AWS CLI.

`delete-event-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-event-subscription`.

AWS CLI

Para eliminar la suscripción a un evento

En el siguiente ejemplo de `delete-event-subscription`, se elimina la suscripción a una notificación de evento especificada.

```
aws redshift delete-event-subscription \
    --subscription-name mysubscription
```

Este comando no produce ninguna salida.

Para obtener más información, consulte Subscribing to Amazon Redshift Event Notifications en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte DeleteEventSubscription en la Referencia de comandos de la AWS CLI.

`delete-hsm-client-certificate`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-hsm-client-certificate`.

AWS CLI

Para eliminar un certificado de cliente HSM

En el siguiente ejemplo de `delete-hsm-client-certificate`, se elimina un certificado de cliente de HSM.

```
aws redshift delete-hsm-client-certificate \
    --hsm-client-certificate-identifier myhsmclientcert
```

Este comando no produce ninguna salida.

Para obtener más información, consulte Amazon Redshift API Permissions Reference en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte DeleteHsmClientCertificate en la Referencia de comandos de la AWS CLI.

`delete-hsm-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-hsm-configuration`.

AWS CLI

Para eliminar una configuración HSM

En el siguiente ejemplo de `delete-hsm-configuration`, se elimina una configuración HSM especificada de la cuenta de AWS especificada.

```
aws redshift delete-hsm-configuration /
    --hsm-configuration-identifier myhsmconnection
```

Este comando no produce ninguna salida.

- Para obtener información sobre la API, consulte DeleteHsmConfiguration en la Referencia de comandos de la AWS CLI.

`delete-scheduled-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-scheduled-action`.

AWS CLI

Para eliminar una acción programada

El siguiente ejemplo de `delete-scheduled-action` elimina una acción programada especificada.

```
aws redshift delete-scheduled-action \
    --scheduled-action-name myscheduledaction
```

Este comando no produce ninguna salida.

- Para obtener información sobre la API, consulte DeleteScheduledAction en la Referencia de comandos de la AWS CLI.

`delete-snapshot-copy-grant`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-snapshot-copy-grant`.

AWS CLI

Para eliminar una concesión de copia de instantánea

En el siguiente ejemplo de `delete-snapshot-copy-grant`, se elimina la concesión de una copia de instantáneas especificada.

```
aws redshift delete-snapshot-copy-grant \
    --snapshot-copy-grant-name mysnapshotcopygrantname
```

Este comando no produce ninguna salida.

Para obtener más información, consulte Cifrado de la base de datos de Amazon Redshift en la Guía de administración de Amazon Redshift.

- Para obtener información sobre la API, consulte DeleteSnapshotCopyGrant en la Referencia de comandos de la AWS CLI.

`delete-snapshot-schedule`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-snapshot-schedule`.

AWS CLI

Para eliminar una programación de instantáneas

En el siguiente ejemplo de `delete-snapshot-schedule`, se elimina la programación de una instantánea especificada. Debe desasociar los clústeres antes de eliminar la programación.

```
aws redshift delete-snapshot-schedule \
    --schedule-identifier mysnapshotschedule
```

Este comando no produce ninguna salida.

Para obtener más información, consulte Programación de instantáneas automatizadas en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte DeleteSnapshotSchedule en la Referencia de comandos de la AWS CLI.

`delete-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-tags`.

AWS CLI

Para eliminar etiquetas de un clúster

En el siguiente ejemplo de `delete-tags`, se eliminan las etiquetas con los nombres de clave especificados del clúster especificado.

```
aws redshift delete-tags \
    --resource-name arn:aws:redshift:us-west-2:123456789012:cluster:mycluster \
    --tag-keys "clustertagkey" "clustertagvalue"
```

Este comando no produce ninguna salida.

Para obtener más información, consulte Etiquetado de recursos en Amazon Redshift en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte DeleteTags en la Referencia de comandos de la AWS CLI.

`describe-account-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-account-attributes`.

AWS CLI

Para describir atributos de una cuenta de AWS

En el siguiente ejemplo de `describe-account-attributes`, se muestran los atributos asociados a la cuenta de AWS que llama.

```
aws redshift describe-account-attributes
```

Salida:

```
{
    "AccountAttributes": [
        {
            "AttributeName": "max-defer-maintenance-duration",
            "AttributeValues": [
                {
                    "AttributeValue": "45"
                }
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeAccountAttributes en la Referencia de comandos de la AWS CLI.

`describe-cluster-db-revisions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cluster-db-revisions`.

AWS CLI

Para describir las revisiones de la base de datos de un clúster

El siguiente ejemplo de `describe-cluster-db-revisions` muestra los detalles de una matriz de objetos `ClusterDbRevision` para el clúster especificado.

```
aws redshift describe-cluster-db-revisions \
    --cluster-identifier mycluster
```

Salida:

```
{
    "ClusterDbRevisions": [
        {
            "ClusterIdentifier": "mycluster",
            "CurrentDatabaseRevision": "11420",
            "DatabaseRevisionReleaseDate": "2019-11-22T16:43:49.597Z",
            "RevisionTargets": []
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeClusterDbRevisions en la Referencia de comandos de la AWS CLI.

`describe-cluster-parameter-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cluster-parameter-groups`.

AWS CLI

Obtención de una descripción de todos los grupos de parámetros del clúster. En este ejemplo se devuelve una descripción de todos los grupos de parámetros del clúster, con encabezados de columna. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift describe-cluster-parameter-groups
```

Resultado:

```
{
   "ParameterGroups": [
      {
         "ParameterGroupFamily": "redshift-1.0",
```

```
         "Description": "My first cluster parameter group",
         "ParameterGroupName": "myclusterparametergroup"
      } ],
   "ResponseMetadata": {
      "RequestId": "8ceb8f6f-64cc-11e2-bea9-49e0ce183f07"
   }
}
```

También puede obtener la misma información en formato de texto mediante la opción `--output text`. Comando:

`--output text` option.Command:

option.Command:

```
aws redshift describe-cluster-parameter-groups --output text
```

Resultado:

```
redshift-1.0        My first cluster parameter group        myclusterparametergroup
RESPONSEMETADATA    9e665a36-64cc-11e2-8f7d-3b939af52818
```

- Para obtener información sobre la API, consulte DescribeClusterParameterGroups en la Referencia de comandos de la AWS CLI.

`describe-cluster-parameters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cluster-parameters`.

AWS CLI

Recupere los parámetros de un grupo de parámetros de clúster especificado. Este ejemplo recupera los parámetros del grupo de parámetros nombrado. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift describe-cluster-parameters --parameter-group-name
 myclusterparametergroup
```

Resultado:

```
{
```

```
   "Parameters": [
      {
         "Description": "Sets the display format for date and time values.",
         "DataType": "string",
         "IsModifiable": true,
         "Source": "engine-default",
         "ParameterValue": "ISO, MDY",
         "ParameterName": "datestyle"
      },
      {
         "Description": "Sets the number of digits displayed for floating-point
 values",
         "DataType": "integer",
         "IsModifiable": true,
         "AllowedValues": "-15-2",
         "Source": "engine-default",
         "ParameterValue": "0",
         "ParameterName": "extra_float_digits"
      },
      (...remaining output omitted...)
   ]
}
```

También puede obtener la misma información en formato de texto mediante la opción `--output text`. Comando:

`--output text` option.Command:

option.Command:

```
aws redshift describe-cluster-parameters --parameter-group-name
 myclusterparametergroup --output text
```

Resultado:

```
RESPONSEMETADATA    cdac40aa-64cc-11e2-9e70-918437dd236d
Sets the display format for date and time values.   string  True    engine-default
 ISO, MDY        datestyle
Sets the number of digits displayed for floating-point values       integer True
 -15-2   engine-default  0       extra_float_digits
This parameter applies a user-defined label to a group of queries that are run
 during the same session..    string  True    engine-default  default query_group
```

```
require ssl for all databaseconnections     boolean True    true,false      engine-
default  false   require_ssl
Sets the schema search order for names that are not schema-qualified.       string
 True    engine-default  $user, public   search_path
Aborts any statement that takes over the specified number of milliseconds.  integer
 True    engine-default  0       statement_timeout
wlm json configuration      string  True    engine-default
 \[{"query_concurrency":5}]      wlm_json_configuration
```

- Para obtener información sobre la API, consulte DescribeClusterParameters en la Referencia de comandos de la AWS CLI.

`describe-cluster-security-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cluster-security-groups`.

AWS CLI

Obtención de una descripción de todos los grupos de seguridad del clúster. En este ejemplo se proporciona una descripción de todos los grupos de seguridad del clúster de la cuenta. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift describe-cluster-security-groups
```

Resultado:

```
{
   "ClusterSecurityGroups": [
      {
         "OwnerId": "100447751468",
         "Description": "default",
         "ClusterSecurityGroupName": "default",
         "EC2SecurityGroups": \[],
         "IPRanges": [
            {
               "Status": "authorized",
               "CIDRIP": "0.0.0.0/0"
            }
         ]
      },
```

```
      {
         "OwnerId": "100447751468",
         "Description": "This is my cluster security group",
         "ClusterSecurityGroupName": "mysecuritygroup",
         "EC2SecurityGroups": \[],
         "IPRanges": \[]
      },
      (...remaining output omitted...)
   ]
}
```

- Para obtener información sobre la API, consulte DescribeClusterSecurityGroups en la Referencia de comandos de la AWS CLI.

`describe-cluster-snapshots`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cluster-snapshots`.

AWS CLI

Obtención de una descripción de todas las instantáneas de clúster. En este ejemplo se proporciona una descripción de todas las instantáneas de clúster de la cuenta. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift describe-cluster-snapshots
```

Resultado:

```
{
   "Snapshots": [
      {
         "Status": "available",
         "SnapshotCreateTime": "2013-07-17T22:02:22.852Z",
         "EstimatedSecondsToCompletion": -1,
         "AvailabilityZone": "us-east-1a",
         "ClusterVersion": "1.0",
         "MasterUsername": "adminuser",
         "Encrypted": false,
         "OwnerAccount": "111122223333",
         "BackupProgressInMegabytes": 20.0,
         "ElapsedTimeInSeconds": 0,
         "DBName": "dev",
```

```
        "CurrentBackupRateInMegabytesPerSecond: 0.0,
        "ClusterCreateTime": "2013-01-22T21:59:29.559Z",
        "ActualIncrementalBackupSizeInMegabytes"; 20.0
        "SnapshotType": "automated",
        "NodeType": "dw.hs1.xlarge",
        "ClusterIdentifier": "mycluster",
        "Port": 5439,
        "TotalBackupSizeInMegabytes": 20.0,
        "NumberOfNodes": "2",
        "SnapshotIdentifier": "cm:mycluster-2013-01-22-22-04-18"
     },
     {
        "EstimatedSecondsToCompletion": 0,
        "OwnerAccount": "111122223333",
        "CurrentBackupRateInMegabytesPerSecond: 0.1534,
        "ActualIncrementalBackupSizeInMegabytes"; 11.0,
        "NumberOfNodes": "2",
        "Status": "available",
        "ClusterVersion": "1.0",
        "MasterUsername": "adminuser",
        "AccountsWithRestoreAccess": [
           {
              "AccountID": "444455556666"
           } ],
        "TotalBackupSizeInMegabytes": 20.0,
        "DBName": "dev",
        "BackupProgressInMegabytes": 11.0,
        "ClusterCreateTime": "2013-01-22T21:59:29.559Z",
        "ElapsedTimeInSeconds": 0,
        "ClusterIdentifier": "mycluster",
        "SnapshotCreateTime": "2013-07-17T22:04:18.947Z",
        "AvailabilityZone": "us-east-1a",
        "NodeType": "dw.hs1.xlarge",
        "Encrypted": false,
        "SnapshotType": "manual",
        "Port": 5439,
        "SnapshotIdentifier": "my-snapshot-id"
     } ]
  }
  (...remaining output omitted...)
```

- Para obtener información sobre la API, consulte DescribeClusterSnapshots en la Referencia de comandos de la AWS CLI.

`describe-cluster-subnet-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cluster-subnet-groups`.

AWS CLI

Obtención de una descripción de todos los grupos de subred del clúster. En este ejemplo se proporciona una descripción de todos los grupos de subred del clúster. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift describe-cluster-subnet-groups
```

Resultado:

```
{
   "ClusterSubnetGroups": [
      {
         "Subnets": [
            {
               "SubnetStatus": "Active",
               "SubnetIdentifier": "subnet-763fdd1c",
               "SubnetAvailabilityZone": {
                  "Name": "us-east-1a"
               }
            }
         ],
         "VpcId": "vpc-7e3fdd14",
         "SubnetGroupStatus": "Complete",
         "Description": "My subnet group",
         "ClusterSubnetGroupName": "mysubnetgroup"
      }
   ],
   "ResponseMetadata": {
      "RequestId": "37fa8c89-6990-11e2-8f75-ab4018764c77"
   }
}
```

- Para obtener información sobre la API, consulte DescribeClusterSubnetGroups en la Referencia de comandos de la AWS CLI.

describe-cluster-tracks

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cluster-tracks`.

AWS CLI

Para describir las pistas del clúster

En el siguiente ejemplo de `describe-cluster-tracks`, se muestran los detalles de las pistas de mantenimiento disponibles.

```
aws redshift describe-cluster-tracks \
    --maintenance-track-name current
```

Salida:

```
{
    "MaintenanceTracks": [
        {
            "MaintenanceTrackName": "current",
            "DatabaseVersion": "1.0.11420",
            "UpdateTargets": [
                {
                    "MaintenanceTrackName": "preview_features",
                    "DatabaseVersion": "1.0.11746",
                    "SupportedOperations": [
                        {
                            "OperationName": "restore-from-cluster-snapshot"
                        }
                    ]
                },
                {
                    "MaintenanceTrackName": "trailing",
                    "DatabaseVersion": "1.0.11116",
                    "SupportedOperations": [
                        {
                            "OperationName": "restore-from-cluster-snapshot"
                        },
                        {
                            "OperationName": "modify-cluster"
                        }
                    ]
                }
```

```
            ]
        }
    ]
}
```

Para obtener más información, consulte Choosing Cluster Maintenance Tracks en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte DescribeClusterTracks en la Referencia de comandos de la AWS CLI.

`describe-cluster-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cluster-versions`.

AWS CLI

Obtener una descripción de todas las versiones del clúster. Este ejemplo proporciona una descripción de todas las versiones del clúster. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift describe-cluster-versions
```

Resultado:

```
{
   "ClusterVersions": [
      {
      "ClusterVersion": "1.0",
      "Description": "Initial release",
      "ClusterParameterGroupFamily": "redshift-1.0"
      } ],
   "ResponseMetadata": {
      "RequestId": "16a53de3-64cc-11e2-bec0-17624ad140dd"
   }
}
```

- Para obtener información sobre la API, consulte DescribeClusterVersions en la Referencia de comandos de la AWS CLI.

`describe-clusters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-clusters`.

AWS CLI

Obtención de una descripción de todos los clústeres En este ejemplo se devuelve una descripción de todos los clústeres de la cuenta. De forma predeterminada, la salida es en JSON format.Command:

```
aws redshift describe-clusters
```

Resultado:

```
{
   "Clusters": [
   {
      "NodeType": "dw.hs1.xlarge",
      "Endpoint": {
         "Port": 5439,
         "Address": "mycluster.coqoarplqhsn.us-east-1.redshift.amazonaws.com"
      },
      "ClusterVersion": "1.0",
      "PubliclyAccessible": "true",
      "MasterUsername": "adminuser",
      "ClusterParameterGroups": [
         {
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "default.redshift-1.0"
         } ],
      "ClusterSecurityGroups": [
         {
            "Status": "active",
            "ClusterSecurityGroupName": "default"
         } ],
      "AllowVersionUpgrade": true,
      "VpcSecurityGroups": \[],
      "AvailabilityZone": "us-east-1a",
      "ClusterCreateTime": "2013-01-22T21:59:29.559Z",
      "PreferredMaintenanceWindow": "sat:03:30-sat:04:00",
      "AutomatedSnapshotRetentionPeriod": 1,
      "ClusterStatus": "available",
      "ClusterIdentifier": "mycluster",
```

```
      "DBName": "dev",
      "NumberOfNodes": 2,
      "PendingModifiedValues": {}
   } ],
   "ResponseMetadata": {
      "RequestId": "65b71cac-64df-11e2-8f5b-e90bd6c77476"
   }
}
```

También puede obtener la misma información en formato de texto mediante la opción `--output text`. Comando:

`--output text` option.Command:

option.Command:

```
aws redshift describe-clusters --output text
```

Resultado:

```
dw.hs1.xlarge       1.0     true    adminuser       True    us-east-1a
 2013-01-22T21:59:29.559Z        sat:03:30-sat:04:00     1       available
 mycluster       dev     2
ENDPOINT    5439    mycluster.coqoarplqhsn.us-east-1.redshift.amazonaws.com
in-sync     default.redshift-1.0
active      default
PENDINGMODIFIEDVALUES
RESPONSEMETADATA    934281a8-64df-11e2-b07c-f7fbdd006c67
```

- Para obtener información sobre la API, consulte DescribeClusters en la Referencia de comandos de la AWS CLI.

`describe-default-cluster-parameters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-default-cluster-parameters`.

AWS CLI

Obtención de una descripción de los parámetros de clúster predeterminados En este ejemplo se proporciona una descripción de los parámetros de clúster predeterminados de la familia `redshift-1.0`. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift describe-default-cluster-parameters --parameter-group-family
 redshift-1.0
```

Resultado:

```
{
   "DefaultClusterParameters": {
   "ParameterGroupFamily": "redshift-1.0",
   "Parameters": [
      {
         "Description": "Sets the display format for date and time values.",
         "DataType": "string",
         "IsModifiable": true,
         "Source": "engine-default",
         "ParameterValue": "ISO, MDY",
         "ParameterName": "datestyle"
      },
      {
         "Description": "Sets the number of digits displayed for floating-point
 values",
         "DataType": "integer",
         "IsModifiable": true,
         "AllowedValues": "-15-2",
         "Source": "engine-default",
         "ParameterValue": "0",
         "ParameterName": "extra_float_digits"
      },
      (...remaining output omitted...)
      ]
   }
}
```

Para ver una lista de familias de grupos de parámetros válidos, use el comando `describe-cluster-parameter-groups`.

comando `describe-cluster-parameter-groups`

comando.

- Para obtener información sobre la API, consulte DescribeDefaultClusterParameters en la Referencia de comandos de la AWS CLI.

`describe-event-categories`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-event-categories`.

AWS CLI

Para describir las categorías de eventos de un clúster

En el siguiente ejemplo de `describe-event-categories`, se muestran los detalles de las categorías de eventos de un clúster.

```
aws redshift describe-event-categories \
    --source-type cluster
```

Salida:

```
{
    "EventCategoriesMapList": [
        {
            "SourceType": "cluster",
            "Events": [
                {
                    "EventId": "REDSHIFT-EVENT-2000",
                    "EventCategories": [
                        "management"
                    ],
                    "EventDescription": "Cluster <cluster name> created at <time in
 UTC>.",
                    "Severity": "INFO"
                },
                {
                    "EventId": "REDSHIFT-EVENT-2001",
                    "EventCategories": [
                        "management"
                    ],
                    "EventDescription": "Cluster <cluster name> deleted at <time in
 UTC>.",
                    "Severity": "INFO"
```

```
                },
                {
                    "EventId": "REDSHIFT-EVENT-3625",
                    "EventCategories": [
                        "monitoring"
                    ],
                    "EventDescription": "The cluster <cluster name> can't be resumed
 with its previous elastic network interface <ENI id>. We will allocate a new
 elastic network interface and associate it with the cluster node.",
                    "Severity": "INFO"
                }
            ]
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeEventCategories en la Referencia de comandos de la AWS CLI.

`describe-event-subscriptions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-event-subscriptions`.

AWS CLI

Para describir suscripciones a eventos

En el siguiente ejemplo de `describe-event-subscriptions`, se muestran las suscripciones a una notificación de evento especificada.

```
aws redshift describe-event-subscriptions \
    --subscription-name mysubscription
```

Salida:

```
{
    "EventSubscriptionsList": [
        {
            "CustomerAwsId": "123456789012",
            "CustSubscriptionId": "mysubscription",
            "SnsTopicArn": "arn:aws:sns:us-west-2:123456789012:MySNStopic",
            "Status": "active",
```

```
            "SubscriptionCreationTime": "2019-12-09T21:50:21.332Z",
            "SourceIdsList": [],
            "EventCategoriesList": [
                "management"
            ],
            "Severity": "ERROR",
            "Enabled": true,
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Subscribing to Amazon Redshift Event Notifications en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte DescribeEventSubscriptions en la Referencia de comandos de la AWS CLI.

`describe-events`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-events`.

AWS CLI

Descripción de todos los eventos: este ejemplo devuelve todos los eventos. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift describe-events
```

Resultado:

```
{
   "Events": [
      {
      "Date": "2013-01-22T19:17:03.640Z",
      "SourceIdentifier": "myclusterparametergroup",
      "Message": "Cluster parameter group myclusterparametergroup has been
 created.",
      "SourceType": "cluster-parameter-group"
      } ],
   "ResponseMetadata": {
      "RequestId": "9f056111-64c9-11e2-9390-ff04f2c1e638"
```

```
    }
}
```

También puede obtener la misma información en formato de texto mediante la opción `--output text`. Comando:

`--output text` option.Command:

option.Command:

```
aws redshift describe-events --output text
```

Resultado:

```
2013-01-22T19:17:03.640Z    myclusterparametergroup Cluster parameter group
 myclusterparametergroup has been created.       cluster-parameter-group
RESPONSEMETADATA    8e5fe765-64c9-11e2-bce3-e56f52c50e17
```

- Para obtener detalles sobre la API, consulte DescribeEvents en la Referencia de comandos de la AWS CLI.

`describe-hsm-client-certificates`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-hsm-client-certificates`.

AWS CLI

Para describir los certificados de cliente HSM

En el siguiente ejemplo de `describe-hsm-client-certificates`, se muestran los detalles del certificado de cliente HSM especificado.

```
aws redshift describe-hsm-client-certificates \
    --hsm-client-certificate-identifier myhsmclientcert
```

Salida:

```
{
    "HsmClientCertificates": [
        {
```

```
        "HsmClientCertificateIdentifier": "myhsmclientcert",
        "HsmClientCertificatePublicKey": "-----BEGIN CERTIFICATE-----\
        EXAMPLECAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
        VVMxCzAJBgNVBAEXAMPLERAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
        b24xFDASBgNVBAsTC0lBTSBDb25zEXAMPLEwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
        BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhEXAMPLEDI1MjA0EXAMPLEN
        EXAMPLE0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
        VQQHEwdTZWF0dGEXAMPLEQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
        b2xlMRIwEAYDVQQDEwlUZXN0Q2lsEXAMPLEdBgkqhkiG9w0BCQEWEG5vb25lQGFt
        YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIEXAMPLEMaK0dn+a4GmWIWJ
        21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
        rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY67EXAMPLEE
        EXAMPLEZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
        nUhVVxYUntneD9EXAMPLE6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
        FFBjvSfpJIlJ00zbhNYS5f6GuoEDEXAMPLEBHjJnyp378OD8uTs7fLvjx79LjSTb
        NYiytVbZPQUQ5Yaxu2jXnimvw3rEXAMPLE=-----END CERTIFICATE-----\n",
        "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Amazon Redshift API Permissions Reference en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte DescribeHsmClientCertificates en la Referencia de comandos de la AWS CLI.

`describe-hsm-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-hsm-configurations`.

AWS CLI

Para describir las configuraciones de HSM

En el siguiente ejemplo de `describe-hsm-configurations`, se muestran los detalles de las configuraciones de HSM disponibles para la cuenta de AWS que realiza la llamada.

```
aws redshift describe-hsm-configurations /
    --hsm-configuration-identifier myhsmconnection
```

Salida:

```
{
    "HsmConfigurations": [
        {
            "HsmConfigurationIdentifier": "myhsmconnection",
            "Description": "My HSM connection",
            "HsmIpAddress": "192.0.2.09",
            "HsmPartitionName": "myhsmpartition",
            "Tags": []
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeHsmConfigurations en la Referencia de comandos de la AWS CLI.

`describe-logging-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-logging-status`.

AWS CLI

Para describir el estado de registro de un clúster

El siguiente ejemplo de `describe-logging-status` muestra si se está registrando información, como consultas e intentos de conexión, para un clúster.

```
aws redshift describe-logging-status \
    --cluster-identifier mycluster
```

Salida:

```
{
    "LoggingEnabled": false
}
```

Para obtener más información, consulte Registro de auditoría de bases de datos en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte DescribeLoggingStatus en la Referencia de comandos de la AWS CLI.

`describe-node-configuration-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-node-configuration-options`.

AWS CLI

Para describir las opciones de configuración de nodos

El siguiente ejemplo de `describe-node-configuration-options` muestra las propiedades de las posibles configuraciones nodos, como por tipo de nodo, número de nodos y el uso del disco para la instantánea del clúster especificada.

```
aws redshift describe-node-configuration-options \
    --action-type restore-cluster \
    --snapshot-identifier rs:mycluster-2019-12-09-16-42-43
```

Salida:

```
{
    "NodeConfigurationOptionList": [
        {
            "NodeType": "dc2.large",
            "NumberOfNodes": 2,
            "EstimatedDiskUtilizationPercent": 19.61
        },
        {
            "NodeType": "dc2.large",
            "NumberOfNodes": 4,
            "EstimatedDiskUtilizationPercent": 9.96
        },
        {
            "NodeType": "ds2.xlarge",
            "NumberOfNodes": 2,
            "EstimatedDiskUtilizationPercent": 1.53
        },
        {
            "NodeType": "ds2.xlarge",
            "NumberOfNodes": 4,
            "EstimatedDiskUtilizationPercent": 0.78
        }
    ]
```

```
}
```

Para obtener más información, consulte Adquisición de nodos reservados de Amazon Redshift en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte DescribeNodeConfigurationOptions en la Referencia de comandos de la AWS CLI.

`describe-orderable-cluster-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-orderable-cluster-options`.

AWS CLI

Descripción de todas las opciones de clúster que se pueden pedir En este ejemplo se muestran descripciones de todas las opciones de clúster que se pueden pedir. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift describe-orderable-cluster-options
```

Resultado:

```
{
   "OrderableClusterOptions": [
      {
         "NodeType": "dw.hs1.8xlarge",
         "AvailabilityZones": [
            { "Name": "us-east-1a" },
            { "Name": "us-east-1b" },
            { "Name": "us-east-1c" } ],
         "ClusterVersion": "1.0",
         "ClusterType": "multi-node"
      },
      {
         "NodeType": "dw.hs1.xlarge",
         "AvailabilityZones": [
            { "Name": "us-east-1a" },
            { "Name": "us-east-1b" },
            { "Name": "us-east-1c" } ],
         "ClusterVersion": "1.0",
         "ClusterType": "multi-node"
```

```
      },
      {
      "NodeType": "dw.hs1.xlarge",
      "AvailabilityZones": [
         { "Name": "us-east-1a" },
         { "Name": "us-east-1b" },
         { "Name": "us-east-1c" } ],
      "ClusterVersion": "1.0",
      "ClusterType": "single-node"
      } ],
   "ResponseMetadata": {
      "RequestId": "f6000035-64cb-11e2-9135-ff82df53a51a"
   }
}
```

También puede obtener la misma información en formato de texto mediante la opción `--output text`. Comando:

`--output text` option.Command:

option.Command:

```
aws redshift describe-orderable-cluster-options --output text
```

Resultado:

```
dw.hs1.8xlarge      1.0     multi-node
us-east-1a
us-east-1b
us-east-1c
dw.hs1.xlarge       1.0     multi-node
us-east-1a
us-east-1b
us-east-1c
dw.hs1.xlarge       1.0     single-node
us-east-1a
us-east-1b
us-east-1c
RESPONSEMETADATA    e648696b-64cb-11e2-bec0-17624ad140dd
```

- Para obtener información sobre la API, consulte DescribeOrderableClusterOptions en la Referencia de comandos de la AWS CLI.

describe-reserved-node-offerings

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-reserved-node-offerings`.

AWS CLI

Describa las ofertas de nodos reservados En este ejemplo se muestran todas las ofertas de nodos reservados que están disponibles para su compra. Comando:

```
aws redshift describe-reserved-node-offerings
```

Resultado:

```
{
   "ReservedNodeOfferings": [
      {
         "OfferingType": "Heavy Utilization",
         "FixedPrice": "",
         "NodeType": "dw.hs1.xlarge",
         "UsagePrice": "",
         "RecurringCharges": [
            {
               "RecurringChargeAmount": "",
               "RecurringChargeFrequency": "Hourly"
            } ],
         "Duration": 31536000,
         "ReservedNodeOfferingId": "ceb6a579-cf4c-4343-be8b-d832c45ab51c"
      },
      {
         "OfferingType": "Heavy Utilization",
         "FixedPrice": "",
         "NodeType": "dw.hs1.8xlarge",
         "UsagePrice": "",
         "RecurringCharges": [
            {
            "RecurringChargeAmount": "",
            "RecurringChargeFrequency": "Hourly"
            } ],
         "Duration": 31536000,
         "ReservedNodeOfferingId": "e5a2ff3b-352d-4a9c-ad7d-373c4cab5dd2"
      },
      ...remaining output omitted...
```

```
    ],
    "ResponseMetadata": {
        "RequestId": "8b1a1a43-75ff-11e2-9666-e142fe91ddd1"
    }
}
```

Si desea comprar una oferta de nodo reservado, puede llamar a `purchase-reserved-node-offering` con un ReservedNodeOfferingId válido.

`purchase-reserved-node-offering` utiliza un ReservedNodeOfferingId válido.

utiliza a ReservedNodeOfferingId válido.

ReservedNodeOfferingId.

.

- Para obtener información sobre la API, consulte DescribeReservedNodeOfferings en la Referencia de comandos de la AWS CLI.

`describe-reserved-nodes`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-reserved-nodes`.

AWS CLI

Describa los nodos reservados. Este ejemplo muestra una oferta de nodos reservados que se ha adquirido. Comando:

```
aws redshift describe-reserved-nodes
```

Resultado:

```
{
    "ResponseMetadata": {
        "RequestId": "bc29ce2e-7600-11e2-9949-4b361e7420b7"
    },
    "ReservedNodes": [
        {
            "OfferingType": "Heavy Utilization",
            "FixedPrice": "",
            "NodeType": "dw.hs1.xlarge",
```

```
            "ReservedNodeId": "1ba8e2e3-bc01-4d65-b35d-a4a3e931547e",
            "UsagePrice": "",
            "RecurringCharges": [
               {
                  "RecurringChargeAmount": "",
                  "RecurringChargeFrequency": "Hourly"
               } ],
            "NodeCount": 1,
            "State": "payment-pending",
            "StartTime": "2013-02-13T17:08:39.051Z",
            "Duration": 31536000,
            "ReservedNodeOfferingId": "ceb6a579-cf4c-4343-be8b-d832c45ab51c"
         }
      ]
}
```

- Para obtener información sobre la API, consulte DescribeReservedNodes en la Referencia de comandos de la AWS CLI.

`describe-resize`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-resize`.

AWS CLI

Describe el cambio de tamaño En este ejemplo se describe el último cambio de tamaño de un clúster. La solicitud era para tres nodos del tipo `dw.hs1.8xlarge`. Comando:

```
aws redshift describe-resize --cluster-identifier mycluster
```

Resultado:

```
{
   "Status": "NONE",
   "TargetClusterType": "multi-node",
   "TargetNodeType": "dw.hs1.8xlarge",
   "ResponseMetadata": {
      "RequestId": "9f52b0b4-7733-11e2-aa9b-318b2909bd27"
   },
   "TargetNumberOfNodes": "3"
}
```

- Para obtener información sobre la API, consulte DescribeResize en la Referencia de comandos de la AWS CLI.

`describe-scheduled-actions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-scheduled-actions`.

AWS CLI

Para describir acciones programadas

En el siguiente ejemplo de `describe-scheduled-actions`, se muestran los detalles de las acciones programadas actualmente.

```
aws redshift describe-scheduled-actions
```

Salida:

```
{
    "ScheduledActions": [
        {
            "ScheduledActionName": "resizecluster",
            "TargetAction": {
                "ResizeCluster": {
                    "ClusterIdentifier": "mycluster",
                    "NumberOfNodes": 4,
                    "Classic": false
                }
            },
            "Schedule": "at(2019-12-10T00:07:00)",
            "IamRole": "arn:aws:iam::123456789012:role/myRedshiftRole",
            "State": "ACTIVE",
            "NextInvocations": [
                "2019-12-10T00:07:00Z"
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeScheduledActions en la Referencia de comandos de la AWS CLI.

`describe-snapshot-copy-grants`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-snapshot-copy-grants`.

AWS CLI

Para describir concesiones de copia de instantánea

En el siguiente ejemplo de `describe-snapshot-copy-grants`, se muestran los detalles de la concesión de copia de instantáneas del clúster especificada.

```
aws redshift describe-snapshot-copy-grants \
    --snapshot-copy-grant-name mysnapshotcopygrantname
```

Salida:

```
{
    "SnapshotCopyGrants": [
        {
            "SnapshotCopyGrantName": "mysnapshotcopygrantname",
            "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/
bPxRfih3yCo8nvbEXAMPLEKEY",
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Cifrado de la base de datos de Amazon Redshift en la Guía de administración de Amazon Redshift.

- Para obtener información sobre la API, consulte DescribeSnapshotCopyGrants en la Referencia de comandos de la AWS CLI.

`describe-snapshot-schedules`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-snapshot-schedules`.

AWS CLI

Para describir las programaciones de instantáneas

En el siguiente ejemplo de `describe-snapshot-schedules`, se muestran los detalles de la programación de instantáneas del clúster especificada.

```
aws redshift describe-snapshot-schedules \
    --cluster-identifier mycluster \
    --schedule-identifier mysnapshotschedule
```

Salida:

```
{
    "SnapshotSchedules": [
        {
            "ScheduleDefinitions": [
                "rate(12 hours)"
            ],
            "ScheduleIdentifier": "mysnapshotschedule",
            "ScheduleDescription": "My schedule description",
            "Tags": [],
            "AssociatedClusterCount": 1,
            "AssociatedClusters": [
                {
                    "ClusterIdentifier": "mycluster",
                    "ScheduleAssociationState": "ACTIVE"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Programación de instantáneas automatizadas en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte DescribeSnapshotSchedules en la Referencia de comandos de la AWS CLI.

`describe-storage`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-storage`.

AWS CLI

Para describir el almacenamiento

En el siguiente ejemplo de `describe-storage`, se muestran detalles sobre el almacenamiento de copias de seguridad y sobre los tamaños de almacenamiento provisional de la cuenta.

```
aws redshift describe-storage
```

Salida:

```
{
    "TotalBackupSizeInMegaBytes": 193149.0,
    "TotalProvisionedStorageInMegaBytes": 655360.0
}
```

Para obtener más información, consulte Managing Snapshot Storage en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte DescribeStorage en la Referencia de comandos de la AWS CLI.

`describe-table-restore-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-table-restore-status`.

AWS CLI

Para describir el estado de las solicitudes de restauración de tablas desde una instantánea del clúster

En el siguiente ejemplo de `describe-table-restore-status`, se muestran los detalles de las solicitudes de restauración de tablas realizadas para el clúster especificado.

```
aws redshift describe-table-restore-status /
    --cluster-identifier mycluster
```

Salida:

```
{
    "TableRestoreStatusDetails": [
        {
            "TableRestoreRequestId": "z1116630-0e80-46f4-ba86-bd9670411ebd",
            "Status": "IN_PROGRESS",
            "RequestTime": "2019-12-27T18:22:12.257Z",
            "ClusterIdentifier": "mycluster",
            "SnapshotIdentifier": "mysnapshotid",
            "SourceDatabaseName": "dev",
```

```
            "SourceSchemaName": "public",
            "SourceTableName": "mytable",
            "TargetDatabaseName": "dev",
            "TargetSchemaName": "public",
            "NewTableName": "mytable-clone"
        }
    ]
}
```

Para obtener más información, consulte Restauración de una tabla a partir de una instantánea en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte DescribeTableRestoreStatus en la Referencia de comandos de la AWS CLI.

`describe-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-tags`.

AWS CLI

Para describir las etiquetas

En el siguiente ejemplo de `describe-tags`, se muestran los recursos que el clúster especificado asoció a los nombres y valores de las etiquetas especificadas.

```
aws redshift describe-tags \
    --resource-name arn:aws:redshift:us-west-2:123456789012:cluster:mycluster \
    --tag-keys clustertagkey \
    --tag-values clustertagvalue
```

Salida:

```
{
    "TaggedResources": [
                    {
            "Tag": {
                "Key": "clustertagkey",
                "Value": "clustertagvalue"
            },
            "ResourceName": "arn:aws:redshift:us-
west-2:123456789012:cluster:mycluster",
            "ResourceType": "cluster"
```

```
        }
    ]
}
```

Para obtener más información, consulte Etiquetado de recursos en Amazon Redshift en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte DescribeTags en la Referencia de comandos de la AWS CLI.

`disable-snapshot-copy`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-snapshot-copy`.

AWS CLI

Para deshabilitar la copia de una instantánea para un clúster

En el siguiente ejemplo de `disable-snapshot-copy`, se deshabilita la copia automática de una instantánea para el clúster especificado.

```
aws redshift disable-snapshot-copy \
    --cluster-identifier mycluster
```

Salida:

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
        "NodeType": "dc2.large",
        "ClusterStatus": "available",
        "ClusterAvailabilityStatus": "Available",
        "MasterUsername": "adminuser",
        "DBName": "dev",
        "Endpoint": {
            "Address": "mycluster.cmeaswqeuae.us-west-2.redshift.amazonaws.com",
            "Port": 5439
        },
        "ClusterCreateTime": "2019-12-05T18:44:36.991Z",
        "AutomatedSnapshotRetentionPeriod": 3,
        "ManualSnapshotRetentionPeriod": -1,
        "ClusterSecurityGroups": [],
        "VpcSecurityGroups": [
```

```
            {
                "VpcSecurityGroupId": "sh-i9b431cd",
                "Status": "active"
            }
        ],
        "ClusterParameterGroups": [
            {
                "ParameterGroupName": "default.redshift-1.0",
                "ParameterApplyStatus": "in-sync"
            }
        ],
        "ClusterSubnetGroupName": "default",
        "VpcId": "vpc-b1fel7t9",
        "AvailabilityZone": "us-west-2f",
        "PreferredMaintenanceWindow": "sat:16:00-sat:16:30",
        "PendingModifiedValues": {
            "NodeType": "dc2.large",
            "NumberOfNodes": 2,
            "ClusterType": "multi-node"
        },
        "ClusterVersion": "1.0",
        "AllowVersionUpgrade": true,
        "NumberOfNodes": 4,
        "PubliclyAccessible": false,
        "Encrypted": false,
        "Tags": [
            {
                "Key": "mytags",
                "Value": "tag1"
            }
        ],
        "EnhancedVpcRouting": false,
        "IamRoles": [
            {
                "IamRoleArn": "arn:aws:iam::123456789012:role/myRedshiftRole",
                "ApplyStatus": "in-sync"
            }
        ],
        "MaintenanceTrackName": "current",
        "DeferredMaintenanceWindows": [],
        "ExpectedNextSnapshotScheduleTime": "2019-12-10T04:42:43.390Z",
        "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
        "NextMaintenanceWindowStartTime": "2019-12-14T16:00:00Z"
    }
```

```
}
```

Para obtener más información, consulte Copia de una instantánea a otra región de AWS en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte DisableSnapshotCopy en la Referencia de comandos de la AWS CLI.

`enable-snapshot-copy`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-snapshot-copy`.

AWS CLI

Para habilitar la copia de una instantánea para un clúster

En el siguiente ejemplo de `enable-snapshot-copy`, se habilita la copia automática de una instantánea para el clúster especificado.

```
aws redshift enable-snapshot-copy \
    --cluster-identifier mycluster \
    --destination-region us-west-1
```

Salida:

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
        "NodeType": "dc2.large",
        "ClusterStatus": "available",
        "ClusterAvailabilityStatus": "Available",
        "MasterUsername": "adminuser",
        "DBName": "dev",
        "Endpoint": {
            "Address": "mycluster.cmeaswqeuae.us-west-2.redshift.amazonaws.com",
            "Port": 5439
        },
        "ClusterCreateTime": "2019-12-05T18:44:36.991Z",
        "AutomatedSnapshotRetentionPeriod": 3,
        "ManualSnapshotRetentionPeriod": -1,
        "ClusterSecurityGroups": [],
        "VpcSecurityGroups": [
            {
```

```
            "VpcSecurityGroupId": "sh-f4c731cd",
            "Status": "active"
        }
    ],
    "ClusterParameterGroups": [
        {
            "ParameterGroupName": "default.redshift-1.0",
            "ParameterApplyStatus": "in-sync"
        }
    ],
    "ClusterSubnetGroupName": "default",
    "VpcId": "vpc-b1ael7t9",
    "AvailabilityZone": "us-west-2f",
    "PreferredMaintenanceWindow": "sat:16:00-sat:16:30",
    "PendingModifiedValues": {
        "NodeType": "dc2.large",
        "NumberOfNodes": 2,
        "ClusterType": "multi-node"
    },
    "ClusterVersion": "1.0",
    "AllowVersionUpgrade": true,
    "NumberOfNodes": 4,
    "PubliclyAccessible": false,
    "Encrypted": false,
    "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "us-west-1",
        "RetentionPeriod": 7,
        "ManualSnapshotRetentionPeriod": -1
    },
    "Tags": [
        {
            "Key": "mytags",
            "Value": "tag1"
        }
    ],
    "EnhancedVpcRouting": false,
    "IamRoles": [
        {
            "IamRoleArn": "arn:aws:iam::123456789012:role/myRedshiftRole",
            "ApplyStatus": "in-sync"
        }
    ],
    "MaintenanceTrackName": "current",
    "DeferredMaintenanceWindows": [],
```

```
        "ExpectedNextSnapshotScheduleTime": "2019-12-10T04:42:43.390Z",
        "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
        "NextMaintenanceWindowStartTime": "2019-12-14T16:00:00Z"
    }
}
```

Para obtener más información, consulte Copia de una instantánea a otra región de AWS en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre las API, consulte EnableSnapshotCopy en la Referencia de comandos de la AWS CLI.

`get-cluster-credentials`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-cluster-credentials`.

AWS CLI

Para obtener las credenciales de clúster de una cuenta AWS

El siguiente ejem plo de `get-cluster-credentials` recupera las credenciales temporales que permiten acceder a una base de datos de Amazon Redshift.

```
aws redshift get-cluster-credentials \
    --db-user adminuser --db-name dev \
    --cluster-identifier mycluster
```

Salida:

```
{
    "DbUser": "IAM:adminuser",
    "DbPassword": "AMAFUyyuros/QjxPTtgzcsuQsqzIasdzJEN04aCtWDzXx1O9d6UmpkBtvEeqFly/
EXAMPLE==",
    "Expiration": "2019-12-10T17:25:05.770Z"
}
```

Para obtener más información, consulte Generación de credenciales de base de datos para una identidad de IAM mediante la CLI o la API de Amazon Redshift en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte GetClusterCredentials en la Referencia de comandos de la AWS CLI.

`get-reserved-node-exchange-offerings`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-reserved-node-exchange-offerings`.

AWS CLI

Para obtener ofertas de intercambio de nodos reservados

El siguiente ejemplo de `get-reserved-node-exchange-offerings` recupera una matriz de `DC2` `ReservedNodeOfferings` que coincide con el nodo reservado `DC1` especificado.

```
aws redshift get-reserved-node-exchange-offerings \
    --reserved-node-id 12345678-12ab-12a1-1a2a-12ab-12a12EXAMPLE
```

Salida:

```
{
    "ReservedNodeOfferings": [
        {
            "ReservedNodeOfferingId": "12345678-12ab-12a1-1a2a-12ab-12a12EXAMPLE",
            "NodeType": "dc2.large",
            "Duration": 31536000,
            "FixedPrice": 0.0,
            "UsagePrice": 0.0,
            "CurrencyCode": "USD",
            "OfferingType": "All Upfront",
            "RecurringCharges": [
                {
                    "RecurringChargeAmount": 0.0,
                    "RecurringChargeFrequency": "Hourly"
                }
            ],
            "ReservedNodeOfferingType": "Regular"
        }
    ]
}
```

Para obtener más información, consulte Upgrading Reserved Nodes With the AWS CLI en la Guía de administración del clúster de Amazon Redshift.

- Para obtener información sobre la API, consulte GetReservedNodeExchangeOfferings en la Referencia de comandos de la AWS CLI.

`modify-cluster-iam-roles`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-cluster-iam-roles`.

AWS CLI

Para modificar el rol de IAM de un clúster

En el siguiente ejemplo de `modify-cluster-iam-roles`, se elimina el rol de IAM AWS especificado del clúster especificado.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --remove-iam-roles arn:aws:iam::123456789012:role/myRedshiftRole
```

Salida:

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
        "NodeType": "dc2.large",
        "ClusterStatus": "available",
        "ClusterAvailabilityStatus": "Available",
        "MasterUsername": "adminuser",
        "DBName": "dev",
        "Endpoint": {
            "Address": "mycluster.cmeaswqeuae.us-west-2.redshift.amazonaws.com",
            "Port": 5439
        },
        "ClusterCreateTime": "2019-12-05T18:44:36.991Z",
        "AutomatedSnapshotRetentionPeriod": 3,
        "ManualSnapshotRetentionPeriod": -1,
        "ClusterSecurityGroups": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sh-f9b731sd",
                "Status": "active"
            }
        ],
        "ClusterParameterGroups": [
            {
                "ParameterGroupName": "default.redshift-1.0",
                "ParameterApplyStatus": "in-sync"
```

```
            }
        ],
        "ClusterSubnetGroupName": "default",
        "VpcId": "vpc-b2fal7t9",
        "AvailabilityZone": "us-west-2f",
        "PreferredMaintenanceWindow": "sat:16:00-sat:16:30",
        "PendingModifiedValues": {
            "NodeType": "dc2.large",
            "NumberOfNodes": 2,
            "ClusterType": "multi-node"
        },
        "ClusterVersion": "1.0",
        "AllowVersionUpgrade": true,
        "NumberOfNodes": 4,
        "PubliclyAccessible": false,
        "Encrypted": false,
        "ClusterSnapshotCopyStatus": {
            "DestinationRegion": "us-west-1",
            "RetentionPeriod": 7,
            "ManualSnapshotRetentionPeriod": -1
        },
        "Tags": [
            {
                "Key": "mytags",
                "Value": "tag1"
            }
        ],
        "EnhancedVpcRouting": false,
        "IamRoles": [],
        "MaintenanceTrackName": "current",
        "DeferredMaintenanceWindows": [],
        "ExpectedNextSnapshotScheduleTime": "2019-12-11T04:42:55.631Z",
        "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
        "NextMaintenanceWindowStartTime": "2019-12-14T16:00:00Z"
    }
}
```

Para obtener más información, consulte Uso de políticas basadas en identidad (políticas de IAM) para Amazon Redshift en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte ModifyClusterIamRoles en la Referencia de comandos de la AWS CLI.

`modify-cluster-maintenance`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-cluster-maintenance`.

AWS CLI

Para modificar el mantenimiento del clúster

El siguiente ejemplo de `modify-cluster-maintenance` aplaza 30 días el mantenimiento del clúster especificado durante 30 días.

```
aws redshift modify-cluster-maintenance \
    --cluster-identifier mycluster \
    --defer-maintenance \
    --defer-maintenance-duration 30
```

Salida:

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
        "NodeType": "dc2.large",
        "ClusterStatus": "available",
        "ClusterAvailabilityStatus": "Available",
        "MasterUsername": "adminuser",
        "DBName": "dev",
        "Endpoint": {
            "Address": "mycluster.cmeaswqeuae.us-west-2.redshift.amazonaws.com",
            "Port": 5439
        },
        "ClusterCreateTime": "2019-12-05T18:44:36.991Z",
        "AutomatedSnapshotRetentionPeriod": 3,
        "ManualSnapshotRetentionPeriod": -1,
        "ClusterSecurityGroups": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sh-a1a123ab",
                "Status": "active"
            }
        ],
        "ClusterParameterGroups": [
            {
                "ParameterGroupName": "default.redshift-1.0",
```

```
                "ParameterApplyStatus": "in-sync"
            }
        ],
        "ClusterSubnetGroupName": "default",
        "VpcId": "vpc-b1ael7t9",
        "AvailabilityZone": "us-west-2f",
        "PreferredMaintenanceWindow": "sat:16:00-sat:16:30",
        "PendingModifiedValues": {
            "NodeType": "dc2.large",
            "NumberOfNodes": 2,
            "ClusterType": "multi-node"
        },
        "ClusterVersion": "1.0",
        "AllowVersionUpgrade": true,
        "NumberOfNodes": 4,
        "PubliclyAccessible": false,
        "Encrypted": false,
        "ClusterSnapshotCopyStatus": {
            "DestinationRegion": "us-west-1",
            "RetentionPeriod": 7,
            "ManualSnapshotRetentionPeriod": -1
        },
        "Tags": [
            {
                "Key": "mytags",
                "Value": "tag1"
            }
        ],
        "EnhancedVpcRouting": false,
        "IamRoles": [],
        "MaintenanceTrackName": "current",
        "DeferredMaintenanceWindows": [
            {
                "DeferMaintenanceIdentifier": "dfm-mUdVIfFcT1B4SGhw6fyF",
                "DeferMaintenanceStartTime": "2019-12-10T18:18:39.354Z",
                "DeferMaintenanceEndTime": "2020-01-09T18:18:39.354Z"
            }
        ],
        "ExpectedNextSnapshotScheduleTime": "2019-12-11T04:42:55.631Z",
        "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
        "NextMaintenanceWindowStartTime": "2020-01-11T16:00:00Z"
    }
}
```

Para obtener más información, consulte Mantenimiento de clústeres en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte ModifyClusterMaintenance en la Referencia de comandos de la AWS CLI.

`modify-cluster-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-cluster-parameter-group`.

AWS CLI

Modificar un parámetro en un grupo de parámetros

El siguiente ejemplo de `modify-cluster-parameter-group` modifica el parámetro wlm_json_configuration para la administración de la carga de trabajo. Acepta los parámetros de un archivo que contiene el contenido JSON que se muestra a continuación.

```
aws redshift modify-cluster-parameter-group \
    --parameter-group-name myclusterparametergroup \
    --parameters file://modify_pg.json
```

Contenido de `modify_pg.json`:

```
[
    {
        "ParameterName": "wlm_json_configuration",
        "ParameterValue": "[{\"user_group\":\"example_user_group1\",\"query_group\":
 \"example_query_group1\", \"query_concurrency\":7},{\"query_concurrency\":5}]"
    }
]
```

Salida:

```
{
   "ParameterGroupStatus": "Your parameter group has been updated but changes won't
 get applied until you reboot the associated Clusters.",
   "ParameterGroupName": "myclusterparametergroup",
   "ResponseMetadata": {
      "RequestId": "09974cc0-64cd-11e2-bea9-49e0ce183f07"
   }
```

```
}
```

- Para obtener información sobre la API, consulte ModifyClusterParameterGroup en la Referencia de comandos de la AWS CLI.

`modify-cluster-snapshot-schedule`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-cluster-snapshot-schedule`.

AWS CLI

Para modificar la programación de instantáneas del clúster

El siguiente ejemplo de `modify-cluster-snapshot-schedule` elimina la programación de instantánea especificada desde el clúster especificado.

```
aws redshift modify-cluster-snapshot-schedule \
    --cluster-identifier mycluster \
    --schedule-identifier mysnapshotschedule \
    --disassociate-schedule
```

Este comando no produce ninguna salida.

Para obtener más información, consulte Programación de instantáneas automatizadas en la Guía de administración de clústeres de Amazon Redshift.

- Para ver los detalles de la API, consulte ModifyClusterSnapshotSchedule en la Referencia de comandos de la AWS CLI.

`modify-cluster-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-cluster-snapshot`.

AWS CLI

Para modificar la instantánea del clúster

El siguiente ejemplo de `modify-cluster-snapshot` establece la configuración del período de retención manual para la instantánea del clúster especificado en un valor de 10 días.

```
aws redshift modify-cluster-snapshot \
```

```
    --snapshot-identifier mycluster-2019-11-06-16-32 \
    --manual-snapshot-retention-period 10
```

Salida:


```
{
    "Snapshot": {
        "SnapshotIdentifier": "mycluster-2019-11-06-16-32",
        "ClusterIdentifier": "mycluster",
        "SnapshotCreateTime": "2019-12-07T00:34:05.633Z",
        "Status": "available",
        "Port": 5439,
        "AvailabilityZone": "us-west-2f",
        "ClusterCreateTime": "2019-12-05T18:44:36.991Z",
        "MasterUsername": "adminuser",
        "ClusterVersion": "1.0",
        "SnapshotType": "manual",
        "NodeType": "dc2.large",
        "NumberOfNodes": 2,
        "DBName": "dev",
        "VpcId": "vpc-b1ce17t9",
        "Encrypted": false,
        "EncryptedWithHSM": false,
        "OwnerAccount": "123456789012",
        "TotalBackupSizeInMegaBytes": 64384.0,
        "ActualIncrementalBackupSizeInMegaBytes": 24.0,
        "BackupProgressInMegaBytes": 24.0,
        "CurrentBackupRateInMegaBytesPerSecond": 13.0011,
        "EstimatedSecondsToCompletion": 0,
        "ElapsedTimeInSeconds": 1,
        "Tags": [
            {
                "Key": "mytagkey",
                "Value": "mytagvalue"
            }
        ],
        "EnhancedVpcRouting": false,
        "MaintenanceTrackName": "current",
        "ManualSnapshotRetentionPeriod": 10,
        "ManualSnapshotRemainingDays": 6,
        "SnapshotRetentionStartTime": "2019-12-07T00:34:07.479Z"
    }
}
```

Para obtener más información, consulte Amazon Redshift Snapshots en la Guía de administración de clúster de Amazon Redshift.

- Para obtener información sobre la API, consulte ModifyClusterSnapshot en la Referencia de comandos de la AWS CLI.

`modify-cluster-subnet-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-cluster-subnet-group`.

AWS CLI

Modificar las subredes de un grupo de subredes de clúster Este ejemplo muestra cómo modificar la lista de subredes de un grupo de subredes de caché. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift modify-cluster-subnet-group --cluster-subnet-group-name mysubnetgroup
 --subnet-ids subnet-763fdd1 subnet-ac830e9
```

Resultado:

```
{
   "ClusterSubnetGroup":
   {
      "Subnets": [
         {
            "SubnetStatus": "Active",
            "SubnetIdentifier": "subnet-763fdd1c",
            "SubnetAvailabilityZone":
               { "Name": "us-east-1a" }
         },
         {
            "SubnetStatus": "Active",
            "SubnetIdentifier": "subnet-ac830e9",
            "SubnetAvailabilityZone":
               { "Name": "us-east-1b" }
         } ],
      "VpcId": "vpc-7e3fdd14",
      "SubnetGroupStatus": "Complete",
      "Description": "My subnet group",
      "ClusterSubnetGroupName": "mysubnetgroup"
   },
```

```
    "ResponseMetadata": {
        "RequestId": "8da93e89-8372-f936-93a8-873918938197a"
    }
}
```

- Para obtener información sobre la API, consulte ModifyClusterSubnetGroup en la Referencia de comandos de la AWS CLI.

`modify-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-cluster`.

AWS CLI

Asociación de un grupo de seguridad a un clúster En este ejemplo se muestra cómo asociar un grupo de seguridad de clúster al clúster especificado. Comando:

```
aws redshift modify-cluster --cluster-identifier mycluster --cluster-security-groups
 mysecuritygroup
```

Modificación del período de mantenimiento de un clúster Aquí se muestra cómo cambiar el período de mantenimiento semanal preferido de un clúster para que sea el período mínimo de cuatro horas, que comience los domingos a las 23:15 y termine los lunes a las 3:15. Comando:

```
aws redshift modify-cluster --cluster-identifier mycluster --preferred-maintenance-
window Sun:23:15-Mon:03:15
```

Cambio de la contraseña maestra del clúster En este ejemplo se muestra cómo cambiar la contraseña maestra de un clúster. Comando:

```
aws redshift modify-cluster --cluster-identifier mycluster --master-user-password
 A1b2c3d4
```

- Para obtener información sobre la API, consulte ModifyCluster en la Referencia de comandos de la AWS CLI.

`modify-event-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-event-subscription`.

AWS CLI

Para modificar la suscripción a un evento

En el siguiente ejemplo de `modify-event-subscription` se deshabilita la suscripción a una notificación de evento especificada.

```
aws redshift modify-event-subscription \
    --subscription-name mysubscription \
    --no-enabled
```

Salida:

```
{
    "EventSubscription": {
        "CustomerAwsId": "123456789012",
        "CustSubscriptionId": "mysubscription",
        "SnsTopicArn": "arn:aws:sns:us-west-2:123456789012:MySNStopic",
        "Status": "active",
        "SubscriptionCreationTime": "2019-12-09T21:50:21.332Z",
        "SourceIdsList": [],
        "EventCategoriesList": [
            "management"
        ],
        "Severity": "ERROR",
        "Enabled": false,
        "Tags": []
    }
}
```

Para obtener más información, consulte Subscribing to Amazon Redshift Event Notifications en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte ModifyEventSubscription en la Referencia de comandos de la AWS CLI.

`modify-scheduled-action`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-scheduled-action`.

AWS CLI

Para modificar una acción programada

En el siguiente ejemplo de `modify-scheduled-action`, se agrega una descripción a la acción programada existente especificada.

```
aws redshift modify-scheduled-action \
    --scheduled-action-name myscheduledaction \
    --scheduled-action-description "My scheduled action"
```

Salida:

```
{
    "ScheduledActionName": "myscheduledaction",
    "TargetAction": {
        "ResizeCluster": {
            "ClusterIdentifier": "mycluster",
            "NumberOfNodes": 2,
            "Classic": false
        }
    },
    "Schedule": "at(2019-12-25T00:00:00)",
    "IamRole": "arn:aws:iam::123456789012:role/myRedshiftRole",
    "ScheduledActionDescription": "My scheduled action",
    "State": "ACTIVE",
    "NextInvocations": [
        "2019-12-25T00:00:00Z"
    ]
}
```

- Para obtener información sobre la API, consulte ModifyScheduledAction en la Referencia de comandos de la AWS CLI.

`modify-snapshot-copy-retention-period`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-snapshot-copy-retention-period`.

AWS CLI

Para modificar el período de retención de la copia de una instantánea

El siguiente ejemplo de `modify-snapshot-copy-retention-period` modifica el número de días para retener las instantáneas de un clúster especificado en la región AWS de destino después de que se hayan copiado desde una región AWS.

```
aws redshift modify-snapshot-copy-retention-period \
    --cluster-identifier mycluster \
    --retention-period 15
```

Salida:

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
        "NodeType": "dc2.large",
        "ClusterStatus": "available",
        "ClusterAvailabilityStatus": "Available",
        "MasterUsername": "adminuser",
        "DBName": "dev",
        "Endpoint": {
            "Address": "mycluster.cmeaswqeuae.us-west-2.redshift.amazonaws.com",
            "Port": 5439
        },
        "ClusterCreateTime": "2019-12-05T18:44:36.991Z",
        "AutomatedSnapshotRetentionPeriod": 3,
        "ManualSnapshotRetentionPeriod": -1,
        "ClusterSecurityGroups": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sh-a1a123ab",
                "Status": "active"
            }
        ],
        "ClusterParameterGroups": [
            {
                "ParameterGroupName": "default.redshift-1.0",
                "ParameterApplyStatus": "in-sync"
            }
        ],
        "ClusterSubnetGroupName": "default",
        "VpcId": "vpc-b1fet7t9",
        "AvailabilityZone": "us-west-2f",
        "PreferredMaintenanceWindow": "sat:16:00-sat:16:30",
        "PendingModifiedValues": {
```

```
            "NodeType": "dc2.large",
            "NumberOfNodes": 2,
            "ClusterType": "multi-node"
        },
        "ClusterVersion": "1.0",
        "AllowVersionUpgrade": true,
        "NumberOfNodes": 4,
        "PubliclyAccessible": false,
        "Encrypted": false,
        "ClusterSnapshotCopyStatus": {
            "DestinationRegion": "us-west-1",
            "RetentionPeriod": 15,
            "ManualSnapshotRetentionPeriod": -1
        },
        "Tags": [
            {
                "Key": "mytags",
                "Value": "tag1"
            }
        ],
        "EnhancedVpcRouting": false,
        "IamRoles": [],
        "MaintenanceTrackName": "current",
        "DeferredMaintenanceWindows": [
            {
                "DeferMaintenanceIdentifier": "dfm-mUdVSfDcT1F4SGhw6fyF",
                "DeferMaintenanceStartTime": "2019-12-10T18:18:39.354Z",
                "DeferMaintenanceEndTime": "2020-01-09T18:18:39.354Z"
            }
        ],
        "NextMaintenanceWindowStartTime": "2020-01-11T16:00:00Z"
    }
}
```

Para obtener más información, consulte Formato de la programación de instantáneas en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte ModifySnapshotCopyRetentionPeriod en la Referencia de comandos de la AWS CLI.

`modify-snapshot-schedule`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-snapshot-schedule`.

AWS CLI

Para modificar la programación de instantáneas

En el siguiente ejemplo de `modify-snapshot-schedule`, se modifica la frecuencia de la programación de instantáneas especificada para que pase a ser cada 10 horas.

```
aws redshift modify-snapshot-schedule \
    --schedule-identifier mysnapshotschedule \
    --schedule-definitions "rate(10 hours)"
```

Salida:

```
{
    "ScheduleDefinitions": [
        "rate(10 hours)"
    ],
    "ScheduleIdentifier": "mysnapshotschedule",
    "ScheduleDescription": "My schedule description",
    "Tags": []
}
```

Para obtener más información, consulte Formato de la programación de instantáneas en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte ModifySnapshotSchedule en la Referencia de comandos de la AWS CLI.

`purchase-reserved-node-offering`

En el siguiente ejemplo de código, se muestra cómo utilizar `purchase-reserved-node-offering`.

AWS CLI

Compra de un nodo reservada En este ejemplo se muestra cómo comprar una oferta de nodo reservada. El `reserved-node-offering-id` se obtiene llamando a `describe-reserved-node-offerings`. Comando:

```
aws redshift purchase-reserved-node-offering --reserved-node-offering-id ceb6a579-cf4c-4343-be8b-d832c45ab51c
```

Resultado:

```
{
   "ReservedNode": {
      "OfferingType": "Heavy Utilization",
      "FixedPrice": "",
      "NodeType": "dw.hs1.xlarge",
      "ReservedNodeId": "1ba8e2e3-bc01-4d65-b35d-a4a3e931547e",
      "UsagePrice": "",
      "RecurringCharges": [
         {
            "RecurringChargeAmount": "",
            "RecurringChargeFrequency": "Hourly"
         }
      ],
      "NodeCount": 1,
      "State": "payment-pending",
      "StartTime": "2013-02-13T17:08:39.051Z",
      "Duration": 31536000,
      "ReservedNodeOfferingId": "ceb6a579-cf4c-4343-be8b-d832c45ab51c"
   },
   "ResponseMetadata": {
      "RequestId": "01bda7bf-7600-11e2-b605-2568d7396e7f"
   }
}
```

- Para obtener detalles sobre la API, consulte PurchaseReservedNodeOffering en la Referencia de comandos de la AWS CLI.

`reboot-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `reboot-cluster`.

AWS CLI

Reiniciar un clúster En este ejemplo se reinicia un clúster. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift reboot-cluster --cluster-identifier mycluster
```

Resultado:

```
{
   "Cluster": {
      "NodeType": "dw.hs1.xlarge",
      "Endpoint": {
         "Port": 5439,
         "Address": "mycluster.coqoarplqhsn.us-east-1.redshift.amazonaws.com"
      },
      "ClusterVersion": "1.0",
      "PubliclyAccessible": "true",
      "MasterUsername": "adminuser",
      "ClusterParameterGroups": [
         {
         "ParameterApplyStatus": "in-sync",
         "ParameterGroupName": "default.redshift-1.0"
         }
      ],
      "ClusterSecurityGroups": [
         {
         "Status": "active",
         "ClusterSecurityGroupName": "default"
         }
      ],
      "AllowVersionUpgrade": true,
      "VpcSecurityGroups": \[],
      "AvailabilityZone": "us-east-1a",
      "ClusterCreateTime": "2013-01-22T21:59:29.559Z",
      "PreferredMaintenanceWindow": "sun:23:15-mon:03:15",
      "AutomatedSnapshotRetentionPeriod": 1,
      "ClusterStatus": "rebooting",
      "ClusterIdentifier": "mycluster",
      "DBName": "dev",
      "NumberOfNodes": 2,
      "PendingModifiedValues": {}
   },
   "ResponseMetadata": {
      "RequestId": "61c8b564-64e8-11e2-8f7d-3b939af52818"
   }
}
```

- Para obtener más información sobre la API, consulte RebootCluster en la Referencia de comandos de la AWS CLI.

`reset-cluster-parameter-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-cluster-parameter-group`.

AWS CLI

Restablecer los parámetros de un grupo de parámetros Este ejemplo muestra cómo restablecer todos los parámetros de un grupo de parámetros. Comando:

```
aws redshift reset-cluster-parameter-group --parameter-group-name
 myclusterparametergroup --reset-all-parameters
```

- Para ver los detalles de la API, consulte ResetClusterParameterGroup en la Referencia de comandos de la AWS CLI.

`resize-cluster`

En el siguiente ejemplo de código, se muestra cómo utilizar `resize-cluster`.

AWS CLI

Para redimensionar un clúster

El siguiente ejemplo de `resize-cluster` redimensiona el clúster especificado.

```
aws redshift resize-cluster \
    --cluster-identifier mycluster \
    --cluster-type multi-node \
    --node-type dc2.large \
    --number-of-nodes 6 \
    --classic
```

Salida:

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
        "NodeType": "dc2.large",
        "ClusterStatus": "resizing",
        "ClusterAvailabilityStatus": "Modifying",
        "MasterUsername": "adminuser",
        "DBName": "dev",
```

```
        "Endpoint": {
            "Address": "mycluster.cmeaswqeuae.us-west-2.redshift.amazonaws.com",
            "Port": 5439
        },
        "ClusterCreateTime": "2019-12-05T18:44:36.991Z",
        "AutomatedSnapshotRetentionPeriod": 3,
        "ManualSnapshotRetentionPeriod": -1,
        "ClusterSecurityGroups": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sh-a1a123ab",
                "Status": "active"
            }
        ],
        "ClusterParameterGroups": [
            {
                "ParameterGroupName": "default.redshift-1.0",
                "ParameterApplyStatus": "in-sync"
            }
        ],
        "ClusterSubnetGroupName": "default",
        "VpcId": "vpc-a1abc1a1",
        "AvailabilityZone": "us-west-2f",
        "PreferredMaintenanceWindow": "sat:16:00-sat:16:30",
        "PendingModifiedValues": {
            "NodeType": "dc2.large",
            "NumberOfNodes": 6,
            "ClusterType": "multi-node"
        },
        "ClusterVersion": "1.0",
        "AllowVersionUpgrade": true,
        "NumberOfNodes": 4,
        "PubliclyAccessible": false,
        "Encrypted": false,
        "ClusterSnapshotCopyStatus": {
            "DestinationRegion": "us-west-1",
            "RetentionPeriod": 15,
            "ManualSnapshotRetentionPeriod": -1
        },
        "Tags": [
            {
                "Key": "mytags",
                "Value": "tag1"
            }
```

```
        ],
        "EnhancedVpcRouting": false,
        "IamRoles": [],
        "MaintenanceTrackName": "current",
        "DeferredMaintenanceWindows": [
            {
                "DeferMaintenanceIdentifier": "dfm-mUdVCfDcT1B4SGhw6fyF",
                "DeferMaintenanceStartTime": "2019-12-10T18:18:39.354Z",
                "DeferMaintenanceEndTime": "2020-01-09T18:18:39.354Z"
            }
        ],
        "NextMaintenanceWindowStartTime": "2020-01-11T16:00:00Z",
        "ResizeInfo": {
            "ResizeType": "ClassicResize",
            "AllowCancelResize": true
        }
    }
}
```

Para obtener más información, consulte Redimensionamiento de un clúster en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte ResizeCluster en la Referencia de comandos de la AWS CLI.

`restore-from-cluster-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-from-cluster-snapshot`.

AWS CLI

Restaurar un clúster a partir de una instantánea Este ejemplo restaura un clúster a partir de una instantánea. Comando:

```
aws redshift restore-from-cluster-snapshot --cluster-identifier mycluster-clone --
snapshot-identifier my-snapshot-id
```

Resultado:

```
{
   "Cluster": {
```

```
      "NodeType": "dw.hs1.xlarge",
      "ClusterVersion": "1.0",
      "PubliclyAccessible": "true",
      "MasterUsername": "adminuser",
      "ClusterParameterGroups": [
         {
         "ParameterApplyStatus": "in-sync",
         "ParameterGroupName": "default.redshift-1.0"
         }
      ],
      "ClusterSecurityGroups": [
         {
         "Status": "active",
         "ClusterSecurityGroupName": "default"
         }
      ],
      "AllowVersionUpgrade": true,
      "VpcSecurityGroups": \[],
      "PreferredMaintenanceWindow": "sun:23:15-mon:03:15",
      "AutomatedSnapshotRetentionPeriod": 1,
      "ClusterStatus": "creating",
      "ClusterIdentifier": "mycluster-clone",
      "DBName": "dev",
      "NumberOfNodes": 2,
      "PendingModifiedValues": {}
   },
   "ResponseMetadata": {
      "RequestId": "77fd512b-64e3-11e2-8f5b-e90bd6c77476"
   }
}
```

- Para ver los detalles de la API, consulte RestoreFromClusterSnapshot en la Referencia de comandos de la AWS CLI.

`restore-table-from-cluster-snapshot`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-table-from-cluster-snapshot`.

AWS CLI

Para restaurar una tabla a partir de la instantánea de un clúster

En el siguiente ejemplo de `restore-table-from-cluster-snapshot`, se crea una tabla nueva a partir de la tabla especificada en la instantánea del clúster especificada.

```
aws redshift restore-table-from-cluster-snapshot /
    --cluster-identifier mycluster /
    --snapshot-identifier mycluster-2019-11-19-16-17 /
    --source-database-name dev /
    --source-schema-name public /
    --source-table-name mytable /
    --target-database-name dev /
    --target-schema-name public /
    --new-table-name mytable-clone
```

Salida:

```
{
    "TableRestoreStatus": {
        "TableRestoreRequestId": "a123a12b-abc1-1a1a-a123-a1234ab12345",
        "Status": "PENDING",
        "RequestTime": "2019-12-20T00:20:16.402Z",
        "ClusterIdentifier": "mycluster",
        "SnapshotIdentifier": "mycluster-2019-11-19-16-17",
        "SourceDatabaseName": "dev",
        "SourceSchemaName": "public",
        "SourceTableName": "mytable",
        "TargetDatabaseName": "dev",
        "TargetSchemaName": "public",
        "NewTableName": "mytable-clone"
    }
}
```

Para obtener más información, consulte Restauración de una tabla a partir de una instantánea en la Guía de administración de clústeres de Amazon Redshift.

- Para obtener información sobre la API, consulte RestoreTableFromClusterSnapshot en la Referencia de comandos de la AWS CLI.

`revoke-cluster-security-group-ingress`

En el siguiente ejemplo de código, se muestra cómo utilizar `revoke-cluster-security-group-ingress`.

AWS CLI

Revocación del acceso a un grupo de seguridad de EC2. Este ejemplo revoca el acceso a un grupo de seguridad de Amazon EC2. Comando:

```
aws redshift revoke-cluster-security-group-ingress --cluster-security-group-name
 mysecuritygroup --ec2-security-group-name myec2securitygroup --ec2-security-group-
owner-id 123445677890
```

Revocación del acceso a un rango de CIDR. Este ejemplo revoca el acceso a un rango de CIDR. Comando:

```
aws redshift revoke-cluster-security-group-ingress --cluster-security-group-name
 mysecuritygroup --cidrip 192.168.100.100/32
```

- Para obtener información sobre la API, consulte RevokeClusterSecurityGroupIngress en la Referencia de comandos de la AWS CLI.

`revoke-snapshot-access`

En el siguiente ejemplo de código, se muestra cómo utilizar `revoke-snapshot-access`.

AWS CLI

Revocación de una cuenta de AWS para restaurar una instantánea. Este ejemplo revoca la autorización de la cuenta de AWS `444455556666` para restaurar la instantánea `my-snapshot-id`. De forma predeterminada, el resultado es en formato JSON. Comando:

```
aws redshift revoke-snapshot-access --snapshot-id my-snapshot-id --account-with-
restore-access 444455556666
```

Resultado:

```
{
   "Snapshot": {
      "Status": "available",
      "SnapshotCreateTime": "2013-07-17T22:04:18.947Z",
      "EstimatedSecondsToCompletion": 0,
      "AvailabilityZone": "us-east-1a",
      "ClusterVersion": "1.0",
      "MasterUsername": "adminuser",
```

```
      "Encrypted": false,
      "OwnerAccount": "111122223333",
      "BackupProgressInMegabytes": 11.0,
      "ElapsedTimeInSeconds": 0,
      "DBName": "dev",
      "CurrentBackupRateInMegabytesPerSecond: 0.1534,
      "ClusterCreateTime": "2013-01-22T21:59:29.559Z",
      "ActualIncrementalBackupSizeInMegabytes"; 11.0,
      "SnapshotType": "manual",
      "NodeType": "dw.hs1.xlarge",
      "ClusterIdentifier": "mycluster",
      "TotalBackupSizeInMegabytes": 20.0,
      "Port": 5439,
      "NumberOfNodes": 2,
      "SnapshotIdentifier": "my-snapshot-id"
   }
}
```

- Para obtener información sobre la API, consulte RevokeSnapshotAccess en la Referencia de comandos de la AWS CLI.

`rotate-encryption-key`

En el siguiente ejemplo de código, se muestra cómo utilizar `rotate-encryption-key`.

AWS CLI

Para rotar la clave de cifrado de un clúster

En el siguiente ejemplo de `rotate-encryption-key`, se rota la clave de cifrado del clúster especificado.

```
aws redshift rotate-encryption-key \
    --cluster-identifier mycluster
```

Salida:

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
        "NodeType": "dc2.large",
        "ClusterStatus": "rotating-keys",
```

```
        "ClusterAvailabilityStatus": "Modifying",
        "MasterUsername": "adminuser",
        "DBName": "dev",
        "Endpoint": {
            "Address": "mycluster.cmeaswqeuae.us-west-2.redshift.amazonaws.com",
            "Port": 5439
        },
        "ClusterCreateTime": "2019-12-10T19:25:45.886Z",
        "AutomatedSnapshotRetentionPeriod": 30,
        "ManualSnapshotRetentionPeriod": -1,
        "ClusterSecurityGroups": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sh-a1a123ab",
                "Status": "active"
            }
        ],
        "ClusterParameterGroups": [
            {
                "ParameterGroupName": "default.redshift-1.0",
                "ParameterApplyStatus": "in-sync"
            }
        ],
        "ClusterSubnetGroupName": "default",
        "VpcId": "vpc-a1abc1a1",
        "AvailabilityZone": "us-west-2a",
        "PreferredMaintenanceWindow": "sat:16:00-sat:16:30",
        "PendingModifiedValues": {},
        "ClusterVersion": "1.0",
        "AllowVersionUpgrade": true,
        "NumberOfNodes": 2,
        "PubliclyAccessible": false,
        "Encrypted": true,
        "Tags": [],
        "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/
bPxRfih3yCo8nvbEXAMPLEKEY",
        "EnhancedVpcRouting": false,
        "IamRoles": [
            {
                "IamRoleArn": "arn:aws:iam::123456789012:role/myRedshiftRole",
                "ApplyStatus": "in-sync"
            }
        ],
        "MaintenanceTrackName": "current",
```

```
        "DeferredMaintenanceWindows": [],
        "NextMaintenanceWindowStartTime": "2019-12-14T16:00:00Z"
    }
}
```

Para obtener más información, consulte Cifrado de la base de datos de Amazon Redshift en la Guía de administración de Amazon Redshift.

- Para obtener información sobre la API, consulte RotateEncryptionKey en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon Rekognition usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon Rekognition.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`compare-faces`

En el siguiente ejemplo de código, se muestra cómo utilizar `compare-faces`.

Para obtener información, consulte Comparación de rostros en imágenes.

AWS CLI

Comparación de rostros en dos imágenes

El siguiente comando `compare-faces` compara rostros en dos imágenes almacenadas en un bucket de Amazon S3.

```
aws rekognition compare-faces \
    --source-image '{"S3Object":{"Bucket":"MyImageS3Bucket","Name":"source.jpg"}}' \
    --target-image '{"S3Object":{"Bucket":"MyImageS3Bucket","Name":"target.jpg"}}'
```

Salida:

```
{
    "UnmatchedFaces": [],
    "FaceMatches": [
        {
            "Face": {
                "BoundingBox": {
                    "Width": 0.12368916720151901,
                    "Top": 0.16007372736930847,
                    "Left": 0.5901257991790771,
                    "Height": 0.25140416622161865
                },
                "Confidence": 100.0,
                "Pose": {
                    "Yaw": -3.7351467609405518,
                    "Roll": -0.10309021919965744,
                    "Pitch": 0.8637830018997192
                },
                "Quality": {
                    "Sharpness": 95.51618957519531,
                    "Brightness": 65.29893493652344
                },
                "Landmarks": [
                    {
                        "Y": 0.26721030473709106,
                        "X": 0.6204193830490112,
                        "Type": "eyeLeft"
                    },
                    {
                        "Y": 0.26831310987472534,
                        "X": 0.6776827573776245,
                        "Type": "eyeRight"
                    },
                    {
                        "Y": 0.3514654338359833,
                        "X": 0.6241428852081299,
                        "Type": "mouthLeft"
                    },
```

```
                    {
                        "Y": 0.35258132219314575,
                        "X": 0.6713621020317078,
                        "Type": "mouthRight"
                    },
                    {
                        "Y": 0.3140771687030792,
                        "X": 0.6428444981575012,
                        "Type": "nose"
                    }
                ]
            },
            "Similarity": 100.0
        }
    ],
    "SourceImageFace": {
        "BoundingBox": {
            "Width": 0.12368916720151901,
            "Top": 0.16007372736930847,
            "Left": 0.5901257991790771,
            "Height": 0.25140416622161865
        },
        "Confidence": 100.0
    }
}
```

Para obtener más información, consulte Comparación de rostros en imágenes en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte CompareFaces en la Referencia de comandos de la AWS CLI.

`create-collection`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-collection`.

Para obtener información, consulte Creación de una colección.

AWS CLI

Creación de una colección

El siguiente comando `create-collection` crea una colección con el nombre especificado.

```
aws rekognition create-collection \
    --collection-id "MyCollection"
```

Salida:

```
{
    "CollectionArn": "aws:rekognition:us-west-2:123456789012:collection/
MyCollection",
    "FaceModelVersion": "4.0",
    "StatusCode": 200
}
```

Para obtener más información, consulte Creación de una colección en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte CreateCollection en la Referencia de comandos de la AWS CLI.

`create-stream-processor`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-stream-processor`.

AWS CLI

Para crear un nuevo procesador de transmisión

En el siguiente ejemplo de `create-stream-processor`, se crea un nuevo procesador de transmisión con la configuración especificada.

```
aws rekognition create-stream-processor --name my-stream-processor\
    --input '{"KinesisVideoStream":{"Arn":"arn:aws:kinesisvideo:us-
west-2:123456789012:stream/macwebcam/1530559711205"}}'\
    --stream-processor-output '{"KinesisDataStream":{"Arn":"arn:aws:kinesis:us-
west-2:123456789012:stream/AmazonRekognitionRekStream"}}'\
    --role-arn arn:aws:iam::123456789012:role/AmazonRekognitionDetect\
    --settings '{"FaceSearch":
{"CollectionId":"MyCollection","FaceMatchThreshold":85.5}}'
```

Salida:

```
{
```

```
    "StreamProcessorArn": "arn:aws:rekognition:us-
west-2:123456789012:streamprocessor/my-stream-processor"
}
```

Para obtener más información, consulte Working with Streaming Videos en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte CreateStreamProcessor en la Referencia de comandos de la AWS CLI.

`delete-collection`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-collection`.

Para obtener información, consulte Eliminación de una colección.

AWS CLI

Eliminación de una colección

El siguiente comando `delete-collection` elimina la colección especificada.

```
aws rekognition delete-collection \
    --collection-id MyCollection
```

Salida:

```
{
    "StatusCode": 200
}
```

Para obtener más información, consulte Eliminación de una colección en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte DeleteCollection en la Referencia de comandos de la AWS CLI.

`delete-faces`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-faces`.

Para obtener información, consulte Eliminación de rostros de una colección.

AWS CLI

Eliminación de los rostros de una colección

El siguiente comando `delete-faces` elimina los rostros especificados de una colección.

```
aws rekognition delete-faces \
    --collection-id MyCollection
    --face-ids '["0040279c-0178-436e-b70a-e61b074e96b0"]'
```

Salida:

```
{
    "DeletedFaces": [
        "0040279c-0178-436e-b70a-e61b074e96b0"
    ]
}
```

Para obtener más información, consulte Eliminación de rostros de una colección en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener detalles sobre la API, consulte DeleteFaces en la Referencia de comandos de la AWS CLI.

`delete-stream-processor`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-stream-processor`.

AWS CLI

Para eliminar un procesador de transmisión

El siguiente comando `delete-stream-processor` elimina el procesador de transmisión especificado.

```
aws rekognition delete-stream-processor \
    --name my-stream-processor
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with Streaming Videos en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte DeleteStreamProcessor en la Referencia de comandos de la AWS CLI.

`describe-collection`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-collection`.

Para obtener información, consulte Descripción de una colección.

AWS CLI

Descripción de una colección

En el siguiente ejemplo de `describe-collection` se muestran los detalles de la colección especificada.

```
aws rekognition describe-collection \
    --collection-id MyCollection
```

Salida:

```
{
    "FaceCount": 200,
    "CreationTimestamp": 1569444828.274,
    "CollectionARN": "arn:aws:rekognition:us-west-2:123456789012:collection/
MyCollection",
    "FaceModelVersion": "4.0"
}
```

Para obtener más información, consulte Descripción de una colección en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte DescribeCollection en la Referencia de comandos de la AWS CLI.

`describe-stream-processor`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-stream-processor`.

AWS CLI

Para obtener información sobre un procesador de transmisión

El siguiente comando `describe-stream-processor` muestra detalles sobre el procesador de transmisión especificado.

```
aws rekognition describe-stream-processor \
    --name my-stream-processor
```

Salida:

```
{
    "Status": "STOPPED",
    "Name": "my-stream-processor",
    "LastUpdateTimestamp": 1532449292.712,
    "Settings": {
        "FaceSearch": {
            "FaceMatchThreshold": 80.0,
            "CollectionId": "my-collection"
        }
    },
    "RoleArn": "arn:aws:iam::123456789012:role/AmazonRekognitionDetectStream",
    "StreamProcessorArn": "arn:aws:rekognition:us-
west-2:123456789012:streamprocessor/my-stream-processpr",
    "Output": {
        "KinesisDataStream": {
            "Arn": "arn:aws:kinesis:us-west-2:123456789012:stream/
AmazonRekognitionRekStream"
        }
    },
    "Input": {
        "KinesisVideoStream": {
            "Arn": "arn:aws:kinesisvideo:us-west-2:123456789012:stream/
macwebcam/123456789012"
        }
    },
    "CreationTimestamp": 1532449292.712
}
```

Para obtener más información, consulte Working with Streaming Videos en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte DescribeStreamProcessor en la Referencia de comandos de la AWS CLI.

`detect-faces`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-faces`.

Para obtener información, consulte Detección de rostros en una imagen.

AWS CLI

Detección de rostros en una imagen

El siguiente comando `detect-faces` detecta rostros en la imagen especificada almacenada en un bucket de Amazon S3.

```
aws rekognition detect-faces \
    --image '{"S3Object":{"Bucket":"MyImageS3Bucket","Name":"MyFriend.jpg"}}' \
    --attributes "ALL"
```

Salida:

```
{
    "FaceDetails": [
        {
            "Confidence": 100.0,
            "Eyeglasses": {
                "Confidence": 98.91107940673828,
                "Value": false
            },
            "Sunglasses": {
                "Confidence": 99.7966537475586,
                "Value": false
            },
            "Gender": {
                "Confidence": 99.56611633300781,
                "Value": "Male"
            },
            "Landmarks": [
                {
                    "Y": 0.26721030473709106,
                    "X": 0.6204193830490112,
                    "Type": "eyeLeft"
```

```
                },
                {
                    "Y": 0.26831310987472534,
                    "X": 0.6776827573776245,
                    "Type": "eyeRight"
                },
                {
                    "Y": 0.3514654338359833,
                    "X": 0.6241428852081299,
                    "Type": "mouthLeft"
                },
                {
                    "Y": 0.35258132219314575,
                    "X": 0.6713621020317078,
                    "Type": "mouthRight"
                },
                {
                    "Y": 0.3140771687030792,
                    "X": 0.6428444981575012,
                    "Type": "nose"
                },
                {
                    "Y": 0.24662546813488007,
                    "X": 0.6001564860343933,
                    "Type": "leftEyeBrowLeft"
                },
                {
                    "Y": 0.24326619505882263,
                    "X": 0.6303644776344299,
                    "Type": "leftEyeBrowRight"
                },
                {
                    "Y": 0.23818562924861908,
                    "X": 0.6146903038024902,
                    "Type": "leftEyeBrowUp"
                },
                {
                    "Y": 0.24373626708984375,
                    "X": 0.6640064716339111,
                    "Type": "rightEyeBrowLeft"
                },
                {
                    "Y": 0.24877218902111053,
                    "X": 0.7025929093360901,
```

```
                    "Type": "rightEyeBrowRight"
                },
                {
                    "Y": 0.23938551545143127,
                    "X": 0.6823262572288513,
                    "Type": "rightEyeBrowUp"
                },
                {
                    "Y": 0.265746533870697,
                    "X": 0.6112898588180542,
                    "Type": "leftEyeLeft"
                },
                {
                    "Y": 0.2676128149032593,
                    "X": 0.6317071914672852,
                    "Type": "leftEyeRight"
                },
                {
                    "Y": 0.262735515832901,
                    "X": 0.6201658248901367,
                    "Type": "leftEyeUp"
                },
                {
                    "Y": 0.27025148272514343,
                    "X": 0.6206279993057251,
                    "Type": "leftEyeDown"
                },
                {
                    "Y": 0.268223375082016,
                    "X": 0.6658390760421753,
                    "Type": "rightEyeLeft"
                },
                {
                    "Y": 0.2672517001628876,
                    "X": 0.687832236289978,
                    "Type": "rightEyeRight"
                },
                {
                    "Y": 0.26383838057518005,
                    "X": 0.6769183874130249,
                    "Type": "rightEyeUp"
                },
                {
                    "Y": 0.27138751745224,
```

```
                    "X": 0.676596462726593,
                    "Type": "rightEyeDown"
                },
                {
                    "Y": 0.32283174991607666,
                    "X": 0.6350004076957703,
                    "Type": "noseLeft"
                },
                {
                    "Y": 0.3219289481639862,
                    "X": 0.6567046642303467,
                    "Type": "noseRight"
                },
                {
                    "Y": 0.3420318365097046,
                    "X": 0.6450609564781189,
                    "Type": "mouthUp"
                },
                {
                    "Y": 0.3664324879646301,
                    "X": 0.6455618143081665,
                    "Type": "mouthDown"
                },
                {
                    "Y": 0.26721030473709106,
                    "X": 0.6204193830490112,
                    "Type": "leftPupil"
                },
                {
                    "Y": 0.26831310987472534,
                    "X": 0.6776827573776245,
                    "Type": "rightPupil"
                },
                {
                    "Y": 0.26343393325805664,
                    "X": 0.5946047306060791,
                    "Type": "upperJawlineLeft"
                },
                {
                    "Y": 0.3543180525302887,
                    "X": 0.6044883728027344,
                    "Type": "midJawlineLeft"
                },
                {
```

```
                    "Y": 0.4084877669811249,
                    "X": 0.6477024555206299,
                    "Type": "chinBottom"
                },
                {
                    "Y": 0.3562754988670349,
                    "X": 0.707981526851654,
                    "Type": "midJawlineRight"
                },
                {
                    "Y": 0.26580461859703064,
                    "X": 0.7234612107276917,
                    "Type": "upperJawlineRight"
                }
            ],
            "Pose": {
                "Yaw": -3.7351467609405518,
                "Roll": -0.10309021919965744,
                "Pitch": 0.8637830018997192
            },
            "Emotions": [
                {
                    "Confidence": 8.74203109741211,
                    "Type": "SURPRISED"
                },
                {
                    "Confidence": 2.501944065093994,
                    "Type": "ANGRY"
                },
                {
                    "Confidence": 0.7378743290901184,
                    "Type": "DISGUSTED"
                },
                {
                    "Confidence": 3.5296201705932617,
                    "Type": "HAPPY"
                },
                {
                    "Confidence": 1.7162904739379883,
                    "Type": "SAD"
                },
                {
                    "Confidence": 9.518536567687988,
                    "Type": "CONFUSED"
```

```
            },
            {
                "Confidence": 0.45474427938461304,
                "Type": "FEAR"
            },
            {
                "Confidence": 72.79895782470703,
                "Type": "CALM"
            }
        ],
        "AgeRange": {
            "High": 48,
            "Low": 32
        },
        "EyesOpen": {
            "Confidence": 98.93987274169922,
            "Value": true
        },
        "BoundingBox": {
            "Width": 0.12368916720151901,
            "Top": 0.16007372736930847,
            "Left": 0.5901257991790771,
            "Height": 0.25140416622161865
        },
        "Smile": {
            "Confidence": 93.4493179321289,
            "Value": false
        },
        "MouthOpen": {
            "Confidence": 90.53053283691406,
            "Value": false
        },
        "Quality": {
            "Sharpness": 95.51618957519531,
            "Brightness": 65.29893493652344
        },
        "Mustache": {
            "Confidence": 89.85221099853516,
            "Value": false
        },
        "Beard": {
            "Confidence": 86.1991195678711,
            "Value": true
        }
```

```
        }
    ]
}
```

Para obtener más información, consulte Detección de rostros en una imagen en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte DetectFaces en la Referencia de comandos de la AWS CLI.

`detect-labels`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-labels`.

Para obtener información, consulte Detección de etiquetas en una imagen.

AWS CLI

Detección de una etiqueta en una imagen

En el siguiente ejemplo de `detect-labels` se detectan escenas y objetos en una imagen almacenada en un bucket de Amazon S3.

```
aws rekognition detect-labels \
    --image '{"S3Object":{"Bucket":"bucket","Name":"image"}}'
```

Salida:

```
{
    "Labels": [
        {
            "Instances": [],
            "Confidence": 99.15271759033203,
            "Parents": [
                {
                    "Name": "Vehicle"
                },
                {
                    "Name": "Transportation"
                }
            ],
            "Name": "Automobile"
        },
```

```
        {
            "Instances": [],
            "Confidence": 99.15271759033203,
            "Parents": [
                {
                    "Name": "Transportation"
                }
            ],
            "Name": "Vehicle"
        },
        {
            "Instances": [],
            "Confidence": 99.15271759033203,
            "Parents": [],
            "Name": "Transportation"
        },
        {
            "Instances": [
                {
                    "BoundingBox": {
                        "Width": 0.10616336017847061,
                        "Top": 0.5039216876029968,
                        "Left": 0.0037978808395564556,
                        "Height": 0.18528179824352264
                    },
                    "Confidence": 99.15271759033203
                },
                {
                    "BoundingBox": {
                        "Width": 0.2429988533258438,
                        "Top": 0.5251884460449219,
                        "Left": 0.7309805154800415,
                        "Height": 0.21577216684818268
                    },
                    "Confidence": 99.1286392211914
                },
                {
                    "BoundingBox": {
                        "Width": 0.14233611524105072,
                        "Top": 0.5333095788955688,
                        "Left": 0.6494812965393066,
                        "Height": 0.15528248250484467
                    },
                    "Confidence": 98.48368072509766
```

```
            },
            {
                "BoundingBox": {
                    "Width": 0.11086395382881165,
                    "Top": 0.5354844927787781,
                    "Left": 0.10355594009160995,
                    "Height": 0.10271988064050674
                },
                "Confidence": 96.45606231689453
            },
            {
                "BoundingBox": {
                    "Width": 0.06254628300666809,
                    "Top": 0.5573825240135193,
                    "Left": 0.46083059906959534,
                    "Height": 0.053911514580249786
                },
                "Confidence": 93.65448760986328
            },
            {
                "BoundingBox": {
                    "Width": 0.10105438530445099,
                    "Top": 0.534368634223938,
                    "Left": 0.5743985772132874,
                    "Height": 0.12226245552301407
                },
                "Confidence": 93.06217193603516
            },
            {
                "BoundingBox": {
                    "Width": 0.056389667093753815,
                    "Top": 0.5235804319381714,
                    "Left": 0.9427769780158997,
                    "Height": 0.17163699865341187
                },
                "Confidence": 92.6864013671875
            },
            {
                "BoundingBox": {
                    "Width": 0.06003860384225845,
                    "Top": 0.5441341400146484,
                    "Left": 0.22409997880458832,
                    "Height": 0.06737709045410156
                },
```

```
            "Confidence": 90.4227066040039
        },
        {
            "BoundingBox": {
                "Width": 0.02848697081208229,
                "Top": 0.5107086896896362,
                "Left": 0,
                "Height": 0.19150497019290924
            },
            "Confidence": 86.65286254882812
        },
        {
            "BoundingBox": {
                "Width": 0.04067881405353546,
                "Top": 0.5566273927688599,
                "Left": 0.316415935754776,
                "Height": 0.03428703173995018
            },
            "Confidence": 85.36471557617188
        },
        {
            "BoundingBox": {
                "Width": 0.043411049991846085,
                "Top": 0.5394920110702515,
                "Left": 0.18293385207653046,
                "Height": 0.0893595889210701
            },
            "Confidence": 82.21705627441406
        },
        {
            "BoundingBox": {
                "Width": 0.031183116137981415,
                "Top": 0.5579366683959961,
                "Left": 0.2853088080883026,
                "Height": 0.03989990055561066
            },
            "Confidence": 81.0157470703125
        },
        {
            "BoundingBox": {
                "Width": 0.031113790348172188,
                "Top": 0.5504819750785828,
                "Left": 0.2580395042896271,
                "Height": 0.056484755128622055
```

```
                },
                "Confidence": 56.13441467285156
            },
            {
                "BoundingBox": {
                    "Width": 0.08586374670267105,
                    "Top": 0.5438792705535889,
                    "Left": 0.5128012895584106,
                    "Height": 0.08550430089235306
                },
                "Confidence": 52.37760925292969
            }
        ],
        "Confidence": 99.15271759033203,
        "Parents": [
            {
                "Name": "Vehicle"
            },
            {
                "Name": "Transportation"
            }
        ],
        "Name": "Car"
    },
    {
        "Instances": [],
        "Confidence": 98.9914321899414,
        "Parents": [],
        "Name": "Human"
    },
    {
        "Instances": [
            {
                "BoundingBox": {
                    "Width": 0.19360728561878204,
                    "Top": 0.35072067379951477,
                    "Left": 0.43734854459762573,
                    "Height": 0.2742200493812561
                },
                "Confidence": 98.9914321899414
            },
            {
                "BoundingBox": {
                    "Width": 0.03801717236638069,
```

```
                    "Top": 0.5010883808135986,
                    "Left": 0.9155802130699158,
                    "Height": 0.06597328186035156
                },
                "Confidence": 85.02790832519531
            }
        ],
        "Confidence": 98.9914321899414,
        "Parents": [],
        "Name": "Person"
    },
    {
        "Instances": [],
        "Confidence": 93.24951934814453,
        "Parents": [],
        "Name": "Machine"
    },
    {
        "Instances": [
            {
                "BoundingBox": {
                    "Width": 0.03561960905790329,
                    "Top": 0.6468243598937988,
                    "Left": 0.7850857377052307,
                    "Height": 0.08878646790981293
                },
                "Confidence": 93.24951934814453
            },
            {
                "BoundingBox": {
                    "Width": 0.02217046171426773,
                    "Top": 0.6149078607559204,
                    "Left": 0.04757237061858177,
                    "Height": 0.07136218994855881
                },
                "Confidence": 91.5025863647461
            },
            {
                "BoundingBox": {
                    "Width": 0.016197510063648224,
                    "Top": 0.6274210214614868,
                    "Left": 0.6472989320755005,
                    "Height": 0.04955997318029404
                },
```

```
            "Confidence": 85.14686584472656
        },
        {
            "BoundingBox": {
                "Width": 0.020207518711686134,
                "Top": 0.6348286867141724,
                "Left": 0.7295016646385193,
                "Height": 0.07059963047504425
            },
            "Confidence": 83.34547424316406
        },
        {
            "BoundingBox": {
                "Width": 0.020280985161662102,
                "Top": 0.6171894669532776,
                "Left": 0.08744934946298599,
                "Height": 0.05297485366463661
            },
            "Confidence": 79.9981460571289
        },
        {
            "BoundingBox": {
                "Width": 0.018318990245461464,
                "Top": 0.623889148235321,
                "Left": 0.6836880445480347,
                "Height": 0.06730121374130249
            },
            "Confidence": 78.87144470214844
        },
        {
            "BoundingBox": {
                "Width": 0.021310249343514442,
                "Top": 0.6167286038398743,
                "Left": 0.004064912907779217,
                "Height": 0.08317798376083374
            },
            "Confidence": 75.89361572265625
        },
        {
            "BoundingBox": {
                "Width": 0.03604431077837944,
                "Top": 0.7030032277107239,
                "Left": 0.9254803657531738,
                "Height": 0.04569442570209503
```

```
                    },
                    "Confidence": 64.402587890625
                },
                {
                    "BoundingBox": {
                        "Width": 0.009834849275648594,
                        "Top": 0.5821820497512817,
                        "Left": 0.28094568848609924,
                        "Height": 0.01964157074689865
                    },
                    "Confidence": 62.79907989501953
                },
                {
                    "BoundingBox": {
                        "Width": 0.01475677452981472,
                        "Top": 0.6137543320655823,
                        "Left": 0.5950819253921509,
                        "Height": 0.039063986390829086
                    },
                    "Confidence": 59.40483474731445
                }
            ],
            "Confidence": 93.24951934814453,
            "Parents": [
                {
                    "Name": "Machine"
                }
            ],
            "Name": "Wheel"
        },
        {
            "Instances": [],
            "Confidence": 92.61514282226562,
            "Parents": [],
            "Name": "Road"
        },
        {
            "Instances": [],
            "Confidence": 92.37877655029297,
            "Parents": [
                {
                    "Name": "Person"
                }
            ],
```

```
            "Name": "Sport"
        },
        {
            "Instances": [],
            "Confidence": 92.37877655029297,
            "Parents": [
                {
                    "Name": "Person"
                }
            ],
            "Name": "Sports"
        },
        {
            "Instances": [
                {
                    "BoundingBox": {
                        "Width": 0.12326609343290329,
                        "Top": 0.6332163214683533,
                        "Left": 0.44815489649772644,
                        "Height": 0.058117982000112534
                    },
                    "Confidence": 92.37877655029297
                }
            ],
            "Confidence": 92.37877655029297,
            "Parents": [
                {
                    "Name": "Person"
                },
                {
                    "Name": "Sport"
                }
            ],
            "Name": "Skateboard"
        },
        {
            "Instances": [],
            "Confidence": 90.62931060791016,
            "Parents": [
                {
                    "Name": "Person"
                }
            ],
            "Name": "Pedestrian"
```

```
        },
        {
            "Instances": [],
            "Confidence": 88.81334686279297,
            "Parents": [],
            "Name": "Asphalt"
        },
        {
            "Instances": [],
            "Confidence": 88.81334686279297,
            "Parents": [],
            "Name": "Tarmac"
        },
        {
            "Instances": [],
            "Confidence": 88.23201751708984,
            "Parents": [],
            "Name": "Path"
        },
        {
            "Instances": [],
            "Confidence": 80.26520538330078,
            "Parents": [],
            "Name": "Urban"
        },
        {
            "Instances": [],
            "Confidence": 80.26520538330078,
            "Parents": [
                {
                    "Name": "Building"
                },
                {
                    "Name": "Urban"
                }
            ],
            "Name": "Town"
        },
        {
            "Instances": [],
            "Confidence": 80.26520538330078,
            "Parents": [],
            "Name": "Building"
        },
```

```
        {
            "Instances": [],
            "Confidence": 80.26520538330078,
            "Parents": [
                {
                    "Name": "Building"
                },
                {
                    "Name": "Urban"
                }
            ],
            "Name": "City"
        },
        {
            "Instances": [],
            "Confidence": 78.37934875488281,
            "Parents": [
                {
                    "Name": "Car"
                },
                {
                    "Name": "Vehicle"
                },
                {
                    "Name": "Transportation"
                }
            ],
            "Name": "Parking Lot"
        },
        {
            "Instances": [],
            "Confidence": 78.37934875488281,
            "Parents": [
                {
                    "Name": "Car"
                },
                {
                    "Name": "Vehicle"
                },
                {
                    "Name": "Transportation"
                }
            ],
            "Name": "Parking"
```

```
        },
        {
            "Instances": [],
            "Confidence": 74.37590026855469,
            "Parents": [
                {
                    "Name": "Building"
                },
                {
                    "Name": "Urban"
                },
                {
                    "Name": "City"
                }
            ],
            "Name": "Downtown"
        },
        {
            "Instances": [],
            "Confidence": 69.84622955322266,
            "Parents": [
                {
                    "Name": "Road"
                }
            ],
            "Name": "Intersection"
        },
        {
            "Instances": [],
            "Confidence": 57.68518829345703,
            "Parents": [
                {
                    "Name": "Sports Car"
                },
                {
                    "Name": "Car"
                },
                {
                    "Name": "Vehicle"
                },
                {
                    "Name": "Transportation"
                }
            ],
```

```
            "Name": "Coupe"
        },
        {
            "Instances": [],
            "Confidence": 57.68518829345703,
            "Parents": [
                {
                    "Name": "Car"
                },
                {
                    "Name": "Vehicle"
                },
                {
                    "Name": "Transportation"
                }
            ],
            "Name": "Sports Car"
        },
        {
            "Instances": [],
            "Confidence": 56.59492111206055,
            "Parents": [
                {
                    "Name": "Path"
                }
            ],
            "Name": "Sidewalk"
        },
        {
            "Instances": [],
            "Confidence": 56.59492111206055,
            "Parents": [
                {
                    "Name": "Path"
                }
            ],
            "Name": "Pavement"
        },
        {
            "Instances": [],
            "Confidence": 55.58770751953125,
            "Parents": [
                {
                    "Name": "Building"
```

```
                },
                {
                    "Name": "Urban"
                }
            ],
            "Name": "Neighborhood"
        }
    ],
    "LabelModelVersion": "2.0"
}
```

Para obtener más información, consulte Detección de etiquetas en una imagen en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte DetectLabels en la Referencia de comandos de la AWS CLI.

`detect-moderation-labels`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-moderation-labels`.

Para obtener información, consulte Detección de imágenes inapropiadas.

AWS CLI

Detección de contenido no seguro en una imagen

El siguiente comando `detect-moderation-labels` detecta contenido no seguro en la imagen especificada almacenada en un bucket de Amazon S3.

```
aws rekognition detect-moderation-labels \
    --image "S3Object={Bucket=MyImageS3Bucket,Name=gun.jpg}"
```

Salida:

```
{
    "ModerationModelVersion": "3.0",
    "ModerationLabels": [
        {
            "Confidence": 97.29618072509766,
            "ParentName": "Violence",
            "Name": "Weapon Violence"
        },
```

```
        {
            "Confidence": 97.29618072509766,
            "ParentName": "",
            "Name": "Violence"
        }
    ]
}
```

Para obtener más información, consulte Detección de imágenes no seguras en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte DetectModerationLabels en la Referencia de comandos de AWS CLI.

`detect-text`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-text`.

Para obtener información, consulte Detección de texto en una imagen.

AWS CLI

Detección de texto en una imagen

El siguiente comando `detect-text` detecta el texto de la imagen especificada.

```
aws rekognition detect-text \
    --image '{"S3Object":{"Bucket":"MyImageS3Bucket","Name":"ExamplePicture.jpg"}}'
```

Salida:

```
{
    "TextDetections": [
        {
            "Geometry": {
                "BoundingBox": {
                    "Width": 0.24624845385551453,
                    "Top": 0.28288066387176514,
                    "Left": 0.391388863325119,
                    "Height": 0.022687450051307678
                },
                "Polygon": [
                    {
```

```
                    "Y": 0.28288066387176514,
                    "X": 0.391388863325119
                },
                {
                    "Y": 0.2826388478279114,
                    "X": 0.6376373171806335
                },
                {
                    "Y": 0.30532628297805786,
                    "X": 0.637677013874054
                },
                {
                    "Y": 0.305568128824234,
                    "X": 0.39142853021621704
                }
            ]
        },
        "Confidence": 94.35709381103516,
        "DetectedText": "ESTD 1882",
        "Type": "LINE",
        "Id": 0
    },
    {
        "Geometry": {
            "BoundingBox": {
                "Width": 0.33933889865875244,
                "Top": 0.32603850960731506,
                "Left": 0.34534579515457153,
                "Height": 0.07126858830451965
            },
            "Polygon": [
                {
                    "Y": 0.32603850960731506,
                    "X": 0.34534579515457153
                },
                {
                    "Y": 0.32633158564567566,
                    "X": 0.684684693813324
                },
                {
                    "Y": 0.3976001739501953,
                    "X": 0.684575080871582
                },
                {
```

```
                    "Y": 0.3973070979118347,
                    "X": 0.345236212015152
                }
            ]
        },
        "Confidence": 99.95779418945312,
        "DetectedText": "BRAINS",
        "Type": "LINE",
        "Id": 1
    },
    {
        "Confidence": 97.22098541259766,
        "Geometry": {
            "BoundingBox": {
                "Width": 0.061079490929841995,
                "Top": 0.2843210697174072,
                "Left": 0.391391396522522,
                "Height": 0.021029088646173477
            },
            "Polygon": [
                {
                    "Y": 0.2843210697174072,
                    "X": 0.391391396522522
                },
                {
                    "Y": 0.2828207015991211,
                    "X": 0.4524524509906769
                },
                {
                    "Y": 0.3038259446620941,
                    "X": 0.4534534513950348
                },
                {
                    "Y": 0.30532634258270264,
                    "X": 0.3923923969268799
                }
            ]
        },
        "DetectedText": "ESTD",
        "ParentId": 0,
        "Type": "WORD",
        "Id": 2
    },
    {
```

```
            "Confidence": 91.49320983886719,
            "Geometry": {
                "BoundingBox": {
                    "Width": 0.07007007300853729,
                    "Top": 0.2828207015991211,
                    "Left": 0.5675675868988037,
                    "Height": 0.02250562608242035
                },
                "Polygon": [
                    {
                        "Y": 0.2828207015991211,
                        "X": 0.5675675868988037
                    },
                    {
                        "Y": 0.2828207015991211,
                        "X": 0.6376376152038574
                    },
                    {
                        "Y": 0.30532634258270264,
                        "X": 0.6376376152038574
                    },
                    {
                        "Y": 0.30532634258270264,
                        "X": 0.5675675868988037
                    }
                ]
            },
            "DetectedText": "1882",
            "ParentId": 0,
            "Type": "WORD",
            "Id": 3
        },
        {
            "Confidence": 99.95779418945312,
            "Geometry": {
                "BoundingBox": {
                    "Width": 0.33933934569358826,
                    "Top": 0.32633158564567566,
                    "Left": 0.3453453481197357,
                    "Height": 0.07127484679222107
                },
                "Polygon": [
                    {
                        "Y": 0.32633158564567566,
```

```
                        "X": 0.3453453481197357
                    },
                    {
                        "Y": 0.32633158564567566,
                        "X": 0.684684693813324
                    },
                    {
                        "Y": 0.39759939908981323,
                        "X": 0.6836836934089661
                    },
                    {
                        "Y": 0.39684921503067017,
                        "X": 0.3453453481197357
                    }
                ]
            },
            "DetectedText": "BRAINS",
            "ParentId": 1,
            "Type": "WORD",
            "Id": 4
        }
    ]
}
```

- Para obtener información sobre la API, consulte DetectText en la Referencia de comandos de la AWS CLI.

`get-celebrity-info`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-celebrity-info`.

AWS CLI

Obtención de información sobre un famoso

El siguiente comando `get-celebrity-info` muestra información sobre el famoso especificado. El parámetro `id` procede de una llamada anterior a `recognize-celebrities`.

```
aws rekognition get-celebrity-info --id nnnnnnn
```

Salida:

```
{
    "Name": "Celeb A",
    "Urls": [
        "www.imdb.com/name/aaaaaaaaa"
    ]
}
```

Para obtener más información, consulte Obtención de información sobre un famoso en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte GetCelebrityInfo en la Referencia de comandos de la AWS CLI.

`get-celebrity-recognition`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-celebrity-recognition`.

AWS CLI

Para obtener los resultados de una operación de reconocimiento de celebridades

El siguiente comando `get-celebrity-recognition` muestra los resultados de una operación de reconocimiento de celebridades que ha iniciado previamente llamando a `start-celebrity-recognition`.

```
aws rekognition get-celebrity-recognition  \
    --job-id 1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef
```

Salida:

```
{
    "NextToken": "3D01ClxlCiT31VsRDkAO3IybLb/h5AtDWSGuhYi
+N1FIJwwPtAkuKzDhL2rV3GcwmNt77+12",
    "Celebrities": [
        {
            "Timestamp": 0,
            "Celebrity": {
                "Confidence": 96.0,
                "Face": {
                    "BoundingBox": {
                        "Width": 0.70333331823349,
                        "Top": 0.16750000417232513,
```

```
                    "Left": 0.19555555284023285,
                    "Height": 0.3956249952316284
                },
                "Landmarks": [
                    {
                        "Y": 0.31031012535095215,
                        "X": 0.441436767578125,
                        "Type": "eyeLeft"
                    },
                    {
                        "Y": 0.3081788718700409,
                        "X": 0.6437258720397949,
                        "Type": "eyeRight"
                    },
                    {
                        "Y": 0.39542075991630554,
                        "X": 0.5572493076324463,
                        "Type": "nose"
                    },
                    {
                        "Y": 0.4597957134246826,
                        "X": 0.4579732120037079,
                        "Type": "mouthLeft"
                    },
                    {
                        "Y": 0.45688048005104065,
                        "X": 0.6349081993103027,
                        "Type": "mouthRight"
                    }
                ],
                "Pose": {
                    "Yaw": 8.943398475646973,
                    "Roll": -2.0309247970581055,
                    "Pitch": -0.5674862861633301
                },
                "Quality": {
                    "Sharpness": 99.40211486816406,
                    "Brightness": 89.47132110595703
                },
                "Confidence": 99.99861145019531
            },
            "Name": "CelebrityA",
            "Urls": [
                "www.imdb.com/name/111111111"
```

```
                ],
                "Id": "nnnnnn"
            }
        },
        {
            "Timestamp": 467,
            "Celebrity": {
                "Confidence": 99.0,
                "Face": {
                    "BoundingBox": {
                        "Width": 0.6877777576446533,
                        "Top": 0.18437500298023224,
                        "Left": 0.20555555820465088,
                        "Height": 0.3868750035762787
                    },
                    "Landmarks": [
                        {
                            "Y": 0.31895750761032104,
                            "X": 0.4411413371562958,
                            "Type": "eyeLeft"
                        },
                        {
                            "Y": 0.3140959143638611,
                            "X": 0.6523157954216003,
                            "Type": "eyeRight"
                        },
                        {
                            "Y": 0.4016456604003906,
                            "X": 0.5682755708694458,
                            "Type": "nose"
                        },
                        {
                            "Y": 0.46894142031669617,
                            "X": 0.4597797095775604,
                            "Type": "mouthLeft"
                        },
                        {
                            "Y": 0.46971091628074646,
                            "X": 0.6286435127258301,
                            "Type": "mouthRight"
                        }
                    ],
                    "Pose": {
                        "Yaw": 10.433465957641602,
```

```
                        "Roll": -3.347442388534546,
                        "Pitch": 1.3709543943405151
                    },
                    "Quality": {
                        "Sharpness": 99.5531005859375,
                        "Brightness": 88.5764389038086
                    },
                    "Confidence": 99.99148559570312
                },
                "Name": "Jane Celebrity",
                "Urls": [
                    "www.imdb.com/name/111111111"
                ],
                "Id": "nnnnnn"
            }
        }
    ],
    "JobStatus": "SUCCEEDED",
    "VideoMetadata": {
        "Format": "QuickTime / MOV",
        "FrameRate": 29.978118896484375,
        "Codec": "h264",
        "DurationMillis": 4570,
        "FrameHeight": 1920,
        "FrameWidth": 1080
    }
}
```

Para obtener más información, consulte Recognizing Celebrities in a Stored Video en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte GetCelebrityRecognition en la Referencia de comandos de la AWS CLI.

`get-content-moderation`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-content-moderation`.

AWS CLI

Para obtener los resultados de una operación de contenido no seguro

El siguiente comando `get-content-moderation` muestra los resultados de una operación de contenido no seguro que ha iniciado previamente llamando a `start-content-moderation`.

```
aws rekognition get-content-moderation \
    --job-id 1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef
```

Salida:

```
{
    "NextToken": "dlhcKMHMzpCBGFukz6IO3JMcWiJAamCVhXHt3r6b4b5Tfbyw3q7o+Jeezt
+ZpgfOnW9FCCgQ",
    "ModerationLabels": [
        {
            "Timestamp": 0,
            "ModerationLabel": {
                "Confidence": 97.39583587646484,
                "ParentName": "",
                "Name": "Violence"
            }
        },
        {
            "Timestamp": 0,
            "ModerationLabel": {
                "Confidence": 97.39583587646484,
                "ParentName": "Violence",
                "Name": "Weapon Violence"
            }
        }
    ],
    "JobStatus": "SUCCEEDED",
    "VideoMetadata": {
        "Format": "QuickTime / MOV",
        "FrameRate": 29.97515869140625,
        "Codec": "h264",
        "DurationMillis": 6039,
        "FrameHeight": 1920,
        "FrameWidth": 1080
    }
}
```

Para obtener más información, consulte Detecting Unsafe Stored Videos en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte GetContentModeration en la Referencia de comandos de la AWS CLI.

`get-face-detection`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-face-detection`.

AWS CLI

Para obtener los resultados de una operación de detección facial

El siguiente comando `get-face-detection` muestra los resultados de una operación de detección facial que ha iniciado previamente llamando a `start-face-detection`.

```
aws rekognition get-face-detection \
    --job-id 1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef
```

Salida:

```
{
    "Faces": [
        {
            "Timestamp": 467,
            "Face": {
                "BoundingBox": {
                    "Width": 0.1560753583908081,
                    "Top": 0.13555361330509186,
                    "Left": -0.0952017530798912,
                    "Height": 0.6934483051300049
                },
                "Landmarks": [
                    {
                        "Y": 0.4013825058937073,
                        "X": -0.041750285774469376,
                        "Type": "eyeLeft"
                    },
                    {
                        "Y": 0.41695496439933777,
                        "X": 0.027979329228401184,
                        "Type": "eyeRight"
                    },
                    {
```

```
                    "Y": 0.6375303268432617,
                    "X": -0.04034662991762161,
                    "Type": "mouthLeft"
                },
                {
                    "Y": 0.6497718691825867,
                    "X": 0.013960429467260838,
                    "Type": "mouthRight"
                },
                {
                    "Y": 0.5238034129142761,
                    "X": 0.008022055961191654,
                    "Type": "nose"
                }
            ],
            "Pose": {
                "Yaw": -58.07863998413086,
                "Roll": 1.9384294748306274,
                "Pitch": -24.66305160522461
            },
            "Quality": {
                "Sharpness": 83.14741516113281,
                "Brightness": 25.75942611694336
            },
            "Confidence": 87.7622299194336
        }
    },
    {
        "Timestamp": 967,
        "Face": {
            "BoundingBox": {
                "Width": 0.28559377789497375,
                "Top": 0.19436298310756683,
                "Left": 0.024553587660193443,
                "Height": 0.7216082215309143
            },
            "Landmarks": [
                {
                    "Y": 0.4650231599807739,
                    "X": 0.16269078850746155,
                    "Type": "eyeLeft"
                },
                {
                    "Y": 0.4843238294124603,
```

```
                        "X": 0.2782580852508545,
                        "Type": "eyeRight"
                    },
                    {
                        "Y": 0.71530681848526,
                        "X": 0.1741468608379364,
                        "Type": "mouthLeft"
                    },
                    {
                        "Y": 0.7310671210289001,
                        "X": 0.26857468485832214,
                        "Type": "mouthRight"
                    },
                    {
                        "Y": 0.582602322101593,
                        "X": 0.2566150426864624,
                        "Type": "nose"
                    }
                ],
                "Pose": {
                    "Yaw": 11.487052917480469,
                    "Roll": 5.074230670928955,
                    "Pitch": 15.396159172058105
                },
                "Quality": {
                    "Sharpness": 73.32209777832031,
                    "Brightness": 54.96497344970703
                },
                "Confidence": 99.99998474121094
            }
        }
    ],
    "NextToken":
"OzL223pDKy9116O/02KXRqFIEAwxjy4PkgYcm3hSo0rdysbXg5Ex0eFgTGEj0ADEac6S037U",
    "JobStatus": "SUCCEEDED",
    "VideoMetadata": {
        "Format": "QuickTime / MOV",
        "FrameRate": 29.970617294311523,
        "Codec": "h264",
        "DurationMillis": 6806,
        "FrameHeight": 1080,
        "FrameWidth": 1920
    }
```

```
}
```

Para obtener más información, consulte Detecting Faces in a Stored Video en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte GetFaceDetection en la Referencia de comandos de la AWS CLI.

`get-face-search`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-face-search`.

AWS CLI

Para obtener los resultados de una operación de búsqueda facial

El siguiente comando `get-face-search` muestra los resultados de una operación de búsqueda facial que haya iniciado previamente llamando a `start-face-search`.

```
aws rekognition get-face-search  \
    --job-id 1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef
```

Salida:

```
{
    "Persons": [
        {
            "Timestamp": 467,
            "FaceMatches": [],
            "Person": {
                "Index": 0,
                "Face": {
                    "BoundingBox": {
                        "Width": 0.1560753583908081,
                        "Top": 0.13555361330509186,
                        "Left": -0.0952017530798912,
                        "Height": 0.6934483051300049
                    },
                    "Landmarks": [
                        {
                            "Y": 0.4013825058937073,
                            "X": -0.041750285774469376,
                            "Type": "eyeLeft"
```

```
                    },
                    {
                        "Y": 0.41695496439933777,
                        "X": 0.027979329228401184,
                        "Type": "eyeRight"
                    },
                    {
                        "Y": 0.6375303268432617,
                        "X": -0.04034662991762161,
                        "Type": "mouthLeft"
                    },
                    {
                        "Y": 0.6497718691825867,
                        "X": 0.013960429467260838,
                        "Type": "mouthRight"
                    },
                    {
                        "Y": 0.5238034129142761,
                        "X": 0.008022055961191654,
                        "Type": "nose"
                    }
                ],
                "Pose": {
                    "Yaw": -58.07863998413086,
                    "Roll": 1.9384294748306274,
                    "Pitch": -24.66305160522461
                },
                "Quality": {
                    "Sharpness": 83.14741516113281,
                    "Brightness": 25.75942611694336
                },
                "Confidence": 87.7622299194336
            }
        }
    },
    {
        "Timestamp": 967,
        "FaceMatches": [
            {
                "Face": {
                    "BoundingBox": {
                        "Width": 0.12368900328874588,
                        "Top": 0.16007399559020996,
                        "Left": 0.5901259779930115,
```

```
                        "Height": 0.2514039874076843
                    },
                    "FaceId": "056a95fa-2060-4159-9cab-7ed4daa030fa",
                    "ExternalImageId": "image3.jpg",
                    "Confidence": 100.0,
                    "ImageId": "08f8a078-8929-37fd-8e8f-aadf690e8232"
                },
                "Similarity": 98.44476318359375
            }
        ],
        "Person": {
            "Index": 1,
            "Face": {
                "BoundingBox": {
                    "Width": 0.28559377789497375,
                    "Top": 0.19436298310756683,
                    "Left": 0.024553587660193443,
                    "Height": 0.7216082215309143
                },
                "Landmarks": [
                    {
                        "Y": 0.4650231599807739,
                        "X": 0.16269078850746155,
                        "Type": "eyeLeft"
                    },
                    {
                        "Y": 0.4843238294124603,
                        "X": 0.2782580852508545,
                        "Type": "eyeRight"
                    },
                    {
                        "Y": 0.71530681848526,
                        "X": 0.1741468608379364,
                        "Type": "mouthLeft"
                    },
                    {
                        "Y": 0.7310671210289001,
                        "X": 0.26857468485832214,
                        "Type": "mouthRight"
                    },
                    {
                        "Y": 0.582602322101593,
                        "X": 0.2566150426864624,
                        "Type": "nose"
```

```
                        }
                    ],
                    "Pose": {
                        "Yaw": 11.487052917480469,
                        "Roll": 5.074230670928955,
                        "Pitch": 15.396159172058105
                    },
                    "Quality": {
                        "Sharpness": 73.32209777832031,
                        "Brightness": 54.96497344970703
                    },
                    "Confidence": 99.99998474121094
                }
            }
        }
    ],
    "NextToken": "5bkgcezyuaqhtWk3C8OTW6cjRghrwV9XDMivm5B3MXm+Lv6G+L+GejyFHPhoNa/
ldXIC4c/d",
    "JobStatus": "SUCCEEDED",
    "VideoMetadata": {
        "Format": "QuickTime / MOV",
        "FrameRate": 29.970617294311523,
        "Codec": "h264",
        "DurationMillis": 6806,
        "FrameHeight": 1080,
        "FrameWidth": 1920
    }
}
```


Para obtener más información, consulte Searching Stored Videos for Faces en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte GetFaceSearch en la Referencia de comandos de la AWS CLI.

`get-label-detection`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-label-detection`.

AWS CLI

Para obtener los resultados de una operación de detección de objetos y escenas

El siguiente comando `get-label-detection` muestra los resultados de una operación de detección de objetos y escenas que haya iniciado previamente llamando a `start-label-detection`.

```
aws rekognition get-label-detection  \
    --job-id 1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef
```

Salida:

```
{
    "Labels": [
        {
            "Timestamp": 0,
            "Label": {
                "Instances": [],
                "Confidence": 50.19071578979492,
                "Parents": [
                    {
                        "Name": "Person"
                    },
                    {
                        "Name": "Crowd"
                    }
                ],
                "Name": "Audience"
            }
        },
        {
            "Timestamp": 0,
            "Label": {
                "Instances": [],
                "Confidence": 55.74115753173828,
                "Parents": [
                    {
                        "Name": "Room"
                    },
                    {
                        "Name": "Indoors"
                    },
                    {
                        "Name": "School"
                    }
                ],
```

```
                "Name": "Classroom"
            }
        }
    ],
    "JobStatus": "SUCCEEDED",
    "LabelModelVersion": "2.0",
    "VideoMetadata": {
        "Format": "QuickTime / MOV",
        "FrameRate": 29.970617294311523,
        "Codec": "h264",
        "DurationMillis": 6806,
        "FrameHeight": 1080,
        "FrameWidth": 1920
    },
    "NextToken": "BMugzAi4L72IERzQdbpyMQuEFBsjlo5W0Yx3mfG+sR9mm98E1/
CpObenspRfs/5FBQFs4X7G"
}
```

Para obtener más información, consulte Detecting Labels in a Video en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte GetLabelDetection en la Referencia de comandos de la AWS CLI.

`get-person-tracking`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-person-tracking`.

AWS CLI

Para obtener los resultados de una operación de recorridos de las personas

El siguiente comando `get-person-tracking` muestra los resultados de una operación de recorridos de personas que haya iniciado previamente llamando a `start-person-tracking`.

```
aws rekognition get-person-tracking  \
    --job-id 1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef
```

Salida:

```
{
```

```
    "Persons": [
        {
            "Timestamp": 500,
            "Person": {
                "BoundingBox": {
                    "Width": 0.4151041805744171,
                    "Top": 0.07870370149612427,
                    "Left": 0.0,
                    "Height": 0.9212962985038757
                },
                "Index": 0
            }
        },
        {
            "Timestamp": 567,
            "Person": {
                "BoundingBox": {
                    "Width": 0.4755208194255829,
                    "Top": 0.07777778059244156,
                    "Left": 0.0,
                    "Height": 0.9194444417953491
                },
                "Index": 0
            }
        }
    ],
    "NextToken": "D/vRIYNyhG79ugdta3f+8cRg9oSRo
+HigGOuxRiYpTn0ExnqTi1CJektVAc4HrAXDv25eHYk",
    "JobStatus": "SUCCEEDED",
    "VideoMetadata": {
        "Format": "QuickTime / MOV",
        "FrameRate": 29.970617294311523,
        "Codec": "h264",
        "DurationMillis": 6806,
        "FrameHeight": 1080,
        "FrameWidth": 1920
    }
}
```


Para obtener más información, consulte People Pathing en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte GetPersonTracking en la Referencia de comandos de la AWS CLI.

`index-faces`

En el siguiente ejemplo de código, se muestra cómo utilizar `index-faces`.

Para obtener información, consulte Adición de rostros a una colección.

AWS CLI

Adición de rostros a una colección

El siguiente comando `index-faces` añade los rostros que se encuentran en una imagen a la colección especificada.

```
aws rekognition index-faces \
    --image '{"S3Object":{"Bucket":"MyVideoS3Bucket","Name":"MyPicture.jpg"}}' \
    --collection-id MyCollection \
    --max-faces 1 \
    --quality-filter "AUTO" \
    --detection-attributes "ALL" \
    --external-image-id "MyPicture.jpg"
```

Salida:

```
{
    "FaceRecords": [
        {
            "FaceDetail": {
                "Confidence": 99.993408203125,
                "Eyeglasses": {
                    "Confidence": 99.11750030517578,
                    "Value": false
                },
                "Sunglasses": {
                    "Confidence": 99.98249053955078,
                    "Value": false
                },
                "Gender": {
                    "Confidence": 99.92769622802734,
                    "Value": "Male"
                },
                "Landmarks": [
                    {
                        "Y": 0.26750367879867554,
                        "X": 0.6202793717384338,
```

```
                    "Type": "eyeLeft"
                },
                {
                    "Y": 0.26642778515815735,
                    "X": 0.6787431836128235,
                    "Type": "eyeRight"
                },
                {
                    "Y": 0.31361380219459534,
                    "X": 0.6421601176261902,
                    "Type": "nose"
                },
                {
                    "Y": 0.3495299220085144,
                    "X": 0.6216195225715637,
                    "Type": "mouthLeft"
                },
                {
                    "Y": 0.35194727778434753,
                    "X": 0.669899046421051,
                    "Type": "mouthRight"
                },
                {
                    "Y": 0.26844894886016846,
                    "X": 0.6210268139839172,
                    "Type": "leftPupil"
                },
                {
                    "Y": 0.26707562804222107,
                    "X": 0.6817160844802856,
                    "Type": "rightPupil"
                },
                {
                    "Y": 0.24834522604942322,
                    "X": 0.6018546223640442,
                    "Type": "leftEyeBrowLeft"
                },
                {
                    "Y": 0.24397172033786774,
                    "X": 0.6172008514404297,
                    "Type": "leftEyeBrowUp"
                },
                {
                    "Y": 0.24677404761314392,
```

```
                    "X": 0.6339119076728821,
                    "Type": "leftEyeBrowRight"
                },
                {
                    "Y": 0.24582654237747192,
                    "X": 0.6619398593902588,
                    "Type": "rightEyeBrowLeft"
                },
                {
                    "Y": 0.23973053693771362,
                    "X": 0.6804757118225098,
                    "Type": "rightEyeBrowUp"
                },
                {
                    "Y": 0.24441994726657867,
                    "X": 0.6978968977928162,
                    "Type": "rightEyeBrowRight"
                },
                {
                    "Y": 0.2695908546447754,
                    "X": 0.6085202693939209,
                    "Type": "leftEyeLeft"
                },
                {
                    "Y": 0.26716896891593933,
                    "X": 0.6315826177597046,
                    "Type": "leftEyeRight"
                },
                {
                    "Y": 0.26289820671081543,
                    "X": 0.6202316880226135,
                    "Type": "leftEyeUp"
                },
                {
                    "Y": 0.27123287320137024,
                    "X": 0.6205548048019409,
                    "Type": "leftEyeDown"
                },
                {
                    "Y": 0.2668408751487732,
                    "X": 0.6663622260093689,
                    "Type": "rightEyeLeft"
                },
                {
```

```
                        "Y": 0.26741549372673035,
                        "X": 0.6910083889961243,
                        "Type": "rightEyeRight"
                    },
                    {
                        "Y": 0.2614026665687561,
                        "X": 0.6785826086997986,
                        "Type": "rightEyeUp"
                    },
                    {
                        "Y": 0.27075251936912537,
                        "X": 0.6789616942405701,
                        "Type": "rightEyeDown"
                    },
                    {
                        "Y": 0.3211299479007721,
                        "X": 0.6324167847633362,
                        "Type": "noseLeft"
                    },
                    {
                        "Y": 0.32276326417922974,
                        "X": 0.6558475494384766,
                        "Type": "noseRight"
                    },
                    {
                        "Y": 0.34385165572166443,
                        "X": 0.6444970965385437,
                        "Type": "mouthUp"
                    },
                    {
                        "Y": 0.3671635091304779,
                        "X": 0.6459195017814636,
                        "Type": "mouthDown"
                    }
                ],
                "Pose": {
                    "Yaw": -9.54541015625,
                    "Roll": -0.5709401965141296,
                    "Pitch": 0.6045494675636292
                },
                "Emotions": [
                    {
                        "Confidence": 39.90074157714844,
                        "Type": "HAPPY"
```

```
            },
            {
                "Confidence": 23.38753890991211,
                "Type": "CALM"
            },
            {
                "Confidence": 5.840933322906494,
                "Type": "CONFUSED"
            }
        ],
        "AgeRange": {
            "High": 63,
            "Low": 45
        },
        "EyesOpen": {
            "Confidence": 99.80887603759766,
            "Value": true
        },
        "BoundingBox": {
            "Width": 0.18562500178813934,
            "Top": 0.1618015021085739,
            "Left": 0.5575000047683716,
            "Height": 0.24770642817020416
        },
        "Smile": {
            "Confidence": 99.69740295410156,
            "Value": false
        },
        "MouthOpen": {
            "Confidence": 99.97393798828125,
            "Value": false
        },
        "Quality": {
            "Sharpness": 95.54405975341797,
            "Brightness": 63.867706298828125
        },
        "Mustache": {
            "Confidence": 97.05007934570312,
            "Value": false
        },
        "Beard": {
            "Confidence": 87.34505462646484,
            "Value": false
        }
```

```
            },
            "Face": {
                "BoundingBox": {
                    "Width": 0.18562500178813934,
                    "Top": 0.1618015021085739,
                    "Left": 0.5575000047683716,
                    "Height": 0.24770642817020416
                },
                "FaceId": "ce7ed422-2132-4a11-ab14-06c5c410f29f",
                "ExternalImageId": "example-image.jpg",
                "Confidence": 99.993408203125,
                "ImageId": "8d67061e-90d2-598f-9fbd-29c8497039c0"
            }
        }
    ],
    "UnindexedFaces": [],
    "FaceModelVersion": "3.0",
    "OrientationCorrection": "ROTATE_0"
}
```

Para obtener más información, consulte Agregar rostros a una colección en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte IndexFaces en la Referencia de comandos de la AWS CLI.

`list-collections`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-collections`.

Para obtener información, consulte Enumerar colecciones.

AWS CLI

Creación de una lista de las colecciones disponibles

El siguiente comando `list-collections` muestra las colecciones disponibles en la cuenta de AWS.

```
aws rekognition list-collections
```

Salida:

```
{
    "FaceModelVersions": [
        "2.0",
        "3.0",
        "3.0",
        "3.0",
        "4.0",
        "1.0",
        "3.0",
        "4.0",
        "4.0",
        "4.0"
    ],
    "CollectionIds": [
        "MyCollection1",
        "MyCollection2",
        "MyCollection3",
        "MyCollection4",
        "MyCollection5",
        "MyCollection6",
        "MyCollection7",
        "MyCollection8",
        "MyCollection9",
        "MyCollection10"
    ]
}
```

Para obtener más información, consulte Listado de colecciones en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte ListCollections en la Referencia de comandos de la AWS CLI.

`list-faces`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-faces`.

Para obtener información, consulte Enumerar rostros en una colección.

AWS CLI

Creación de una lista de rostros en una colección

El siguiente comando `list-faces` muestra los rostros de la colección especificada.

```
aws rekognition list-faces \
    --collection-id MyCollection
```

Salida:

```
{
    "FaceModelVersion": "3.0",
    "Faces": [
        {
            "BoundingBox": {
                "Width": 0.5216310024261475,
                "Top": 0.3256250023841858,
                "Left": 0.13394300639629364,
                "Height": 0.3918749988079071
            },
            "FaceId": "0040279c-0178-436e-b70a-e61b074e96b0",
            "ExternalImageId": "image1.jpg",
            "Confidence": 100.0,
            "ImageId": "f976e487-3719-5e2d-be8b-ea2724c26991"
        },
        {
            "BoundingBox": {
                "Width": 0.5074880123138428,
                "Top": 0.3774999976158142,
                "Left": 0.18302799761295319,
                "Height": 0.3812499940395355
            },
            "FaceId": "086261e8-6deb-4bc0-ac73-ab22323cc38d",
            "ExternalImageId": "image2.jpg",
            "Confidence": 99.99930572509766,
            "ImageId": "ae1593b0-a8f6-5e24-a306-abf529e276fa"
        },
        {
            "BoundingBox": {
                "Width": 0.5574039816856384,
                "Top": 0.37187498807907104,
                "Left": 0.14559100568294525,
                "Height": 0.4181250035762787
            },
            "FaceId": "11c4bd3c-19c5-4eb8-aecc-24feb93a26e1",
            "ExternalImageId": "image3.jpg",
```

```
            "Confidence": 99.99960327148438,
            "ImageId": "80739b4d-883f-5b78-97cf-5124038e26b9"
        },
        {
            "BoundingBox": {
                "Width": 0.18562500178813934,
                "Top": 0.1618019938468933,
                "Left": 0.5575000047683716,
                "Height": 0.24770599603652954
            },
            "FaceId": "13692fe4-990a-4679-b14a-5ac23d135eab",
            "ExternalImageId": "image4.jpg",
            "Confidence": 99.99340057373047,
            "ImageId": "8df18239-9ad1-5acd-a46a-6581ff98f51b"
        },
        {
            "BoundingBox": {
                "Width": 0.5307819843292236,
                "Top": 0.2862499952316284,
                "Left": 0.1564060002565384,
                "Height": 0.3987500071525574
            },
            "FaceId": "2eb5f3fd-e2a9-4b1c-a89f-afa0a518fe06",
            "ExternalImageId": "image5.jpg",
            "Confidence": 99.99970245361328,
            "ImageId": "3c314792-197d-528d-bbb6-798ed012c150"
        },
        {
            "BoundingBox": {
                "Width": 0.5773710012435913,
                "Top": 0.34437501430511475,
                "Left": 0.12396000325679779,
                "Height": 0.4337500035762787
            },
            "FaceId": "57189455-42b0-4839-a86c-abda48b13174",
            "ExternalImageId": "image6.jpg",
            "Confidence": 100.0,
            "ImageId": "0aff2f37-e7a2-5dbc-a3a3-4ef6ec18eaa0"
        },
        {
            "BoundingBox": {
                "Width": 0.5349419713020325,
                "Top": 0.29124999046325684,
                "Left": 0.16389399766921997,
```

```
                "Height": 0.40187498927116394
            },
            "FaceId": "745f7509-b1fa-44e0-8b95-367b1359638a",
            "ExternalImageId": "image7.jpg",
            "Confidence": 99.99979400634766,
            "ImageId": "67a34327-48d1-5179-b042-01e52ccfeada"
        },
        {
            "BoundingBox": {
                "Width": 0.41499999165534973,
                "Top": 0.09187500178813934,
                "Left": 0.28083300590515137,
                "Height": 0.3112500011920929
            },
            "FaceId": "8d3cfc70-4ba8-4b36-9644-90fba29c2dac",
            "ExternalImageId": "image8.jpg",
            "Confidence": 99.99769592285156,
            "ImageId": "a294da46-2cb1-5cc4-9045-61d7ca567662"
        },
        {
            "BoundingBox": {
                "Width": 0.48166701197624207,
                "Top": 0.20999999344348907,
                "Left": 0.21250000596046448,
                "Height": 0.36125001311302185
            },
            "FaceId": "bd4ceb4d-9acc-4ab7-8ef8-1c2d2ba0a66a",
            "ExternalImageId": "image9.jpg",
            "Confidence": 99.99949645996094,
            "ImageId": "5e1a7588-e5a0-5ee3-bd00-c642518dfe3a"
        },
        {
            "BoundingBox": {
                "Width": 0.18562500178813934,
                "Top": 0.1618019938468933,
                "Left": 0.5575000047683716,
                "Height": 0.24770599603652954
            },
            "FaceId": "ce7ed422-2132-4a11-ab14-06c5c410f29f",
            "ExternalImageId": "image10.jpg",
            "Confidence": 99.99340057373047,
            "ImageId": "8d67061e-90d2-598f-9fbd-29c8497039c0"
        }
    ]
```

```
}
```

Para obtener más información, consulte Listado de rostros en una colección en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte ListFaces en la Referencia de comandos de la AWS CLI.

`list-stream-processors`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-stream-processors`.

AWS CLI

Para enumerar los procesadores de transmisión de su cuenta

El siguiente comando de `list-stream-processors` muestra los procesadores de transmisión de su cuenta y el estado de cada uno de ellos.

```
aws rekognition list-stream-processors
```

Salida:

```
{
    "StreamProcessors": [
        {
            "Status": "STOPPED",
            "Name": "my-stream-processor"
        }
    ]
}
```

Para obtener más información, consulte Working with Streaming Videos en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte ListStreamProcessors en la Referencia de comandos de la AWS CLI.

`recognize-celebrities`

En el siguiente ejemplo de código, se muestra cómo utilizar `recognize-celebrities`.

Para obtener información, consulte Reconocimiento de famosos en una imagen.

AWS CLI

Reconocimiento de famosos en una imagen

El siguiente comando `recognize-celebrities` reconoce a famosos en la imagen especificada almacenada en un bucket de Amazon S3:

```
aws rekognition recognize-celebrities \
    --image "S3Object={Bucket=MyImageS3Bucket,Name=moviestars.jpg}"
```

Salida:

```
{
    "UnrecognizedFaces": [
        {
            "BoundingBox": {
                "Width": 0.14416666328907013,
                "Top": 0.07777778059244156,
                "Left": 0.625,
                "Height": 0.2746031880378723
            },
            "Confidence": 99.9990234375,
            "Pose": {
                "Yaw": 10.80408763885498,
                "Roll": -12.761146545410156,
                "Pitch": 10.96889877319336
            },
            "Quality": {
                "Sharpness": 94.1185531616211,
                "Brightness": 79.18367004394531
            },
            "Landmarks": [
                {
                    "Y": 0.18220913410186768,
                    "X": 0.6702951788902283,
                    "Type": "eyeLeft"
                },
                {
                    "Y": 0.16337193548679352,
                    "X": 0.7188183665275574,
                    "Type": "eyeRight"
```

```
                },
                {
                    "Y": 0.20739148557186127,
                    "X": 0.7055801749229431,
                    "Type": "nose"
                },
                {
                    "Y": 0.2889308035373688,
                    "X": 0.687512218952179,
                    "Type": "mouthLeft"
                },
                {
                    "Y": 0.2706988751888275,
                    "X": 0.7250053286552429,
                    "Type": "mouthRight"
                }
            ]
        }
    ],
    "CelebrityFaces": [
        {
            "MatchConfidence": 100.0,
            "Face": {
                "BoundingBox": {
                    "Width": 0.14000000059604645,
                    "Top": 0.1190476194024086,
                    "Left": 0.82833331823349,
                    "Height": 0.2666666805744171
                },
                "Confidence": 99.99359130859375,
                "Pose": {
                    "Yaw": -10.509642601013184,
                    "Roll": -14.51749324798584,
                    "Pitch": 13.799399375915527
                },
                "Quality": {
                    "Sharpness": 78.74752044677734,
                    "Brightness": 42.201324462890625
                },
                "Landmarks": [
                    {
                        "Y": 0.2290833294391632,
                        "X": 0.8709492087364197,
                        "Type": "eyeLeft"
```

```
                    },
                    {
                        "Y": 0.20639978349208832,
                        "X": 0.9153988361358643,
                        "Type": "eyeRight"
                    },
                    {
                        "Y": 0.25417643785476685,
                        "X": 0.8907724022865295,
                        "Type": "nose"
                    },
                    {
                        "Y": 0.32729196548461914,
                        "X": 0.8876466155052185,
                        "Type": "mouthLeft"
                    },
                    {
                        "Y": 0.3115464746952057,
                        "X": 0.9238573312759399,
                        "Type": "mouthRight"
                    }
                ]
            },
            "Name": "Celeb A",
            "Urls": [
                "www.imdb.com/name/aaaaaaaaa"
            ],
            "Id": "1111111"
        },
        {
            "MatchConfidence": 97.0,
            "Face": {
                "BoundingBox": {
                    "Width": 0.13333334028720856,
                    "Top": 0.24920634925365448,
                    "Left": 0.4449999928474426,
                    "Height": 0.2539682686328888
                },
                "Confidence": 99.99979400634766,
                "Pose": {
                    "Yaw": 6.557040691375732,
                    "Roll": -7.316643714904785,
                    "Pitch": 9.272967338562012
                },
```

```
                "Quality": {
                    "Sharpness": 83.23492431640625,
                    "Brightness": 78.83267974853516
                },
                "Landmarks": [
                    {
                        "Y": 0.3625510632991791,
                        "X": 0.48898839950561523,
                        "Type": "eyeLeft"
                    },
                    {
                        "Y": 0.35366007685661316,
                        "X": 0.5313721299171448,
                        "Type": "eyeRight"
                    },
                    {
                        "Y": 0.3894785940647125,
                        "X": 0.5173314809799194,
                        "Type": "nose"
                    },
                    {
                        "Y": 0.44889405369758606,
                        "X": 0.5020005702972412,
                        "Type": "mouthLeft"
                    },
                    {
                        "Y": 0.4408611059188843,
                        "X": 0.5351271629333496,
                        "Type": "mouthRight"
                    }
                ]
            },
            "Name": "Celeb B",
            "Urls": [
                "www.imdb.com/name/bbbbbbbbb"
            ],
            "Id": "2222222"
        },
        {
            "MatchConfidence": 100.0,
            "Face": {
                "BoundingBox": {
                    "Width": 0.12416666746139526,
                    "Top": 0.2968254089355469,
```

```
                    "Left": 0.2150000035762787,
                    "Height": 0.23650793731212616
                },
                "Confidence": 99.99958801269531,
                "Pose": {
                    "Yaw": 7.801797866821289,
                    "Roll": -8.326810836791992,
                    "Pitch": 7.844768047332764
                },
                "Quality": {
                    "Sharpness": 86.93206024169922,
                    "Brightness": 79.81291198730469
                },
                "Landmarks": [
                    {
                        "Y": 0.4027804136276245,
                        "X": 0.2575301229953766,
                        "Type": "eyeLeft"
                    },
                    {
                        "Y": 0.3934555947780609,
                        "X": 0.2956969439983368,
                        "Type": "eyeRight"
                    },
                    {
                        "Y": 0.4309830069541931,
                        "X": 0.2837020754814148,
                        "Type": "nose"
                    },
                    {
                        "Y": 0.48186683654785156,
                        "X": 0.26812544465065,
                        "Type": "mouthLeft"
                    },
                    {
                        "Y": 0.47338807582855225,
                        "X": 0.29905644059181213,
                        "Type": "mouthRight"
                    }
                ]
            },
            "Name": "Celeb C",
            "Urls": [
                "www.imdb.com/name/ccccccccc"
```

```
            ],
            "Id": "3333333"
        },
        {
            "MatchConfidence": 97.0,
            "Face": {
                "BoundingBox": {
                    "Width": 0.11916666477918625,
                    "Top": 0.3698412775993347,
                    "Left": 0.008333333767950535,
                    "Height": 0.22698412835597992
                },
                "Confidence": 99.99999237060547,
                "Pose": {
                    "Yaw": 16.38478660583496,
                    "Roll": -1.0260354280471802,
                    "Pitch": 5.975185394287109
                },
                "Quality": {
                    "Sharpness": 83.23492431640625,
                    "Brightness": 61.408443450927734
                },
                "Landmarks": [
                    {
                        "Y": 0.4632347822189331,
                        "X": 0.049406956881284714,
                        "Type": "eyeLeft"
                    },
                    {
                        "Y": 0.46388113498687744,
                        "X": 0.08722897619009018,
                        "Type": "eyeRight"
                    },
                    {
                        "Y": 0.5020678639411926,
                        "X": 0.0758260041475296,
                        "Type": "nose"
                    },
                    {
                        "Y": 0.544157862663269,
                        "X": 0.054029736667871475,
                        "Type": "mouthLeft"
                    },
                    {
```

```
                        "Y": 0.5463630557060242,
                        "X": 0.08464983850717545,
                        "Type": "mouthRight"
                    }
                ]
            },
            "Name": "Celeb D",
            "Urls": [
                "www.imdb.com/name/ddddddddd"
            ],
            "Id": "4444444"
        }
    ]
}
```

Para obtener más información, consulte Reconocimiento de famosos en una imagen en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte RecognizeCelebrities en la Referencia de comandos de la AWS CLI.

`search-faces-by-image`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-faces-by-image`.

Para obtener información, consulte Búsqueda de un rostro (imagen).

AWS CLI

Búsqueda de rostros en una colección que coincida con el rostro de mayor tamaño en una imagen.

El siguiente comando `search-faces-by-image` busca rostros en una colección que coincidan con el rostro más grande de la imagen especificada:

```
aws rekognition search-faces-by-image \
    --image '{"S3Object":{"Bucket":"MyImageS3Bucket","Name":"ExamplePerson.jpg"}}' \
    --collection-id MyFaceImageCollection

{
    "SearchedFaceBoundingBox": {
        "Width": 0.18562500178813934,
        "Top": 0.1618015021085739,
```

```
            "Left": 0.5575000047683716,
            "Height": 0.24770642817020416
        },
        "SearchedFaceConfidence": 99.993408203125,
        "FaceMatches": [
            {
                "Face": {
                    "BoundingBox": {
                        "Width": 0.18562500178813934,
                        "Top": 0.1618019938468933,
                        "Left": 0.5575000047683716,
                        "Height": 0.24770599603652954
                    },
                    "FaceId": "ce7ed422-2132-4a11-ab14-06c5c410f29f",
                    "ExternalImageId": "example-image.jpg",
                    "Confidence": 99.99340057373047,
                    "ImageId": "8d67061e-90d2-598f-9fbd-29c8497039c0"
                },
                "Similarity": 99.97913360595703
            },
            {
                "Face": {
                    "BoundingBox": {
                        "Width": 0.18562500178813934,
                        "Top": 0.1618019938468933,
                        "Left": 0.5575000047683716,
                        "Height": 0.24770599603652954
                    },
                    "FaceId": "13692fe4-990a-4679-b14a-5ac23d135eab",
                    "ExternalImageId": "image3.jpg",
                    "Confidence": 99.99340057373047,
                    "ImageId": "8df18239-9ad1-5acd-a46a-6581ff98f51b"
                },
                "Similarity": 99.97913360595703
            },
            {
                "Face": {
                    "BoundingBox": {
                        "Width": 0.41499999165534973,
                        "Top": 0.09187500178813934,
                        "Left": 0.28083300590515137,
                        "Height": 0.3112500011920929
                    },
                    "FaceId": "8d3cfc70-4ba8-4b36-9644-90fba29c2dac",
```

```
            "ExternalImageId": "image2.jpg",
            "Confidence": 99.99769592285156,
            "ImageId": "a294da46-2cb1-5cc4-9045-61d7ca567662"
        },
        "Similarity": 99.18069458007812
    },
    {
        "Face": {
            "BoundingBox": {
                "Width": 0.48166701197624207,
                "Top": 0.20999999344348907,
                "Left": 0.21250000596046448,
                "Height": 0.36125001311302185
            },
            "FaceId": "bd4ceb4d-9acc-4ab7-8ef8-1c2d2ba0a66a",
            "ExternalImageId": "image1.jpg",
            "Confidence": 99.99949645996094,
            "ImageId": "5e1a7588-e5a0-5ee3-bd00-c642518dfe3a"
        },
        "Similarity": 98.66607666015625
    },
    {
        "Face": {
            "BoundingBox": {
                "Width": 0.5349419713020325,
                "Top": 0.29124999046325684,
                "Left": 0.16389399766921997,
                "Height": 0.40187498927116394
            },
            "FaceId": "745f7509-b1fa-44e0-8b95-367b1359638a",
            "ExternalImageId": "image9.jpg",
            "Confidence": 99.99979400634766,
            "ImageId": "67a34327-48d1-5179-b042-01e52ccfeada"
        },
        "Similarity": 98.24278259277344
    },
    {
        "Face": {
            "BoundingBox": {
                "Width": 0.5307819843292236,
                "Top": 0.2862499952316284,
                "Left": 0.1564060002565384,
                "Height": 0.3987500071525574
            },
```

```
            "FaceId": "2eb5f3fd-e2a9-4b1c-a89f-afa0a518fe06",
            "ExternalImageId": "image10.jpg",
            "Confidence": 99.99970245361328,
            "ImageId": "3c314792-197d-528d-bbb6-798ed012c150"
        },
        "Similarity": 98.10665893554688
    },
    {
        "Face": {
            "BoundingBox": {
                "Width": 0.5074880123138428,
                "Top": 0.3774999976158142,
                "Left": 0.18302799761295319,
                "Height": 0.3812499940395355
            },
            "FaceId": "086261e8-6deb-4bc0-ac73-ab22323cc38d",
            "ExternalImageId": "image6.jpg",
            "Confidence": 99.99930572509766,
            "ImageId": "ae1593b0-a8f6-5e24-a306-abf529e276fa"
        },
        "Similarity": 98.10526275634766
    },
    {
        "Face": {
            "BoundingBox": {
                "Width": 0.5574039816856384,
                "Top": 0.37187498807907104,
                "Left": 0.14559100568294525,
                "Height": 0.4181250035762787
            },
            "FaceId": "11c4bd3c-19c5-4eb8-aecc-24feb93a26e1",
            "ExternalImageId": "image5.jpg",
            "Confidence": 99.99960327148438,
            "ImageId": "80739b4d-883f-5b78-97cf-5124038e26b9"
        },
        "Similarity": 97.94659423828125
    },
    {
        "Face": {
            "BoundingBox": {
                "Width": 0.5773710012435913,
                "Top": 0.34437501430511475,
                "Left": 0.12396000325679779,
                "Height": 0.4337500035762787
```

```
                },
                "FaceId": "57189455-42b0-4839-a86c-abda48b13174",
                "ExternalImageId": "image8.jpg",
                "Confidence": 100.0,
                "ImageId": "0aff2f37-e7a2-5dbc-a3a3-4ef6ec18eaa0"
            },
            "Similarity": 97.93476867675781
        }
    ],

 "FaceModelVersion": "3.0"
}
```

Para obtener más información, consulte Búsqueda de un rostro utilizando una imagen en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte SearchFacesByImage en la Referencia de comandos de la AWS CLI.

`search-faces`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-faces`.

Para obtener información, consulte Búsqueda de un rostro (ID de rostro).

AWS CLI

Búsqueda de rostros en una colección que coincidan con un ID de rostro.

El siguiente comando `search-faces` busca rostros en una colección que coincidan con el ID de rostro especificado.

```
aws rekognition search-faces \
    --face-id 8d3cfc70-4ba8-4b36-9644-90fba29c2dac \
    --collection-id MyCollection
```

Salida:

```
{
    "SearchedFaceId": "8d3cfc70-4ba8-4b36-9644-90fba29c2dac",
    "FaceModelVersion": "3.0",
    "FaceMatches": [
        {
```

```
            "Face": {
                "BoundingBox": {
                    "Width": 0.48166701197624207,
                    "Top": 0.20999999344348907,
                    "Left": 0.21250000596046448,
                    "Height": 0.36125001311302185
                },
                "FaceId": "bd4ceb4d-9acc-4ab7-8ef8-1c2d2ba0a66a",
                "ExternalImageId": "image1.jpg",
                "Confidence": 99.99949645996094,
                "ImageId": "5e1a7588-e5a0-5ee3-bd00-c642518dfe3a"
            },
            "Similarity": 99.30997467041016
        },
        {
            "Face": {
                "BoundingBox": {
                    "Width": 0.18562500178813934,
                    "Top": 0.1618019938468933,
                    "Left": 0.5575000047683716,
                    "Height": 0.24770599603652954
                },
                "FaceId": "ce7ed422-2132-4a11-ab14-06c5c410f29f",
                "ExternalImageId": "example-image.jpg",
                "Confidence": 99.99340057373047,
                "ImageId": "8d67061e-90d2-598f-9fbd-29c8497039c0"
            },
            "Similarity": 99.24862670898438
        },
        {
            "Face": {
                "BoundingBox": {
                    "Width": 0.18562500178813934,
                    "Top": 0.1618019938468933,
                    "Left": 0.5575000047683716,
                    "Height": 0.24770599603652954
                },
                "FaceId": "13692fe4-990a-4679-b14a-5ac23d135eab",
                "ExternalImageId": "image3.jpg",
                "Confidence": 99.99340057373047,
                "ImageId": "8df18239-9ad1-5acd-a46a-6581ff98f51b"
            },
            "Similarity": 99.24862670898438
        },
```

```
        {
            "Face": {
                "BoundingBox": {
                    "Width": 0.5349419713020325,
                    "Top": 0.29124999046325684,
                    "Left": 0.16389399766921997,
                    "Height": 0.40187498927116394
                },
                "FaceId": "745f7509-b1fa-44e0-8b95-367b1359638a",
                "ExternalImageId": "image9.jpg",
                "Confidence": 99.99979400634766,
                "ImageId": "67a34327-48d1-5179-b042-01e52ccfeada"
            },
            "Similarity": 96.73158264160156
        },
        {
            "Face": {
                "BoundingBox": {
                    "Width": 0.5307819843292236,
                    "Top": 0.2862499952316284,
                    "Left": 0.1564060002565384,
                    "Height": 0.3987500071525574
                },
                "FaceId": "2eb5f3fd-e2a9-4b1c-a89f-afa0a518fe06",
                "ExternalImageId": "image10.jpg",
                "Confidence": 99.99970245361328,
                "ImageId": "3c314792-197d-528d-bbb6-798ed012c150"
            },
            "Similarity": 96.48291015625
        },
        {
            "Face": {
                "BoundingBox": {
                    "Width": 0.5074880123138428,
                    "Top": 0.3774999976158142,
                    "Left": 0.18302799761295319,
                    "Height": 0.3812499940395355
                },
                "FaceId": "086261e8-6deb-4bc0-ac73-ab22323cc38d",
                "ExternalImageId": "image6.jpg",
                "Confidence": 99.99930572509766,
                "ImageId": "ae1593b0-a8f6-5e24-a306-abf529e276fa"
            },
            "Similarity": 96.43287658691406
```

```
        },
        {
            "Face": {
                "BoundingBox": {
                    "Width": 0.5574039816856384,
                    "Top": 0.37187498807907104,
                    "Left": 0.14559100568294525,
                    "Height": 0.4181250035762787
                },
                "FaceId": "11c4bd3c-19c5-4eb8-aecc-24feb93a26e1",
                "ExternalImageId": "image5.jpg",
                "Confidence": 99.99960327148438,
                "ImageId": "80739b4d-883f-5b78-97cf-5124038e26b9"
            },
            "Similarity": 95.25305938720703
        },
        {
            "Face": {
                "BoundingBox": {
                    "Width": 0.5773710012435913,
                    "Top": 0.34437501430511475,
                    "Left": 0.12396000325679779,
                    "Height": 0.4337500035762787
                },
                "FaceId": "57189455-42b0-4839-a86c-abda48b13174",
                "ExternalImageId": "image8.jpg",
                "Confidence": 100.0,
                "ImageId": "0aff2f37-e7a2-5dbc-a3a3-4ef6ec18eaa0"
            },
            "Similarity": 95.22837829589844
        }
    ]
}
```

Para obtener más información, consulte Búsqueda de un rostro utilizando su ID de rostro en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte SearchFaces en la Referencia de comandos de la AWS CLI.

`start-celebrity-recognition`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-celebrity-recognition`.

AWS CLI

Para iniciar el reconocimiento de celebridades en un vídeo almacenado

El siguiente comando `start-celebrity-recognition` inicia un trabajo para buscar a celebridades en el archivo de vídeo especificado almacenado en un bucket de Amazon S3.

```
aws rekognition start-celebrity-recognition \
    --video "S3Object={Bucket=MyVideoS3Bucket,Name=MyVideoFile.mpg}"
```

Salida:

```
{
    "JobId": "1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef"
}
```

Para obtener más información, consulte Recognizing Celebrities in a Stored Video en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte StartCelebrityRecognition en la Referencia de comandos de la AWS CLI.

`start-content-moderation`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-content-moderation`.

AWS CLI

Para iniciar el reconocimiento de contenido no seguro en un vídeo almacenado

El siguiente comando `start-content-moderation` inicia un trabajo para detectar contenido no seguro en el vídeo especificado almacenado en un bucket de Amazon S3.

```
aws rekognition start-content-moderation \
    --video "S3Object={Bucket=MyVideoS3Bucket,Name=MyVideoFile.mpg}"
```

Salida:

```
{
    "JobId": "1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef"
```

```
}
```

Para obtener más información, consulte Detecting Unsafe Stored Videos en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte StartContentModeration en la Referencia de comandos de la AWS CLI.

`start-face-detection`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-face-detection`.

AWS CLI

Para detectar rostros en un vídeo

El siguiente comando `start-face-detection` inicia un trabajo para detectar rostros en el vídeo especificado almacenado en un bucket de Amazon S3.

```
aws rekognition start-face-detection
    --video "S3Object={Bucket=MyVideoS3Bucket,Name=MyVideoFile.mpg}"
```

Salida:

```
{
    "JobId": "1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef"
}
```

Para obtener más información, consulte Detecting Faces in a Stored Video en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte StartFaceDetection en la Referencia de comandos de la AWS CLI.

`start-face-search`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-face-search`.

AWS CLI

Para buscar rostros en una colección que coincidan con un rostros detectados en un vídeo

El siguiente comando `start-face-search` inicia un trabajo para buscar rostros en una colección que coincidan con las detectadas en un archivo de vídeo especificado en un bucket de Amazon S3.

```
aws rekognition start-face-search \
    --video "S3Object={Bucket=MyVideoS3Bucket,Name=MyVideoFile.mpg}" \
    --collection-id collection
```

Salida:

```
{
    "JobId": "1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef"
}
```

Para obtener más información, consulte Searching Stored Videos for Faces en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte StartFaceSearch en la Referencia de comandos de la AWS CLI.

`start-label-detection`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-label-detection`.

AWS CLI

Para detectar objetos y escenas en un vídeo

El siguiente comando `start-label-detection` inicia un trabajo para detectar objetos y escenas en el vídeo especificado almacenado en un bucket de Amazon S3.

```
aws rekognition start-label-detection \
    --video "S3Object={Bucket=MyVideoS3Bucket,Name=MyVideoFile.mpg}"
```

Salida:

```
{
    "JobId": "1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef"
}
```

Para obtener más información, consulte Detecting Labels in a Video en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte StartLabelDetection en la Referencia de comandos de la AWS CLI.

`start-person-tracking`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-person-tracking`.

AWS CLI

Para iniciar el recorrido de las personas en un vídeo almacenado

El siguiente comando `start-person-tracking` inicia un trabajo para realizar un seguimiento de los recorridos que siguen las personas en el archivo de vídeo especificado almacenado en un bucket de Amazon S3:

```
aws rekognition start-person-tracking \
    --video "S3Object={Bucket=MyVideoS3Bucket,Name=MyVideoFile.mpg}"
```

Salida:

```
{
    "JobId": "1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef"
}
```

Para obtener más información, consulte People Pathing en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte StartPersonTracking en la Referencia de comandos de la AWS CLI.

`start-stream-processor`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-stream-processor`.

AWS CLI

Para iniciar el procesador de transmisiones

El siguiente comando `start-stream-processor` inicia el procesador de transmisión de vídeo especificado.

```
aws rekognition start-stream-processor \
    --name my-stream-processor
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with Streaming Videos en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte StartStreamProcessor en la Referencia de comandos de la AWS CLI.

`stop-stream-processor`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-stream-processor`.

AWS CLI

Para detener un procesador de transmisión en ejecución

El siguiente comando `stop-stream-processor` detiene el procesador de transmisión en ejecución especificado.

```
aws rekognition stop-stream-processor \
    --name my-stream-processor
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with Streaming Videos en la Guía para desarrolladores de Amazon Rekognition.

- Para obtener información sobre la API, consulte StopStreamProcessor en la Referencia de comandos de la AWS CLI.

AWS RAM Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS RAM.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`accept-resource-share-invitation`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-resource-share-invitation`.

AWS CLI

Para aceptar una invitación a recursos compartidos

En el siguiente ejemplo de `accept-resource-share-invitation`, se acepta la invitación a un recurso compartido especificado. Las entidades principales de la cuenta invitada pueden empezar a utilizar inmediatamente los recursos del recurso compartido.

```
aws ram accept-resource-share-invitation \
    --resource-share-invitation-arn arn:aws:ram:us-west-2:111111111111:resource-share-invitation/1e3477be-4a95-46b4-bbe0-c4001EXAMPLE
```

Salida:

```
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-west-2:111111111111:resource-share-invitation/1e3477be-4a95-46b4-bbe0-c4001EXAMPLE",
        "resourceShareName": "MyLicenseShare",
        "resourceShareArn": "arn:aws:ram:us-west-2:111111111111:resource-share/27d09b4b-5e12-41d1-a4f2-19dedEXAMPLE",
        "senderAccountId": "111111111111",
        "receiverAccountId": "222222222222",
        "invitationTimestamp": "2021-09-22T15:07:35.620000-07:00",
```

```
        "status": "ACCEPTED"
    }
}
```

- Para obtener información sobre la API, consulte AcceptResourceShareInvitation en la Referencia de comandos de la AWS CLI.

`associate-resource-share-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-resource-share-permission`.

AWS CLI

Para asociar un permiso administrado por RAM con un recurso compartido

En el siguiente ejemplo de `associate-resource-share-permission`, se reemplaza el permiso administrado existente por el tipo de recurso correspondiente con el permiso administrado especificado. El acceso a todos los recursos del tipo de recurso correspondiente se rige por el nuevo permiso.

```
aws ram associate-resource-share-permission \
    --permission-arn arn:aws:ram::aws:permission/
AWSRAMPermissionGlueDatabaseReadWrite \
    --replace \
    --resource-share-arn arn:aws:ram:us-west-2:123456789012:resource-
share/27d09b4b-5e12-41d1-a4f2-19dedEXAMPLE
```

Salida:

```
{
    "returnValue": true
}
```

- Para obtener información sobre la API, consulte AssociateResourceSharePermission en la Referencia de comandos de la AWS CLI.

`associate-resource-share`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-resource-share`.

AWS CLI

Ejemplo 1: asociación de un recurso a un recurso compartido

En el siguiente ejemplo de `associate-resource-share`, se añade una configuración de licencia al recurso compartido especificado.

```
aws ram associate-resource-share \
    --resource-share arn:aws:ram:us-west-2:123456789012:resource-
share/27d09b4b-5e12-41d1-a4f2-19dedEXAMPLE \
    --resource-arns arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-36be0485f5ae379cc74cf8e92EXAMPLE
```

Salida:

```
{
    "resourceShareAssociations": [
        {
            "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-
share/27d09b4b-5e12-41d1-a4f2-19dedEXAMPLE",
            "associatedEntity": "arn:aws:license-manager:us-
west-2:123456789012:license-configuration:lic-36be0485f5ae379cc74cf8e92EXAMPLE",
            "associationType": "RESOURCE",
            "status": "ASSOCIATING",
            "external": false
        }
    ]
}
```

Ejemplo 2: asociación de una entidad principal a un recurso compartido

En el siguiente ejemplo de `associate-resource-share`, se concede acceso al recurso compartido especificado a todas las cuentas de la unidad organizativa especificada.

```
aws ram associate-resource-share \
    --resource-share-arn arn:aws:ram:us-west-2:123456789012:resource-
share/27d09b4b-5e12-41d1-a4f2-19dedEXAMPLE \
    --principals arn:aws:organizations::123456789012:ou/o-63bEXAMPLE/ou-46xi-
rEXAMPLE
```

Salida:

```
{
    "resourceShareAssociations": [
        {
            "status": "ASSOCIATING",
            "associationType": "PRINCIPAL",
            "associatedEntity": "arn:aws:organizations::123456789012:ou/
o-63bEXAMPLE/ou-46xi-rEXAMPLE",
            "external": false,
            "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-
share/27d09b4b-5e12-41d1-a4f2-19dedEXAMPLE"
        }
    ]
}
```

- Para obtener información sobre la API, consulte AssociateResourceShare en la Referencia de comandos de la AWS CLI.

`create-resource-share`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-resource-share`.

AWS CLI

Ejemplo 1: creación de un recurso compartido

En el siguiente ejemplo de `create-resource-share`, se crea un recurso compartido vacío con un nombre específico. Debe agregar los recursos, las entidades principales y los permisos al recurso compartido por separado.

```
aws ram create-resource-share \
    --name MyNewResourceShare
```

Salida:

```
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-
share/4476c27d-8feb-4b21-afe9-7de23EXAMPLE",
        "name": "MyNewResourceShare",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": true,
```

```
        "status": "ACTIVE",
        "creationTime": 1634586271.302,
        "lastUpdatedTime": 1634586271.302
    }
}
```

Ejemplo 2: creación de un recurso compartido con cuentas de AWS como entidades principales

En el siguiente de `create-resource-share` ejemplo, se crea un recurso compartido y se concede acceso a la cuenta de AWS especificada (222222222222). Si las entidades principales especificadas no forman parte de la misma organización de AWS, las invitaciones se envían y deben aceptarse antes de conceder el acceso.

```
aws ram create-resource-share \
    --name MyNewResourceShare \
    --principals 222222222222
```

Ejemplo 3: creación de un recurso compartido restringido a su organización AWS

El siguiente ejemplo de `create-resource-share` crea un recurso compartido que está restringido a las cuentas de la organización AWS a la que pertenezca su cuenta y agrega la unidad organizativa especificada como entidad principal. Todas las cuentas de esa unidad organizativa pueden usar los recursos del recurso compartido.

```
aws ram create-resource-share \
    --name MyNewResourceShare \
    --no-allow-external-principals \
    --principals arn:aws:organizations::123456789012:ou/o-63bEXAMPLE/ou-46xi-
rEXAMPLE
```

Salida:

```
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-
share/7be8694e-095c-41ca-9ce8-7be4aEXAMPLE",
        "name": "MyNewResourceShare",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": false,
        "status": "ACTIVE",
        "creationTime": 1634587042.49,
```

```
        "lastUpdatedTime": 1634587042.49
    }
}
```

- Para obtener información sobre la API, consulte CreateResourceShare en la Referencia de comandos de la AWS CLI.

`delete-resource-share`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-resource-share`.

AWS CLI

Para eliminar un recurso compartido

En el siguiente ejemplo de `delete-resource-share`, se elimina el recurso compartido especificado.

```
aws ram delete-resource-share \
    --resource-share-arn arn:aws:ram:us-west-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
```

El siguiente resultado indica que se ha realizado correctamente:

```
{
    "returnValue": true
}
```

- Para obtener información sobre la API, consulte DeleteResourceShare en la Referencia de comandos de la AWS CLI.

`disassociate-resource-share-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-resource-share-permission`.

AWS CLI

Para eliminar un permiso administrado por RAM para un tipo de recurso desde un recurso compartido

En el siguiente ejemplo de `disassociate-resource-share-permission`, se elimina el permiso administrado por RAM para las bases de datos Glue del recurso compartido especificado.

```
aws ram disassociate-resource-share-permission \
    --resource-share-arn arn:aws:ram:us-west-2:123456789012:resource-share/27d09b4b-5e12-41d1-a4f2-19dedEXAMPLE \
    --permission-arn arn:aws:ram::aws:permission/AWSRAMPermissionGlueDatabaseReadWrite
```

Salida:

```
{
    "returnValue": true
}
```

- Para obtener información sobre la API, consulte DisassociateResourceSharePermission en la Referencia de comandos de AWS CLI.

`disassociate-resource-share`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-resource-share`.

AWS CLI

Eliminar un recurso de un recurso compartido

En el siguiente ejemplo de `disassociate-resource-share`, se elimina el recurso especificado, en este caso una subred de VPC, del recurso compartido especificado. Las entidades principales con acceso al recurso compartido ya no pueden realizar operaciones en ese recurso.

```
aws ram disassociate-resource-share \
    --resource-arns arn:aws:ec2:us-west-2:123456789012:subnet/subnet-0250c25a1fEXAMPLE \
    --resource-share-arn arn:aws:ram:us-west-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
```

Salida:

```
{
```

```
    "resourceShareAssociations": [
        "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "associatedEntity": "arn:aws:ec2:us-west-2:123456789012:subnet/
subnet-0250c25a1fEXAMPLE",
        "associationType": "RESOURCE",
        "status": "DISASSOCIATING",
        "external": false
    ]
}
```

- Para obtener información sobre la API, consulte DisassociateResourceShare en la Referencia de la comandos de la AWS CLI.

`enable-sharing-with-aws-organization`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-sharing-with-aws-organization`.

AWS CLI

Habilitar recursos compartidos en AWS Organizations

El siguiente ejemplo de `enable-sharing-with-aws-organization` permite compartir recursos entre la organización y las unidades organizativas.

```
aws ram enable-sharing-with-aws-organization
```

El siguiente resultado indica que se ha realizado correctamente.

```
{
    "returnValue": true
}
```

- Para obtener información sobre la API, consulte EnableSharingWithAwsOrganization en la Referencia de comandos de la AWS CLI.

`get-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-permission`.

AWS CLI

Para recuperar los detalles de un permiso administrado por RAM

En el siguiente ejemplo de `get-permission` se muestran los detalles de la versión predeterminada del permiso administrado por RAM especificado.

```
aws ram get-permission \
    --permission-arn arn:aws:ram::aws:permission/
AWSRAMPermissionGlueTableReadWriteForDatabase
```

Salida:

```
{
    "permission": {
        "arn": "arn:aws:ram::aws:permission/
AWSRAMPermissionGlueTableReadWriteForDatabase",
        "version": "2",
        "defaultVersion": true,
        "name": "AWSRAMPermissionGlueTableReadWriteForDatabase",
        "resourceType": "glue:Database",
        "permission": "{\"Effect\":\"Allow\",\"Action\":[\"glue:GetTable
\", \"glue:UpdateTable\", \"glue:DeleteTable\", \"glue:BatchDeleteTable\",
 \"glue:BatchDeleteTableVersion\", \"glue:GetTableVersion\", \"glue:GetTableVersions
\", \"glue:GetPartition\", \"glue:GetPartitions\", \"glue:BatchGetPartition\",
 \"glue:BatchCreatePartition\", \"glue:CreatePartition\", \"glue:UpdatePartition
\", \"glue:BatchDeletePartition\", \"glue:DeletePartition\", \"glue:GetTables\",
 \"glue:SearchTables\"]}",
        "creationTime": 1624912434.431,
        "lastUpdatedTime": 1624912434.431,
        "isResourceTypeDefault": false
    }
}
```

- Para obtener información sobre la API, consulte GetPermission en la Referencia de comandos de la AWS CLI.

`get-resource-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource-policies`.

AWS CLI

Para obtener las políticas de un recurso

En el siguiente ejemplo de `get-resource-policies`, se muestran las políticas de permisos basadas en recursos para el recurso especificado asociado a un recurso compartido.

```
aws ram get-resource-policies \
    --resource-arns arn:aws:ec2:us-west-2:123456789012:subnet/
subnet-0250c25a1fEXAMPLE
```

Salida:

```
{
    "policies": [
        "{\"Version\":\"2008-10-17\",\"Statement\":[{\"Sid\":\"RamStatement1\",
\"Effect\":\"Allow\",\"Principal\":{\"AWS\":[]},\"Action\":[\"ec2:RunInstances
\",\"ec2:CreateNetworkInterface\",\"ec2:DescribeSubnets\"],\"Resource\":
\"arn:aws:ec2:us-west-2:123456789012:subnet/subnet-0250c25a1fEXAMPLE\"}]}"
    ]
}
```

- Para obtener información sobre la API, consulte GetResourcePolicies en la Referencia de comandos de la AWS CLI.

`get-resource-share-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource-share-associations`.

AWS CLI

Ejemplo 1: enumeración de todas las asociaciones de recursos de todos los tipos de recursos

El siguiente ejemplo de `get-resource-share-associations` muestra las asociaciones de recursos para todos los tipos de recursos en todos sus recursos compartidos.

```
aws ram get-resource-share-associations \
    --association-type RESOURCE
```

Salida:

```
{
    "resourceShareAssociations": [
        {
            "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
            "associatedEntity": "arn:aws:ec2:us-west-2:123456789012:subnet/
subnet-0250c25a1fEXAMPLE",
            "resourceShareName": "MySubnetShare",
            "associationType": "RESOURCE",
            "status": "ASSOCIATED",
            "creationTime": 1565303590.973,
            "lastUpdatedTime": 1565303591.695,
            "external": false
        },
        {
            "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-
share/8167bdfe-4480-4a01-8632-315e0EXAMPLE",
            "associatedEntity": "arn:aws:license-manager:us-
west-2:123456789012:license-configuration:lic-36be0485f5ae379cc74cf8e92EXAMPLE",
            "resourceShareName": "MyLicenseShare",
            "associationType": "RESOURCE",
            "status": "ASSOCIATED",
            "creationTime": 1632342958.457,
            "lastUpdatedTime": 1632342958.907,
            "external": false
        }
    ]
}
```

Ejemplo 2: enumeración de las asociaciones de las entidades principales de un recurso compartido

En el siguiente ejemplo de `get-resource-share-associations`, se enumeran solo las asociaciones de las entidades principales únicamente para el recurso compartido especificado.

```
aws ram get-resource-share-associations \
   --resource-share-arns arn:aws:ram:us-west-2:123456789012:resource-
share/7be8694e-095c-41ca-9ce8-7be4aEXAMPLE \
   --association-type PRINCIPAL
```

Salida:

```
{
    "resourceShareAssociations": [
        {
            "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-
share/7be8694e-095c-41ca-9ce8-7be4aEXAMPLE",
            "resourceShareName": "MyNewResourceShare",
            "associatedEntity": "arn:aws:organizations::123456789012:ou/
o-63bEXAMPLE/ou-46xi-rEXAMPLE",
            "associationType": "PRINCIPAL",
            "status": "ASSOCIATED",
            "creationTime": 1634587042.49,
            "lastUpdatedTime": 1634587044.291,
            "external": false
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetResourceShareAssociations en la Referencia de comandos de la AWS CLI.

`get-resource-share-invitations`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource-share-invitations`.

AWS CLI

Para enumerar sus invitaciones a compartir recursos

En el siguiente ejemplo de `get-resource-share-invitations`, se muestran las invitaciones actuales para compartir recursos.

```
aws ram get-resource-share-invitations
```

Salida:

```
{
    "resourceShareInvitations": [
        {
            "resourceShareInvitationArn": "arn:aws:ram:us-
west2-1:111111111111:resource-share-invitation/32b639f0-14b8-7e8f-55ea-
e6117EXAMPLE",
            "resourceShareName": "project-resource-share",
```

```
            "resourceShareArn": "arn:aws:ram:us-west-2:111111111111:resource-share/
fcb639f0-1449-4744-35bc-a983fEXAMPLE",
            "senderAccountId": "111111111111",
            "receiverAccountId": "222222222222",
            "invitationTimestamp": 1565312166.258,
            "status": "PENDING"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetResourceShareInvitations en la Referencia de comandos de la AWS CLI.

`get-resource-shares`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource-shares`.

AWS CLI

Ejemplo 1: enumeración de los recursos compartidos que le pertenecen y compartirlos con otros

En el siguiente ejemplo de `get-resource-shares`, se enumeran los recursos compartidos que se crearon y que se comparten con otros.

```
aws ram get-resource-shares \
    --resource-owner SELF
```

Salida:

```
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-
share/3ab63985-99d9-1cd2-7d24-75e93EXAMPLE",
            "name": "my-resource-share",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": false,
            "status": "ACTIVE",
            "tags": [
                {
                    "key": "project",
                    "value": "lima"
```

```
                }
            ]
            "creationTime": 1565295733.282,
            "lastUpdatedTime": 1565295733.282
        },
        {
            "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
            "name": "my-resource-share",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": 1565295733.282,
            "lastUpdatedTime": 1565295733.282
        }
    ]
}
```

Ejemplo 2: enumeración de los recursos compartidos propiedad de otros y compartidos con usted

En el siguiente ejemplo de `get-resource-shares`, se enumeran los recursos compartidos que han creado otros y que han compartido con usted. En este ejemplo, no hay ninguno.

```
aws ram get-resource-shares \
    --resource-owner OTHER-ACCOUNTS
```

Salida:

```
{
    "resourceShares": []
}
```

- Para obtener información sobre la API, consulte GetResourceShares en la Referencia de comandos de la AWS CLI.

`list-pending-invitation-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-pending-invitation-resources`.

AWS CLI

Para enumerar los recursos que están disponibles en un recurso compartido pendiente

En el siguiente ejemplo de `list-pending-invitation-resources`, se enumeran todos los recursos que se encuentran en el recurso compartido asociado a la invitación especificada.

```
aws ram list-pending-invitation-resources \
    --resource-share-invitation-arn arn:aws:ram:us-west-2:123456789012:resource-share-invitation/1e3477be-4a95-46b4-bbe0-c4001EXAMPLE
```

Salida:

```
{
   "resources": [
        {
            "arn": "arn:aws:ec2:us-west-2:123456789012:subnet/
subnet-04a555b0e6EXAMPLE",
            "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-
share/7be8694e-095c-41ca-9ce8-7be4aEXAMPLE",
            "creationTime": 1634676051.269,
            "lastUpdatedTime": 1634676052.07,
            "status": "AVAILABLE",
            "type": "ec2:Subnet"
        },
        {
            "arn": "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-36be0485f5ae379cc74cf8e92EXAMPLE",
            "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
            "creationTime": 1624912434.431,
            "lastUpdatedTime": 1624912434.431,
            "status": "AVAILABLE",
            "type": "license-manager:LicenseConfiguration"
      }
   ]
}
```

- Para obtener información sobre la API, consulte ListPendingInvitationResources en la Referencia de comandos de la AWS CLI.

`list-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-permissions`.

AWS CLI

Para enumerar los permisos administrados por RAM disponibles

El siguiente ejemplo de `list-permissions` enumera todos los permisos administrados por RAM disponibles únicamente para el tipo de recurso de la base de datos AWS Glue.

```
aws ram list-permissions \
    --resource-type glue:Database
```

Salida:

```
{
    "permissions": [
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionGlueDatabase",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMDefaultPermissionGlueDatabase",
            "resourceType": "glue:Database",
            "creationTime": 1592007820.935,
            "lastUpdatedTime": 1592007820.935,
            "isResourceTypeDefault": true
        },
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMPermissionGlueAllTablesReadWriteForDatabase",
            "version": "2",
            "defaultVersion": true,
            "name": "AWSRAMPermissionGlueAllTablesReadWriteForDatabase",
            "resourceType": "glue:Database",
            "creationTime": 1624912413.323,
            "lastUpdatedTime": 1624912413.323,
            "isResourceTypeDefault": false
        },
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMPermissionGlueDatabaseReadWrite",
```

```
            "version": "2",
            "defaultVersion": true,
            "name": "AWSRAMPermissionGlueDatabaseReadWrite",
            "resourceType": "glue:Database",
            "creationTime": 1624912417.4,
            "lastUpdatedTime": 1624912417.4,
            "isResourceTypeDefault": false
        },
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMPermissionGlueTableReadWriteForDatabase",
            "version": "2",
            "defaultVersion": true,
            "name": "AWSRAMPermissionGlueTableReadWriteForDatabase",
            "resourceType": "glue:Database",
            "creationTime": 1624912434.431,
            "lastUpdatedTime": 1624912434.431,
            "isResourceTypeDefault": false
        }
    ]
}
```

El siguiente ejemplo de `list-permissions` muestra los permisos administrados por RAM disponibles para todos los tipos de recursos.

```
aws ram list-permissions
```

Salida:

```
{
    "permissions": [
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
            "version": "1",
            "defaultVersion": true,
            "name":
 "AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
            "resourceType": "acm-pca:CertificateAuthority",
            "creationTime": 1623264861.085,
            "lastUpdatedTime": 1623264861.085,
            "isResourceTypeDefault": false
        },
```

```
        {
            "arn": "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAppMesh",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMDefaultPermissionAppMesh",
            "resourceType": "appmesh:Mesh",
            "creationTime": 1589307188.584,
            "lastUpdatedTime": 1589307188.584,
            "isResourceTypeDefault": true
        },
        ...TRUNCATED FOR BREVITY...
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMSubordinateCACertificatePathLen0IssuanceCertificateAuthority",
            "version": "1",
            "defaultVersion": true,
            "name":
 "AWSRAMSubordinateCACertificatePathLen0IssuanceCertificateAuthority",
            "resourceType": "acm-pca:CertificateAuthority",
            "creationTime": 1623264876.75,
            "lastUpdatedTime": 1623264876.75,
            "isResourceTypeDefault": false
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListPermissions en la Referencia de comandos de la AWS CLI.

`list-principals`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-principals`.

AWS CLI

Para enumerar las entidades principales con acceso a un recurso

En el siguiente ejemplo de `list-principals`, se muestra una lista de las entidades principales que pueden acceder a los recursos del tipo especificado a través de cualquier recurso compartido.

```
aws ram list-principals \
```

```
    --resource-type ec2:Subnet
```

Salida:

```
{
    "principals": [
        {
            "id": "arn:aws:organizations::123456789012:ou/o-gx7EXAMPLE/ou-29c5-
zEXAMPLE",
            "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
            "creationTime": 1565298209.737,
            "lastUpdatedTime": 1565298211.019,
            "external": false
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListPrincipals en la Referencia de comandos de la AWS CLI.

`list-resource-share-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-share-permissions`.

AWS CLI

Para enumerar todos los permisos de RAM administrados actualmente asociados a un recurso compartido

En el siguiente ejemplo de `list-resource-share-permissions` se enumeran todos los permisos administrados por RAM asociados al recurso compartido especificado.

```
aws ram list-resource-share-permissions \
    --resource-share-arn arn:aws:ram:us-west-2:123456789012:resource-
share/27d09b4b-5e12-41d1-a4f2-19dedEXAMPLE
```

Salida:

```
{
```

```
    "permissions": [
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionLicenseConfiguration",
            "version": "1",
            "resourceType": "license-manager:LicenseConfiguration",
            "status": "ASSOCIATED",
            "lastUpdatedTime": 1632342984.234
        },
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMPermissionGlueDatabaseReadWrite",
            "version": "2",
            "resourceType": "glue:Database",
            "status": "ASSOCIATED",
            "lastUpdatedTime": 1632512462.297
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListResourceSharePermissions en la Referencia de comandos de la AWS CLI.

`list-resource-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-types`.

AWS CLI

Para enumerar los tipos de recursos que admite AWS RAM

En el siguiente ejemplo de `list-resource-types`, se enumeran todos los tipos de recursos que actualmente admite AWS RAM.

```
aws ram list-resource-types
```

Salida:

```
{
    "resourceTypes": [
        {
```

```
            "resourceType": "route53resolver:FirewallRuleGroup",
            "serviceName": "route53resolver"
        },
        {
            "resourceType": "ec2:LocalGatewayRouteTable",
            "serviceName": "ec2"
        },
        ...OUTPUT TRUNCATED FOR BREVITY...
        {
            "resourceType": "ec2:Subnet",
            "serviceName": "ec2"
        },
        {
            "resourceType": "ec2:TransitGatewayMulticastDomain",
            "serviceName": "ec2"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListResourceTypes en la Referencia de comandos de la AWS CLI.

`list-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resources`.

AWS CLI

Para enumerar los recursos asociados a un recurso compartido

En el siguiente ejemplo de `list-resources`, se enumeran todos los recursos del recurso compartido especificado que son del tipo de recurso especificado.

```
aws ram list-resources \
    --resource-type ec2:Subnet \
    --resource-owner SELF \
    --resource-share-arn arn:aws:ram:us-west-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
```

Salida:

```
{
```

```
    "resources": [
        {
            "arn": "aarn:aws:ec2:us-west-2:123456789012:subnet/
subnet-0250c25a1f4e15235",
            "type": "ec2:Subnet",
            "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
            "creationTime": 1565301545.023,
            "lastUpdatedTime": 1565301545.947
        }
    ]
}
```

- Para obtener más información sobre la API, consulte ListResources en la Referencia de comandos de la AWS CLI.

`promote-resource-share-created-from-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `promote-resource-share-created-from-policy`.

AWS CLI

Para promover un recurso compartido basado en políticas de recursos con el objetivo de lograr una funcionalidad completa en AWS RAM

El siguiente ejemplo de `promote-resource-share-created-from-policy` toma un recurso compartido que usted ha creado implícitamente al adjuntar una política basada en recursos y lo convierte para que sea completamente funcional con la consola AWS RAM y sus operaciones de CLI y API.

```
aws ram promote-resource-share-created-from-policy \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/91fa8429-2d06-4032-909a-90909EXAMPLE
```

Salida:

```
{
    "returnValue": true
}
```

- Para obtener información sobre la API, consulte PromoteResourceShareCreatedFromPolicy en la Referencia de comandos de la AWS CLI.

`reject-resource-share-invitation`

En el siguiente ejemplo de código, se muestra cómo utilizar `reject-resource-share-invitation`.

AWS CLI

Para rechazar una invitación de un recurso compartido

En el siguiente ejemplo de `reject-resource-share-invitation`, se rechaza la invitación de un recurso compartido especificado.

```
aws ram reject-resource-share-invitation \
    --resource-share-invitation-arn arn:aws:ram:us-west-2:111111111111:resource-share-invitation/32b639f0-14b8-7e8f-55ea-e6117EXAMPLE
```

Salida:

```
"resourceShareInvitations": [
    {
        "resourceShareInvitationArn": "arn:aws:ram:us-west2-1:111111111111:resource-share-invitation/32b639f0-14b8-7e8f-55ea-e6117EXAMPLE",
        "resourceShareName": "project-resource-share",
        "resourceShareArn": "arn:aws:ram:us-west-2:111111111111:resource-share/fcb639f0-1449-4744-35bc-a983fEXAMPLE",
        "senderAccountId": "111111111111",
        "receiverAccountId": "222222222222",
        "invitationTimestamp": 1565319592.463,
        "status": "REJECTED"
    }
]
```

- Para obtener información sobre la API, consulte RejectResourceShareInvitation en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para agregar etiquetas a un recurso compartido

En el siguiente ejemplo de `tag-resource`, se agrega una clave de etiqueta de `project` y un valor `lima` asociado al recurso compartido especificado.

```
aws ram tag-resource \
    --tags key=project,value=lima \
    --resource-share-arn arn:aws:ram:us-west-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar etiquetas de un recurso compartido

En el siguiente ejemplo de `untag-resource`, se elimina la clave de etiqueta `project` y su valor asociado desde el recurso compartido especificado.

```
aws ram untag-resource \
    --tag-keys project \
    --resource-share-arn arn:aws:ram:us-west-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-resource-share`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-resource-share`.

AWS CLI

Para actualizar un recurso compartido

En el siguiente ejemplo de `update-resource-share`, se cambia el recurso compartido especificado para permitir el acceso a las entidades principales externas que no estén en una organización AWS.

```
aws ram update-resource-share \
    --allow-external-principals \
    --resource-share-arn arn:aws:ram:us-west-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
```

Salida:

```
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "name": "my-resource-share",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": 1565295733.282,
        "lastUpdatedTime": 1565303080.023
    }
}
```

- Para obtener información sobre la API, consulte UpdateResourceShare en la Referencia de comandos de la AWS CLI.

Ejemplos de Resource Explorer que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando la AWS Command Line Interface con Resource Explorer.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-default-view`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-default-view`.

AWS CLI

Para configurar una vista de Resource Explorer como predeterminada para su región de AWS

El siguiente ejemplo de `associate-default-view` establece una vista, según lo especificado por su ARN, como la vista predeterminada de la región de AWS en la que se llama a la operación.

```
aws resource-explorer-2 associate-default-view \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-Main-View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111
```

Salida:

```
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-Main-View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111"
}
```

Para obtener más información, consulte Setting a default view in an AWS Region en la Guía del usuario de AWS Resource Explorer.

- Para obtener información sobre la API, consulte AssociateDefaultView en la Referencia de comandos de la AWS CLI.

`batch-get-view`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-view`.

AWS CLI

Para recuperar detalles sobre varias vistas del Resource Explorer

En el siguiente ejemplo de `batch-get-view`, se muestran los detalles de dos vistas especificadas por sus ARN. Utilice espacios para separar los múltiples ARN en el parámetro --view-arn.

```
aws resource-explorer-2 batch-get-view \
    --view-arns arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-EC2-Only-View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE22222, \
                arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-Main-View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111
```

Salida:

```
{
    "Views": [
        {
            "Filters": {
                "FilterString": "service:ec2"
            },
            "IncludedProperties": [
                {
                    "Name": "tags"
                }
            ],
            "LastUpdatedAt": "2022-07-13T21:33:45.249000+00:00",
            "Owner": "123456789012",
            "Scope": "arn:aws:iam::123456789012:root",
            "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-EC2-Only-View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE22222"
        },
        {
            "Filters": {
                "FilterString": ""
            },
            "IncludedProperties": [
                {
                    "Name": "tags"
                }
            ],
            "LastUpdatedAt": "2022-07-13T20:34:11.314000+00:00",
```

```
            "Owner": "123456789012",
            "Scope": "arn:aws:iam::123456789012:root",
            "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-
Main-View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111"
        }
    ]
    "Errors": []
}
```

Para obtener más información sobre las vistas, consulte About Resource Explorer views en la Guía del usuario de AWS Resource Explorer.

- Para obtener información de la API, consulte BatchGetView en la Referencia de comandos de la AWS CLI.

`create-index`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-index`.

AWS CLI

Para activar Resource Explorer en una región de AWS al crear un índice

El siguiente ejemplo de `create-index` crea un índice local en la región de AWS en la que se llama a la operación. La CLI de AWS genera automáticamente un valor de parámetro `client-token` aleatorio y lo incluye en la llamada a AWS si no se especifica un valor.

```
aws resource-explorer-2 create-index \
    --region us-east-1
```

Salida:

```
{
    "Arn": "arn:aws:resource-explorer-2:us-east-1:123456789012:index/EXAMPLE8-90ab-
cdef-fedc-EXAMPLE22222c",
    "CreatedAt": "2022-11-01T20:00:59.149Z",
    "State": "CREATING"
}
```

Tras crear un índice local, puede convertirlo en el índice agregador de la cuenta ejecutando el comando update-index-type.

Para más información, consulte Turning on Resource Explorer in an AWS Region to index your resources en la Guía del usuario de AWS Resource Explorer.

- Para obtener información sobre la API, consulte CreateIndex en la Referencia de comandos de la AWS CLI.

`create-view`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-view`.

AWS CLI

Ejemplo 1: crear una vista sin filtrar del índice de una región de AWS

El siguiente ejemplo de `create-view` crea una vista en la región de AWS especificada que devuelve todos los resultados de la región sin ningún tipo de filtrado. La vista incluye el campo Tags opcional en los resultados devueltos. Como esta vista se crea en la región que contiene el índice agregador, puede incluir los resultados de todas las regiones de la cuenta que contienen un índice de Resource Explorer.

```
aws resource-explorer-2 create-view \
    --view-name My-Main-View \
    --included-properties Name=tags \
    --region us-east-1
```

Salida:

```
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
        ],
        "LastUpdatedAt": "2022-07-13T20:34:11.314000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
        "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-Main-
View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111"
```

```
    }
}
```

Ejemplo 2: crear una vista que devuelva solo los recursos asociados a Amazon EC2

Este `create-view` crea una vista en la región de AWS `us-east-1` que devuelve solo los recursos de la región que están asociados al servicio de Amazon EC2. La vista incluye el campo `Tags` opcional en los resultados devueltos. Como esta vista se crea en la región que contiene el índice agregador, puede incluir los resultados de todas las regiones de la cuenta que contienen un índice de Resource Explorer.

```
aws resource-explorer-2 create-view \
    --view-name My-EC2-Only-View \
    --included-properties Name=tags \
    --filters FilterString="service:ec2" \
    --region us-east-1
```

Salida:

```
{
    "View": {
        "Filters": {
            "FilterString": "service:ec2"
        },
        "IncludedProperties": [
            {
                "Name":"tags"
            }
        ],
        "LastUpdatedAt": "2022-07-13T21:35:09.059Z",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
        "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-EC2-
Only-View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE22222"
    }
}
```

Para obtener más información, consulte Creating views for search en la Guía del usuario de AWS Resource Explorer.

- Para obtener información sobre la API, consulte CreateView en la Referencia de comandos de la AWS CLI.

`delete-index`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-index`.

AWS CLI

Para desactivar Resource Explorer en una región de AWS eliminando su índice

En el siguiente ejemplo de `delete-index`, se elimina el índice de Resource Explorer especificado en la región de AWS en la que se realiza la solicitud.

```
aws resource-explorer-2 delete-index \
    --arn arn:aws:resource-explorer-2:us-west-2:123456789012:index/EXAMPLE8-90ab-cdef-fedc-EXAMPLE22222 \
    --region us-west-2
```

Salida:

```
{
    "Arn": "arn:aws:resource-explorer-2:us-west-2:123456789012:index/EXAMPLE8-90ab-cdef-fedc-EXAMPLE22222",
    "State": "DELETING"
}
```

Para más información, consulte Turning off AWS Resource Explorer in an AWS Region en la Guía del usuario de AWS Resource Explorer.

- Para obtener información sobre la API, consulte DeleteIndex en la Referencia de comandos de la AWS CLI.

`delete-view`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-view`.

AWS CLI

Para eliminar una vista de Resource Explorer

En el siguiente ejemplo de `delete-view`, se elimina una vista especificada por su ARN.

```
aws resource-explorer-2 delete-view \
```

```
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/EC2-Only-
View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111
```

Salida:

```
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/EC2-Only-
View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111"
}
```

Para obtener más información, consulte Deleting views en la Guía del usuario de AWS Resource Explorer.

- Para obtener información sobre la API, consulte DeleteView en la Referencia de comandos de la AWS CLI.

`disassociate-default-view`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-default-view`.

AWS CLI

Para eliminar la vista predeterminada de Resource Explorer de una región de AWS

Este `disassociate-default-view` elimina la vista predeterminada de Resource Explorer de la región de AWS en la que se llama a la operación. Tras realizar esta operación, todas las operaciones de búsqueda de la región deben especificar explícitamente una vista; de lo contrario, la operación fallará.

```
aws resource-explorer-2 disassociate-default-view
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Setting a default view in an AWS Region en la Guía del usuario de AWS Resource Explorer.

- Para obtener más información sobre la API, consulte DisassociateDefaultView en la Referencia de comandos de la AWS CLI.

`get-default-view`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-default-view`.

AWS CLI

Para recuperar una vista de Resource Explorer como predeterminada para su región de AWS

El siguiente ejemplo de `get-default-view` recupera el ARN de la vista que es la predeterminada para la región AWS desde la que llamó a la operación.

```
aws resource-explorer-2 get-default-view
```

Salida:

```
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/default-
view/EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111"
}
```

Para obtener más información, consulte Setting a default view in an AWS Region en la Guía del usuario de AWS Resource Explorer.

- Para obtener información sobre la API, consulte GetDefaultView en la Referencia de comandos de la AWS CLI.

`get-index`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-index`.

AWS CLI

Ejemplo 1: recuperar los detalles de un índice agregador de Resource Explorer

En el siguiente ejemplo de `get-index`, se muestran los detalles del índice de Resource Explorer en la región de AWS especificada. Como la región especificada contiene el índice agregador de la cuenta, el resultado enumera las regiones que replican los datos en el índice de esta región.

```
aws resource-explorer-2 get-index \
    --region us-east-1
```

Salida:

```
{
    "Arn": "arn:aws:resource-explorer-2:us-east-1:123456789012:index/EXAMPLE8-90ab-
cdef-fedc-EXAMPLE11111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [
        "ap-south-1",
        "us-west-2"
    ],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "AGGREGATOR"
}
```

Ejemplo 2: recuperar los detalles de un índice local de Resource Explorer

En el siguiente ejemplo de `get-index`, se muestran los detalles del índice de Resource Explorer en la región de AWS especificada. Como la región especificada contiene un índice local, el resultado muestra la región en la que se replican los datos del índice de esta región.

```
aws resource-explorer-2 get-index \
    --region us-west-2
```

Salida:

```
{
    "Arn": "arn:aws:resource-explorer-2:us-west-2:123456789012:index/EXAMPLE8-90ab-
cdef-fedc-EXAMPLE22222",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingTo": [
        "us-west-2"
    ],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "LOCAL"
}
```

Para obtener más información sobre los índices, consulte Checking which AWS Regions have Resource Explorer turned on en la Guía del usuario de AWS Resource Explorer.

- Para obtener información sobre la API, consulte GetIndex en la Referencia de comandos de la AWS CLI.

`get-view`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-view`.

AWS CLI

Para recuperar detalles sobre una vista del Resource Explorer

En el siguiente ejemplo de `get-view`, se muestran los detalles sobre una vista especificada por sus ARN.

```
aws resource-explorer-2 get-view \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/EC2-Only-View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111
```

Salida:

```
{
  "Tags" : {},
  "View" : {
        "Filters" : {
            "FilterString" : "service:ec2"
        },
        "IncludedProperties" : [
            {
                "Name" : "tags"
            }
        ],
        "LastUpdatedAt" : "2022-07-13T21:33:45.249Z",
        "Owner" : "123456789012",
        "Scope" : "arn:aws:iam::123456789012:root",
        "ViewArn" : "arn:aws:resource-explorer-2:us-east-1:123456789012:view/EC2-Only-View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111"
  }
}
```

Para obtener más información sobre las vistas, consulte About Resource Explorer views en la Guía del usuario de AWS Resource Explorer.

- Para obtener información sobre la API, consulte GetView en la Referencia de comandos de la AWS CLI.

`list-indexes`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-indexes`.

AWS CLI

Para enumerar las regiones de AWS en las que Resource Explorer tiene índices

El siguiente ejemplo de `list-indexes` muestra los índices de todas las regiones en las que Resource Explorer tiene un índice. La respuesta especifica el tipo de cada índice, su región de AWS y su ARN.

```
aws resource-explorer-2 list-indexes
```

Salida:

```
{
    "Indexes": [
        {
            "Arn": "arn:aws:resource-explorer-2:us-west-2:123456789012:index/
EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111",
            "Region": "us-west-2",
            "Type": "AGGREGATOR"
        },
        {
            "Arn": "arn:aws:resource-explorer-2:us-east-1:123456789012:index/
EXAMPLE8-90ab-cdef-fedc-EXAMPLE22222",
            "Region": "us-east-1",
            "Type": "LOCAL"
        },
        {
            "Arn": "arn:aws:resource-explorer-2:us-east-2:123456789012:index/
EXAMPLE8-90ab-cdef-fedc-EXAMPLE33333",
            "Region": "us-east-2",
            "Type": "LOCAL"
        },
        {
            "Arn": "arn:aws:resource-explorer-2:us-west-1:123456789012:index/
EXAMPLE8-90ab-cdef-fedc-EXAMPLE44444",
```

```
            "Region": "us-west-1",
            "Type": "LOCAL"
        }
    ]
}
```

Para obtener más información sobre los índices, consulte Checking which AWS Regions have Resource Explorer turned on en la Guía del usuario de AWS Resource Explorer.

- Para obtener información sobre la API, consulte ListIndexes en la Referencia de comandos de la AWS CLI.

`list-supported-resource-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-supported-resource-types`.

AWS CLI

Para enumerar las regiones de AWS en las que Resource Explorer tiene índices

En el siguiente ejemplo de `list-supported-resource-types`, se enumeran todos los tipos de recursos que actualmente admite &AREXlong;. La respuesta de ejemplo incluye un valor `NextToken` que indica que hay más resultados disponibles para recuperar con llamadas adicionales.

```
aws resource-explorer-2 list-supported-resource-types \
    --max-items 10
```

Salida:

```
{
    "ResourceTypes": [
        {
            "ResourceType": "cloudfront:cache-policy",
            "Service": "cloudfront"
        },
        {
            "ResourceType": "cloudfront:distribution",
            "Service": "cloudfront"
        },
        {
            "ResourceType": "cloudfront:function",
```

```
            "Service": "cloudfront"
        },
        {
            "ResourceType": "cloudfront:origin-access-identity",
            "Service": "cloudfront"
        },
        {
            "ResourceType": "cloudfront:origin-request-policy",
            "Service": "cloudfront"
        },
        {
            "ResourceType": "cloudfront:realtime-log-config",
            "Service": "cloudfront"
        },
        {
            "ResourceType": "cloudfront:response-headers-policy",
            "Service": "cloudfront"
        },
        {
            "ResourceType": "cloudwatch:alarm",
            "Service": "cloudwatch"
        },
        {
            "ResourceType": "cloudwatch:dashboard",
            "Service": "cloudwatch"
        },
        {
            "ResourceType": "cloudwatch:insight-rule",
            "Service": "cloudwatch"
        }
    ],
    "NextToken": "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxMH0="
}
```

Para obtener la siguiente parte del resultado, vuelva a llamar a la operación y use el valor de respuesta `NextToken` de la llamada anterior como el valor de `--starting-token`. Repita el procedimiento hasta que `NextToken` no aparezca en la respuesta.

```
aws resource-explorer-2 list-supported-resource-types \
    --max-items 10  \
    --starting-
token eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxMH0=
```

Salida:


```
{
    "ResourceTypes": [
        {
            "ResourceType": "cloudwatch:metric-stream",
            "Service": "cloudwatch"
        },
        {
            "ResourceType": "dynamodb:table",
            "Service": "dynamodb"
        },
        {
            "ResourceType": "ec2:capacity-reservation",
            "Service": "ec2"
        },
        {
            "ResourceType": "ec2:capacity-reservation-fleet",
            "Service": "ec2"
        },
        {
            "ResourceType": "ec2:client-vpn-endpoint",
            "Service": "ec2"
        },
        {
            "ResourceType": "ec2:customer-gateway",
            "Service": "ec2"
        },
        {
            "ResourceType": "ec2:dedicated-host",
            "Service": "ec2"
        },
        {
            "ResourceType": "ec2:dhcp-options",
            "Service": "ec2"
        },
        {
            "ResourceType": "ec2:egress-only-internet-gateway",
            "Service": "ec2"
        },
        {
            "ResourceType": "ec2:elastic-gpu",
            "Service": "ec2"
        }
```

```
    ],
    "NextToken": "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAyMH0="
}
```

Para obtener más información sobre los índices, consulte Checking which AWS Regions have Resource Explorer turned on en la Guía del usuario de AWS Resource Explorer.

- Para obtener información sobre la API, consulte ListSupportedResourceTypes en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas adjuntas a una vista o índice de Resource Explorer

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran los pares de clave y valor asociados a la vista con el ARN especificado. Debe llamar a la operación desde la región de AWS que contiene el recurso.

```
aws resource-explorer-2 list-tags-for-resource \
    --resource-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111
```

Salida:

```
{
    "Tags": {
        "application": "MainCorpApp",
        "department": "1234"
    }
}
```

Para obtener más información sobre el etiquetado de vistas, consulte Tagging views for access control en la Guía del usuario del AWS Resource Explorer.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-views`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-views`.

AWS CLI

Para enumerar las vistas de Resource Explorer que están disponibles en una región de AWS

En el siguiente ejemplo de `list-views`, se enumeran todas las vistas disponibles en la región en la que se invoca la operación.

```
aws resource-explorer-2 list-views
```

Salida:

```
{
    "Views": [
        "arn:aws:resource-explorer-2:us-east-1:123456789012:view/EC2-Only-View/
EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111",
        "arn:aws:resource-explorer-2:us-east-1:123456789012:view/Default-All-
Resources-View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE22222",
        "arn:aws:resource-explorer-2:us-east-1:123456789012:view/Production-Only-
View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE33333"
    ]
}
```

Para obtener más información sobre las vistas, consulte About Resource Explorer views en la Guía del usuario de AWS Resource Explorer.

- Para obtener información sobre la API, consulte ListViews en la Referencia de comandos de la AWS CLI.

`search`

En el siguiente ejemplo de código, se muestra cómo utilizar `search`.

AWS CLI

Ejemplo 1: buscar mediante la vista predeterminada

En el siguiente ejemplo de `search`, se muestran todos los recursos asociados con el servicio. La búsqueda utiliza la vista predeterminada para la región. La respuesta de ejemplo incluye un

valor `NextToken` que indica que hay más resultados disponibles para recuperar con llamadas adicionales.

```
aws resource-explorer-2 search \
    --query-string "service:iam"
```

Salida:

```
{
    "Count": {
        "Complete": true,
        "TotalResources": 55
    },
    "NextToken":
 "AG9VOEF1KLEXAMPLEOhJHVwo5chEXAMPLER5XiEpNrgsEXAMPLE...b0CmOFOryHEXAMPLE",
    "Resources": [{
        "Arn": "arn:aws:iam::123456789012:policy/service-role/Some-Policy-For-A-
Service-Role",
        "LastReportedAt": "2022-07-21T12:34:42Z",
        "OwningAccountId": "123456789012",
        "Properties": [],
        "Region": "global",
        "ResourceType": "iam:policy",
        "Service": "iam"
    }, {
        "Arn": "arn:aws:iam::123456789012:policy/service-role/Another-Policy-For-A-
Service-Role",
        "LastReportedAt": "2022-07-21T12:34:42Z",
        "OwningAccountId": "123456789012",
        "Properties": [],
        "Region": "global",
        "ResourceType": "iam:policy",
        "Service": "iam"
    }, {
       ... TRUNCATED FOR BREVITY ...
    }],
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/my-default-
view/EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111"
}
```

Ejemplo 2: buscar mediante una vista específica

El siguiente ejemplo de `search` de búsqueda muestra todos los recursos (*) de la región de AWS especificada que están visibles a través de la vista especificada. Los resultados incluyen solo los recursos asociados a Amazon EC2 debido a los filtros adjuntos a la vista.

```
aws resource-explorer-2 search \
    -- query-string "*" \
    -- view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-EC2-view/
EXAMPLE8-90ab-cdef-fedc-EXAMPLE22222
```

Salida:

```
HTTP/1.1 200 OK
Date: Tue, 01 Nov 2022 20:00:59 GMT
Content-Type: application/json
Content-Length: <PayloadSizeBytes>

    {
        "Count": {
            "Complete": true,
            "TotalResources": 67
        },
        "Resources": [{
            "Arn": "arn:aws:ec2:us-east-1:123456789012:network-acl/acl-1a2b3c4d",
            "LastReportedAt": "2022-07-21T18:52:02Z",
            "OwningAccountId": "123456789012",
            "Properties": [{
                "Data": [{
                    "Key": "Department",
                    "Value": "AppDevelopment"
                }, {
                    "Key": "Environment",
                    "Value": "Production"
                }],
                "LastReportedAt": "2021-11-15T14:48:29Z",
                "Name": "tags"
            }],
            "Region": "us-east-1",
            "ResourceType": "ec2:network-acl",
            "Service": "ec2"
        }, {
            "Arn": "arn:aws:ec2:us-east-1:123456789012:subnet/subnet-1a2b3c4d",
            "LastReportedAt": "2022-07-21T21:22:23Z",
            "OwningAccountId": "123456789012",
```

```
            "Properties": [{
                "Data": [{
                    "Key": "Department",
                    "Value": "AppDevelopment"
                }, {
                    "Key": "Environment",
                    "Value": "Production"
                }],
                "LastReportedAt": "2021-07-29T19:02:39Z",
                "Name": "tags"
            }],
            "Region": "us-east-1",
            "ResourceType": "ec2:subnet",
            "Service": "ec2"
        }, {
            "Arn": "arn:aws:ec2:us-east-1:123456789012:dhcp-options/dopt-1a2b3c4d",
            "LastReportedAt": "2022-07-21T06:08:53Z",
            "OwningAccountId": "123456789012",
            "Properties": [{
                "Data": [{
                    "Key": "Department",
                    "Value": "AppDevelopment"
                }, {
                    "Key": "Environment",
                    "Value": "Production"
                }],
                "LastReportedAt": "2021-11-15T15:11:05Z",
                "Name": "tags"
            }],
            "Region": "us-east-1",
            "ResourceType": "ec2:dhcpoptions",
            "Service": "ec2"
        }, {
            ... TRUNCATED FOR BREVITY ...
        }],
        "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-EC2-
view/EXAMPLE8-90ab-cdef-fedc-EXAMPLE22222"
    }
```

Para obtener más información, consulte Using AWS Resource Explorer to search for resources en la Guía de recursos de AWS Resource Explorer.

- Para obtener información sobre la API, consulte Search en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para eliminar una vista de Resource Explorer

En el siguiente ejemplo de `tag-resource`, se agrega la clave de etiqueta environment con el valor production a la vista con el ARN especificado.

```
aws resource-explorer-2 tag-resource \
    --resource-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-View//
EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111 \
    --tags environment=production
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging views for access control en la Guía del usuario de AWS Resource Explorer.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar una etiqueta de una vista de Resource Explorer

El siguiente ejemplo de `untag-resource` elimina las etiquetas con la nombre de clave environment de la vista con el ARN especificado.

```
aws resource-explorer-2 untag-resource \
    --resource-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-View//
EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111 \
    --tag-keys environment
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging views for access control en la Guía del usuario de AWS Resource Explorer.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-index-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-index-type`.

AWS CLI

Para cambiar el tipo de índice de Resource Explorer

En el siguiente ejemplo de `update-index-type`, se convierte el índice especificado de un tipo `local` a otro tipo `aggregator` para activar la posibilidad de buscar recursos en todas las regiones de AWS de la cuenta. Debe enviar la solicitud a la región de AWS que contiene el índice que desea actualizar.

```
aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-east-1:123456789012:index/EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111 \
    --type aggregator \
    --region us-east-1
```

Salida:

```
{
    "Arn":"arn:aws:resource-explorer-2:us-east-1:123456789012:index/EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111",
    "LastUpdatedAt":"2022-07-13T18:41:58.799Z",
    "State":"updating",
    "Type":"aggregator"
}
```

Para obtener información sobre cambiar un tipo de índice, consulte Turning on cross-Region search by creating an aggregator index en la Guía del usuario de AWS Resource Explorer.

- Para obtener información sobre la API, consulte UpdateIndexType en la Referencia de comandos de la AWS CLI.

update-view

En el siguiente ejemplo de código, se muestra cómo utilizar `update-view`.

AWS CLI

Ejemplo 1: actualizar el campo IncludedProperties para una vista de Resource Explorer

En el siguiente ejemplo de `update-view`, se actualiza la vista especificada agregando `` `tags` `` a la opcional `` `IncludedProperties` ``. Tras ejecutar esta operación, las operaciones de búsqueda que utilizan esta vista incluyen información sobre las etiquetas asociadas a los recursos que aparecen en los resultados.

```
aws resource-explorer-2 update-view \
    --included-properties Name=tags \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-View/
EXAMPLE8-90ab-cdef-fedc-EXAMPLE22222
```

Salida:

```
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
        ],
        "LastUpdatedAt": "2022-07-19T17:41:21.710000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
        "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-EC2-
Only-View/EXAMPLE8-90ab-cdef-fedc-EXAMPLE11111"
    }
}
```

Ejemplo 2: actualizar los filtros adjuntos a una vista

En el siguiente ejemplo de `update-view`, se actualiza la vista especificada para utilizar un filtro que limite los resultados únicamente a los tipos de recursos asociados al servicio Amazon EC2.

```
aws resource-explorer-2 update-view \
    --filters FilterString="service:ec2" \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-View/
EXAMPLE8-90ab-cdef-fedc-EXAMPLE22222
```

Salida:

```
{
    "View": {
    "Filters": {
        "FilterString": "service:ec2"
    },
    "IncludedProperties": [],
    "LastUpdatedAt": "2022-07-19T17:41:21.710000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
        "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-View/
EXAMPLE8-90ab-cdef-fedc-EXAMPLE22222"
    }
}
```

Para obtener más información sobre las vistas, consulte About Resource Explorer views en la Guía del usuario de AWS Resource Explorer.

- Para obtener información sobre la API, consulte UpdateView en la Referencia de comandos de la AWS CLI.

Ejemplos de Resource Groups que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando la AWS Command Line Interface con Resource Groups.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-group`.

AWS CLI

Ejemplo 1: crear un grupo de recursos basado en etiquetas

En el siguiente ejemplo de `create-group`, se crea un grupo de recursos basado en etiquetas de instancias de Amazon EC2 de la región actual. Se basa en una consulta de recursos que están etiquetados con la clave `Name` y el valor `WebServers`. El nombre del grupo es `tbq-WebServer`. La consulta se encuentra en un archivo JSON independiente que se pasa al comando.

```
aws resource-groups create-group \
    --name tbq-WebServer \
    --resource-query file://query.json
```

Contenido de `query.json`:

```
{
    "Type": "TAG_FILTERS_1_0",
    "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"Name\", \"Values\":[\"WebServers\"]}]}"
}
```

Salida:

```
{
    "Group": {
        "GroupArn": "arn:aws:resource-groups:us-west-2:123456789012:group/tbq-
WebServer",
        "Name": "tbq-WebServer"
    },
    "ResourceQuery": {
        "Type": "TAG_FILTERS_1_0",
        "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"Name\", \"Values\":[\"WebServers\"]}]}"
    }
}
```

Ejemplo 2: crear un grupo de recursos basado en la pila de CloudFormation

En el siguiente ejemplo de `create-group`, se crea un grupo de recursos basado en una pila de AWS CloudFormation denominado `sampleCFNstackgroup`. La consulta incluye todos los recursos de la pila de CloudFormation especificada que son compatibles con AWS Resource Groups.

```
aws resource-groups create-group \
    --name cbq-CFNstackgroup \
    --resource-query file://query.json
```

Contenido de `query.json`:

```
{
    "Type": "CLOUDFORMATION_STACK_1_0",
    "Query": "{\"ResourceTypeFilters\":[\"AWS::AllSupported\"],\"StackIdentifier
\":\"arn:aws:cloudformation:us-west-2:123456789012:stack/MyCFNStack/1415z9z0-
z39z-11z8-97z5-500z212zz6fz\"}"
}
```

Salida:

```
{
    "Group": {
        "GroupArn": "arn:aws:resource-groups:us-west-2:123456789012:group/cbq-
CFNstackgroup",
        "Name": "cbq-CFNstackgroup"
    },
    "ResourceQuery": {
        "Type": "CLOUDFORMATION_STACK_1_0",
        "Query": "{\"ResourceTypeFilters\":[\"AWS::AllSupported\"],\"StackIdentifier
\":\"arn:aws:cloudformation:us-east-2:123456789012:stack/MyCFNStack/1415z9z0-
z39z-11z8-97z5-500z212zz6fz\"}"}'
    }
}
```

Para obtener más información, consulte Create Groups en la Guía del usuario de AWS Resource Groups.

- Para obtener información sobre la API, consulte CreateGroup en la Referencia de comandos de la AWS CLI.

`delete-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-group`.

AWS CLI

Para actualizar la descripción de un grupo de recursos

En el siguiente ejemplo de `delete-group`, se actualiza el grupo de recurso especificado.

```
aws resource-groups delete-group \
    --group-name tbq-WebServer
```

Salida:

```
{
    "Group": {
        "GroupArn": "arn:aws:resource-groups:us-west-2:1234567890:group/tbq-
WebServer",
        "Name": "tbq-WebServer"
    }
}
```

Para obtener más información, consulte Delete Groups en la Guía del usuario de AWS Resource Groups.

- Para obtener información sobre la API, consulte DeleteGroup en la Referencia de comandos de la AWS CLI.

`get-group-query`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-group-query`.

AWS CLI

Para asociar la consulta a un grupo de recursos

En el siguiente ejemplo de `get-group-query`, se muestra la consulta asociada al grupo de recursos especificado.

```
aws resource-groups get-group-query \
    --group-name tbq-WebServer
```

Salida:

```
{
    "GroupQuery": {
        "GroupName": "tbq-WebServer",
        "ResourceQuery": {
            "Type": "TAG_FILTERS_1_0",
            "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters
\":[{\"Key\":\"Name\", \"Values\":[\"WebServers\"]}]}"
        }
    }
}
```

- Para obtener información sobre la API, consulte GetGroupQuery en la Referencia de comandos de la AWS CLI.

`get-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-group`.

AWS CLI

Para obtener información sobre un grupo de recursos

En el siguiente ejemplo de `get-group`, se muestran los detalles sobre el grupo de recursos especificado. Para adjuntar la consulta al grupo, utilice `get-group-query`.

```
aws resource-groups get-group \
    --group-name tbq-WebServer
```

Salida:

```
{
    "Group": {
        "GroupArn": "arn:aws:resource-groups:us-west-2:123456789012:group/tbq-
WebServer",
        "Name": "tbq-WebServer",
        "Description": "A tag-based query resource group of WebServers."
    }
}
```

- Para obtener información sobre la API, consulte GetGroup en la Referencia de comandos de la AWS CLI.

`get-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-tags`.

AWS CLI

Para recuperar las etiquetas adjuntas a un grupo de recursos

En el siguiente ejemplo de `get-tags`, se muestran los pares de claves y valores de etiquetas asociados al grupo de recursos especificado (el grupo en sí, no sus miembros).

```
aws resource-groups get-tags \
    --arn arn:aws:resource-groups:us-west-2:123456789012:group/tbq-WebServer
```

Salida:

```
{
    "Arn": "arn:aws:resource-groups:us-west-2:123456789012:group/tbq-WebServer",
    "Tags": {
        "QueryType": "tags",
        "QueryResources": "ec2-instances"
    }
}
```

- Para obtener detalles sobre la API, consulte GetTags en la Referencia de comandos de la AWS CLI.

`list-group-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-group-resources`.

AWS CLI

Para enumerar todos los recursos de un grupo de recursos

Ejemplo 1: en el siguiente ejemplo de `list-resource-groups`, se enumeran todos los recursos que forman parte del grupo de recursos especificado.

```
aws resource-groups list-group-resources \
    --group-name tbq-WebServer
```

Salida:

```
{
    "ResourceIdentifiers": [
        {
            "ResourceArn": "arn:aws:ec2:us-west-2:123456789012:instance/
i-09f77fa38c12345ab",
            "ResourceType": "AWS::EC2::Instance"
        }
    ]
}
```

Ejemplo 2: en el siguiente ejemplo se enumeran todos los recursos del grupo que también tienen un resource-type AWS::EC2::Instance.

aws resource-groups list-group-resources --group-name tbq-WebServer --filters Name=resource-type,Values=AWS::EC2::Instance

- Para obtener información sobre la API, consulte ListGroupResources en la Referencia de comandos de la AWS CLI.

`list-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-groups`.

AWS CLI

Para enumerar los grupos de recursos disponibles

En el siguiente ejemplo de `list-groups`, se muestra una lista de todos los grupos de recursos.

```
aws resource-groups list-groups
```

Salida:

```
{
    "GroupIdentifiers": [
        {
```

```
            "GroupName": "tbq-WebServer",
            "GroupArn": "arn:aws:resource-groups:us-west-2:123456789012:group/tbq-
WebServer3"
        },
        {
            "GroupName": "cbq-CFNStackQuery",
            "GroupArn": "arn:aws:resource-groups:us-west-2:123456789012:group/cbq-
CFNStackQuery"
        }
    ],
    "Groups": [
        {
            "GroupArn": "arn:aws:resource-groups:us-west-2:123456789012:group/tbq-
WebServer",
            "Name": "tbq-WebServer"
        },
        {
            "GroupArn": "arn:aws:resource-groups:us-west-2:123456789012:group/cbq-
CFNStackQuery",
            "Name": "cbq-CFNStackQuery"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListGroups en la Referencia de comandos de la AWS CLI.

`list-resource-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-groups`.

AWS CLI

Para enumerar todos los recursos de un grupo de recursos

En el siguiente ejemplo de `list-resource-groups`, se enumeran todos los recursos que forman parte del grupo de recursos especificado.

```
aws resource-groups list-group-resources \
    --group-name tbq-WebServer
```

Salida:

```
{
    "ResourceIdentifiers": [
        {
            "ResourceArn": "arn:aws:ec2:us-west-2:123456789012:instance/
i-09f77fa38c12345ab",
            "ResourceType": "AWS::EC2::Instance"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListResourceGroups en la Referencia de comandos de la AWS CLI.

`put-group-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-group-configuration`.

AWS CLI

Para asociar una configuración de servicio a un grupo de recursos

Ejemplo 1: el siguiente ejemplo de `put-group-configuration` especifica que el grupo de recursos debe contener únicamente reservas de capacidad de Amazon EC2 para las instancias de las familias `C5` o `M5`.

```
aws resource-groups put-group-configuration \
    --group MyTestGroup \
    --configuration file://config.json
```

Contenido de `config.json`:

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "allowed-host-families",
                "Values": [ "c5", "m5" ]
            },
                {
                    "Name": "any-host-based-license-configuration",
                    "Values": [ "true" ]
```

```
                }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::Host" ]
            },
            {
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
]
```

Este comando no genera ninguna salida si se realiza correctamente.

Para obtener más información, consulte Service configurations for resource groups en la Guía de referencia de la API de Resource Groups.

- Para obtener información sobre la API, consulte PutGroupConfiguration en la Referencia de comandos de la AWS CLI.

`search-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-resources`.

AWS CLI

Para encontrar recursos que coincidan con una consulta

El siguiente ejemplo de `search-resources` recupera una lista de todos los recursos AWS que coinciden con la consulta especificada.

```
aws resource-groups search-resources \
    --resource-query file://query.json
```

Contenido de `query.json`:

```
{
```

```
    "Type": "TAG_FILTERS_1_0",
    "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"Patch Group\", \"Values\":[\"Dev\"]}]}"
}
```

Salida:

```
{
    "ResourceIdentifiers": [
        {
            "ResourceArn": "arn:aws:ec2:us-west-2:123456789012:instance/
i-01a23bc45d67890ef",
            "ResourceType": "AWS::EC2::Instance"
        }
    ]
}
```

- Para obtener información sobre la API, consulte SearchResources en la Referencia de comandos de la AWS CLI.

`tag`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag`.

AWS CLI

Para asociar una etiqueta a un grupo de recursos

En el siguiente ejemplo de `tag`, se asocian los pares de claves y valores de etiquetas especificados al grupo de recursos especificado (al grupo en sí, no a sus miembros).

```
aws resource-groups tag \
    --tags QueryType=tags,QueryResources=ec2-instances \
    --arn arn:aws:resource-groups:us-west-2:128716708097:group/tbq-WebServer
```

Salida:

```
{
    "Arn": "arn:aws:resource-groups:us-west-2:128716708097:group/tbq-WebServer",
    "Tags": {
        "QueryType": "tags",
        "QueryResources": "ec2-instances"
```

```
    }
}
```

Para obtener más información, consulte el Manage tags en la Guía del usuario de AWS Resource Groups.

- Para obtener información sobre la API, consulte Tag en la Referencia de comandos de la AWS CLI.

`untag`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag`.

AWS CLI

Cómo eliminar etiquetas de un grupo de recursos

El siguiente ejemplo de `untags` elimina cualquier etiqueta con la clave especificada del propio grupo de recursos, no de sus miembros.

```
aws resource-groups untag \
    --arn arn:aws:resource-groups:us-west-2:123456789012:group/tbq-WebServer \
    --keys QueryType
```

Salida:

```
{
    "Arn": "arn:aws:resource-groups:us-west-2:123456789012:group/tbq-WebServer",
    "Keys": [
        "QueryType"
    ]
}
```

Para obtener más información, consulte el Manage tags en la Guía del usuario de AWS Resource Groups.

- Para obtener información sobre la API, consulte Untag en la Referencia de comandos de la AWS CLI.

`update-group-query`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-group-query`.

AWS CLI

Ejemplo 1: actualizar la consulta de un grupo de recursos basado en etiquetas

En el siguiente ejemplo de `update-group-query`, se actualiza la consulta asociada al grupo de recursos basado en etiquetas especificado.

```
aws resource-groups update-group-query \
    --group-name tbq-WebServer \
    --resource-query '{"Type":"TAG_FILTERS_1_0", "Query":"{\"ResourceTypeFilters\":
[\"AWS::EC2::Instance\"],\"TagFilters\":[{\"Key\":\"Name\", \"Values\":[\"WebServers
\"]}]}"}'
```

Salida:

```
{
    "Group": {
        "GroupArn": "arn:aws:resource-groups:us-east-2:123456789012:group/tbq-
WebServer",
        "Name": "tbq-WebServer"
    },
    "ResourceQuery": {
        "Type": "TAG_FILTERS_1_0",
        "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"Name\", \"Values\":[\"WebServers\"]}]}"
    }
}
```

Para obtener más información, consulte Update Groups en la Guía del usuario de AWS Resource Groups.

Ejemplo 2: actualizar la consulta para un grupo de recursos basado en la pila de CloudFormation

En el siguiente ejemplo de `update-group-query`, se actualiza la consulta asociada al grupo de recursos basado en la pila de AWS CloudFormation especificada.

```
aws resource-groups update-group-query \
    --group-name cbq-CFNstackgroup \
    --resource-query '{"Type": "CLOUDFORMATION_STACK_1_0", "Query":
 "{\"ResourceTypeFilters\":[\"AWS::AllSupported\"],\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:123456789012:stack/MyCFNStack/1415z9z0-
z39z-11z8-97z5-500z212zz6fz\"}"}'
```

Salida:

```
{
    "Group": {
        "GroupArn": "arn:aws:resource-groups:us-west-2:123456789012:group/cbq-
CFNstackgroup",
        "Name": "cbq-CFNstackgroup"
    },
    "ResourceQuery": {
        "Type": "CLOUDFORMATION_STACK_1_0",
        "Query": "{\"ResourceTypeFilters\":[\"AWS::AllSupported\"],\"StackIdentifier
\":\"arn:aws:cloudformation:us-west-2:123456789012:stack/MyCFNStack/1415z9z0-
z39z-11z8-97z5-500z212zz6fz\"}"
    }
}
```

Para obtener más información, consulte Update Groups en la Guía del usuario de AWS Resource Groups.

- Para obtener información sobre la API, consulte UpdateGroupQuery en la Referencia de comandos de la AWS CLI.

`update-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-group`.

AWS CLI

Para actualizar la descripción de un grupo de recursos

En el siguiente ejemplo de `update-group`, se actualiza la descripción del grupo de recursos especificado.

```
aws resource-groups update-group \
    --group-name tbq-WebServer \
    --description "Resource group for all web server resources."
```

Salida:

```
{
    "Group": {
```

```
        "GroupArn": "arn:aws:resource-groups:us-west-2:123456789012:group/tbq-
WebServer",
        "Name": "tbq-WebServer"
        "Description": "Resource group for all web server resources."
    }
}
```

Para obtener más información, consulte Update Groups en la Guía del usuario de AWS Resource Groups.

- Para obtener información sobre la API, consulte UpdateGroup en la Referencia de comandos de la AWS CLI.

Ejemplos de la API para Resource Groups Tagging que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo llevar a cabo acciones e implementar escenarios comunes mediante la AWS Command Line Interface con el API de Resource Groups Tagging.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`get-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resources`.

AWS CLI

Para obtener una lista de recursos etiquetados

En el siguiente ejemplo de `get-resources`, se muestra una lista de los recursos de la cuenta que están etiquetados con el nombre y el valor clave especificados.

```
aws resourcegroupstaggingapi get-resources \
    --tag-filters Key=Environment,Values=Production \
    --tags-per-page 100
```

Salida:

```
{
    "ResourceTagMappingList": [
        {
            "ResourceARN": " arn:aws:inspector:us-west-2:123456789012:target/0-
nvgVhaxX/template/0-7sbz2Kz0",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte GetResources en la Referencia de la API de Resource Groups Tagging.

- Para obtener detalles sobre la API, consulte GetResources en la Referencia de comandos de la AWS CLI.

`get-tag-keys`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-tag-keys`.

AWS CLI

Para obtener una lista de todas las claves de etiqueta

En el siguiente ejemplo de `get-tag-keys` se recupera la lista de todos los nombres de las claves de etiqueta que utilizan los recursos de la cuenta.

```
aws resourcegroupstaggingapi get-tag-keys
```

Salida:

```
{
    "TagKeys": [
        "Environment",
        "CostCenter",
        "Department"
    ]
}
```

Para obtener más información, consulte GetTagKeys en la Referencia de la API de Resource Groups Tagging.

- Para obtener información sobre la API, consulte GetTagKeys en la Referencia de comandos de la AWS CLI.

`get-tag-values`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-tag-values`.

AWS CLI

Para obtener una lista de todos los valores de etiqueta

En el ejemplo siguiente de `get-tag-values`, se muestran todos los valores utilizados para la clave especificada de todos los recursos del

```
aws resourcegroupstaggingapi get-tag-values \
    --key=Environment
```

Salida:

```
{
    "TagValues": [
        "Alpha",
        "Gamma",
        "Production"
    ]
}
```

Para obtener más información, consulte GetTagValues en la Referencia de la API de Resource Groups Tagging.

- Para obtener información sobre la API, consulte GetTagValues en la Referencia de comandos de la AWS CLI.

`tag-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resources`.

AWS CLI

Para asociar una etiqueta a un recurso

El siguiente ejemplo de `tag-resources` etiqueta el recurso especificado con un nombre y un valor clave.

```
aws resourcegroupstaggingapi tag-resources \
    --resource-arn-list arn:aws:s3:::MyProductionBucket \
    --tags Environment=Production,CostCenter=1234
```

Salida:

```
{
    "FailedResourcesMap": {}
}
```

Para obtener más información, consulte TagResources en la Referencia de la API de Resource Groups Tagging.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resources`.

AWS CLI

Para eliminar una etiqueta de un recurso

El siguiente ejemplo de `untag-resources` elimina las claves de etiqueta especificadas y cualquier valor asociado de un recurso especificado.

```
aws resourcegroupstaggingapi untag-resources \
    --resource-arn-list arn:aws:s3:::amzn-s3-demo-bucket \
    --tag-keys Environment CostCenter
```

Salida:

```
{
    "FailedResourcesMap": {}
}
```

Para obtener más información, consulte UntagResources en la Referencia de la API de Resource Groups Tagging.

- Para obtener información sobre la API, consulte UntagResources en la Referencia de comandos de la AWS CLI.

Ejemplos de Route 53 que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Route 53.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`change-resource-record-sets`

En el siguiente ejemplo de código, se muestra cómo utilizar `change-resource-record-sets`.

AWS CLI

Para crear, actualizar o eliminar un conjunto de registros de recursos

El siguiente comando `change-resource-record-sets` crea un conjunto de registros de recursos mediante `hosted-zone-id` `Z1R8UBAEXAMPLE` y la configuración con formato JSON del archivo `C:\awscli\route53\change-resource-record-sets.json`:

```
aws route53 change-resource-record-sets --hosted-zone-id Z1R8UBAEXAMPLE --change-batch file://C:\awscli\route53\change-resource-record-sets.json
```

Para obtener más información, consulte POST ChangeResourceRecordSets en la Referencia de la API de Amazon Route 53.

La configuración del archivo JSON depende del tipo de conjunto de registros de recursos que quiera crear:

BasicWeightedAliasWeighted AliasLatencyLatency AliasFailoverFailover Alias

Sintaxis básica:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ]
      }
    },
    {...}
  ]
}
```

Sintaxis ponderada:

```
{
  "Comment": "optional comment about the changes in this change batch request",
```

```
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Weight": value between 0 and 255,
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

Sintaxis de alias:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution, Amazon
 S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
```

```
    {...}
  ]
}
```

Sintaxis de alias ponderada:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Weight": value between 0 and 255,
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution, Amazon
 S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

Sintaxis de latencia:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Region": "Amazon EC2 region name",
```

```
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

Sintaxis de alias de latencia:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Region": "Amazon EC2 region name",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution, Amazon
 S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

Sintaxis de conmutación por error:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Failover": "PRIMARY" | "SECONDARY",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

Sintaxis del alias de conmutación por error:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Failover": "PRIMARY" | "SECONDARY",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution, Amazon
 S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
```

```
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

- Para obtener información sobre de la API, consulte ChangeResourceRecordSets en la Referencia de comandos de la AWS CLI.

`change-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `change-tags-for-resource`.

AWS CLI

El siguiente comando agrega una etiqueta denominada `owner` a un recurso de verificación de estado identificado con el ID:

```
aws route53 change-tags-for-resource --resource-type healthcheck --resource-
id 6233434j-18c1-34433-ba8e-3443434 --add-tags Key=owner,Value=myboss
```

El siguiente comando elimina una etiqueta denominada `owner` de un recurso de zona alojada identificada con el ID:

```
aws route53 change-tags-for-resource --resource-type hostedzone --resource-
id Z1523434445 --remove-tag-keys owner
```

- Para obtener detalles de la API, consulte ChangeTagsForResource en la Referencia de comandos de la AWS CLI.

`create-health-check`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-health-check`.

AWS CLI

Para crear una comprobación de estado

El siguiente comando `create-health-check` crea una comprobación de estado con la referencia de la persona que llama `2014-04-01-18:47` y la configuración con formato JSON del archivo `C:\awscli\route53\create-health-check.json`:

```
aws route53 create-health-check --caller-reference 2014-04-01-18:47 --health-check-config file://C:\awscli\route53\create-health-check.json
```

Sintaxis de JSON:

```
{
  "IPAddress": "IP address of the endpoint to check",
  "Port": port on the endpoint to check--required when Type is "TCP",
  "Type": "HTTP"|"HTTPS"|"HTTP_STR_MATCH"|"HTTPS_STR_MATCH"|"TCP",
  "ResourcePath": "path of the file that you want Amazon Route 53 to request--all
 Types except TCP",
  "FullyQualifiedDomainName": "domain name of the endpoint to check--all Types
 except TCP",
  "SearchString": "if Type is HTTP_STR_MATCH or HTTPS_STR_MATCH, the string to
 search for in the response body from the specified resource",
  "RequestInterval": 10 | 30,
  "FailureThreshold": integer between 1 and 10
}
```

Para añadir la comprobación de estado a un conjunto de registros de recursos de Route 53, utilice el comando `change-resource-record-sets`.

Para obtener más información, consulte Amazon Route 53 Health Checks and DNS Failover en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte CreateHealthCheck en la Referencia de comandos de la AWS CLI.

`create-hosted-zone`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-hosted-zone`.

AWS CLI

Para crear una zona alojada

El siguiente comando `create-hosted-zone` agrega una zona alojada denominada `example.com` mediante la referencia de intermediario `2014-04-01-18:47`. El comentario opcional incluye un espacio, por lo que debe escribirse entre comillas:

```
aws route53 create-hosted-zone --name example.com --caller-
reference 2014-04-01-18:47 --hosted-zone-config Comment="command-line version"
```

Para obtener más información, consulte Working with Hosted Zones en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte CreateHostedZone en la Referencia de comandos de la AWS CLI.

`delete-health-check`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-health-check`.

AWS CLI

Para eliminar una comprobación de estado

El siguiente comando `delete-health-check` elimina la comprobación de estado con el `health-check-id` `e75b48d9-547a-4c3d-88a5-ae4002397608`:

```
aws route53 delete-health-check --health-check-id e75b48d9-547a-4c3d-88a5-
ae4002397608
```

- Para obtener información sobre la API, consulte DeleteHealthCheck en la Referencia de comandos de la AWS CLI.

`delete-hosted-zone`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-hosted-zone`.

AWS CLI

Para eliminar una zona alojada

El siguiente comando `delete-hosted-zone` elimina la zona alojada con el `id` `Z36KTIQEXAMPLE`:

```
aws route53 delete-hosted-zone --id Z36KTIQEXAMPLE
```

- Para obtener información sobre la API, consulte DeleteHostedZone en la Referencia de comandos de la AWS CLI.

`get-change`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-change`.

AWS CLI

Para obtener el estado de un cambio en los conjuntos de registros de recursos

El siguiente comando `get-change` obtiene el estado y otra información de la solicitud `change-resource-record-sets` que tiene el `Id` `/change/CWPIK4URU2I5S`:

```
aws route53 get-change --id /change/CWPIK4URU2I5S
```

- Para obtener información sobre la API, consulte GetChange en la Referencia de comandos de AWS CLI.

`get-health-check`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-health-check`.

AWS CLI

Para obtener información acerca de una comprobación de estado

El siguiente `get-health-check` comando obtiene información sobre la comprobación de estado que tiene el `health-check-id` `02ec8401-9879-4259-91fa-04e66d094674`:

```
aws route53 get-health-check --health-check-id 02ec8401-9879-4259-91fa-04e66d094674
```

- Para obtener información sobre la API, consulte GetHealthCheck en la Referencia de comandos de la AWS CLI.

`get-hosted-zone`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-hosted-zone`.

AWS CLI

Para obtener información acerca de una zona alojada

El siguiente comando `get-hosted-zone` obtiene información sobre la zona alojada con un `id` `Z1R8UBAEXAMPLE`:

```
aws route53 get-hosted-zone --id Z1R8UBAEXAMPLE
```

- Para obtener información sobre la API, consulte GetHostedZone en la Referencia de comandos de la AWS CLI.

`list-health-checks`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-health-checks`.

AWS CLI

Para enumerar las comprobaciones de estado asociadas a una cuenta actual de AWS

El siguiente comando `list-health-checks` enumera información detallada sobre las 100 comprobaciones de estado que están asociadas con la cuenta de AWS actual:

```
aws route53 list-health-checks
```

Si tiene más de 100 comprobaciones de estado o si desea enumerarlas en grupos de menos de 100, incluya el parámetro `--maxitems`. Por ejemplo, para enumerar las comprobaciones de estado, utilice el siguiente comando:

```
aws route53 list-health-checks --max-items 1
```

Para ver información sobre la siguiente comprobación de estado, tome el valor de `NextToken` de la respuesta al comando anterior e inclúyalo en el parámetro `--starting-token`, por ejemplo:

```
aws route53 list-health-checks --max-items 1 --starting-token Z3M3LMPEXAMPLE
```

- Para obtener información sobre la API, consulte ListHealthChecks en la Referencia de comandos de la AWS CLI.

`list-hosted-zones-by-name`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-hosted-zones-by-name`.

AWS CLI

En el siguiente comando se enumeran hasta 100 zonas alojadas ordenadas por nombre de dominio:

```
aws route53 list-hosted-zones-by-name
```

Salida:

```
{
  "HostedZones": [
      {
          "ResourceRecordSetCount": 2,
          "CallerReference": "test20150527-2",
          "Config": {
              "Comment": "test2",
              "PrivateZone": false
          },
          "Id": "/hostedzone/Z119WBBTVP5WFX",
          "Name": "2.example.com."
      },
      {
          "ResourceRecordSetCount": 2,
          "CallerReference": "test20150527-1",
          "Config": {
              "Comment": "test",
              "PrivateZone": false
          },
          "Id": "/hostedzone/Z3P5QSUBK4POTI",
          "Name": "www.example.com."
      }
  ],
  "IsTruncated": false,
  "MaxItems": "100"
}
```

En el siguiente comando se muestran las zonas alojadas ordenadas por nombre, empezando por `www.example.com`:

```
aws route53 list-hosted-zones-by-name --dns-name www.example.com
```

Salida:

```
{
  "HostedZones": [
      {
          "ResourceRecordSetCount": 2,
          "CallerReference": "mwunderl20150527-1",
          "Config": {
              "Comment": "test",
              "PrivateZone": false
          },
          "Id": "/hostedzone/Z3P5QSUBK4POTI",
          "Name": "www.example.com."
      }
  ],
  "DNSName": "www.example.com",
  "IsTruncated": false,
  "MaxItems": "100"
}
```

- Para obtener información sobre la API, consulte ListHostedZonesByName en la Referencia de comandos de la AWS CLI.

`list-hosted-zones`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-hosted-zones`.

AWS CLI

Cómo enumerar las zonas alojadas asociadas a una cuenta actual de AWS

El siguiente comando de `list-hosted-zones` enumera información resumida sobre las 100 zonas alojadas que están asociadas con la cuenta actual de AWS:

```
aws route53 list-hosted-zones
```

Si tiene más de 100 zonas alojadas o si desea enumerarlas en grupos de menos de 100, incluya el parámetro `--max-items`. Por ejemplo, para enumerar las zonas alojadas, utilice el siguiente comando:

```
aws route53 list-hosted-zones --max-items 1
```

Para ver información sobre la siguiente zona alojada, tome el valor de `NextToken` de la respuesta al comando anterior e inclúyalo en el parámetro `--starting-token`, por ejemplo:

```
aws route53 list-hosted-zones --max-items 1 --starting-token Z3M3LMPEXAMPLE
```

- Para obtener información sobre la API, consulte ListHostedZones en la Referencia de comandos de la AWS CLI.

`list-query-logging-configs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-query-logging-configs`.

AWS CLI

Para enumerar las configuraciones de registro de consultas

En el siguiente ejemplo de `list-query-logging-configs`, se muestra información acerca de las 100 primeras configuraciones de registro de consultas de su cuenta de AWS para la zona alojada `Z1OX3WQEXAMPLE`.

```
aws route53 list-query-logging-configs \
    --hosted-zone-id Z1OX3WQEXAMPLE
```

Salida:

```
{
    "QueryLoggingConfigs": [
        {
            "Id": "964ff34e-ae03-4f06-80a2-9683cexample",
            "HostedZoneId": "Z1OX3WQEXAMPLE",
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/route53/example.com:*"
        }
    ]
}
```

Para obtener más información, consulte Logging DNS queries en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte ListQueryLoggingConfigs en la Referencia de comandos de la AWS CLI.

`list-resource-record-sets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-record-sets`.

AWS CLI

Para actualizar los conjuntos de registros de recursos en una zona alojada

El siguiente comando `list-resource-record-sets` muestra información resumida sobre los primeros 100 conjuntos de registros de recursos de una zona alojada específica:

```
aws route53 list-resource-record-sets --hosted-zone-id Z2LD58HEXAMPLE
```

Si la zona alojada contiene más de 100 conjuntos de registros de recursos o si desea enumerarlos en grupos de menos de 100, incluya el parámetro `--maxitems`. Por ejemplo, para enumerar los conjuntos de registros de recursos, utilice el siguiente comando:

```
aws route53 list-resource-record-sets --hosted-zone-id Z2LD58HEXAMPLE --max-items 1
```

Para ver información sobre el siguiente conjunto de registros de recursos, tome el valor de `NextToken` de la respuesta al comando anterior e inclúyalo en el parámetro `--starting-token`, por ejemplo:

```
aws route53 list-resource-record-sets --hosted-zone-id Z2LD58HEXAMPLE --max-items 1
 --starting-token Z3M3LMPEXAMPLE
```

Para ver todos los conjuntos de registros de recursos que tengan un nombre concreto, utilice el parámetro `--query` para filtrarlos. Por ejemplo:

```
aws route53 list-resource-record-sets --hosted-zone-id Z2LD58HEXAMPLE --
query "ResourceRecordSets[?Name == 'example.domain.']"
```

- Para obtener información sobre la API, consulte ListResourceRecordSets en la Referencia de comandos de la AWS CLI.

Ejemplos de registro de dominios de Route 53 usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con el registro de dominios de Route 53.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`check-domain-availability`

En el siguiente ejemplo de código, se muestra cómo utilizar `check-domain-availability`.

AWS CLI

Para determinar si se puede registrar un nombre de dominio con Route 53

El siguiente comando `check-domain-availability` devuelve información sobre si el nombre de dominio `example.com` está disponible para registrarse utilizando Route 53.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains check-domain-availability \
    --region us-east-1 \
    --domain-name example.com
```

Salida:

```
{
    "Availability": "UNAVAILABLE"
}
```

Route 53 admite una gran cantidad de dominios de nivel superior (TLD), como `.com` y `.jp`, pero no se admiten todos los TLD disponibles. Si comprueba la disponibilidad de un dominio y Route 53 no admite el TLD, `check-domain-availability` devuelve el siguiente mensaje.

```
An error occurred (UnsupportedTLD) when calling the CheckDomainAvailability
 operation: <top-level domain> tld is not supported.
```

Para obtener una lista de los TLD que puede usar para registrar un dominio con Route 53 consulte Domains That You Can Register with Amazon Route 53 en la Guía para desarrolladores de Amazon Route 53. Para obtener más información sobre el uso de Route 53 para registrar un dominio, consulte Registering a New Domain en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte CheckDomainAvailability en la Referencia de comandos de la AWS CLI.

`check-domain-transferability`

En el siguiente ejemplo de código, se muestra cómo utilizar `check-domain-transferability`.

AWS CLI

Para determinar si un dominio puede transferirse a Route 53

El siguiente comando `check-domain-transferability` devuelve información sobre si se puede transferir el nombre de dominio `example.com` a Route 53.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains check-domain-transferability \
    --region us-east-1 \
    --domain-name example.com
```

Salida:

```
{
    "Transferability": {
        "Transferable": "UNTRANSFERABLE"
    }
```

```
}
```

Para obtener más información, consulte Transferring Registration for a Domain to Amazon Route 53 en la Guía para desarrolladores de Amazon Route 53.

- Para ver los detalles de la API, consulte CheckDomainTransferability en la Referencia de comandos de la AWS CLI.

`delete-tags-for-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-tags-for-domain`.

AWS CLI

Para eliminar las etiquetas de un dominio

El siguiente comando `delete-tags-for-domain` elimina tres etiquetas del dominio especificado. Tenga en cuenta que solo especifica la clave de la etiqueta, no el valor de la etiqueta.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains delete-tags-for-domain \
    --region us-east-1 \
    --domain-name example.com \
    --tags-to-delete accounting-key hr-key engineering-key
```

Este comando no genera ninguna salida.

Para confirmar que se eliminaron las etiquetas, puede ejecutar list-tags-for-domain. Para obtener más información, consulte Tagging Amazon Route 53 Resources en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte DeleteTagsForDomain en la Referencia de comandos de la AWS CLI.

`disable-domain-auto-renew`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-domain-auto-renew`.

AWS CLI

Para deshabilitar la renovación automática de un dominio

El siguiente comando `disable-domain-auto-renew` configura Route 53 para que no renueve automáticamente el dominio `example.com` antes de que caduque el registro del dominio.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains disable-domain-auto-renew \
    --region us-east-1 \
    --domain-name example.com
```

Este comando no genera ninguna salida.

Para confirmar que se ha cambiado la configuración, puede ejecutar get-domain-detail. Si la renovación automática está deshabilitada, el valor de `AutoRenew` es `False`. Para obtener más información sobre la renovación automática, consulte Renewing Registration for a Domain < https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-renew.html en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte DisableDomainAutoRenew en la Referencia de comandos de la AWS CLI.

`disable-domain-transfer-lock`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-domain-transfer-lock`.

AWS CLI

Para deshabilitar el bloqueo de transferencia en un dominio

El siguiente comando `disable-domain-transfer-lock` elimina el bloqueo de transferencia del dominio `example.com` para que el dominio se pueda transferir a otro registrador. Este comando cambia el estado `clientTransferProhibited`.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains disable-domain-transfer-lock \
```

```
    --region us-east-1 \
    --domain-name example.com
```

Salida:

```
{
    "OperationId": "3f28e0ac-126a-4113-9048-cc930example"
}
```

Para confirmar que se ha cambiado el bloqueo de transferencia, puede ejecutar get-domain-detail. Cuando el bloqueo de transferencia está desactivado, el valor de `StatusList` no incluye`clientTransferProhibited`.

Para obtener más información, consulte Transferring a Domain from Amazon Route 53 to Another Registrar en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte DisableDomainTransferLock en la Referencia de la comandos de la AWS CLI.

`enable-domain-auto-renew`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-domain-auto-renew`.

AWS CLI

Para habilitar la renovación automática de un dominio

El siguiente comando `enable-domain-auto-renew` configura Route 53 para que renueve automáticamente el dominio `example.com` antes de que caduque el registro del dominio.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains enable-domain-auto-renew \
    --region us-east-1 \
    --domain-name example.com
```

Este comando no genera ninguna salida. Para confirmar que se ha cambiado la configuración, puede ejecutar get-domain-detail. Si la renovación automática está habilitada, el valor de `AutoRenew` es `True`.

Para obtener más información sobre la renovación automática, consulte Renewing Registration for a Domain < https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-renew.html en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte EnableDomainAutoRenew en la Referencia de comandos de la AWS CLI.

`enable-domain-transfer-lock`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-domain-transfer-lock`.

AWS CLI

Para habilitar el bloqueo de transferencia en un dominio

El siguiente comando `enable-domain-transfer-lock` bloquea de transferencia del dominio especificado para que no se pueda transferir a otro registrador. Este comando cambia el estado `clientTransferProhibited`.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains enable-domain-transfer-lock \
    --region us-east-1 \
    --domain-name example.com
```

Salida:

```
{
    "OperationId": "3f28e0ac-126a-4113-9048-cc930example"
}
```

Para confirmar que se ha cambiado el bloqueo de transferencia, puede ejecutar get-domain-detail. Cuando el bloqueo de transferencia está activado, el valor de `StatusList` incluye `clientTransferProhibited`.

Para obtener más información, consulte Transferring a Domain from Amazon Route 53 to Another Registrar en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte EnableDomainTransferLock en la Referencia de comandos de la AWS CLI.

`get-contact-reachability-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-contact-reachability-status`.

AWS CLI

Para determinar si el contacto titular ha respondido a un correo electrónico de confirmación

El siguiente comando `get-contact-reachability-status` devuelve información sobre si el contacto titular del dominio especificado ha respondido a un correo electrónico de confirmación.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains get-contact-reachability-status \
    --region us-east-1 \
    --domain-name example.com
```

Salida:

```
{
    "domainName": "example.com",
    "status": "DONE"
}
```

Para obtener más información, consulte Resending Authorization and Confirmation Emails en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte GetContactReachabilityStatus en la Referencia de comandos de la AWS CLI.

`get-domain-detail`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-domain-detail`.

AWS CLI

Para obtener información detallada acerca de un dominio específico

El siguiente comando `get-domain-detail` muestra información detallada sobre el dominio especificado.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

Salida:

```
{
    "DomainName": "example.com",
    "Nameservers": [
        {
            "Name": "ns-2048.awsdns-64.com",
            "GlueIps": []
        },
        {
            "Name": "ns-2049.awsdns-65.net",
            "GlueIps": []
        },
        {
            "Name": "ns-2050.awsdns-66.org",
            "GlueIps": []
        },
        {
            "Name": "ns-2051.awsdns-67.co.uk",
            "GlueIps": []
        }
    ],
    "AutoRenew": true,
    "AdminContact": {
        "FirstName": "Saanvi",
        "LastName": "Sarkar",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "ssarkar@example.com",
        "ExtraParams": []
```

```
    },
    "RegistrantContact": {
        "FirstName": "Alejandro",
        "LastName": "Rosalez",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "arosalez@example.com",
        "ExtraParams": []
    },
    "TechContact": {
        "FirstName": "Wang",
        "LastName": "Xiulan",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "wxiulan@example.com",
        "ExtraParams": []
    },
    "AdminPrivacy": true,
    "RegistrantPrivacy": true,
    "TechPrivacy": true,
    "RegistrarName": "Amazon Registrar, Inc.",
    "WhoIsServer": "whois.registrar.amazon",
    "RegistrarUrl": "http://registrar.amazon.com",
    "AbuseContactEmail": "abuse@registrar.amazon.com",
    "AbuseContactPhone": "+1.2062661000",
    "CreationDate": 1444934889.601,
    "ExpirationDate": 1602787689.0,
    "StatusList": [
        "clientTransferProhibited"
    ]
}
```

- Para obtener información sobre la API, consulte GetDomainDetail en la Referencia de comandos de la AWS CLI.

`get-domain-suggestions`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-domain-suggestions`.

AWS CLI

Para obtener una lista de los nombres de dominio sugeridos

El siguiente comando `get-domain-suggestions` muestra una lista de los nombres de dominio sugeridos en función del nombre de dominio `example.com`. La respuesta incluye solo los nombres de dominio que están disponibles. Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains get-domain-suggestions \
    --region us-east-1 \
    --domain-name example.com \
    --suggestion-count 10 \
    --only-available
```

Salida:

```
{
    "SuggestionsList": [
        {
            "DomainName": "egzaampal.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplelaw.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplehouse.net",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "homeexample.net",
            "Availability": "AVAILABLE"
```

```
        },
        {
            "DomainName": "examplelist.com",
            "Availability": "AVAILABLE"
       },
        {
            "DomainName": "examplenews.net",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "officeexample.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "exampleworld.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "exampleart.com",
            "Availability": "AVAILABLE"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetDomainSuggestions en la Referencia de comandos de la AWS CLI.

`get-operation-detail`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-operation-detail`.

AWS CLI

Para obtener el estado actual de una operación

Algunas operaciones de registro de dominio funcionan de forma asíncrona y devuelven una respuesta antes de que finalicen. Estas operaciones devuelven un ID de operación que puede usar para obtener el estado actual. El siguiente comando `get-operation-detail` devuelve el estado de la operación especificada.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains get-operation-detail \
    --region us-east-1 \
    --operation-id edbd8d63-7fe7-4343-9bc5-54033example
```

Salida:

```
{
    "OperationId": "edbd8d63-7fe7-4343-9bc5-54033example",
    "Status": "SUCCESSFUL",
    "DomainName": "example.com",
    "Type": "DOMAIN_LOCK",
    "SubmittedDate": 1573749367.864
}
```

- Para obtener información sobre la API, consulte GetOperationDetail en la Referencia de comandos de la AWS CLI.

`list-domains`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-domains`.

AWS CLI

Para enumerar los dominios que están registrados en la cuenta actual de AWS

El siguiente comando `list-domains` enumera información resumida acerca de los dominios que están registrados en la cuenta actual de AWS.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains list-domains
    --region us-east-1
```

Salida:

```
{
    "Domains": [
        {
            "DomainName": "example.com",
            "AutoRenew": true,
```

```
            "TransferLock": true,
            "Expiry": 1602712345.0
        },
        {
            "DomainName": "example.net",
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602723456.0
        },
        {
            "DomainName": "example.org",
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602734567.0
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListDomains en la Referencia de comandos de la AWS CLI.

`list-operations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-operations`.

AWS CLI

Para enumerar el estado de las operaciones que devuelven un ID de operación

Algunas operaciones de registro de dominios se ejecutan de forma asíncrona y devuelven una respuesta antes de que finalicen. Estas operaciones devuelven un ID de operación que puede usar para obtener el estado actual. El siguiente comando `list-operations` enumera información resumida, incluido el estado, sobre las operaciones actuales de registro de dominio.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains list-operations
    --region us-east-1
```

Salida:

```
{
    "Operations": [
        {
            "OperationId": "aab9822f-1da0-4bf3-8a15-fd4e0example",
            "Status": "SUCCESSFUL",
            "Type": "DOMAIN_LOCK",
            "SubmittedDate": 1455321739.986
        },
        {
            "OperationId": "c24379ed-76be-42f8-bdad-9379bexample",
            "Status": "SUCCESSFUL",
            "Type": "UPDATE_NAMESERVER",
            "SubmittedDate": 1468960475.109
        },
        {
            "OperationId": "f47e1297-ef9e-4c2b-ae1e-a5fcbexample",
            "Status": "SUCCESSFUL",
            "Type": "RENEW_DOMAIN",
            "SubmittedDate": 1473561835.943
        },
        {
            "OperationId": "75584f23-b15f-459e-aed7-dc6f5example",
            "Status": "SUCCESSFUL",
            "Type": "UPDATE_DOMAIN_CONTACT",
            "SubmittedDate": 1547501003.41
        }
    ]
}
```

El resultado incluye todas las operaciones que devuelven un ID de operación y que ha realizado en todos los dominios que haya registrado alguna vez con la cuenta actual de AWS. Si desea obtener solo las operaciones que envió después de una fecha específica, puede incluir el parámetro `submitted-since` y especificar una fecha en formato Unix y en hora universal coordinada (UTC). El siguiente comando obtiene el estado de todas las operaciones que se enviaron después de las 00.00 h UTC del 1 de enero de 2020.

```
aws route53domains list-operations \
    --submitted-since 1577836800
```

- Para obtener información sobre la API, consulte ListOperations en la Referencia de comandos de la AWS CLI.

`list-tags-for-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-domain`.

AWS CLI

Para generar una lista de las etiquetas de un dominio

El siguiente comando `list-tags-for-domain` genera una lista de las etiquetas asignadas actualmente al dominio especificado.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains list-tags-for-domain \
    --region us-east-1 \
    --domain-name example.com
```

Salida:

```
{
    "TagList": [
        {
            "Key": "key1",
            "Value": "value1"
        },
        {
            "Key": "key2",
            "Value": "value2"
        }
    ]
}
```

Para obtener más información, consulte Tagging Amazon Route 53 Resources en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte ListTagsForDomain en la Referencia de comandos de la AWS CLI.

`register-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-domain`.

AWS CLI

Para registrar un dominio

El siguiente comando `register-domain` registra un dominio y recupera todos los valores de los parámetros de un archivo con formato JSON.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains register-domain \
    --region us-east-1 \
    --cli-input-json file://register-domain.json
```

Contenido de `register-domain.json`:

```
{
    "DomainName": "example.com",
    "DurationInYears": 1,
    "AutoRenew": true,
    "AdminContact": {
        "FirstName": "Martha",
        "LastName": "Rivera",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "mrivera@example.com"
    },
    "RegistrantContact": {
        "FirstName": "Li",
        "LastName": "Juan",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
```

```
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "ljuan@example.com"
    },
    "TechContact": {
        "FirstName": "Mateo",
        "LastName": "Jackson",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "mjackson@example.com"
    },
    "PrivacyProtectAdminContact": true,
    "PrivacyProtectRegistrantContact": true,
    "PrivacyProtectTechContact": true
}
```

Salida:

```
{
    "OperationId": "b114c44a-9330-47d1-a6e8-a0b11example"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar `get-operation-detail`. Para obtener más información, consulte get-operation-detail.

Para obtener más información, consulte Registering a New Domain en la Guía para desarrolladores de Amazon Route 53.

Para obtener información sobre los dominios de nivel superior (TLD) que requieren valores `ExtraParams` y cuáles son los valores válidos, consulte ExtraParam en la Referencia de la API de Amazon Route 53.

- Para obtener información sobre la API, consulte RegisterDomain en la Referencia de comandos de la AWS CLI.

`renew-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `renew-domain`.

AWS CLI

Para renovar un dominio

El siguiente comando `renew-domain` renueva el dominio especificado durante cinco años. Para obtener el valor de `current-expiry-year`, utilice el comando `get-domain-detail` y convierta el valor de `ExpirationDate` desde el formato Unix.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains renew-domain \
    --region us-east-1 \
    --domain-name example.com \
    --duration-in-years 5 \
    --current-expiry-year 2020
```

Salida:

```
{
    "OperationId": "3f28e0ac-126a-4113-9048-cc930example"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar `get-operation-detail`. Para obtener más información, consulte get-operation-detail.

El registro de cada dominio de nivel superior (TLD), como .com o .org, controla el número máximo de años durante los que se puede renovar un dominio. Para obtener el período de renovación máximo para su dominio, consulte la sección período de registro y renovación de su TLD en Domains That You Can Register with Amazon Route 53 en la Guía para desarrolladores de Amazon Route 53.

Para obtener más información, consulte Renewing Registration for a Domain en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte RenewDomain en la Referencia de comandos de la AWS CLI.

`resend-contact-reachability-email`

En el siguiente ejemplo de código, se muestra cómo utilizar `resend-contact-reachability-email`.

AWS CLI

Para reenviar el correo electrónico de confirmación a la dirección de correo actual para el contacto titular

El siguiente comando `resend-contact-reachability-email` reenvía el correo electrónico de confirmación a la dirección de correo electrónico actual para el contacto titular del dominio example.com.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains resend-contact-reachability-email \
    --region us-east-1 \
    --domain-name example.com
```

Salida:

```
{
    "domainName": "example.com",
    "emailAddress": "moliveira@example.com",
    "isAlreadyVerified": true
}
```

Si el valor de `isAlreadyVerified` es`true`, como en este ejemplo, el contacto titular ya ha confirmado que se puede acceder a la dirección de correo electrónico especificada.

Para obtener más información, consulte Resending Authorization and Confirmation Emails en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte ResendContactReachabilityEmail en la Referencia de comandos de la AWS CLI.

`retrieve-domain-auth-code`

En el siguiente ejemplo de código, se muestra cómo utilizar `retrieve-domain-auth-code`.

AWS CLI

Para obtener el código de autorización de un dominio para poder transferirlo a otro titular

El siguiente comando `retrieve-domain-auth-code` obtiene el código de autorización actual para el dominio example.com. Le proporciona este valor a otro titular de dominios cuando desea transferir el dominio a ese titular.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains retrieve-domain-auth-code \
    --region us-east-1 \
    --domain-name example.com
```

Salida:

```
{
    "AuthCode": ")o!v3dJeXampLe"
}
```

Para obtener más información, consulte Transferring a Domain from Amazon Route 53 to Another Registrar en la Guía para desarrolladores de Amazon Route 53.

- Para obtener detalles sobre la API, consulte RetrieveDomainAuthCode en la Referencia de comandos de la AWS CLI.

`transfer-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `transfer-domain`.

AWS CLI

Para transferir un dominio a Amazon Route 53

El siguiente comando `transfer-domain` transfiere un dominio a Route 53, con los parámetros proporcionados por el archivo con formato JSON `C:\temp\transfer-domain.json`.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains transfer-domain \
    --region us-east-1 \
    --cli-input-json file://C:\temp\transfer-domain.json
```

Contenido de `transfer-domain.json`:

```
{
    "DomainName": "example.com",
    "DurationInYears": 1,
    "Nameservers": [
        {
            "Name": "ns-2048.awsdns-64.com"
        },
        {
            "Name": "ns-2049.awsdns-65.net"
        },
        {
            "Name": "ns-2050.awsdns-66.org"
        },
        {
            "Name": "ns-2051.awsdns-67.co.uk"
        }
    ],
    "AuthCode": ")o!v3dJeXampLe",
    "AutoRenew": true,
    "AdminContact": {
        "FirstName": "Martha",
        "LastName": "Rivera",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "mrivera@example.com"
    },
    "RegistrantContact": {
        "FirstName": "Li",
        "LastName": "Juan",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
```

```
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "ljuan@example.com"
    },
    "TechContact": {
        "FirstName": "Mateo",
        "LastName": "Jackson",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "mjackson@example.com"
    },
    "PrivacyProtectAdminContact": true,
    "PrivacyProtectRegistrantContact": true,
    "PrivacyProtectTechContact": true
}
```

Salida:

```
{
    "OperationId": "b114c44a-9330-47d1-a6e8-a0b11example"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar `get-operation-detail`. Para obtener más información, consulte get-operation-detail.

Para obtener más información, consulte Transferring Registration for a Domain to Amazon Route 53 en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte TransferDomain en la Referencia de comandos de la AWS CLI.

update-domain-contact-privacy

En el siguiente ejemplo de código, se muestra cómo utilizar update-domain-contact-privacy.

AWS CLI

Para actualizar la configuración de privacidad de los contactos de un dominio

El siguiente comando update-domain-contact-privacy desactiva la protección de privacidad del contacto administrativo del dominio example.com. Este comando solo se ejecuta en la región us-east-1.

Si su región predeterminada está configurada en us-east-1, puede omitir el parámetro region.

```
aws route53domains update-domain-contact-privacy \
    --region us-east-1 \
    --domain-name example.com \
    --no-admin-privacy
```

Salida:

```
{
    "OperationId": "b3a219e9-d801-4244-b533-b7256example"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar get-operation-detail. Para obtener más información, consulte get-operation-detail.

Para obtener más información, consulte Enabling or Disabling Privacy Protection for Contact Information for a Domain en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información acerca de la API, consulte UpdateDomainContactPrivacy en la Referencia de comandos de la AWS CLI.

update-domain-contact

En el siguiente ejemplo de código, se muestra cómo utilizar update-domain-contact.

AWS CLI

Para actualizar la información de contacto de un dominio

El siguiente comando `update-domain-contact` actualiza la información de contacto de un dominio y obtiene los parámetros del archivo con formato JSON `C:\temp\update-domain-contact.json`.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains update-domain-contact \
    --region us-east-1 \
    --cli-input-json file://C:\temp\update-domain-contact.json
```

Contenido de `update-domain-contact.json`:

```
{
    "AdminContact": {
        "AddressLine1": "101 Main Street",
        "AddressLine2": "Suite 1a",
        "City": "Seattle",
        "ContactType": "COMPANY",
        "CountryCode": "US",
        "Email": "w.xiulan@example.com",
        "FirstName": "Wang",
        "LastName": "Xiulan",
        "OrganizationName": "Example",
        "PhoneNumber": "+1.8005551212",
        "State": "WA",
        "ZipCode": "98101"
    },
    "DomainName": "example.com",
    "RegistrantContact": {
        "AddressLine1": "101 Main Street",
        "AddressLine2": "Suite 1a",
        "City": "Seattle",
        "ContactType": "COMPANY",
        "CountryCode": "US",
        "Email": "w.xiulan@example.com",
        "FirstName": "Wang",
        "LastName": "Xiulan",
        "OrganizationName": "Example",
        "PhoneNumber": "+1.8005551212",
        "State": "WA",
        "ZipCode": "98101"
    },
```

```
    "TechContact": {
        "AddressLine1": "101 Main Street",
        "AddressLine2": "Suite 1a",
        "City": "Seattle",
        "ContactType": "COMPANY",
        "CountryCode": "US",
        "Email": "w.xiulan@example.com",
        "FirstName": "Wang",
        "LastName": "Xiulan",
        "OrganizationName": "Example",
        "PhoneNumber": "+1.8005551212",
        "State": "WA",
        "ZipCode": "98101"
    }
}
```

Salida:

```
{
    "OperationId": "b3a219e9-d801-4244-b533-b7256example"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar get-domain-detail. Para obtener más información, consulte Updating Contact Information for a Domain en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte UpdateDomainContact en la Referencia de comandos de la AWS CLI.

`update-domain-nameservers`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-domain-nameservers`.

AWS CLI

Para actualizar los servidores de nombres de un dominio

El siguiente comando `update-domain-nameservers` actualiza los servidores de nombres de un dominio.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains update-domain-nameservers \
    --region us-east-1 \
    --domain-name example.com \
    --
nameservers Name=ns-1.awsdns-01.org Name=ns-2.awsdns-02.co.uk Name=ns-3.awsdns-03.net Name=n
```

Salida:

```
{
    "OperationId": "f1691ec4-0e7a-489e-82e0-b19d3example"
}
```

Para confirmar que la operación se ha realizado correctamente, puede ejecutar get-domain-detail.

Para obtener más información, consulte Adding or Changing Name Servers and Glue Records for a Domain en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte UpdateDomainNameservers en la Referencia de comandos de la AWS CLI.

`update-tags-for-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-tags-for-domain`.

AWS CLI

Para añadir o actualizar las etiquetas de un dominio

El siguiente comando `update-tags-for-domain` agrega o actualiza dos claves y los valores correspondientes para el dominio example.com. Para actualizar el valor de una clave, simplemente incluya la clave y el valor nuevo. Puede agregar o actualizar etiquetas solo en un dominio a la vez.

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains update-tags-for-domain \
    --region us-east-1 \
    --domain-name example.com \
    --tags-to-update "Key=key1,Value=value1" "Key=key2,Value=value2"
```

Este comando no genera ninguna salida. Para confirmar que se agregaron o actualizaron las etiquetas, puede ejecutar list-tags-for-domain.

Para obtener más información, consulte Tagging Amazon Route 53 Resources en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte UpdateTagsForDomain en la Referencia de comandos de la AWS CLI.

`view-billing`

En el siguiente ejemplo de código, se muestra cómo utilizar `view-billing`.

AWS CLI

Para obtener la información de facturación de los cargos por registro de dominio de la cuenta actual de AWS

El siguiente comando `view-billing` devuelve todos los registros de facturación relacionados con el dominio de la cuenta actual durante el período comprendido entre el 1 de enero de 2018 (1514764800 en horario Unix) y la medianoche del 31 de diciembre de 2019 (1577836800 en horario Unix).

Este comando solo se ejecuta en la región `us-east-1`. Si su región predeterminada está configurada en `us-east-1`, puede omitir el parámetro `region`.

```
aws route53domains view-billing \
    --region us-east-1 \
    --start-time 1514764800 \
    --end-time 1577836800
```

Salida:

```
{
    "BillingRecords": [
        {
            "DomainName": "example.com",
            "Operation": "RENEW_DOMAIN",
            "InvoiceId": "149962827",
            "BillDate": 1536618063.181,
            "Price": 12.0
```

```
        },
        {
            "DomainName": "example.com",
            "Operation": "RENEW_DOMAIN",
            "InvoiceId": "290913289",
            "BillDate": 1568162630.884,
            "Price": 12.0
        }
    ]
}
```

Para obtener más información, consulte ViewBilling en la Referencia de la API de Amazon Route 53.

- Para obtener información sobre la API, consulte ViewBilling en la Referencia de comandos de la AWS CLI.

Ejemplos de Perfiles de Route 53 que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Perfiles de Route 53.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-profile`.

AWS CLI

Para asociar un perfil

En el siguiente ejemplo de `associate-profile`, se asocia un perfil a una VPC.

```
aws route53profiles associate-profile \
    --name test-association \
    --profile-id rp-4987774726example \
    --resource-id vpc-0af3b96b3example
```

Salida:

```
{
    "ProfileAssociation": {
        "CreationTime": 1710851336.527,
        "Id": "rpassoc-489ce212fexample",
        "ModificationTime": 1710851336.527,
        "Name": "test-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceId": "vpc-0af3b96b3example",
        "Status": "CREATING",
        "StatusMessage": "Creating Profile Association"
    }
}
```

Para más información, consulte Using Profiles en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte AssociateProfile en la Referencia de comandos de la AWS CLI.

`associate-resource-to-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-resource-to-profile`.

AWS CLI

Para asociar un recurso a un perfil

En el siguiente ejemplo de `associate-resource-to-profile`, se asocia un grupo de reglas de DNS Firewall con una prioridad de 102 a un perfil.

```
aws route53profiles associate-resource-to-profile \
```

```
    --name test-resource-association \
    --profile-id rp-4987774726example \
    --resource-arn arn:aws:route53resolver:us-east-1:123456789012:firewall-rule-
group/rslvr-frg-cfe7f72example \
    --resource-properties "{\"priority\": 102}"
```

Salida:

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710851216.613,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":102}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Profile to DNS Firewall rule group
 association"
    }
}
```

- Para obtener información sobre la API, consulte AssociateResourceToProfile en la Referencia de comandos de la AWS CLI.

`create-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-profile`.

AWS CLI

Para crear un perfil

En el ejemplo siguiente de `create-profile`, se crea un perfil.

```
aws route53profiles create-profile \
    --name test
```

Salida:

```
{
    "Profile": {
        "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-6ffe47d5example",
        "ClientToken": "2ca1a304-32b3-4f5f-bc4c-EXAMPLE11111",
        "CreationTime": 1710850903.578,
        "Id": "rp-6ffe47d5example",
        "ModificationTime": 1710850903.578,
        "Name": "test",
        "OwnerId": "123456789012",
        "ShareStatus": "NOT_SHARED",
        "Status": "COMPLETE",
        "StatusMessage": "Created Profile"
    }
}
```

- Para obtener información sobre la API, consulte CreateProfile en la Referencia de comandos de la AWS CLI.

`delete-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-profile`.

AWS CLI

Para eliminar un perfil

En el siguiente ejemplo de `delete-profile`, se elimina un perfil.

```
aws route53profiles delete-profile \
    --profile-id rp-6ffe47d5example
```

Salida:

```
{
    "Profile": {
        "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-6ffe47d5example",
        "ClientToken": "0a15fec0-05d9-4f78-bec0-EXAMPLE11111",
```

```
        "CreationTime": 1710850903.578,
        "Id": "rp-6ffe47d5example",
        "ModificationTime": 1710850903.578,
        "Name": "test",
        "OwnerId": "123456789012",
        "ShareStatus": "NOT_SHARED",
        "Status": "DELETED",
        "StatusMessage": "Deleted Profile"
    }
}
```

- Para obtener información sobre la API, consulte DeleteProfile en la Referencia de comandos de AWS CLI.

`disassociate-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-profile`.

AWS CLI

Para desasociar un perfil

En el siguiente ejemplo de `disassociate-profile`, se desvincula un perfil de una VPC.

```
aws route53profiles disassociate-profile \
    --profile-id rp-4987774726example \
    --resource-id vpc-0af3b96b3example
```

Salida:

```
{
    "ProfileAssociation": {
        "CreationTime": 1710851336.527,
        "Id": "rpassoc-489ce212fexample",
        "ModificationTime": 1710851401.362,
        "Name": "test-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceId": "vpc-0af3b96b3example",
        "Status": "DELETING",
        "StatusMessage": "Deleting Profile Association"
    }
```

```
}
```

- Para obtener información sobre la API, consulte DisassociateProfile en la Referencia de comandos de la AWS CLI.

`disassociate-resource-from-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-resource-from-profile`.

AWS CLI

Para desasociar un recurso de un perfil

En el siguiente ejemplo de `disassociate-resource-from-profile`, se desvincula un grupo de reglas de DNS Firewall de un perfil.

```
aws route53profiles disassociate-resource-from-profile \
    --profile-id rp-4987774726example \
    --resource-arn arn:aws:route53resolver:us-east-1:123456789012:firewall-rule-
group/rslvr-frg-cfe7f72example
```

Salida:

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710852624.36,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":105}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "DELETING",
        "StatusMessage": "Deleting the Profile to DNS Firewall rule group
 association"
    }
}
```

- Para obtener información sobre la API, consulte DisassociateResourceFromProfile en la Referencia de comandos de la AWS CLI.

`get-profile-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-profile-association`.

AWS CLI

Para obtener información sobre una asociación de perfiles

En el siguiente ejemplo de `get-profile-association`, se devuelve información sobre la asociación de perfiles especificada.

```
aws route53profiles get-profile-association \
    --profile-association-id rpassoc-489ce212fexample
```

Salida:

```
{
    "ProfileAssociation": {
        "CreationTime": 1709338817.148,
        "Id": "rrpassoc-489ce212fexample",
        "ModificationTime": 1709338974.772,
        "Name": "test-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceId": "vpc-0af3b96b3example",
        "Status": "COMPLETE",
        "StatusMessage": "Created Profile Association"
    }
}
```

- Para obtener información sobre la API, consulte GetProfileAssociation en la Referencia de comandos de la AWS CLI.

`get-profile-resource-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-profile-resource-association`.

AWS CLI

Para obtener información sobre un recurso asociado a un perfil

En el siguiente ejemplo de `get-profile-resource-association`, se devuelve información sobre la asociación de recursos especificada a un perfil.

```
aws route53profiles get-profile-resource-association \
    --profile-resource-association-id rpr-001913120a7example
```

Salida:

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710852303.798,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":105}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "COMPLETE",
        "StatusMessage": "Completed creation of Profile to DNS Firewall rule group
 association"
    }
}
```

- Para obtener información sobre la API, consulte GetProfileResourceAssociation en la Referencia de comandos de la AWS CLI.

`get-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-profile`.

AWS CLI

Para obtener información sobre un perfil

En el siguiente ejemplo de `get-profile`, se devuelve información sobre el perfil especificado.

```
aws route53profiles get-profile \
    --profile-id rp-4987774726example
```

Salida:

```
{
    "Profile": {
        "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-4987774726example",
        "ClientToken": "0cbc5ae7-4921-4204-bea9-EXAMPLE11111",
        "CreationTime": 1710851044.288,
        "Id": "rp-4987774726example",
        "ModificationTime": 1710851044.288,
        "Name": "test",
        "OwnerId": "123456789012",
        "ShareStatus": "NOT_SHARED",
        "Status": "COMPLETE",
        "StatusMessage": "Created Profile"
    }
}
```

- Para obtener información sobre la API, consulte GetProfile en la Referencia de comandos de la AWS CLI.

`list-profile-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-profile-associations`.

AWS CLI

Para enumerar las asociaciones de perfiles

En el siguiente ejemplo de `list-profile-associations`, se enumeran las asociaciones de perfiles de su cuenta de AWS.

```
aws route53profiles list-profile-associations
```

Salida:

```
{
```

```
    "ProfileAssociations": [
        {
            "CreationTime": 1709338817.148,
            "Id": "rpassoc-489ce212fexample",
            "ModificationTime": 1709338974.772,
            "Name": "test-association",
            "OwnerId": "123456789012",
            "ProfileId": "rp-4987774726example",
            "ResourceId": "vpc-0af3b96b3example",
            "Status": "COMPLETE",
            "StatusMessage": "Created Profile Association"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListProfileAssociations en la Referencia de comandos de la AWS CLI.

`list-profile-resource-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-profile-resource-associations`.

AWS CLI

Para enumerar las asociaciones de recursos de perfiles

En el siguiente ejemplo de `list-profile-resource-associations`, se enumeran las asociaciones de recursos de perfiles para el perfil especificado.

```
aws route53profiles list-profile-resource-associations \
    --profile-id rp-4987774726example
```

Salida:

```
{
     "ProfileResourceAssociations": [
         {
             "CreationTime": 1710851216.613,
             "Id": "rpr-001913120a7example",
             "ModificationTime": 1710851216.613,
```

```
            "Name": "test-resource-association",
            "OwnerId": "123456789012",
            "ProfileId": "rp-4987774726example",
            "ResourceArn": "arn:aws:route53resolver:us-
east-1:123456789012:firewall-rule-group/rslvr-frg-cfe7f72example",
            "ResourceProperties": "{\"priority\":102}",
            "ResourceType": "FIREWALL_RULE_GROUP",
            "Status": "COMPLETE",
            "StatusMessage": "Completed creation of Profile to DNS Firewall rule
 group association"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListProfileResourceAssociations en la Referencia de comandos de la AWS CLI.

`list-profiles`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-profiles`.

AWS CLI

Para enumerar los perfiles

En el siguiente ejemplo de `list-profiles`, se enumeran los perfiles de su cuenta de AWS y se muestra información adicional sobre los mismos.

```
aws route53profiles list-profiles
```

Salida:

```
{
    "ProfileSummaries": [
        {
            "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-4987774726example",
            "Id": "rp-4987774726example",
            "Name": "test",
            "ShareStatus": "NOT_SHARED"
        }
    ]
```

```
}
```

- Para obtener información sobre la API, consulte ListProfiles en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran las etiquetas para el recurso especificado.

```
aws route53profiles list-tags-for-resource \
    --resource-arn arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-4987774726example
```

Salida:

```
{
    "Tags": {
        "my-key-2": "my-value-2",
        "my-key-1": "my-value-1"
    }
}
```

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`update-profile-resource-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-profile-resource-association`.

AWS CLI

Para actualizar un recurso asociado a un perfil

En el siguiente ejemplo de `update-profile-resource-association`, se actualiza una prioridad de un grupo de reglas de DNS Firewall asociado a un perfil.

```
aws route53profiles update-profile-resource-association \
    --profile-resource-association-id rpr-001913120a7example \
    --resource-properties "{\"priority\": 105}"
```

Salida:

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710852303.798,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":105}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Profile to DNS Firewall rule group
 association"
    }
}
```

- Para obtener más información sobre la API, consulte UpdateProfileResourceAssociation en la Referencia de comandos de la AWS CLI.

Ejemplos de Route 53 Resolver que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Route 53 Resolver.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-firewall-rule-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-firewall-rule-group`.

AWS CLI

Para asociar un grupo de reglas de firewall a una VPC

En el siguiente ejemplo de `associate-firewall-rule-group`, se asocia un grupo de reglas de DNS Firewall a una Amazon VPC.

```
aws route53resolver associate-firewall-rule-group \
    --name test-association \
    --firewall-rule-group-id rslvr-frg-47f93271fexample \
    --vpc-id vpc-31e92222 \
    --priority 101
```

Salida:

```
{
    "FirewallRuleGroupAssociation": {
        "Id": "rslvr-frgassoc-57e8873d7example",
        "Arn": "arn:aws:route53resolver:us-west-2:123456789012:firewall-rule-group-
association/rslvr-frgassoc-57e8873d7example",
        "FirewallRuleGroupId": "rslvr-frg-47f93271fexample",
        "VpcId": "vpc-31e92222",
        "Name": "test-association",
        "Priority": 101,
        "MutationProtection": "DISABLED",
        "Status": "UPDATING",
        "StatusMessage": "Creating Firewall Rule Group Association",
        "CreatorRequestId": "2ca1a304-32b3-4f5f-bc4c-EXAMPLE11111",
        "CreationTime": "2021-05-25T21:47:48.755768Z",
        "ModificationTime": "2021-05-25T21:47:48.755768Z"
    }
}
```

Para obtener más información, consulte Managing associations between your VPC and Route 53 Resolver DNS Firewall rule groups en la Guía del desarrollador de Amazon Route 53.

- Para obtener información sobre la API, consulte AssociateFirewallRuleGroup en la Referencia de comandos de la AWS CLI.

`associate-resolver-endpoint-ip-address`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-resolver-endpoint-ip-address`.

AWS CLI

Para asociar otra dirección IP a un punto de conexión de Resolver

En el siguiente ejemplo de `associate-resolver-endpoint-ip-address`, se asocia otra dirección IP a un punto de conexión de Resolver entrante. Si especifica solo un ID de subred y omite la dirección IP en el parámetro `--ip-address`, Resolver elige una dirección IP de las direcciones IP disponibles en la subred especificada.

```
aws route53resolver associate-resolver-endpoint-ip-address \
    --resolver-endpoint-id rslvr-in-497098ad5example \
    --ip-address="SubnetId=subnet-12d8exam,Ip=192.0.2.118"
```

Salida:

```
{
    "ResolverEndpoint": {
        "Id": "rslvr-in-497098ad5example",
        "CreatorRequestId": "AWSConsole.25.0123456789",
        "Arn": "arn:aws:route53resolver:us-west-2:111122223333:resolver-endpoint/
rslvr-in-497098ad5example",
        "Name": "my-inbound-endpoint",
        "SecurityGroupIds": [
            "sg-05cd7b25d6example"
        ],
        "Direction": "INBOUND",
        "IpAddressCount": 3,
        "HostVPCId": "vpc-304bexam",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Resolver Endpoint",
```

```
        "CreationTime": "2020-01-02T23:25:45.538Z",
        "ModificationTime": "2020-01-02T23:25:45.538Z"
    }
}
```

Para obtener más información, consulte Values That You Specify When You Create or Edit Inbound Endpoints en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte AssociateResolverEndpointIpAddress en la Referencia de comandos de la AWS CLI.

`associate-resolver-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-resolver-rule`.

AWS CLI

Para asociar un grupo de reglas a una VPC

En el siguiente ejemplo de `associate-resolver-rule`, se asocia una regla de Resolver con una Amazon VPC. Tras ejecutar el comando, Resolver comienza a reenviar las consultas de DNS a la red en función de la configuración de la regla, como el nombre de dominio de las consultas que se reenvían.

```
aws route53resolver associate-resolver-rule \
    --name my-resolver-rule-association \
    --resolver-rule-id rslvr-rr-42b60677c0example \
    --vpc-id vpc-304bexam
```

Salida:

```
{
    "ResolverRuleAssociation": {
        "Id": "rslvr-rrassoc-d61cbb2c8bexample",
        "ResolverRuleId": "rslvr-rr-42b60677c0example",
        "Name": "my-resolver-rule-association",
        "VPCId": "vpc-304bexam",
        "Status": "CREATING",
        "StatusMessage": "[Trace id: 1-5dc5a8fa-ec2cc480d2ef07617example] Creating
 the association."
    }
```

```
}
```

Para obtener más información, consulte Forwarding Outbound DNS Queries to Your Network en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte AssociateResolverRule en la Referencia de comandos de la AWS CLI.

`create-firewall-domain-list`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-firewall-domain-list`.

AWS CLI

Para crear una lista de dominios de DNS Firewall de Route 53 Resolver

En el siguiente ejemplo de `create-firewall-domain-list`, se crea una lista de dominios de Route 53 Resolver DNS Firewall, denominada test, en su cuenta de AWS.

```
aws route53resolver create-firewall-domain-list \
    --creator-request-id my-request-id \
    --name test
```

Salida:

```
{
    "FirewallDomainList": {
        "Id": "rslvr-fdl-d61cbb2cbexample",
        "Arn": "arn:aws:route53resolver:us-west-2:123456789012:firewall-domain-list/
rslvr-fdl-d61cbb2cbexample",
        "Name": "test",
        "DomainCount": 0,
        "Status": "COMPLETE",
        "StatusMessage": "Created Firewall Domain List",
        "CreatorRequestId": "my-request-id",
        "CreationTime": "2021-05-25T15:55:51.115365Z",
        "ModificationTime": "2021-05-25T15:55:51.115365Z"
    }
}
```

Para obtener más información, consulte Managing your own domain lists en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte CreateFirewallDomainList en la Referencia de comandos de la AWS CLI.

`create-firewall-rule-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-firewall-rule-group`.

AWS CLI

Para crear un grupo de reglas de Firewall

En el siguiente ejemplo de `create-firewall-rule-group`, se crea un grupo de reglas de DNS Firewall.

```
aws route53resolver create-firewall-rule-group \
    --creator-request-id my-request-id \
    --name test
```

Salida:

```
{
    "FirewallRuleGroup": {
        "Id": "rslvr-frg-47f93271fexample",
        "Arn": "arn:aws:route53resolver:us-west-2:123456789012:firewall-rule-group/
rslvr-frg-47f93271fexample",
        "Name": "test",
        "RuleCount": 0,
        "Status": "COMPLETE",
        "StatusMessage": "Created Firewall Rule Group",
        "OwnerId": "123456789012",
        "CreatorRequestId": "my-request-id",
        "ShareStatus": "NOT_SHARED",
        "CreationTime": "2021-05-25T18:59:26.490017Z",
        "ModificationTime": "2021-05-25T18:59:26.490017Z"
    }
}
```

Para obtener más información, consulte Managing rule groups and rules in DNS Firewall en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte CreateFirewallRuleGroup en la Referencia de comandos de la AWS CLI.

`create-firewall-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-firewall-rule`.

AWS CLI

Para crear una regla de firewall

En el siguiente ejemplo de `create-firewall-rule`, se crea una regla de firewall en una regla de DNS Firewall los dominios incluidos en una lista de dominios de DNS Firewall.

```
aws route53resolver create-firewall-rule \
    --name allow-rule \
    --firewall-rule-group-id rslvr-frg-47f93271fexample \
    --firewall-domain-list-id rslvr-fdl-9e956e9ffexample \
    --priority 101 \
    --action ALLOW
```

Salida:

```
{
    "FirewallRule": {
        "FirewallRuleGroupId": "rslvr-frg-47f93271fexample",
        "FirewallDomainListId": "rslvr-fdl-9e956e9ffexample",
        "Name": "allow-rule",
        "Priority": 101,
        "Action": "ALLOW",
        "CreatorRequestId": "d81e3fb7-020b-415e-939f-EXAMPLE11111",
        "CreationTime": "2021-05-25T21:44:00.346093Z",
        "ModificationTime": "2021-05-25T21:44:00.346093Z"
    }
}
```

Para obtener más información, consulte Managing rule groups and rules in DNS Firewall en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte CreateFirewallRule en la Referencia de comandos de la AWS CLI.

`create-resolver-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-resolver-endpoint`.

AWS CLI

Para crear un punto de conexión de Resolver de entrada

En el siguiente ejemplo de `create-resolver-endpoint`, se crea un punto de conexión de Resolver entrante. Puede usar el mismo comando para crear puntos de conexión entrantes y salientes.

aws route53resolver create-resolver-endpoint --name my-inbound-endpoint --creator-request-id 2020-01-01-18:47 --security-group-ids "sg-f62bexam" --direction INBOUND --ip-addresses SubnetId=subnet-ba47exam,Ip=192.0.2.255 SubnetId=subnet-12d8exam,Ip=192.0.2.254

Salida:

```
{
    "ResolverEndpoint": {
        "Id": "rslvr-in-f9ab8a03f1example",
        "CreatorRequestId": "2020-01-01-18:47",
        "Arn": "arn:aws:route53resolver:us-west-2:111122223333:resolver-endpoint/
rslvr-in-f9ab8a03f1example",
        "Name": "my-inbound-endpoint",
        "SecurityGroupIds": [
            "sg-f62bexam"
        ],
        "Direction": "INBOUND",
        "IpAddressCount": 2,
        "HostVPCId": "vpc-304examp",
        "Status": "CREATING",
        "StatusMessage": "[Trace id: 1-5dc1ff84-f3477826e4a190025example] Creating
 the Resolver Endpoint",
        "CreationTime": "2020-01-01T23:02:29.583Z",
        "ModificationTime": "2020-01-01T23:02:29.583Z"
    }
}
```

Para crear un punto de conexión de Resolver de salida

En el siguiente ejemplo de `create-resolver-endpoint`, se crea un punto de conexión de resolución saliente con los valores del documento con formato JSON `create-outbound-resolver-endpoint.json`.

```
aws route53resolver create-resolver-endpoint \
```

```
    --cli-input-json file://c:\temp\create-outbound-resolver-endpoint.json
```

Contenido de `create-outbound-resolver-endpoint.json`:

```
{
   "CreatorRequestId": "2020-01-01-18:47",
   "Direction": "OUTBOUND",
   "IpAddresses": [
      {
         "Ip": "192.0.2.255",
         "SubnetId": "subnet-ba47exam"
      },
      {
         "Ip": "192.0.2.254",
         "SubnetId": "subnet-12d8exam"
      }
   ],
   "Name": "my-outbound-endpoint",
   "SecurityGroupIds": [ "sg-05cd7b25d6example" ],
   "Tags": [
      {
         "Key": "my-key-name",
         "Value": "my-key-value"
      }
   ]
}
```

Para obtener más información, consulte Resolving DNS Queries Between VPCs and Your Network en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte CreateResolverEndpoint en la Referencia de comandos de la AWS CLI.

`create-resolver-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-resolver-rule`.

AWS CLI

Para crear una regla de Resolver

En el siguiente ejemplo de `create-resolver-rule`, se crea una regla de reenvío de Resolver. La regla usa el punto de conexión saliente rslvr-out-d5e5920e37example para reenviar las consultas de DNS de `example.com` a las direcciones IP 10.24.8.75 y 10.24.8.156.

```
aws route53resolver create-resolver-rule \
    --creator-request-id 2020-01-02-18:47 \
    --domain-name example.com \
    --name my-rule \
    --resolver-endpoint-id rslvr-out-d5e5920e37example \
    --rule-type FORWARD \
    --target-ips "Ip=10.24.8.75" "Ip=10.24.8.156"
```

Salida:

```
{
    "ResolverRule": {
        "Status": "COMPLETE",
        "RuleType": "FORWARD",
        "ResolverEndpointId": "rslvr-out-d5e5920e37example",
        "Name": "my-rule",
        "DomainName": "example.com.",
        "CreationTime": "2022-05-10T21:35:30.923187Z",
        "TargetIps": [
            {
                "Ip": "10.24.8.75",
                "Port": 53
            },
            {
                "Ip": "10.24.8.156",
                "Port": 53
            }
        ],
        "CreatorRequestId": "2022-05-10-16:33",
        "ModificationTime": "2022-05-10T21:35:30.923187Z",
        "ShareStatus": "NOT_SHARED",
        "Arn": "arn:aws:route53resolver:us-east-1:111117012054:resolver-rule/rslvr-
rr-b1e0b905e93611111",
        "OwnerId": "111111111111",
        "Id": "rslvr-rr-rslvr-rr-b1e0b905e93611111",
        "StatusMessage": "[Trace id: 1-22222222-3e56afcc71a3724664f22e24]
 Successfully created Resolver Rule."
    }
```

```
}
```

- Para obtener información sobre la API, consulte CreateResolverRule en la Referencia de comandos de la AWS CLI.

`delete-firewall-domain-list`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-firewall-domain-list`.

AWS CLI

Para eliminar una lista de dominios de DNS Firewall de Route 53 Resolver

En el siguiente ejemplo de `delete-firewall-domain-list`, se elimina una lista de dominios de Route 53 Resolver DNS Firewall, denominada test, en su cuenta de AWS.

```
aws route53resolver delete-firewall-domain-list \
    --firewall-domain-list-id rslvr-fdl-9e956e9ffexample
```

Salida:

```
{
    "FirewallDomainList": {
        "Id": "rslvr-fdl-9e956e9ffexample",
        "Arn": "arn:aws:route53resolver:us-west-2:123456789012:firewall-domain-list/
rslvr-fdl-9e956e9ffexample",
        "Name": "test",
        "DomainCount": 6,
        "Status": "DELETING",
        "StatusMessage": "Deleting the Firewall Domain List",
        "CreatorRequestId": "my-request-id",
        "CreationTime": "2021-05-25T15:55:51.115365Z",
        "ModificationTime": "2021-05-25T18:58:05.588024Z"
    }
}
```

Para obtener más información, consulte Managing your own domain lists en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte DeleteFirewallDomainList en la Referencia de comandos de la AWS CLI.

`delete-firewall-rule-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-firewall-rule-group`.

AWS CLI

Para eliminar un grupo de reglas de firewall

En el siguiente ejemplo de `delete-firewall-rule-group`, se elimina un grupo de reglas de firewall.

```
aws route53resolver delete-firewall-rule-group \
    --firewall-rule-group-id rslvr-frg-47f93271fexample
```

Salida:

```
{
    "FirewallRuleGroup": {
        "Id": "rslvr-frg-47f93271fexample",
        "Arn": "arn:aws:route53resolver:us-west-2:123456789012:firewall-rule-group/
rslvr-frg-47f93271fexample",
        "Name": "test",
        "RuleCount": 0,
        "Status": "UPDATING",
        "StatusMessage": "Updating Firewall Rule Group",
        "OwnerId": "123456789012",
        "CreatorRequestId": "my-request-id",
        "ShareStatus": "NOT_SHARED",
        "CreationTime": "2021-05-25T18:59:26.490017Z",
        "ModificationTime": "2021-05-25T21:51:53.028688Z"
    }
}
```

Para obtener más información, consulte Managing rule groups and rules in DNS Firewall en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte DeleteFirewallRuleGroup en la Referencia de comandos de la AWS CLI.

`delete-firewall-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-firewall-rule`.

AWS CLI

Para eliminar una regla de firewall

En el siguiente ejemplo de `delete-firewall-rule`, se elimina una regla de firewall especificada.

```
aws route53resolver delete-firewall-rule \
    --firewall-rule-group-id rslvr-frg-47f93271fexample \
    --firewall-domain-list-id rslvr-fdl-9e956e9ffexample
```

Salida:

```
{
    "FirewallRule": {
        "FirewallRuleGroupId": "rslvr-frg-47f93271fexample",
        "FirewallDomainListId": "rslvr-fdl-9e956e9ffexample",
        "Name": "allow-rule",
        "Priority": 102,
        "Action": "ALLOW",
        "CreatorRequestId": "d81e3fb7-020b-415e-939f-EXAMPLE11111",
        "CreationTime": "2021-05-25T21:44:00.346093Z",
        "ModificationTime": "2021-05-25T21:45:59.611600Z"
    }
}
```

Para obtener más información, consulte Managing rule groups and rules in DNS Firewall en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte DeleteFirewallRule en la Referencia de comandos de la AWS CLI.

`delete-resolver-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-resolver-endpoint`.

AWS CLI

Para eliminar un punto de conexión de Resolver

En el siguiente ejemplo de `delete-resolver-endpoint`, se elimina el punto de conexión especificado.

Importante: Si elimina un punto de conexión de entrada, las consultas de DNS procedentes de su red ya no se reenvían al solucionador de la VPC que ha especificado en el punto de conexión. Si elimina un punto de conexión de salida, Resolver deja de reenviar las consultas de DNS desde su VPC a la red para las reglas que especifican el punto de conexión de salida eliminado.

```
aws route53resolver delete-resolver-endpoint \
    --resolver-endpoint-id rslvr-in-497098ad59example
```

Salida:

```
{
    "ResolverEndpoint": {
        "Id": "rslvr-in-497098ad59example",
        "CreatorRequestId": "AWSConsole.25.157290example",
        "Arn": "arn:aws:route53resolver:us-west-2:111122223333:resolver-endpoint/
rslvr-in-497098ad59example",
        "Name": "my-inbound-endpoint",
        "SecurityGroupIds": [
            "sg-05cd7b25d6example"
        ],
        "Direction": "INBOUND",
        "IpAddressCount": 5,
        "HostVPCId": "vpc-304bexam",
        "Status": "DELETING",
        "StatusMessage": "[Trace id: 1-5dc5b658-811b5be0922bbc382example] Deleting
 ResolverEndpoint.",
        "CreationTime": "2020-01-01T23:25:45.538Z",
        "ModificationTime": "2020-01-02T23:25:45.538Z"
    }
}
```

- Para obtener información sobre la API, consulte DeleteResolverEndpoint en la Referencia de comandos de la AWS CLI.

`delete-resolver-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-resolver-rule`.

AWS CLI

Para eliminar una regla de Resolver

En el siguiente ejemplo de `delete-resolver-rule`, se elimina la regla especificada.

Nota: Si la regla de reenvío está asociada a alguna VPC, debe anular la asociación de la regla de las VPC para poder eliminarla.

```
aws route53resolver delete-resolver-rule \
    --resolver-rule-id rslvr-rr-5b3809426bexample
```

Salida:

```
{
    "ResolverRule": {
        "Id": "rslvr-rr-5b3809426bexample",
        "CreatorRequestId": "2020-01-03-18:47",
        "Arn": "arn:aws:route53resolver:us-west-2:111122223333:resolver-rule/rslvr-
rr-5b3809426bexample",
        "DomainName": "zenith.example.com.",
        "Status": "DELETING",
        "StatusMessage": "[Trace id: 1-5dc5e05b-602e67b052cb74f05example] Deleting
 Resolver Rule.",
        "RuleType": "FORWARD",
        "Name": "my-resolver-rule",
        "TargetIps": [
            {
                "Ip": "192.0.2.50",
                "Port": 53
            }
        ],
        "ResolverEndpointId": "rslvr-out-d5e5920e3example",
        "OwnerId": "111122223333",
        "ShareStatus": "NOT_SHARED"
    }
}
```

- Para obtener información sobre la API, consulte DeleteResolverRule en la Referencia de comandos de la AWS CLI.

`disassociate-firewall-rule-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-firewall-rule-group`.

AWS CLI

Para desasociar un grupo de reglas de firewall de una VPC

En el siguiente ejemplo de `disassociate-firewall-rule-group`, se desvincula un grupo de reglas de DNS Firewall de una Amazon VPC.

```
aws route53resolver disassociate-firewall-rule-group \
    --firewall-rule-group-association-id rslvr-frgassoc-57e8873d7example
```

Salida:

```
{
    "FirewallRuleGroupAssociation": {
        "Id": "rslvr-frgassoc-57e8873d7example",
        "Arn": "arn:aws:route53resolver:us-west-2:123456789012:firewall-rule-group-
association/rslvr-frgassoc-57e8873d7example",
        "FirewallRuleGroupId": "rslvr-frg-47f93271fexample",
        "VpcId": "vpc-31e92222",
        "Name": "test-association",
        "Priority": 103,
        "MutationProtection": "DISABLED",
        "Status": "DELETING",
        "StatusMessage": "Deleting the Firewall Rule Group Association",
        "CreatorRequestId": "2ca1a304-32b3-4f5f-bc4c-EXAMPLE11111",
        "CreationTime": "2021-05-25T21:47:48.755768Z",
        "ModificationTime": "2021-05-25T21:51:02.377887Z"
    }
}
```

Para obtener más información, consulte Managing associations between your VPC and Route 53 Resolver DNS Firewall rule groups en la Guía del desarrollador de Amazon Route 53.

- Para obtener información sobre la API, consulte DisassociateFirewallRuleGroup en la Referencia de comandos de la AWS CLI.

`disassociate-resolver-endpoint-ip-address`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-resolver-endpoint-ip-address`.

AWS CLI

Para desasociar una dirección IP de un punto de conexión de Resolver

En el siguiente ejemplo de `disassociate-resolver-endpoint-ip-address`, se elimina una dirección IP de un punto de conexión entrante o saliente de Resolver especificado.

Nota: Un punto de conexión debe tener al menos dos direcciones IP. Si un punto de conexión actualmente solo tiene dos direcciones IP y desea reemplazar una dirección por otra, primero debe usar associate-resolver-endpoint-ip-address para asociar la nueva dirección IP. A continuación, puede desasociar una de las direcciones IP originales del punto de conexión.

```
aws route53resolver disassociate-resolver-endpoint-ip-address \
    --resolver-endpoint-id rslvr-in-f9ab8a03f1example \
    --ip-address="SubnetId=subnet-12d8a459,Ip=172.31.40.121"
```

Salida:

```
{
    "ResolverEndpoint": {
        "Id": "rslvr-in-f9ab8a03f1example",
        "CreatorRequestId": "2020-01-01-18:47",
        "Arn": "arn:aws:route53resolver:us-west-2:111122223333:resolver-endpoint/
rslvr-in-f9ab8a03f1example",
        "Name": "my-inbound-endpoint",
        "SecurityGroupIds": [
            "sg-f62bexam"
        ],
        "Direction": "INBOUND",
        "IpAddressCount": 3,
        "HostVPCId": "vpc-304bexam",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Resolver Endpoint",
        "CreationTime": "2020-01-01T23:02:29.583Z",
        "ModificationTime": "2020-01-05T23:02:29.583Z"
    }
}
```

- Para obtener información sobre la API, consulte DisassociateResolverEndpointIpAddress en la Referencia de comandos de AWS CLI.

`disassociate-resolver-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-resolver-rule`.

AWS CLI

Para desasociar una regla de Resolver de una Amazon VPC

En el siguiente ejemplo de `disassociate-resolver-rule`, se elimina la asociación entre la regla de Resolver y la VPC especificadas. Puede anular la asociación de una regla de una VPC en las siguientes circunstancias:

Para las consultas de DNS que se originan en esta VPC, recomendamos que Resolver deje de reenviar consultas a su red las consultas para el nombre de dominio especificado en la regla. Le recomendamos que elimine la regla de reenvío. Si una regla está asociada actualmente a una o varias VPC, debe anular la asociación de la regla de todas las VPC para poder eliminarla.

```
aws route53resolver disassociate-resolver-rule \
    --resolver-rule-id rslvr-rr-4955cb98ceexample \
    --vpc-id vpc-304bexam
```

Salida:

```
{
    "ResolverRuleAssociation": {
        "Id": "rslvr-rrassoc-322f4e8b9cexample",
        "ResolverRuleId": "rslvr-rr-4955cb98ceexample",
        "Name": "my-resolver-rule-association",
        "VPCId": "vpc-304bexam",
        "Status": "DELETING",
        "StatusMessage": "[Trace id: 1-5dc5ffa2-a26c38004c1f94006example] Deleting
 Association"
    }
}
```

- Para obtener información sobre la API, consulte DisassociateResolverRule en la Referencia de la comandos de la AWS CLI.

`get-firewall-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-firewall-config`.

AWS CLI

Para obtener una configuración de firewall para una VPC

En el siguiente ejemplo de `get-firewall-config`, se recupera el comportamiento de DNS Firewall de la VPC especificada.

```
aws route53resolver get-firewall-config \
    --resource-id vpc-31e92222
```

Salida:

```
{
    "FirewallConfig": {
        "Id": "rslvr-fc-86016850cexample",
        "ResourceId": "vpc-31e9222",
        "OwnerId": "123456789012",
        "FirewallFailOpen": "DISABLED"
    }
}
```

Para obtener más información, consulte DNS Firewall VPC configuration en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte GetFirewallConfig en la Referencia de comandos de la AWS CLI.

`get-firewall-domain-list`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-firewall-domain-list`.

AWS CLI

Para obtener una lista de dominios de DNS Firewall de Route 53 Resolver

En el siguiente ejemplo de `get-firewall-domain-list`, se recupera la lista de dominios con el ID que especifique.

```
aws route53resolver get-firewall-domain-list \
    --firewall-domain-list-id rslvr-fdl-42b60677cexample
```

Salida:

```
{
    "FirewallDomainList": {
        "Id": "rslvr-fdl-9e956e9ffexample",
        "Arn": "arn:aws:route53resolver:us-west-2:123457689012:firewall-domain-list/
rslvr-fdl-42b60677cexample",
        "Name": "test",
        "DomainCount": 0,
        "Status": "COMPLETE",
        "StatusMessage": "Created Firewall Domain List",
        "CreatorRequestId": "my-request-id",
        "CreationTime": "2021-05-25T15:55:51.115365Z",
        "ModificationTime": "2021-05-25T15:55:51.115365Z"
    }
}
```

Para obtener más información, consulte Managing your own domain lists en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte GetFirewallDomainList en la Referencia de comandos de la AWS CLI.

`get-firewall-rule-group-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-firewall-rule-group-association`.

AWS CLI

Para obtener una asociación de grupos de reglas de firewall

En el siguiente ejemplo de `get-firewall-rule-group-association`, se recupera una asociación de grupos de reglas de firewall.

```
aws route53resolver get-firewall-rule-group-association \
    --firewall-rule-group-association-id rslvr-frgassoc-57e8873d7example
```

Salida:

```
{
```

```
    "FirewallRuleGroupAssociation": {
        "Id": "rslvr-frgassoc-57e8873d7example",
        "Arn": "arn:aws:route53resolver:us-west-2:123456789012:firewall-rule-group-
association/rslvr-frgassoc-57e8873d7example",
        "FirewallRuleGroupId": "rslvr-frg-47f93271fexample",
        "VpcId": "vpc-31e92222",
        "Name": "test-association",
        "Priority": 101,
        "MutationProtection": "DISABLED",
        "Status": "COMPLETE",
        "StatusMessage": "Finished rule group association update",
        "CreatorRequestId": "2ca1a304-32b3-4f5f-bc4c-EXAMPLE11111",
        "CreationTime": "2021-05-25T21:47:48.755768Z",
        "ModificationTime": "2021-05-25T21:47:48.755768Z"
    }
}
```

Para obtener más información, consulte Managing associations between your VPC and Route 53 Resolver DNS Firewall rule groups en la Guía del desarrollador de Amazon Route 53.

- Para obtener información sobre la API, consulte GetFirewallRuleGroupAssociation en la Referencia de comandos de la AWS CLI.

`get-firewall-rule-group-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-firewall-rule-group-policy`.

AWS CLI

Para obtener una política de AWS IAM

En el siguiente ejemplo de `get-firewall-rule-group-policy`, se obtiene la política de AWS Identity and Access Management (AWS IAM) para compartir el grupo de reglas especificado.

```
aws route53resolver get-firewall-rule-group-policy \
    --arn arn:aws:route53resolver:us-west-2:AWS_ACCOUNT_ID:firewall-rule-group/
rslvr-frg-47f93271fexample
```

Salida:

```
{
```

```
    "FirewallRuleGroupPolicy": "{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Sid\":\"test\",\"Effect\":\"Allow\",\"Principal
\":{\"AWS\":\"arn:aws:iam::AWS_ACCOUNT_ID:root\"},\"Action\":
[\"route53resolver:GetFirewallRuleGroup\",\"route53resolver:ListFirewallRuleGroups
\"],\"Resource\":\"arn:aws:route53resolver:us-east-1:AWS_ACCOUNT_ID:firewall-rule-
group/rslvr-frg-47f93271fexample\"}]}"
}
```

Para obtener más información, consulte Managing rule groups and rules in DNS Firewall en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte GetFirewallRuleGroupPolicy en la Referencia de comandos de la AWS CLI.

`get-firewall-rule-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-firewall-rule-group`.

AWS CLI

Para obtener un grupo de reglas de Firewall

En el siguiente ejemplo de `get-firewall-rule-group`, se recupera información sobre un grupo de reglas de DNS Firewall con el ID que proporcione.

```
aws route53resolver get-firewall-rule-group \
    --firewall-rule-group-id rslvr-frg-47f93271fexample
```

Salida:

```
{
    "FirewallRuleGroup": {
        "Id": "rslvr-frg-47f93271fexample",
        "Arn": "arn:aws:route53resolver:us-west-2:123456789012:firewall-rule-group/
rslvr-frg-47f93271fexample",
        "Name": "test",
        "RuleCount": 0,
        "Status": "COMPLETE",
        "StatusMessage": "Created Firewall Rule Group",
        "OwnerId": "123456789012",
        "CreatorRequestId": "my-request-id",
```

```
        "ShareStatus": "NOT_SHARED",
        "CreationTime": "2021-05-25T18:59:26.490017Z",
        "ModificationTime": "2021-05-25T18:59:26.490017Z"
    }
}
```

Para obtener más información, consulte Managing rule groups and rules in DNS Firewall en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte GetFirewallRuleGroup en la Referencia de comandos de la AWS CLI.

`get-resolver-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resolver-endpoint`.

AWS CLI

Para obtener información sobre un punto de conexión de Resolver

En el ejemplo siguiente de `get-resolver-endpoint`, se muestran los detalles del punto de conexión saliente especificado. Puede usar `get-resolver-endpoint` para los puntos de conexión entrantes y salientes especificando el ID de punto de conexión correspondiente.

```
aws route53resolver get-resolver-endpoint \
    --resolver-endpoint-id rslvr-out-d5e5920e37example
```

Salida:

```
{
    "ResolverEndpoint": {
        "Id": "rslvr-out-d5e5920e37example",
        "CreatorRequestId": "2020-01-01-18:47",
        "Arn": "arn:aws:route53resolver:us-west-2:111122223333:resolver-endpoint/
rslvr-out-d5e5920e37example",
        "Name": "my-outbound-endpoint",
        "SecurityGroupIds": [
            "sg-05cd7b25d6example"
        ],
        "Direction": "OUTBOUND",
        "IpAddressCount": 2,
```

```
        "HostVPCId": "vpc-304bexam",
        "Status": "OPERATIONAL",
        "StatusMessage": "This Resolver Endpoint is operational.",
        "CreationTime": "2020-01-01T23:50:50.979Z",
        "ModificationTime": "2020-01-02T23:50:50.979Z"
    }
}
```

Para obtener más información, consulte Values That You Specify When You Create or Edit Inbound Endpoints en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte GetResolverEndpoint en la Referencia de comandos de la AWS CLI.

`get-resolver-rule-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resolver-rule-association`.

AWS CLI

Para obtener información acerca de la asociación entre una regla de Resolver y una VPC

En el siguiente ejemplo de `get-resolver-rule-association`, se muestran detalles acerca de la asociación entre una regla de Resolver especificada y una VPC. Para asociar una regla de solucionador y una VPC, utilice associate-resolver-rule.

```
aws route53resolver get-resolver-rule-association \
    --resolver-rule-association-id rslvr-rrassoc-d61cbb2c8bexample
```

Salida:

```
{
    "ResolverRuleAssociation": {
        "Id": "rslvr-rrassoc-d61cbb2c8bexample",
        "ResolverRuleId": "rslvr-rr-42b60677c0example",
        "Name": "my-resolver-rule-association",
        "VPCId": "vpc-304bexam",
        "Status": "COMPLETE",
        "StatusMessage": ""
    }
}
```

- Para obtener información sobre la API, consulte GetResolverRuleAssociation en la Referencia de comandos de la AWS CLI.

`get-resolver-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resolver-rule`.

AWS CLI

Para obtener información sobre un punto de conexión de Resolver

En el siguiente ejemplo de `get-resolver-rule`, se muestran detalles acerca de la regla de Resolver especificada, como, por ejemplo, el nombre de dominio al que la regla envía las consultas de DNS y el ID del punto de conexión de resolución saliente al que está asociada la regla.

```
aws route53resolver get-resolver-rule \
    --resolver-rule-id rslvr-rr-42b60677c0example
```

Salida:

```
{
    "ResolverRule": {
        "Id": "rslvr-rr-42b60677c0example",
        "CreatorRequestId": "2020-01-01-18:47",
        "Arn": "arn:aws:route53resolver:us-west-2:111122223333:resolver-rule/rslvr-
rr-42b60677c0example",
        "DomainName": "example.com.",
        "Status": "COMPLETE",
        "StatusMessage": "[Trace id: 1-5dc4b177-ff1d9d001a0f80005example]
 Successfully created Resolver Rule.",
        "RuleType": "FORWARD",
        "Name": "my-rule",
        "TargetIps": [
            {
                "Ip": "192.0.2.45",
                "Port": 53
            }
        ],
        "ResolverEndpointId": "rslvr-out-d5e5920e37example",
        "OwnerId": "111122223333",
```

```
        "ShareStatus": "NOT_SHARED"
    }
}
```

Para obtener más información, consulte Values That You Specify When You Create or Edit Rules en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte GetResolverRule en la Referencia de comandos de la AWS CLI.

`import-firewall-domains`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-firewall-domains`.

AWS CLI

Para importar dominios a una lista de dominios

En el siguiente ejemplo de `import-firewall-domains`, se importa un conjunto de dominios de un archivo a la lista de dominios de Firewall DNS que especifique.

```
aws route53resolver import-firewall-domains \
    --firewall-domain-list-id rslvr-fdl-d61cbb2cbexample \
    --operation REPLACE \
    --domain-file-url s3://PATH/TO/YOUR/FILE
```

Salida:

```
{
    "Id": "rslvr-fdl-d61cbb2cbexample",
    "Name": "test",
    "Status": "IMPORTING",
    "StatusMessage": "Importing domains from provided file."
}
```

Para obtener más información, consulte Managing your own domain lists en la Guía para desarrolladores de Amazon Route 53.

- Para obtener detalles sobre la API, consulte ImportFirewallDomains en la Referencia de comandos de la AWS CLI.

`list-firewall-configs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-firewall-configs`.

AWS CLI

Para ver una lista de las configuraciones de firewall

En el siguiente ejemplo de `list-firewall-configs`, se muestran todas las configuraciones de DNS Firewall.

```
aws route53resolver list-firewall-configs
```

Salida:

```
{
    "FirewallConfigs": [
        {
            "Id": "rslvr-fc-86016850cexample",
            "ResourceId": "vpc-31e92222",
            "OwnerId": "123456789012",
            "FirewallFailOpen": "DISABLED"
        }
    ]
}
```

Para obtener más información, consulte DNS Firewall VPC configuration en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte ListFirewallConfigs en la Referencia de comandos de la AWS CLI.

`list-firewall-domain-lists`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-firewall-domain-lists`.

AWS CLI

Para ver todas las listas de dominios de DNS Firewall de Route 53 Resolver

En el siguiente ejemplo de `list-firewall-domain-lists`, se enumeran todas las listas de dominios.

```
aws route53resolver list-firewall-domain-lists
```

Salida:

```
{
    "FirewallDomainLists": [
        {
            "Id": "rslvr-fdl-2c46f2ecfexample",
            "Arn": "arn:aws:route53resolver:us-west-2:123456789012:firewall-domain-
list/rslvr-fdl-2c46f2ecfexample",
            "Name": "AWSManagedDomainsMalwareDomainList",
            "CreatorRequestId": "AWSManagedDomainsMalwareDomainList",
            "ManagedOwnerName": "Route 53 Resolver DNS Firewall"
        },
        {
            "Id": "rslvr-fdl-aa970e9e1example",
            "Arn": "arn:aws:route53resolver:us-west-2:123456789012:firewall-domain-
list/rslvr-fdl-aa970e9e1example",
            "Name": "AWSManagedDomainsBotnetCommandandControl",
            "CreatorRequestId": "AWSManagedDomainsBotnetCommandandControl",
            "ManagedOwnerName": "Route 53 Resolver DNS Firewall"
        },
        {
            "Id": "rslvr-fdl-42b60677cexample",
            "Arn": "arn:aws:route53resolver:us-west-2:123456789111:firewall-domain-
list/rslvr-fdl-42b60677cexample",
            "Name": "test",
            "CreatorRequestId": "my-request-id"
        }
    ]
}
```

Para obtener más información, consulte Route 53 Resolver DNS Firewall domain lists en la Guía del desarrollador de Amazon Route 53.

- Para obtener información sobre la API, consulte ListFirewallDomainLists en la Referencia de comandos de la AWS CLI.

`list-firewall-domains`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-firewall-domains`.

AWS CLI

Para enumerar los dominios de una lista de dominios

En el siguiente ejemplo de `list-firewall-domains`, se enumeran los dominios de una lista de dominios de DNS Firewall que especifique.

```
aws route53resolver list-firewall-domains \
    --firewall-domain-list-id rslvr-fdl-d61cbb2cbexample
```

Salida:

```
{
    "Domains": [
        "test1.com.",
        "test2.com.",
        "test3.com."
    ]
}
```

Para obtener más información, consulte Managing your own domain lists en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte ListFirewallDomains en la Referencia de comandos de la AWS CLI.

`list-firewall-rule-group-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-firewall-rule-group-associations`.

AWS CLI

Para enumerar las asociaciones de grupos de reglas de DNS Firewall

En el siguiente ejemplo de `list-firewall-rule-group-associations`, se enumera sus asociaciones de grupo de reglas de DNS Firewall con una Amazon VPC.

```
aws route53resolver list-firewall-rule-group-associations
```

Salida:

```
{
    "FirewallRuleGroupAssociations": [
        {
            "Id": "rslvr-frgassoc-57e8873d7example",
            "Arn": "arn:aws:route53resolver:us-west-2:123456789012:firewall-rule-
group-association/rslvr-frgassoc-57e8873d7example",
            "FirewallRuleGroupId": "rslvr-frg-47f93271fexample",
            "VpcId": "vpc-31e92222",
            "Name": "test-association",
            "Priority": 101,
            "MutationProtection": "DISABLED",
            "Status": "UPDATING",
            "StatusMessage": "Creating Firewall Rule Group Association",
            "CreatorRequestId": "2ca1a304-32b3-4f5f-bc4c-EXAMPLE11111",
            "CreationTime": "2021-05-25T21:47:48.755768Z",
            "ModificationTime": "2021-05-25T21:47:48.755768Z"
        }
    ]
}
```

Para obtener más información, consulte Managing associations between your VPC and Route 53 Resolver DNS Firewall rule group en la Guía del desarrollador de Amazon Route 53.

- Para obtener información sobre la API, consulte ListFirewallRuleGroupAssociations en la Referencia de comandos de la AWS CLI.

`list-firewall-rule-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-firewall-rule-groups`.

AWS CLI

Para obtener una lista de sus grupos de reglas de firewall

En el siguiente ejemplo de `list-firewall-rule-groups`, se enumeran grupos de reglas de DNS Firewall.

```
aws route53resolver list-firewall-rule-groups
```

Salida:

```
{
```

```
    "FirewallRuleGroups": [
        {
            "Id": "rslvr-frg-47f93271fexample",
            "Arn": "arn:aws:route53resolver:us-west-2:123456789012:firewall-rule-
group/rslvr-frg-47f93271fexample",
            "Name": "test",
            "OwnerId": "123456789012",
            "CreatorRequestId": "my-request-id",
            "ShareStatus": "NOT_SHARED"
        }
    ]
}
```

Para obtener más información, consulte Managing rule groups and rules in DNS Firewall en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte ListFirewallRuleGroups en la Referencia de comandos de la AWS CLI.

`list-firewall-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-firewall-rules`.

AWS CLI

Para enumerar las reglas de firewall

En el siguiente ejemplo de `list-firewall-rules`, se enumeran todas las reglas de DNS Firewall dentro de un grupo de reglas de firewall.

```
aws route53resolver list-firewall-rules \
    --firewall-rule-group-id rslvr-frg-47f93271fexample
```

Salida:

```
{
    "FirewallRules": [
        {
            "FirewallRuleGroupId": "rslvr-frg-47f93271fexample",
            "FirewallDomainListId": "rslvr-fdl-9e956e9ffexample",
            "Name": "allow-rule",
            "Priority": 101,
```

```
            "Action": "ALLOW",
            "CreatorRequestId": "d81e3fb7-020b-415e-939f-EXAMPLE11111",
            "CreationTime": "2021-05-25T21:44:00.346093Z",
            "ModificationTime": "2021-05-25T21:44:00.346093Z"
        }
    ]
}
```

Para obtener más información, consulte Managing rule groups and rules in DNS Firewall en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte ListFirewallRules en la Referencia de comandos de la AWS CLI.

`list-resolver-endpoint-ip-addresses`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resolver-endpoint-ip-addresses`.

AWS CLI

Para enumerar las direcciones IP de un punto de conexión entrante o saliente específico

En el siguiente ejemplo de `list-resolver-endpoint-ip-addresses`, se enumera la información sobre las direcciones IP asociadas al punto de conexión entrante `rslvr-in-f9ab8a03f1example`. También puede utilizar `list-resolver-endpoint-ip-addresses` para los puntos de conexión salientes especificando el ID de punto de conexión correspondiente.

```
aws route53resolver list-resolver-endpoint-ip-addresses \
    --resolver-endpoint-id rslvr-in-f9ab8a03f1example
```

Salida:

```
{
    "MaxResults": 10,
    "IpAddresses": [
        {
            "IpId": "rni-1de60cdbfeexample",
            "SubnetId": "subnet-ba47exam",
            "Ip": "192.0.2.44",
            "Status": "ATTACHED",
```

```
            "StatusMessage": "This IP address is operational.",
            "CreationTime": "2020-01-03T23:02:29.587Z",
            "ModificationTime": "2020-01-03T23:03:05.555Z"
        },
        {
            "IpId": "rni-aac7085e38example",
            "SubnetId": "subnet-12d8exam",
            "Ip": "192.0.2.45",
            "Status": "ATTACHED",
            "StatusMessage": "This IP address is operational.",
            "CreationTime": "2020-01-03T23:02:29.593Z",
            "ModificationTime": "2020-01-03T23:02:55.060Z"
        }
    ]
}
```

Para obtener más información sobre los valores de la salida, consulte Values That You Specify When You Create or Edit Inbound Endpoints y Values That You Specify When You Create or Edit Outbound Endpoints en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte ListResolverEndpointIpAddresses en la Referencia de comandos de la AWS CLI.

`list-resolver-endpoints`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resolver-endpoints`.

AWS CLI

Para enumerar los puntos de conexión de Resolver en una región de AWS

En el siguiente ejemplo de `list-resolver-endpoints`, se enumeran los puntos de conexión de Resolver entrantes y salientes que existen en la cuenta actual.

```
aws route53resolver list-resolver-endpoints
```

Salida:

```
{
    "MaxResults": 10,
    "ResolverEndpoints": [
        {
```

```
            "Id": "rslvr-in-497098ad59example",
            "CreatorRequestId": "2020-01-01-18:47",
            "Arn": "arn:aws:route53resolver:us-west-2:111122223333:resolver-
endpoint/rslvr-in-497098ad59example",
            "Name": "my-inbound-endpoint",
            "SecurityGroupIds": [
                "sg-05cd7b25d6example"
            ],
            "Direction": "INBOUND",
            "IpAddressCount": 2,
            "HostVPCId": "vpc-304bexam",
            "Status": "OPERATIONAL",
            "StatusMessage": "This Resolver Endpoint is operational.",
            "CreationTime": "2020-01-01T23:25:45.538Z",
            "ModificationTime": "2020-01-01T23:25:45.538Z"
        },
        {
            "Id": "rslvr-out-d5e5920e37example",
            "CreatorRequestId": "2020-01-01-18:48",
            "Arn": "arn:aws:route53resolver:us-west-2:111122223333:resolver-
endpoint/rslvr-out-d5e5920e37example",
            "Name": "my-outbound-endpoint",
            "SecurityGroupIds": [
                "sg-05cd7b25d6example"
            ],
            "Direction": "OUTBOUND",
            "IpAddressCount": 2,
            "HostVPCId": "vpc-304bexam",
            "Status": "OPERATIONAL",
            "StatusMessage": "This Resolver Endpoint is operational.",
            "CreationTime": "2020-01-01T23:50:50.979Z",
            "ModificationTime": "2020-01-01T23:50:50.979Z"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListResolverEndpoints en la Referencia de comandos de la AWS CLI.

`list-resolver-rule-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resolver-rule-associations`.

AWS CLI

Para enumerar las asociaciones entre reglas de Resolver y VPC

En el siguiente ejemplo de `list-resolver-rule-associations`, se enumeran las asociaciones entre las reglas de resolución y las VPC de la cuenta actual de AWS.

```
aws route53resolver list-resolver-rule-associations
```

Salida:

```
{
    "MaxResults": 30,
    "ResolverRuleAssociations": [
        {
            "Id": "rslvr-autodefined-assoc-vpc-304bexam-internet-resolver",
            "ResolverRuleId": "rslvr-autodefined-rr-internet-resolver",
            "Name": "System Rule Association",
            "VPCId": "vpc-304bexam",
            "Status": "COMPLETE",
            "StatusMessage": ""
        },
        {
            "Id": "rslvr-rrassoc-d61cbb2c8bexample",
            "ResolverRuleId": "rslvr-rr-42b60677c0example",
            "Name": "my-resolver-rule-association",
            "VPCId": "vpc-304bexam",
            "Status": "COMPLETE",
            "StatusMessage": ""
        }
    ]
}
```

Para obtener más información, consulte How Route 53 Resolver Forwards DNS Queries from Your VPCs to Your Network en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte ListResolverRuleAssociations en la Referencia de comandos de la AWS CLI.

`list-resolver-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resolver-rules`.

AWS CLI

Para enumerar las reglas de Resolver

En el siguiente ejemplo de `list-resolver-rules`, se enumeran todas las reglas de Resolver de la cuenta actual de AWS.

```
aws route53resolver list-resolver-rules
```

Salida:

```
{
    "MaxResults": 30,
    "ResolverRules": [
        {
            "Id": "rslvr-autodefined-rr-internet-resolver",
            "CreatorRequestId": "",
            "Arn": "arn:aws:route53resolver:us-west-2::autodefined-rule/rslvr-
autodefined-rr-internet-resolver",
            "DomainName": ".",
            "Status": "COMPLETE",
            "RuleType": "RECURSIVE",
            "Name": "Internet Resolver",
            "OwnerId": "Route 53 Resolver",
            "ShareStatus": "NOT_SHARED"
        },
        {
            "Id": "rslvr-rr-42b60677c0example",
            "CreatorRequestId": "2020-01-01-18:47",
            "Arn": "arn:aws:route53resolver:us-west-2:111122223333:resolver-rule/
rslvr-rr-42b60677c0bc4e299",
            "DomainName": "example.com.",
            "Status": "COMPLETE",
            "StatusMessage": "[Trace id: 1-5dc4b177-ff1d9d001a0f80005example]
 Successfully created Resolver Rule.",
            "RuleType": "FORWARD",
            "Name": "my-rule",
            "TargetIps": [
                {
                    "Ip": "192.0.2.45",
                    "Port": 53
                }
            ],
```

```
            "ResolverEndpointId": "rslvr-out-d5e5920e37example",
            "OwnerId": "111122223333",
            "ShareStatus": "NOT_SHARED"
        }
    ]
}
```

Para obtener más información, consulte How Route 53 Resolver Forwards DNS Queries from Your VPCs to Your Network en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte ListResolverRules en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas para un recurso de Resolver

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran todas las etiquetas asignadas a la regla de Resolver especificada.

```
aws route53resolver list-tags-for-resource \
    --resource-arn "arn:aws:route53resolver:us-west-2:111122223333:resolver-rule/
rslvr-rr-42b60677c0example"
```

Salida:

```
{
    "Tags": [
        {
            "Key": "my-key-1",
            "Value": "my-value-1"
        },
        {
            "Key": "my-key-2",
            "Value": "my-value-2"
        }
    ]
}
```

Para obtener más información sobre el uso de etiquetas para la asignación de costos, consulte Using Cost Allocation Tags en la Guía del usuario de Administración de facturación y costos de AWS.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`put-firewall-rule-group-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-firewall-rule-group-policy`.

AWS CLI

Para asociar una política de AWS IAM para compartir una política de grupo de reglas de firewall

En el siguiente ejemplo de `put-firewall-rule-group-policy`, se asocia una política de AWS Identity and Access Management (AWS IAM) para compartir el grupo de reglas.

```
aws route53resolver put-firewall-rule-group-policy \
    --firewall-rule-group-policy "{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Sid\":\"test\",\"Effect\":\"Allow\",\"Principal
\":{\"AWS\":\"arn:aws:iam::AWS_ACCOUNT_ID:root\"},\"Action\":
[\"route53resolver:GetFirewallRuleGroup\",\"route53resolver:ListFirewallRuleGroups
\"],\"Resource\":\"arn:aws:route53resolver:us-east-1:AWS_ACCOUNT_ID:firewall-rule-
group/rslvr-frg-47f93271fexample\"}]}"
```

Salida:

```
{
    "ReturnValue": true
}
```

Para obtener más información, consulte Managing rule groups and rules in DNS Firewall en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte PutFirewallRuleGroupPolicy en la Referencia de Cmdlet de AWS CLI.

`put-resolver-rule-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-resolver-rule-policy`.

AWS CLI

Para compartir una regla de Resolver con otra cuenta de AWS

En el siguiente ejemplo de `put-resolver-rule-policy`, se especifica una regla de Resolver que desea compartir con otra cuenta de AWS, la cuenta con la que desea compartir la regla y las operaciones relacionadas con las reglas que desea que la cuenta pueda realizar en las reglas.

Nota: Debe ejecutar este comando con las credenciales de la misma cuenta que ha creado la regla.

```
aws route53resolver put-resolver-rule-policy \
    --region us-east-1 \
    --arn "arn:aws:route53resolver:us-east-1:111122223333:resolver-rule/rslvr-rr-42b60677c0example" \
    --resolver-rule-policy "{\"Version\": \"2012-10-17\", \
        \"Statement\": [ { \
        \"Effect\" : \"Allow\", \
        \"Principal\" : {\"AWS\" : \"444455556666\" }, \
        \"Action\" : [ \
            \"route53resolver:GetResolverRule\", \
            \"route53resolver:AssociateResolverRule\", \
            \"route53resolver:DisassociateResolverRule\", \
            \"route53resolver:ListResolverRules\", \
            \"route53resolver:ListResolverRuleAssociations\" ], \
        \"Resource\" : [ \"arn:aws:route53resolver:us-east-1:111122223333:resolver-rule/rslvr-rr-42b60677c0example\" ] } ] }"
```

Salida:

```
{
    "ReturnValue": true
}
```

Después de ejecutar `put-resolver-rule-policy`, puede ejecutar los dos siguientes comandos de Resource Access Manager (RAM). Debe usar la cuenta con la que desea compartir la regla:

`get-resource-share-invitations` devuelve el valor `resourceShareInvitationArn`. Necesita este valor para aceptar la invitación a usar la regla compartida. `accept-resource-share-invitation` acepta la invitación a usar la regla compartida.

Para obtener más información, consulte la documentación siguiente:

get-resource-share-invitationsaccept-resource-share-invitationsSharing Forwarding Rules with Other AWS Accounts and Using Shared Rules en la Guía para desarrolladores de Amazon Route 53

- Para obtener información sobre la API, consulte PutResolverRulePolicy en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para asociar etiquetas a un recurso de Resolver

En el siguiente ejemplo de `tag-resource`, se asocian dos pares clave-valor de etiqueta a la regla de Resolver especificada.

```
aws route53resolver tag-resource \
    --resource-arn "arn:aws:route53resolver:us-west-2:111122223333:resolver-rule/
rslvr-rr-42b60677c0example" \
    --tags "Key=my-key-1,Value=my-value-1" "Key=my-key-2,Value=my-value-2"
```

Este comando no genera ninguna salida.

Para obtener más información sobre el uso de etiquetas para la asignación de costos, consulte Using Cost Allocation Tags en la Guía del usuario de Administración de facturación y costos de AWS.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar etiquetas de un recurso de Resolver

En el siguiente ejemplo de `untag-resource`, se eliminan dos etiquetas de la regla de Resolver especificada.

```
aws route53resolver untag-resource \
    --resource-arn "arn:aws:route53resolver:us-west-2:111122223333:resolver-rule/
rslvr-rr-42b60677c0example" \
    --tag-keys my-key-1 my-key-2
```

Este comando no genera ninguna salida. Para confirmar que se han eliminado las etiquetas, puede usar list-tags-for-resource.

Para obtener más información sobre el uso de etiquetas para la asignación de costos, consulte Using Cost Allocation Tags en la Guía del usuario de Administración de facturación y costos de AWS.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-firewall-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-firewall-config`.

AWS CLI

Para actualizar una configuración de firewall

En el siguiente ejemplo de `update-firewall-config`, se actualiza la configuración de DNS Firewall.

```
aws route53resolver update-firewall-config \
    --resource-id vpc-31e92222 \
    --firewall-fail-open DISABLED
```

Salida:

```
{
    "FirewallConfig": {
        "Id": "rslvr-fc-86016850cexample",
        "ResourceId": "vpc-31e92222",
        "OwnerId": "123456789012",
```

```
        "FirewallFailOpen": "DISABLED"
    }
}
```

Para obtener más información, consulte DNS Firewall VPC configuration en la Guía para desarrolladores de Amazon Route 53.

- Para obtener detalles sobre la API, consulte UpdateFirewallConfig en la Referencia de comandos de la AWS CLI.

`update-firewall-domains`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-firewall-domains`.

AWS CLI

Para actualizar una lista de dominios

En el siguiente ejemplo de `update-firewall-domains`, se agregan los dominios a una lista de dominios con el ID que proporcione.

```
aws route53resolver update-firewall-domains \
    --firewall-domain-list-id rslvr-fdl-42b60677cexampleb \
    --operation ADD \
    --domains test1.com test2.com test3.com
```

Salida:

```
{
    "Id": "rslvr-fdl-42b60677cexample",
    "Name": "test",
    "Status": "UPDATING",
    "StatusMessage": "Updating the Firewall Domain List"
}
```

Para obtener más información, consulte Managing your own domain lists en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información sobre la API, consulte UpdateFirewallDomains en la Referencia de comandos de la AWS CLI.

update-firewall-rule-group-association

En el siguiente ejemplo de código, se muestra cómo utilizar update-firewall-rule-group-association.

AWS CLI

Para actualizar una asociación de grupos de reglas de firewall

En el siguiente ejemplo de update-firewall-rule-group-association, se actualiza una asociación de grupos de reglas de firewall.

```
aws route53resolver update-firewall-rule-group-association \
    --firewall-rule-group-association-id rslvr-frgassoc-57e8873d7example \
    --priority 103
```

Salida:

```
{
    "FirewallRuleGroupAssociation": {
        "Id": "rslvr-frgassoc-57e8873d7example",
        "Arn": "arn:aws:route53resolver:us-west-2:123456789012:firewall-rule-group-
association/rslvr-frgassoc-57e8873d7example",
        "FirewallRuleGroupId": "rslvr-frg-47f93271fexample",
        "VpcId": "vpc-31e92222",
        "Name": "test-association",
        "Priority": 103,
        "MutationProtection": "DISABLED",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Firewall Rule Group Association Attributes",
        "CreatorRequestId": "2ca1a304-32b3-4f5f-bc4c-EXAMPLE11111",
        "CreationTime": "2021-05-25T21:47:48.755768Z",
        "ModificationTime": "2021-05-25T21:50:09.272569Z"
    }
}
```

Para obtener más información, consulte Managing associations between your VPC and Route 53 Resolver DNS Firewall rule group en la Guía del desarrollador de Amazon Route 53.

- Para obtener información acerca de la API, consulte UpdateFirewallRuleGroupAssociation en la Referencia de comandos de la AWS CLI.

update-firewall-rule

En el siguiente ejemplo de código, se muestra cómo utilizar `update-firewall-rule`.

AWS CLI

Para actualizar una regla de firewall

En el siguiente ejemplo de `update-firewall-rule`, se actualiza una regla de firewall con los parámetros que especifique.

```
aws route53resolver update-firewall-rule \
    --firewall-rule-group-id rslvr-frg-47f93271fexample \
    --firewall-domain-list-id rslvr-fdl-9e956e9ffexample \
    --priority 102
```

Salida:

```
{
    "FirewallRule": {
        "FirewallRuleGroupId": "rslvr-frg-47f93271fexample",
        "FirewallDomainListId": "rslvr-fdl-9e956e9ffexample",
        "Name": "allow-rule",
        "Priority": 102,
        "Action": "ALLOW",
        "CreatorRequestId": "d81e3fb7-020b-415e-939f-EXAMPLE11111",
        "CreationTime": "2021-05-25T21:44:00.346093Z",
        "ModificationTime": "2021-05-25T21:45:59.611600Z"
    }
}
```

Para obtener más información, consulte Managing rule groups and rules in DNS Firewall en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información acerca de la API, consulte UpdateFirewallRule en la Referencia de comandos de la AWS CLI.

update-resolver-endpoint

En el siguiente ejemplo de código, se muestra cómo utilizar `update-resolver-endpoint`.

AWS CLI

Para actualizar el nombre de un punto de conexión de Resolver

En el siguiente ejemplo de `update-resolver-endpoint`, se actualiza el nombre de un punto de conexión de Resolver. No se pueden actualizar otros valores.

```
aws route53resolver update-resolver-endpoint \
    --resolver-endpoint-id rslvr-in-b5d45e32bdc445f09 \
    --name my-renamed-inbound-endpoint
```

Salida:

```
{
    "ResolverEndpoint": {
        "Id": "rslvr-in-b5d45e32bdexample",
        "CreatorRequestId": "2020-01-02-18:48",
        "Arn": "arn:aws:route53resolver:us-west-2:111122223333:resolver-endpoint/
rslvr-in-b5d45e32bdexample",
        "Name": "my-renamed-inbound-endpoint",
        "SecurityGroupIds": [
            "sg-f62bexam"
        ],
        "Direction": "INBOUND",
        "IpAddressCount": 2,
        "HostVPCId": "vpc-304bexam",
        "Status": "OPERATIONAL",
        "StatusMessage": "This Resolver Endpoint is operational.",
        "CreationTime": "2020-01-01T18:33:59.265Z",
        "ModificationTime": "2020-01-08T18:33:59.265Z"
    }
}
```

- Para obtener información sobre la API, consulte UpdateResolverEndpoint en la Referencia de comandos de la AWS CLI.

`update-resolver-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-resolver-rule`.

AWS CLI

Ejemplo 1: actualización de la configuración de Punto de conexión de Resolver

En el siguiente ejemplo de `update-resolver-rule`, se actualiza el nombre de la regla, las direcciones IP de la red local en las instalaciones a las que se reenvían las consultas de DNS y el ID del punto de conexión de Resolver saliente que utiliza para reenviar las consultas a la red.

Nota: Los valores existentes para `TargetIps` se sobrescriben, por lo que debe especificar todas las direcciones IP que desee que tenga la regla después de la actualización.

```
aws route53resolver update-resolver-rule \
    --resolver-rule-id rslvr-rr-1247fa64f3example \
    --config Name="my-2nd-rule",TargetIps=[{Ip=192.0.2.45,Port=53},
{Ip=192.0.2.46,Port=53}],ResolverEndpointId=rslvr-out-7b89ed0d25example
```

Salida:

```
{
    "ResolverRule": {
        "Id": "rslvr-rr-1247fa64f3example",
        "CreatorRequestId": "2020-01-02-18:47",
        "Arn": "arn:aws:route53resolver:us-west-2:111122223333:resolver-rule/rslvr-
rr-1247fa64f3example",
        "DomainName": "www.example.com.",
        "Status": "COMPLETE",
        "StatusMessage": "[Trace id: 1-5dcc90b9-8a8ee860aba1ebd89example]
 Successfully updated Resolver Rule.",
        "RuleType": "FORWARD",
        "Name": "my-2nd-rule",
        "TargetIps": [
            {
                "Ip": "192.0.2.45",
                "Port": 53
            },
            {
                "Ip": "192.0.2.46",
                "Port": 53
            }
        ],
        "ResolverEndpointId": "rslvr-out-7b89ed0d25example",
        "OwnerId": "111122223333",
        "ShareStatus": "NOT_SHARED"
```

```
    }
}
```

Ejemplo 2: actualización de la configuración de Punto de conexión de Resolver que utilizar un archivo con los ajustes de configuración

También puede incluir los ajustes de `config` en un archivo JSON y, a continuación, especificar ese archivo cuando llame a `update-resolver-rule`.

```
aws route53resolver update-resolver-rule \
    --resolver-rule-id rslvr-rr-1247fa64f3example \
    --config file://c:\temp\update-resolver-rule.json
```

Contenido de `update-resolver-rule.json`.

```
{
    "Name": "my-2nd-rule",
    "TargetIps": [
        {
            "Ip": "192.0.2.45",
            "Port": 53
        },
        {
            "Ip": "192.0.2.46",
            "Port": 53
        }
    ],
    "ResolverEndpointId": "rslvr-out-7b89ed0d25example"
}
```

Para obtener más información, consulte Values That You Specify When You Create or Edit Rules en la Guía para desarrolladores de Amazon Route 53.

- Para obtener información acerca de la API, consulte UpdateResolverRule en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon S3 que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon S3.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`abort-multipart-upload`

En el siguiente ejemplo de código, se muestra cómo utilizar `abort-multipart-upload`.

AWS CLI

Anular la carga multiparte especificada

El siguiente comando `abort-multipart-upload` anula una carga multiparte de la clave `multipart/01` en el bucket `amzn-s3-demo-bucket`.

```
aws s3api abort-multipart-upload \
    --bucket amzn-s3-demo-bucket \
    --key multipart/01 \
    --upload-
id dfRtDYU0WWCCcH43C3WFbkRONycyCpTJJvxu2i5GYkZljF.Yxwh6XG7WfS2vC4to6HiV6Yjlx.cph0gtNBtJ8P3UR
```

El ID de carga requerido por este comando se genera mediante `create-multipart-upload` y también se puede recuperar con `list-multipart-uploads`.

- Para obtener información sobre la API, consulte AbortMultipartUploads en la Referencia de comandos de la AWS CLI.

`complete-multipart-upload`

En el siguiente ejemplo de código, se muestra cómo utilizar `complete-multipart-upload`.

AWS CLI

El siguiente comando completa una carga multiparte de la clave `multipart/01`en el bucket `amzn-s3-demo-bucket`:

```
aws s3api complete-multipart-upload --multipart-upload file://
mpustruct --bucket amzn-s3-demo-bucket --key 'multipart/01' --upload-
id dfRtDYU0WWCCcH43C3WFbkRONycyCpTJJvxu2i5GYkZljF.Yxwh6XG7WfS2vC4to6HiV6Yjlx.cph0gtNBtJ8P3UR
```

El ID de carga requerido por este comando se genera mediante `create-multipart-upload` y también se puede recuperar con `list-multipart-uploads`.

La opción de carga multiparte del comando anterior utiliza una estructura JSON que describe las partes de la carga multiparte que se deben volver a ensamblar en el archivo completo. En este ejemplo, el prefijo `file://` se usa para cargar la estructura JSON desde un archivo de la carpeta local denominada `mpustruct`.

mpustruct:

```
{
  "Parts": [
    {
      "ETag": "e868e0f4719e394144ef36531ee6824c",
      "PartNumber": 1
    },
    {
      "ETag": "6bb2b12753d66fe86da4998aa33fffb0",
      "PartNumber": 2
    },
    {
      "ETag": "d0a0112e841abec9c9ec83406f0159c8",
      "PartNumber": 3
    }
  ]
}
```

El valor de ETag de cada parte que se carga aparece cada vez que se carga una parte mediante el comando `upload-part` y también se puede recuperar mediante una llamada a `list-parts` o calcularse mediante la suma de comprobación MD5 de cada parte.

Salida:

```
{
    "ETag": "\"3944a9f7a4faab7f78788ff6210f63f0-3\"",
    "Bucket": "amzn-s3-demo-bucket",
    "Location": "https://amzn-s3-demo-bucket.s3.amazonaws.com/multipart%2F01",
    "Key": "multipart/01"
}
```

- Para obtener información sobre la API, consulte CompleteMultipartUpload en la Referencia de comandos de la AWS CLI.

`copy-object`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-object`.

AWS CLI

El siguiente comando copia un objeto de `bucket-1` a `bucket-2`:

```
aws s3api copy-object --copy-source bucket-1/test.txt --key test.txt --
bucket bucket-2
```

Salida:

```
{
    "CopyObjectResult": {
        "LastModified": "2015-11-10T01:07:25.000Z",
        "ETag": "\"589c8b79c230a6ecd5a7e1d040a9a030\""
    },
    "VersionId": "YdnYvTCVDqRRFA.NFJjy36p0hxifMlkA"
}
```

- Para obtener información sobre la API, consulte CopyObject en la Referencia de comandos de AWS CLI.

`cp`

En el siguiente ejemplo de código, se muestra cómo utilizar `cp`.

AWS CLI

Ejemplo 1: copia de un archivo local en S3

El siguiente comando cp copia un único archivo en un bucket y una clave específicos:

```
aws s3 cp test.txt s3://amzn-s3-demo-bucket/test2.txt
```

Salida:

```
upload: test.txt to s3://amzn-s3-demo-bucket/test2.txt
```

Ejemplo 2: copia de un archivo local en S3 con una fecha de caducidad

El siguiente comando cp copia un único archivo en un bucket y una clave específicos que expiran en una marca temporal ISO 8601 especificada:

```
aws s3 cp test.txt s3://amzn-s3-demo-bucket/test2.txt \
    --expires 2014-10-01T20:30:00Z
```

Salida:

```
upload: test.txt to s3://amzn-s3-demo-bucket/test2.txt
```

Ejemplo 3: copia de un archivo desde S3 a S3

El siguiente comando cp copia un único objeto S3 en un bucket y una clave específicos:

```
aws s3 cp s3://amzn-s3-demo-bucket/test.txt s3://amzn-s3-demo-bucket/test2.txt
```

Salida:

```
copy: s3://amzn-s3-demo-bucket/test.txt to s3://amzn-s3-demo-bucket/test2.txt
```

Ejemplo 4: copia de un objeto de S3 en un archivo local

El siguiente comando cp copia un único objeto en un archivo específico localmente:

```
aws s3 cp s3://amzn-s3-demo-bucket/test.txt test2.txt
```

Salida:

```
download: s3://amzn-s3-demo-bucket/test.txt to test2.txt
```

Ejemplo 5: copia de un objeto de S3 desde un bucket a otro

El siguiente comando `cp` copia un único objeto en un bucket específico sin perder su nombre original:

```
aws s3 cp s3://amzn-s3-demo-bucket/test.txt s3://amzn-s3-demo-bucket2/
```

Salida:

```
copy: s3://amzn-s3-demo-bucket/test.txt to s3://amzn-s3-demo-bucket2/test.txt
```

Ejemplo 6: copia recursiva de objetos de S3 en un directorio local

Cuando se pasa con el parámetro `--recursive`, el siguiente comando `cp` copia de forma recursiva todos los objetos con un prefijo y un bucket específicos en un directorio concreto. En este ejemplo, el bucket `amzn-s3-demo-bucket` contiene los objetos `test1.txt` y `test2.txt`:

```
aws s3 cp s3://amzn-s3-demo-bucket . \
    --recursive
```

Salida:

```
download: s3://amzn-s3-demo-bucket/test1.txt to test1.txt
download: s3://amzn-s3-demo-bucket/test2.txt to test2.txt
```

Ejemplo 7: copia de archivos locales en S3

Cuando se pasa con el parámetro `--recursive`, el siguiente comando `cp` copia de forma recursiva todos los archivos de un directorio determinado en un bucket y prefijo específicos. También excluye algunos archivos con el parámetro `--exclude`. En este ejemplo, el directorio `myDir` contiene los archivos `test1.txt` y `test2.jpg`:

```
aws s3 cp myDir s3://amzn-s3-demo-bucket/ \
    --recursive \
    --exclude "*.jpg"
```

Salida:

```
upload: myDir/test1.txt to s3://amzn-s3-demo-bucket/test1.txt
```

Ejemplo 8: copia recursiva de objetos de S3 en otro bucket

Cuando se pasa con el parámetro `--recursive`, el siguiente comando `--exclude` copia de forma recursiva todos los objetos de un bucket determinado en otro bucket. También excluye algunos objetos con el parámetro `cp`. En este ejemplo, el bucket `amzn-s3-demo-bucket` contiene los objetos `test1.txt` y `another/test1.txt`:

```
aws s3 cp s3://amzn-s3-demo-bucket/ s3://amzn-s3-demo-bucket2/ \
    --recursive \
    --exclude "another/*"
```

Salida:

```
copy: s3://amzn-s3-demo-bucket/test1.txt to s3://amzn-s3-demo-bucket2/test1.txt
```

Puede combinar las opciones `--exclude` y `--include` para copiar solo los objetos que coincidan con un patrón, excluyendo todos los demás:

```
aws s3 cp s3://amzn-s3-demo-bucket/logs/ s3://amzn-s3-demo-bucket2/logs/ \
    --recursive \
    --exclude "*" \
    --include "*.log"
```

Salida:

```
copy: s3://amzn-s3-demo-bucket/logs/test/test.log to s3://amzn-s3-demo-bucket2/logs/
test/test.log
copy: s3://amzn-s3-demo-bucket/logs/test3.log to s3://amzn-s3-demo-bucket2/logs/
test3.log
```

Ejemplo 9: configuración de la lista de control de acceso (ACL) al copiar un objeto de S3

En el siguiente comando `cp`, se copia un único objeto en un bucket y una clave específicos, y se configura ACL en `public-read-write`:

```
aws s3 cp s3://amzn-s3-demo-bucket/test.txt s3://amzn-s3-demo-bucket/test2.txt \
```

```
    --acl public-read-write
```

Salida:

```
copy: s3://amzn-s3-demo-bucket/test.txt to s3://amzn-s3-demo-bucket/test2.txt
```

Tenga en cuenta que, si utiliza la opción `--acl`, debe asegurarse de que todas las políticas de IAM asociadas incluyan la acción `"s3:PutObjectAcl"`:

```
aws iam get-user-policy \
    --user-name myuser \
    --policy-name mypolicy
```

Salida:

```
{
    "UserName": "myuser",
    "PolicyName": "mypolicy",
    "PolicyDocument": {
        "Version":"2012-10-17",
        "Statement": [
            {
                "Action": [
                    "s3:PutObject",
                    "s3:PutObjectAcl"
                ],
                "Resource": [
                    "arn:aws:s3:::amzn-s3-demo-bucket/*"
                ],
                "Effect": "Allow",
                "Sid": "Stmt1234567891234"
            }
        ]
    }
}
```

Ejemplo 10: concesión de permisos a un objeto de S3

El siguiente comando `cp` ilustra el uso de la opción `--grants` para conceder acceso de lectura a todos los usuarios identificados por su URI y el control total a un usuario específico identificado por su ID canónico:

```
aws s3 cp file.txt s3://amzn-s3-demo-bucket/ --grants read=uri=http://
acs.amazonaws.com/groups/global/
AllUsers full=id=79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Salida:

```
upload: file.txt to s3://amzn-s3-demo-bucket/file.txt
```

Ejemplo 11: carga de un flujo de archivos local a S3

PowerShell puede alterar la codificación o añadir un CRLF a la entrada canalizada.

El siguiente comando `cp` carga un flujo de archivos local desde la entrada estándar a un bucket y una clave específicos:

```
aws s3 cp - s3://amzn-s3-demo-bucket/stream.txt
```

Ejemplo 12: carga de un flujo de archivos local de más de 50 GB a S3

El siguiente comando `cp` carga un flujo de archivos local de 51 GB desde la entrada estándar a un bucket y una clave específicos. Se debe proporcionar la opción `--expected-size`, ya que, de lo contrario, la carga podría fallar si se alcanza el límite predeterminado de 10 000 piezas:

```
aws s3 cp - s3://amzn-s3-demo-bucket/stream.txt --expected-size 54760833024
```

Ejemplo 13: descarga de un objeto de S3 como flujo de archivos local

PowerShell podría alterar la codificación o agregar un CRLF a la salida canalizada o redirigida.

El siguiente comando `cp` descarga un objeto S3 de forma local como una transmisión de la salida estándar. La descarga como flujo no es compatible actualmente con el parámetro `--recursive`:

```
aws s3 cp s3://amzn-s3-demo-bucket/stream.txt -
```

Ejemplo 14: carga de un punto de acceso de S3

El siguiente `cp` comando carga un único archivo (`mydoc.txt`) en el punto de acceso (`myaccesspoint`) en la clave (`mykey`):

```
aws s3 cp mydoc.txt s3://arn:aws:s3:us-west-2:123456789012:accesspoint/
myaccesspoint/mykey
```

Salida:

```
upload: mydoc.txt to s3://arn:aws:s3:us-west-2:123456789012:accesspoint/
myaccesspoint/mykey
```

Ejemplo 15: descarga desde un punto de acceso de S3

El siguiente `cp` comando descarga un único objeto (`mykey`) desde el punto de acceso (`myaccesspoint`) al archivo local (`mydoc.txt`):

```
aws s3 cp s3://arn:aws:s3:us-west-2:123456789012:accesspoint/myaccesspoint/
mykey mydoc.txt
```

Salida:

```
download: s3://arn:aws:s3:us-west-2:123456789012:accesspoint/myaccesspoint/mykey to
 mydoc.txt
```

- Para obtener información sobre la API, consulte Cp en la Referencia de comandos de la AWS CLI.

`create-bucket`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-bucket`.

AWS CLI

Ejemplo 1: Creación de un bucket

En los siguientes ejemplos de `create-bucket` se crea un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region us-east-1
```

Salida:

```
{
    "Location": "/amzn-s3-demo-bucket"
}
```

Para obtener más información, consulte Crear un bucket en la Guía del usuario de Amazon S3.

Ejemplo 2: Creación de un bucket con propietario obligatorio

En el siguiente ejemplo de `create-bucket` se crea un bucket denominado `amzn-s3-demo-bucket` que utiliza la configuración Aplicada al propietario del bucket de S3 Object Ownership.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region us-east-1 \
    --object-ownership BucketOwnerEnforced
```

Salida:

```
{
    "Location": "/amzn-s3-demo-bucket"
}
```

Para obtener más información, consulte Control de la propiedad de objetos y desactivación de las ACL en la Guía del usuario de Amazon S3.

Ejemplo 3: creación de un bucket fuera de la región us-east-1

En el siguiente ejemplo `create-bucket`, se crea un bucket denominado `amzn-s3-demo-bucket` en la región `eu-west-1`. Las regiones situadas fuera de `us-east-1` requieren que se especifique el `LocationConstraint` correspondiente para poder crear el bucket en la región deseada.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region eu-west-1 \
    --create-bucket-configuration LocationConstraint=eu-west-1
```

Salida:

```
{
    "Location": "http://amzn-s3-demo-bucket.s3.amazonaws.com/"
}
```

Para obtener más información, consulte Crear un bucket en la Guía del usuario de Amazon S3.

- Para obtener información sobre la API, consulte CreateBucket en la Referencia de comandos de AWS CLI.

`create-multipart-upload`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-multipart-upload`.

AWS CLI

El siguiente comando crea una carga multiparte en el bucket `amzn-s3-demo-bucket` con la clave `multipart/01`:

```
aws s3api create-multipart-upload --bucket amzn-s3-demo-bucket --key 'multipart/01'
```

Salida:

```
{
    "Bucket": "amzn-s3-demo-bucket",
    "UploadId":
 "dfRtDYU0WWCCcH43C3WFbkRONycyCpTJJvxu2i5GYkZljF.Yxwh6XG7WfS2vC4to6HiV6Yjlx.cph0gtNBtJ8P3URC
    "Key": "multipart/01"
}
```

El archivo completo se denominará `01` en una carpeta llamada `multipart` en el bucket `amzn-s3-demo-bucket`. Guarde el ID de carga, la clave y el nombre del bucket para usarlos con el comando `upload-part`.

- Para obtener información sobre la API, consulte CreateMultipartUpload en la Referencia de comandos de la AWS CLI.

`delete-bucket-analytics-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bucket-analytics-configuration`.

AWS CLI

Eliminar una configuración de análisis de un bucket

En el siguiente ejemplo de `delete-bucket-analytics-configuration`, se elimina la configuración de análisis para el bucket e ID especificados.

```
aws s3api delete-bucket-analytics-configuration \
    --bucket amzn-s3-demo-bucket \
    --id 1
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteBucketAnalyticsConfiguration en la Referencia de comandos de la AWS CLI.

`delete-bucket-cors`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bucket-cors`.

AWS CLI

El siguiente comando elimina la configuración de uso compartido de recursos entre orígenes desde un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api delete-bucket-cors --bucket amzn-s3-demo-bucket
```

- Para obtener información sobre la API, consulte DeleteBucketCors en la Referencia de comandos de la AWS CLI.

`delete-bucket-encryption`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bucket-encryption`.

AWS CLI

Eliminar la configuración de cifrado del servidor de un bucket

En el siguiente ejemplo de `delete-bucket-encryption`, se elimina la configuración de cifrado del servidor del bucket especificado.

```
aws s3api delete-bucket-encryption \
    --bucket amzn-s3-demo-bucket
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteBucketEncryption en la Referencia de comandos de la AWS CLI.

`delete-bucket-intelligent-tiering-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bucket-intelligent-tiering-configuration`.

AWS CLI

Para eliminar una configuración de S3 Intelligent-Tiering en un bucket

En el siguiente ejemplo de `delete-bucket-intelligent-tiering-configuration`, se elimina una configuración de S3 Intelligent-Tiering, denominada ExampleConfig, de un bucket.

```
aws s3api delete-bucket-intelligent-tiering-configuration \
    --bucket amzn-s3-demo-bucket \
    --id ExampleConfig
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de S3 Intelligent-Tiering en la Guía del usuario de Amazon S3.

- Para obtener información sobre la API, consulte DeleteBucketIntelligentTieringConfiguration en la Referencia de comandos de la AWS CLI.

`delete-bucket-inventory-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bucket-inventory-configuration`.

AWS CLI

Eliminar la configuración de inventario de un bucket

En el siguiente ejemplo de `delete-bucket-inventory-configuration`, se elimina la configuración de inventario con el ID 1 del bucket especificado.

```
aws s3api delete-bucket-inventory-configuration \
    --bucket amzn-s3-demo-bucket \
    --id 1
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteBucketInventoryConfiguration en la Referencia de comandos de la AWS CLI.

`delete-bucket-lifecycle`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bucket-lifecycle`.

AWS CLI

El comando siguiente elimina una configuración del ciclo de vida de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api delete-bucket-lifecycle --bucket amzn-s3-demo-bucket
```

- Para obtener información sobre la API, consulte DeleteBucketLifecycle en la Referencia de comandos de la AWS CLI.

`delete-bucket-metrics-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bucket-metrics-configuration`.

AWS CLI

Eliminar una configuración de métricas de un bucket

En el siguiente ejemplo de `delete-bucket-metrics-configuration`, se elimina la configuración de métricas para el bucket e ID especificados.

```
aws s3api delete-bucket-metrics-configuration \
    --bucket amzn-s3-demo-bucket \
    --id 123
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteBucketMetricsConfiguration en la Referencia de comandos de la AWS CLI.

`delete-bucket-ownership-controls`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bucket-ownership-controls`.

AWS CLI

Para eliminar la configuración de propiedad de un bucket

En el siguiente ejemplo de `delete-bucket-ownership-controls`, se elimina la configuración de propiedad de un bucket.

```
aws s3api delete-bucket-ownership-controls \
    --bucket amzn-s3-demo-bucket
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de la propiedad de objetos en un bucket existente en la Guía del usuario de Amazon S3.

- Para obtener información sobre la API, consulte DeleteBucketOwnershipControls en la Referencia de comandos de la AWS CLI.

`delete-bucket-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bucket-policy`.

AWS CLI

El comando siguiente elimina una política de bucket de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api delete-bucket-policy --bucket amzn-s3-demo-bucket
```

- Para obtener información sobre la API, consulte DeleteBucketPolicy en la Referencia de comandos de la AWS CLI.

`delete-bucket-replication`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bucket-replication`.

AWS CLI

El siguiente comando elimina la configuración de replicación de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api delete-bucket-replication --bucket amzn-s3-demo-bucket
```

- Para obtener información sobre la API, consulte DeleteBucketReplication en la Referencia de comandos de la AWS CLI.

`delete-bucket-tagging`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bucket-tagging`.

AWS CLI

El siguiente comando elimina la configuración de etiquetado de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api delete-bucket-tagging --bucket amzn-s3-demo-bucket
```

- Para obtener información sobre la API, consulte DeleteBucketTagging en la Referencia de comandos de la AWS CLI.

`delete-bucket-website`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bucket-website`.

AWS CLI

El siguiente comando elimina la configuración de un sitio web de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api delete-bucket-website --bucket amzn-s3-demo-bucket
```

- Para obtener información sobre la API, consulte DeleteBucketWebsite en la Referencia de comandos de la AWS CLI.

`delete-bucket`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-bucket`.

AWS CLI

El comando siguiente elimina un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api delete-bucket --bucket amzn-s3-demo-bucket --region us-east-1
```

- Para obtener información sobre la API, consulte DeleteBucket en la Referencia de comandos de AWS CLI.

`delete-object-tagging`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-object-tagging`.

AWS CLI

Eliminar los conjuntos de etiquetas de un objeto

En el siguiente ejemplo de `delete-object-tagging`, se elimina del objeto `doc1.rtf` la etiqueta con la clave especificada.

```
aws s3api delete-object-tagging \
    --bucket amzn-s3-demo-bucket \
    --key doc1.rtf
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteObjectTagging en la Referencia de comandos de la AWS CLI.

`delete-object`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-object`.

AWS CLI

El comando siguiente elimina un objeto denominado `test.txt` de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key test.txt
```

Si el control de versiones del bucket está activado, el resultado contendrá el ID de versión del marcador de eliminación:

```
{
  "VersionId": "9_gKg5vG56F.TTEUdwkxGpJ3tNDlWlGq",
  "DeleteMarker": true
}
```

Para obtener más información acerca de la eliminación de objetos, consulte Eliminación de objetos en la Guía para desarrolladores de Amazon S3.

- Para obtener información sobre la API, consulte DeleteObject en la Referencia de comandos de AWS CLI.

`delete-objects`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-objects`.

AWS CLI

El comando siguiente elimina un objeto denominado de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete file://delete.json
```

`delete.json` es un documento JSON en el directorio actual que especifica el objeto que se va a eliminar:

```
{
  "Objects": [
    {
      "Key": "test1.txt"
    }
  ],
  "Quiet": false
}
```

Salida:

```
{
    "Deleted": [
        {
            "DeleteMarkerVersionId": "mYAT5Mc6F7aeUL8SS7FAAqUPO1koHwzU",
            "Key": "test1.txt",
            "DeleteMarker": true
        }
    ]
}
```

- Para obtener información sobre la API, consulte DeleteObjects en la Referencia de comandos de AWS CLI.

`delete-public-access-block`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-public-access-block`.

AWS CLI

Eliminar la configuración de bloqueo de acceso público de un bucket

En el siguiente ejemplo de `delete-public-access-block`, se elimina la configuración de bloqueo de acceso público en el bucket especificado.

```
aws s3api delete-public-access-block \
    --bucket amzn-s3-demo-bucket
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeletePublicAccessBlock en la Referencia de comandos de la AWS CLI.

`get-bucket-accelerate-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-accelerate-configuration`.

AWS CLI

Recuperar la configuración acelerada de un bucket

En el siguiente ejemplo de `get-bucket-accelerate-configuration`, se recupera la configuración acelerada para el bucket especificado.

```
aws s3api get-bucket-accelerate-configuration \
    --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "Status": "Enabled"
}
```

- Para obtener información sobre la API, consulte GetBucketAccelerateConfiguration en la Referencia de comandos de la AWS CLI.

`get-bucket-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-acl`.

AWS CLI

El siguiente comando recupera la lista de control de acceso de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api get-bucket-acl --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "Owner": {
        "DisplayName": "my-username",
        "ID": "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd087d36c32"
    },
    "Grants": [
        {
            "Grantee": {
                "DisplayName": "my-username",
                "ID":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd087d36c32"
            },
```

```
            "Permission": "FULL_CONTROL"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetBucketAcl en la Referencia de comandos de la AWS CLI.

`get-bucket-analytics-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-analytics-configuration`.

AWS CLI

Recuperar la configuración de análisis de un bucket con un ID específico

En el siguiente ejemplo de `get-bucket-analytics-configuration`, se muestra la configuración de análisis para el bucket e ID especificados.

```
aws s3api get-bucket-analytics-configuration \
    --bucket amzn-s3-demo-bucket \
    --id 1
```

Salida:

```
{
    "AnalyticsConfiguration": {
        "StorageClassAnalysis": {},
        "Id": "1"
    }
}
```

- Para obtener información sobre la API, consulte GetBucketAnalyticsConfiguration en la Referencia de comandos de la AWS CLI.

`get-bucket-cors`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-cors`.

AWS CLI

El siguiente comando recupera la configuración de uso compartido de recursos entre orígenes para un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api get-bucket-cors --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "CORSRules": [
        {
            "AllowedHeaders": [
                "*"
            ],
            "ExposeHeaders": [
                "x-amz-server-side-encryption"
            ],
            "AllowedMethods": [
                "PUT",
                "POST",
                "DELETE"
            ],
            "MaxAgeSeconds": 3000,
            "AllowedOrigins": [
                "http://www.example.com"
            ]
        },
        {
            "AllowedHeaders": [
                "Authorization"
            ],
            "MaxAgeSeconds": 3000,
            "AllowedMethods": [
                "GET"
            ],
            "AllowedOrigins": [
                "*"
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetBucketCors en la Referencia de comandos de la AWS CLI.

`get-bucket-encryption`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-encryption`.

AWS CLI

Recuperar la configuración de cifrado del servidor de un bucket

En el siguiente ejemplo de `get-bucket-encryption`, se recupera la configuración de cifrado del lado del servidor del bucket `amzn-s3-demo-bucket`.

```
aws s3api get-bucket-encryption \
    --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "ServerSideEncryptionConfiguration": {
        "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "AES256"
                }
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte GetBucketEncryption en la Referencia de comandos de la AWS CLI.

`get-bucket-intelligent-tiering-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-intelligent-tiering-configuration`.

AWS CLI

Para obtener una configuración de S3 Intelligent-Tiering en un bucket

En el siguiente ejemplo de `get-bucket-intelligent-tiering-configuration`, se recupera una configuración de S3 Intelligent-Tiering, denominada ExampleConfig, de un bucket.

```
aws s3api get-bucket-intelligent-tiering-configuration \
    --bucket amzn-s3-demo-bucket \
    --id ExampleConfig
```

Salida:

```
{
    "IntelligentTieringConfiguration": {
        "Id": "ExampleConfig2",
        "Filter": {
            "Prefix": "images"
        },
        "Status": "Enabled",
        "Tierings": [
            {
                "Days": 90,
                "AccessTier": "ARCHIVE_ACCESS"
            },
            {
                "Days": 180,
                "AccessTier": "DEEP_ARCHIVE_ACCESS"
            }
        ]
    }
}
```

Para obtener más información, consulte Uso de S3 Intelligent-Tiering en la Guía del usuario de Amazon S3.

- Para obtener información sobre la API, consulte GetBucketIntelligentTieringConfiguration en la Referencia de comandos de la AWS CLI.

`get-bucket-inventory-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-inventory-configuration`.

AWS CLI

Recuperar la configuración de inventario de un bucket

En el siguiente ejemplo de `get-bucket-inventory-configuration`, se recupera la configuración de inventario del bucket especificado con el ID 1.

```
aws s3api get-bucket-inventory-configuration \
    --bucket amzn-s3-demo-bucket \
    --id 1
```

Salida:

```
{
    "InventoryConfiguration": {
        "IsEnabled": true,
        "Destination": {
            "S3BucketDestination": {
                "Format": "ORC",
                "Bucket": "arn:aws:s3:::amzn-s3-demo-bucket",
                "AccountId": "123456789012"
            }
        },
        "IncludedObjectVersions": "Current",
        "Id": "1",
        "Schedule": {
            "Frequency": "Weekly"
        }
    }
}
```

- Para obtener información sobre la API, consulte GetBucketInventoryConfiguration en la Referencia de comandos de la AWS CLI.

`get-bucket-lifecycle-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-lifecycle-configuration`.

AWS CLI

El siguiente comando recupera la configuración del ciclo de vida de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api get-bucket-lifecycle-configuration --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "Rules": [
        {
            "ID": "Move rotated logs to Glacier",
            "Prefix": "rotated/",
            "Status": "Enabled",
            "Transitions": [
                {
                    "Date": "2015-11-10T00:00:00.000Z",
                    "StorageClass": "GLACIER"
                }
            ]
        },
        {
            "Status": "Enabled",
            "Prefix": "",
            "NoncurrentVersionTransitions": [
                {
                    "NoncurrentDays": 0,
                    "StorageClass": "GLACIER"
                }
            ],
            "ID": "Move old versions to Glacier"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetBucketLifecycleConfiguration en la Referencia de comandos de la AWS CLI.

`get-bucket-lifecycle`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-lifecycle`.

AWS CLI

El siguiente comando recupera la configuración del ciclo de vida de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api get-bucket-lifecycle --bucket amzn-s3-demo-bucket
```

Salida:

```
{
  "Rules": [
    {
      "ID": "Move to Glacier after sixty days (objects in logs/2015/)",
      "Prefix": "logs/2015/",
      "Status": "Enabled",
      "Transition": {
        "Days": 60,
        "StorageClass": "GLACIER"
      }
    },
    {
      "Expiration": {
        "Date": "2016-01-01T00:00:00.000Z"
      },
      "ID": "Delete 2014 logs in 2016.",
      "Prefix": "logs/2014/",
      "Status": "Enabled"
    }
  ]
}
```

- Para obtener información sobre la API, consulte GetBucketLifecycle en la Referencia de comandos de la AWS CLI.

`get-bucket-location`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-location`.

AWS CLI

El siguiente comando recupera la restricción de ubicación de un bucket denominado `amzn-s3-demo-bucket`, si existe una restricción:

```
aws s3api get-bucket-location --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "LocationConstraint": "us-west-2"
}
```

- Para obtener información sobre la API, consulte GetBucketLocation en la Referencia de comandos de la AWS CLI.

`get-bucket-logging`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-logging`.

AWS CLI

Recuperar el estado de registros de un bucket

En el siguiente ejemplo de `get-bucket-logging`, se recupera el estado de registros del bucket especificado.

```
aws s3api get-bucket-logging \
    --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "LoggingEnabled": {
        "TargetPrefix": "",
        "TargetBucket": "amzn-s3-demo-bucket-logs"
          }
}
```

- Para obtener información sobre la API, consulte GetBucketLogging en la Referencia de comandos de la AWS CLI.

`get-bucket-metrics-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-metrics-configuration`.

AWS CLI

Recuperar la configuración de métricas de un bucket con un ID específico

En el siguiente ejemplo de `get-bucket-metrics-configuration`, se muestra la configuración de métricas para el bucket e ID especificados.

```
aws s3api get-bucket-metrics-configuration \
    --bucket amzn-s3-demo-bucket \
    --id 123
```

Salida:

```
{
    "MetricsConfiguration": {
        "Filter": {
            "Prefix": "logs"
        },
        "Id": "123"
    }
}
```

- Para obtener información sobre la API, consulte GetBucketMetricsConfiguration en la Referencia de comandos de la AWS CLI.

`get-bucket-notification-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-notification-configuration`.

AWS CLI

El siguiente comando recupera la configuración de notificaciones de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api get-bucket-notification-configuration --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "TopicConfigurations": [
        {
            "Id": "YmQzMmEwM2EjZWVlI0NGItNzVtZjI1MC00ZjgyLWZDBiZWNl",
            "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-notification-topic",
            "Events": [
                "s3:ObjectCreated:*"
            ]
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetBucketNotificationConfiguration en la Referencia de comandos de la AWS CLI.

`get-bucket-notification`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-notification`.

AWS CLI

El siguiente comando recupera la configuración de notificaciones de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api get-bucket-notification --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "TopicConfiguration": {
        "Topic": "arn:aws:sns:us-west-2:123456789012:my-notification-topic",
        "Id": "YmQzMmEwM2EjZWVlI0NGItNzVtZjI1MC00ZjgyLWZDBiZWNl",
        "Event": "s3:ObjectCreated:*",
        "Events": [
            "s3:ObjectCreated:*"
        ]
    }
}
```

- Para obtener información sobre la API, consulte GetBucketNotification en la Referencia de comandos de la AWS CLI.

`get-bucket-ownership-controls`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-ownership-controls`.

AWS CLI

Para obtener la configuración de propiedad de un bucket

En el siguiente ejemplo de `get-bucket-ownership-controls`, se recupera la configuración de propiedad de un bucket.

```
aws s3api get-bucket-ownership-controls \
    --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "OwnershipControls": {
        "Rules": [
            {
                "ObjectOwnership": "BucketOwnerEnforced"
            }
        ]
    }
}
```

Para obtener más información, consulte Visualización de la configuración de propiedad de objetos para un bucket de S3 en la Guía del usuario de Amazon Simple Storage Service.

- Para obtener información sobre la API, consulte GetBucketOwnershipControls en la Referencia de comandos de la AWS CLI.

`get-bucket-policy-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-policy-status`.

AWS CLI

Recuperar el estado de política de un bucket que indica si el bucket es público

En el siguiente ejemplo de `get-bucket-policy-status`, se recupera el estado de política del bucket `amzn-s3-demo-bucket`.

```
aws s3api get-bucket-policy-status \
    --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "PolicyStatus": {
        "IsPublic": false
    }
}
```

- Para obtener información sobre la API, consulte GetBucketPolicyStatus en la Referencia de comandos de la AWS CLI.

`get-bucket-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-policy`.

AWS CLI

El siguiente comando recupera la política de bucket de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api get-bucket-policy --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "Policy": "{\"Version\":\"2008-10-17\",\"Statement\":[{\"Sid\":\"\",\"Effect
\":\"Allow\",\"Principal\":\"*\",\"Action\":\"s3:GetObject\",\"Resource\":
\"arn:aws:s3:::amzn-s3-demo-bucket/*\"},{\"Sid\":\"\",\"Effect\":\"Deny\",
\"Principal\":\"*\",\"Action\":\"s3:GetObject\",\"Resource\":\"arn:aws:s3:::amzn-s3-
demo-bucket/secret/*\"}]}"
}
```

Obtención y colocación de una política de bucket En el siguiente ejemplo se muestra cómo se puede descargar una política de bucket de Amazon S3, realizar modificaciones en el archivo y

luego usar `put-bucket-policy` para aplicar la política de bucket modificada. Para descargar la política de bucket a un archivo, puede ejecutar:

```
aws s3api get-bucket-policy --bucket amzn-s3-demo-bucket --query Policy --output
 text > policy.json
```

A continuación, puede modificar el archivo `policy.json` según sea necesario. Por último, puede volver a aplicar esta política modificada al bucket de S3 ejecutando:

archivo `policy.json` según sea necesario. Por último, puede volver a aplicar esta política modificada al bucket de S3 ejecutando:

archivo según sea necesario. Por último, puede volver a aplicar esta política modificada al bucket de S3 ejecutando:

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://policy.json
```

- Para obtener información sobre la API, consulte GetBucketPolicy en la Referencia de comandos de la AWS CLI.

`get-bucket-replication`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-replication`.

AWS CLI

El siguiente comando recupera la configuración de replicación de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api get-bucket-replication --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "ReplicationConfiguration": {
        "Rules": [
            {
                "Status": "Enabled",
                "Prefix": "",
```

```
                "Destination": {
                    "Bucket": "arn:aws:s3:::amzn-s3-demo-bucket-backup",
                    "StorageClass": "STANDARD"
                },
                "ID": "ZmUwNzE4ZmQ4tMjVhOS00MTlkLOGI4NDkzZTIWJjNTUtYTA1"
            }
        ],
        "Role": "arn:aws:iam::123456789012:role/s3-replication-role"
    }
}
```

- Para obtener información sobre la API, consulte GetBucketReplication en la Referencia de comandos de la AWS CLI.

`get-bucket-request-payment`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-request-payment`.

AWS CLI

Recuperar la configuración de pagos de solicitudes de un bucket

En el siguiente ejemplo de `get-bucket-request-payment`, se recupera la configuración de pagos por el solicitante para el bucket especificado.

```
aws s3api get-bucket-request-payment \
    --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "Payer": "BucketOwner"
}
```

- Para obtener información sobre la API, consulte GetBucketRequestPayment en la Referencia de comandos de la AWS CLI.

`get-bucket-tagging`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-tagging`.

AWS CLI

El siguiente comando recupera la configuración de etiquetado de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api get-bucket-tagging --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "TagSet": [
        {
            "Value": "marketing",
            "Key": "organization"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetBucketTagging en la Referencia de comandos de la AWS CLI.

`get-bucket-versioning`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-versioning`.

AWS CLI

El siguiente comando recupera la configuración del control de versiones de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api get-bucket-versioning --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "Status": "Enabled"
}
```

- Para obtener información sobre la API, consulte GetBucketVersioning en la Referencia de comandos de la AWS CLI.

`get-bucket-website`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-bucket-website`.

AWS CLI

El siguiente comando recupera la configuración de sitio web estática de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api get-bucket-website --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "IndexDocument": {
        "Suffix": "index.html"
    },
    "ErrorDocument": {
        "Key": "error.html"
    }
}
```

- Para obtener información sobre la API, consulte GetBucketWebsite en la Referencia de comandos de la AWS CLI.

`get-object-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-object-acl`.

AWS CLI

El siguiente comando recupera la lista de control de acceso de un objeto en un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api get-object-acl --bucket amzn-s3-demo-bucket --key index.html
```

Salida:

```
{
```

```
    "Owner": {
        "DisplayName": "my-username",
        "ID": "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd087d36c32"
    },
    "Grants": [
        {
            "Grantee": {
                "DisplayName": "my-username",
                "ID":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd087d36c32"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetObjectAcl en la Referencia de comandos de la AWS CLI.

`get-object-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-object-attributes`.

AWS CLI

Para recuperar metadatos de un objeto sin devolver el objeto en sí

En el siguiente ejemplo de `get-object-attributes`, se recuperan los metadatos del objeto `doc1.rtf`.

```
aws s3api get-object-attributes \
    --bucket amzn-s3-demo-bucket \
    --key doc1.rtf \
    --object-attributes "StorageClass" "ETag" "ObjectSize"
```

Salida:

```
{
    "LastModified": "2022-03-15T19:37:31+00:00",
    "VersionId": "IuCPjXTDzHNfldAuitVBIKJpF2p1fg4P",
    "ETag": "b662d79adeb7c8d787ea7eafb9ef6207",
    "StorageClass": "STANDARD",
    "ObjectSize": 405
}
```

Para obtener más información, consulte GetObjectAttributes en la Referencia de la API de Amazon S3.

- Para obtener información sobre la API, consulte GetObjectAttributes en la Referencia de comandos de la AWS CLI.

`get-object-legal-hold`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-object-legal-hold`.

AWS CLI

Recupera el estado de retención legal de un objeto

En el siguiente ejemplo de `get-object-legal-hold`, se recupera el estado de retención legal del objeto especificado.

```
aws s3api get-object-legal-hold \
    --bucket amzn-s3-demo-bucket-with-object-lock \
    --key doc1.rtf
```

Salida:

```
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

- Para obtener información sobre la API, consulte GetObjectLegalHold en la Referencia de comandos de la AWS CLI.

`get-object-lock-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-object-lock-configuration`.

AWS CLI

Para recuperar una configuración de bloqueo de objetos para un bucket

En el siguiente ejemplo de `get-object-lock-configuration`, se recupera la configuración de bloqueo de objetos para el bucket especificado.

```
aws s3api get-object-lock-configuration \
    --bucket amzn-s3-demo-bucket-with-object-lock
```

Salida:

```
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 50
            }
        }
    }
}
```

- Para obtener información sobre la API, consulte GetObjectLockConfiguration en la Referencia de comandos de la AWS CLI.

`get-object-retention`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-object-retention`.

AWS CLI

Para recuperar la configuración de retención de un objeto

En el siguiente ejemplo de `get-object-retention`, se recupera la configuración de retención del objeto especificado.

```
aws s3api get-object-retention \
    --bucket amzn-s3-demo-bucket-with-object-lock \
    --key doc1.rtf
```

Salida:

```
{
    "Retention": {
        "Mode": "GOVERNANCE",
        "RetainUntilDate": "2025-01-01T00:00:00.000Z"
    }
}
```

- Para obtener información sobre la API, consulte GetObjectRetention en la Referencia de comandos de la AWS CLI.

`get-object-tagging`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-object-tagging`.

AWS CLI

Recuperar las etiquetas asociadas a un objeto

El siguiente ejemplo de `get-object-tagging` recupera los valores de la clave especificada del objeto especificado.

```
aws s3api get-object-tagging \
    --bucket amzn-s3-demo-bucket \
    --key doc1.rtf
```

Salida:

```
{
    "TagSet": [
        {
            "Value": "confidential",
            "Key": "designation"
        }
    ]
}
```

El siguiente ejemplo de `get-object-tagging` intenta recuperar los conjuntos de etiquetas del objeto `doc2.rtf`, que no tiene etiquetas.

```
aws s3api get-object-tagging \
    --bucket amzn-s3-demo-bucket \
    --key doc2.rtf
```

Salida:

```
{
    "TagSet": []
}
```

El siguiente ejemplo de `get-object-tagging` recupera los conjuntos de etiquetas del objeto `doc3.rtf`, que tiene varias etiquetas.

```
aws s3api get-object-tagging \
    --bucket amzn-s3-demo-bucket \
    --key doc3.rtf
```

Salida:

```
{
    "TagSet": [
        {
            "Value": "confidential",
            "Key": "designation"
        },
        {
            "Value": "finance",
            "Key": "department"
        },
        {
            "Value": "payroll",
            "Key": "team"
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetObjectTagging en la Referencia de comandos de la AWS CLI.

`get-object-torrent`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-object-torrent`.

AWS CLI

El siguiente comando crea un archivo torrent para un objeto en un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api get-object-torrent --bucket amzn-s3-demo-bucket --key large-video-file.mp4 large-video-file.torrent
```

El archivo torrent se guarda localmente en la carpeta actual. Tenga en cuenta que el nombre del archivo de salida (`large-video-file.torrent`) se especifica sin un nombre de opción y debe ser el último argumento del comando.

- Para obtener información sobre la API, consulte GetObjectTorrent en la Referencia de comandos de la AWS CLI.

`get-object`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-object`.

AWS CLI

En el siguiente ejemplo se utiliza el comando `get-object` para descargar un objeto de Amazon S3.

```
aws s3api get-object --bucket text-content --key dir/my_images.tar.bz2 my_images.tar.bz2
```

Tenga en cuenta que el parámetro outfile se especifica sin un nombre de opción, como "--outfile". El nombre del archivo de salida debe ser el último parámetro del comando.

El siguiente ejemplo muestra el uso de `--range` para descargar un intervalo de bytes específico de un objeto. Tenga en cuenta que los intervalos de bytes deben tener el prefijo "bytes=":

```
aws s3api get-object --bucket text-content --key dir/my_data --range bytes=8888-9999 my_data_range
```

Para obtener más información acerca de la recuperación de objetos, consulte Obtención de objetos en la Guía para desarrolladores de Amazon S3.

- Para obtener información sobre la API, consulte GetObject en la Referencia de comandos de AWS CLI.

`get-public-access-block`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-public-access-block`.

AWS CLI

Establecer o modificar la configuración de bloqueo de acceso público de un bucket

En el siguiente ejemplo de `get-public-access-block`, se elimina la configuración de bloqueo de acceso público del bucket especificado.

```
aws s3api get-public-access-block \
    --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "PublicAccessBlockConfiguration": {
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "BlockPublicAcls": true,
        "RestrictPublicBuckets": true
    }
}
```

- Para obtener información sobre la API, consulte GetPublicAccessBlock en la Referencia de comandos de la AWS CLI.

`head-bucket`

En el siguiente ejemplo de código, se muestra cómo utilizar `head-bucket`.

AWS CLI

El siguiente comando verifica el acceso a un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api head-bucket --bucket amzn-s3-demo-bucket
```

Si el bucket existe y tiene acceso a él, no se muestra ningún resultado. De lo contrario, se mostrará un mensaje de error. Por ejemplo:

```
A client error (404) occurred when calling the HeadBucket operation: Not Found
```

- Para obtener información sobre la API, consulte HeadBucket en la Referencia de comandos de AWS CLI.

`head-object`

En el siguiente ejemplo de código, se muestra cómo utilizar `head-object`.

AWS CLI

El siguiente comando recupera los metadatos de un objeto de un bucket denominado . `amzn-s3-demo-bucket`:

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key index.html
```

Salida:

```
{
    "AcceptRanges": "bytes",
    "ContentType": "text/html",
    "LastModified": "Thu, 16 Apr 2015 18:19:14 GMT",
    "ContentLength": 77,
    "VersionId": "null",
    "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
    "Metadata": {}
}
```

- Para obtener información de la API, consulte HeadObject en la Referencia de comandos de AWS CLI.

`list-bucket-analytics-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-bucket-analytics-configurations`.

AWS CLI

Recuperar una lista de configuraciones de análisis para un bucket

El siguiente `list-bucket-analytics-configurations` recupera una lista de configuraciones de análisis para el bucket especificado.

```
aws s3api list-bucket-analytics-configurations \
    --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "AnalyticsConfigurationList": [
        {
            "StorageClassAnalysis": {},
            "Id": "1"
        }
    ],
    "IsTruncated": false
}
```

- Para obtener información sobre la API, consulte ListBucketAnalyticsConfigurations en la Referencia de comandos de la AWS CLI.

`list-bucket-intelligent-tiering-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-bucket-intelligent-tiering-configurations`.

AWS CLI

Para obtener todas las configuraciones de S3 Intelligent-Tiering en un bucket

En el siguiente ejemplo de `list-bucket-intelligent-tiering-configurations`, se recupera toda la configuración de S3 Intelligent-Tiering de un bucket.

```
aws s3api list-bucket-intelligent-tiering-configurations \
    --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "IsTruncated": false,
    "IntelligentTieringConfigurationList": [
        {
            "Id": "ExampleConfig",
            "Filter": {
                "Prefix": "images"
            },
            "Status": "Enabled",
            "Tierings": [
                {
                    "Days": 90,
                    "AccessTier": "ARCHIVE_ACCESS"
                },
                {
                    "Days": 180,
                    "AccessTier": "DEEP_ARCHIVE_ACCESS"
                }
            ]
        },
        {
            "Id": "ExampleConfig2",
            "Status": "Disabled",
            "Tierings": [
                {
                    "Days": 730,
                    "AccessTier": "ARCHIVE_ACCESS"
                }
            ]
        },
        {
            "Id": "ExampleConfig3",
            "Filter": {
                "Tag": {
                    "Key": "documents",
                    "Value": "taxes"
                }
            },
            "Status": "Enabled",
            "Tierings": [
                {
                    "Days": 90,
```

```
                    "AccessTier": "ARCHIVE_ACCESS"
                },
                {
                    "Days": 365,
                    "AccessTier": "DEEP_ARCHIVE_ACCESS"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Uso de S3 Intelligent-Tiering en la Guía del usuario de Amazon S3.

- Para obtener información sobre la API, consulte ListBucketIntelligentTieringConfigurations en la Referencia de comandos de la AWS CLI.

`list-bucket-inventory-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-bucket-inventory-configurations`.

AWS CLI

Recuperar una lista de las configuraciones de inventario de un bucket

En el siguiente ejemplo de `list-bucket-inventory-configurations`, se enumeran las configuraciones de inventario del bucket especificado.

```
aws s3api list-bucket-inventory-configurations \
    --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "InventoryConfigurationList": [
        {
            "IsEnabled": true,
            "Destination": {
                "S3BucketDestination": {
                    "Format": "ORC",
                    "Bucket": "arn:aws:s3:::amzn-s3-demo-bucket",
```

```
                    "AccountId": "123456789012"
                }
            },
            "IncludedObjectVersions": "Current",
            "Id": "1",
            "Schedule": {
                "Frequency": "Weekly"
            }
        },
        {
            "IsEnabled": true,
            "Destination": {
                "S3BucketDestination": {
                    "Format": "CSV",
                    "Bucket": "arn:aws:s3:::amzn-s3-demo-bucket",
                    "AccountId": "123456789012"
                }
            },
            "IncludedObjectVersions": "Current",
            "Id": "2",
            "Schedule": {
                "Frequency": "Daily"
            }
        }
    ],
    "IsTruncated": false
}
```

- Para obtener información sobre la API, consulte ListBucketInventoryConfigurations en la Referencia de comandos de la AWS CLI.

`list-bucket-metrics-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-bucket-metrics-configurations`.

AWS CLI

Para recuperar una lista de las configuraciones de métricas para un bucket

En el siguiente ejemplo de `list-bucket-metrics-configurations` se recupera una lista de configuraciones de métricas para el bucket especificado.

```
aws s3api list-bucket-metrics-configurations \
    --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "IsTruncated": false,
    "MetricsConfigurationList": [
        {
            "Filter": {
                "Prefix": "logs"
            },
            "Id": "123"
        },
        {
            "Filter": {
                "Prefix": "tmp"
            },
            "Id": "234"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListBucketMetricsConfigurations en la Referencia de comandos de la AWS CLI.

`list-buckets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-buckets`.

AWS CLI

El siguiente comando usa el comando `list-buckets` para mostrar los nombres de todos los buckets de Amazon S3 (en todas las regiones):

```
aws s3api list-buckets --query "Buckets[].Name"
```

La opción de consultas filtra la salida de `list-buckets` únicamente a los nombres de los buckets.

Para obtener más información sobre los buckets, consulte Trabajo con buckets de Amazon S3 en la Guía para desarrolladores de Amazon S3.

- Para obtener información sobre la API, consulte ListBuckets en la Referencia de comandos de la AWS CLI.

`list-multipart-uploads`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-multipart-uploads`.

AWS CLI

El siguiente comando muestra todas las cargas multiparte activas de un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api list-multipart-uploads --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "Uploads": [
        {
            "Initiator": {
                "DisplayName": "username",
                "ID": "arn:aws:iam::0123456789012:user/username"
            },
            "Initiated": "2015-06-02T18:01:30.000Z",
            "UploadId":
 "dfRtDYU0WWCCcH43C3WFbkRONycyCpTJJvxu2i5GYkZljF.Yxwh6XG7WfS2vC4to6HiV6Yjlx.cph0gtNBtJ8P3URC
            "StorageClass": "STANDARD",
            "Key": "multipart/01",
            "Owner": {
                "DisplayName": "aws-account-name",
                "ID":
 "100719349fc3b6dcd7c820a124bf7aecd408092c3d7b51b38494939801fc248b"
            }
        }
    ],
    "CommonPrefixes": []
}
```

Las cargas multiparte en curso conllevan costos de almacenamiento en Amazon S3. Complete o anule una carga multiparte activa para eliminar sus partes de su cuenta.

- Para obtener información sobre la API, consulte ListMultipartUploads en la Referencia de comandos de la AWS CLI.

`list-object-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-object-versions`.

AWS CLI

El siguiente comando recupera la información de la versión de un objeto en un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api list-object-versions --bucket amzn-s3-demo-bucket --prefix index.html
```

Salida:

```
{
    "DeleteMarkers": [
        {
            "Owner": {
                "DisplayName": "my-username",
                "ID":
 "7009a8971cd660687538875e7c86c5b672fe116bd438f46db45460ddcd036c32"
            },
            "IsLatest": true,
            "VersionId": "B2VsEK5saUNNHKcOAJj7hIE86RozToyq",
            "Key": "index.html",
            "LastModified": "2015-11-10T00:57:03.000Z"
        },
        {
            "Owner": {
                "DisplayName": "my-username",
                "ID":
 "7009a8971cd660687538875e7c86c5b672fe116bd438f46db45460ddcd036c32"
            },
            "IsLatest": false,
            "VersionId": ".FLQEZscLIcfxSq.jsFJ.szUkmng2Yw6",
            "Key": "index.html",
            "LastModified": "2015-11-09T23:32:20.000Z"
        }
```

```
    ],
    "Versions": [
        {
            "LastModified": "2015-11-10T00:20:11.000Z",
            "VersionId": "Rb_l2T8UHDkFEwCgJjhlgPOZC0qJ.vpD",
            "ETag": "\"0622528de826c0df5db1258a23b80be5\"",
            "StorageClass": "STANDARD",
            "Key": "index.html",
            "Owner": {
                "DisplayName": "my-username",
                "ID":
"7009a8971cd660687538875e7c86c5b672fe116bd438f46db45460ddcd036c32"
            },
            "IsLatest": false,
            "Size": 38
        },
        {
            "LastModified": "2015-11-09T23:26:41.000Z",
            "VersionId": "rasWWGpgk9E4s0LyTJgusGeRQKLVIAFf",
            "ETag": "\"06225825b8028de826c0df5db1a23be5\"",
            "StorageClass": "STANDARD",
            "Key": "index.html",
            "Owner": {
                "DisplayName": "my-username",
                "ID":
"7009a8971cd660687538875e7c86c5b672fe116bd438f46db45460ddcd036c32"
            },
            "IsLatest": false,
            "Size": 38
        },
        {
            "LastModified": "2015-11-09T22:50:50.000Z",
            "VersionId": "null",
            "ETag": "\"d1f45267a863c8392e07d24dd592f1b9\"",
            "StorageClass": "STANDARD",
            "Key": "index.html",
            "Owner": {
                "DisplayName": "my-username",
                "ID":
"7009a8971cd660687538875e7c86c5b672fe116bd438f46db45460ddcd036c32"
            },
            "IsLatest": false,
            "Size": 533823
        }
```

```
    ]
}
```

- Para obtener información sobre la API, consulte ListObjectVersions en la Referencia de comandos de la AWS CLI.

`list-objects-v2`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-objects-v2`.

AWS CLI

Obtención de una lista de objetos en un bucket

En el siguiente ejemplo de `list-objects-v2` se muestran los objetos del bucket especificado.

```
aws s3api list-objects-v2 \
    --bucket amzn-s3-demo-bucket
```

Salida:

```
{
    "Contents": [
        {
            "LastModified": "2019-11-05T23:11:50.000Z",
            "ETag": "\"621503c373607d548b37cff8778d992c\"",
            "StorageClass": "STANDARD",
            "Key": "doc1.rtf",
            "Size": 391
        },
        {
            "LastModified": "2019-11-05T23:11:50.000Z",
            "ETag": "\"a2cecc36ab7c7fe3a71a273b9d45b1b5\"",
            "StorageClass": "STANDARD",
            "Key": "doc2.rtf",
            "Size": 373
        },
        {
            "LastModified": "2019-11-05T23:11:50.000Z",
            "ETag": "\"08210852f65a2e9cb999972539a64d68\"",
            "StorageClass": "STANDARD",
```

```
            "Key": "doc3.rtf",
            "Size": 399
        },
        {
            "LastModified": "2019-11-05T23:11:50.000Z",
            "ETag": "\"d1852dd683f404306569471af106988e\"",
            "StorageClass": "STANDARD",
            "Key": "doc4.rtf",
            "Size": 6225
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListObjectsV2 en la Referencia de comandos de AWS CLI.

`list-objects`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-objects`.

AWS CLI

En el siguiente ejemplo se utiliza el comando `list-objects` para mostrar los nombres de todos los objetos del bucket especificado:

```
aws s3api list-objects --bucket text-content --query 'Contents[].{Key: Key, Size:
 Size}'
```

En el ejemplo se utiliza el argumento `--query` para filtrar la salida de `list-objects` hasta el valor de la clave y el tamaño de cada objeto

Para obtener más información sobre los objetos, consulte Trabajo con objetos de Amazon S3 en la Guía para desarrolladores de Amazon S3.

- Para obtener detalles de la API, consulte ListObjects en la Referencia de comandos de AWS CLI.

`list-parts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-parts`.

AWS CLI

El siguiente comando muestra todas las partes que se han cargado para una carga multiparte con la clave `multipart/01` del bucket `amzn-s3-demo-bucket`:

```
aws s3api list-parts --bucket amzn-s3-demo-bucket --key 'multipart/01' --upload-
id dfRtDYU0WWCCcH43C3WFbkRONycyCpTJJvxu2i5GYkZljF.Yxwh6XG7WfS2vC4to6HiV6Yjlx.cph0gtNBtJ8P3UR
```

Salida:

```
{
    "Owner": {
        "DisplayName": "aws-account-name",
        "ID": "100719349fc3b6dcd7c820a124bf7aecd408092c3d7b51b38494939801fc248b"
    },
    "Initiator": {
        "DisplayName": "username",
        "ID": "arn:aws:iam::0123456789012:user/username"
    },
    "Parts": [
        {
            "LastModified": "2015-06-02T18:07:35.000Z",
            "PartNumber": 1,
            "ETag": "\"e868e0f4719e394144ef36531ee6824c\"",
            "Size": 5242880
        },
        {
            "LastModified": "2015-06-02T18:07:42.000Z",
            "PartNumber": 2,
            "ETag": "\"6bb2b12753d66fe86da4998aa33fffb0\"",
            "Size": 5242880
        },
        {
            "LastModified": "2015-06-02T18:07:47.000Z",
            "PartNumber": 3,
            "ETag": "\"d0a0112e841abec9c9ec83406f0159c8\"",
            "Size": 5242880
        }
    ],
    "StorageClass": "STANDARD"
}
```

- Para obtener información sobre la API, consulte ListParts en la Referencia de comandos de la AWS CLI.

`ls`

En el siguiente ejemplo de código, se muestra cómo utilizar `ls`.

AWS CLI

Ejemplo 1: lista de todos los buckets propiedad del usuario

El siguiente comando `ls` muestra todos los buckets que son propiedad del usuario. En este ejemplo, el usuario es propietario de los buckets `amzn-s3-demo-bucket` y `amzn-s3-demo-bucket2`. La marca de tiempo es la fecha en que se creó el bucket y se muestra en la zona horaria de su equipo. Esta fecha puede cambiar al realizar cambios en el bucket, por ejemplo, al editar la política de bucket. Tenga en cuenta que si `s3://` se usa como argumento de ruta `<S3Uri>`, también se mostrarán todos los buckets.

```
aws s3 ls
```

Salida:

```
2013-07-11 17:08:50 amzn-s3-demo-bucket
2013-07-24 14:55:44 amzn-s3-demo-bucket2
```

Ejemplo 2: lista de todos los prefijos y objetos de un bucket

El siguiente comando `ls` enumera los objetos y los prefijos comunes incluidos en un bucket y un prefijo específicos. En este ejemplo, el usuario es propietario del bucket `amzn-s3-demo-bucket` con los buckets `test.txt` y `somePrefix/test.txt`. `LastWriteTime` y `Length` son arbitrarios. Tenga en cuenta que, dado que el comando `ls` no interactúa con el sistema de archivos local, el esquema de URI `s3://` no debe resolver la ambigüedad y puede omitirse.

```
aws s3 ls s3://amzn-s3-demo-bucket
```

Salida:

```
                           PRE somePrefix/
2013-07-25 17:06:27         88 test.txt
```

Ejemplo 3: lista de todos los prefijos y objetos de un bucket y un prefijo específicos

El siguiente comando `ls` enumera los objetos y los prefijos comunes incluidos en un bucket y un prefijo específicos. Sin embargo, no hay objetos ni prefijos comunes en el bucket y el prefijo especificados.

```
aws s3 ls s3://amzn-s3-demo-bucket/noExistPrefix
```

Salida:

```
None
```

Ejemplo 4: lista recursiva de todos los prefijos y objetos de un bucket

El siguiente comando `ls` mostrará una lista de los objetos de un bucket de forma recursiva. En lugar de mostrar `PRE dirname/` en la salida, todo el contenido de un bucket se mostrará en orden.

```
aws s3 ls s3://amzn-s3-demo-bucket \
    --recursive
```

Salida:

```
2013-09-02 21:37:53         10 a.txt
2013-09-02 21:37:53    2863288 foo.zip
2013-09-02 21:32:57         23 foo/bar/.baz/a
2013-09-02 21:32:58         41 foo/bar/.baz/b
2013-09-02 21:32:57        281 foo/bar/.baz/c
2013-09-02 21:32:57         73 foo/bar/.baz/d
2013-09-02 21:32:57        452 foo/bar/.baz/e
2013-09-02 21:32:57        896 foo/bar/.baz/hooks/bar
2013-09-02 21:32:57        189 foo/bar/.baz/hooks/foo
2013-09-02 21:32:57        398 z.txt
```

Ejemplo 5: resumen de todos los prefijos y objetos de un bucket

El siguiente comando `ls` muestra el mismo comando con las opciones --human-readable y --summarize. --human-readable muestra el tamaño del archivo en Bytes/MiB/KiB/GiB/TiB/PiB/EiB. --summarize muestra el número total de objetos y el tamaño total al final de la lista de resultados:

```
aws s3 ls s3://amzn-s3-demo-bucket \
```

```
    --recursive \
    --human-readable \
    --summarize
```

Salida:

```
2013-09-02 21:37:53   10 Bytes a.txt
2013-09-02 21:37:53  2.9 MiB foo.zip
2013-09-02 21:32:57   23 Bytes foo/bar/.baz/a
2013-09-02 21:32:58   41 Bytes foo/bar/.baz/b
2013-09-02 21:32:57  281 Bytes foo/bar/.baz/c
2013-09-02 21:32:57   73 Bytes foo/bar/.baz/d
2013-09-02 21:32:57  452 Bytes foo/bar/.baz/e
2013-09-02 21:32:57  896 Bytes foo/bar/.baz/hooks/bar
2013-09-02 21:32:57  189 Bytes foo/bar/.baz/hooks/foo
2013-09-02 21:32:57  398 Bytes z.txt

Total Objects: 10
   Total Size: 2.9 MiB
```

Ejemplo 6: lista desde un punto de acceso de S3

El siguiente comando `ls` enumera los objetos del punto de acceso (`myaccesspoint`):

```
aws s3 ls s3://arn:aws:s3:us-west-2:123456789012:accesspoint/myaccesspoint/
```

Salida:

```
                           PRE somePrefix/
2013-07-25 17:06:27         88 test.txt
```

- Para obtener información sobre la API, consulte Ls en la Referencia de comandos de la AWS CLI.

mb

En el siguiente ejemplo de código, se muestra cómo utilizar `mb`.

AWS CLI

Ejemplo 1: creación de un bucket

El siguiente comando mb crea un bucket. En este ejemplo, el usuario crea el bucket amzn-s3-demo-bucket. El bucket se crea en la región especificada en el archivo de configuración del usuario:

```
aws s3 mb s3://amzn-s3-demo-bucket
```

Salida:

```
make_bucket: s3://amzn-s3-demo-bucket
```

Ejemplo 2: creación de un bucket en la región especificada

El siguiente comando mb crea un bucket en una región especificada por el parámetro --region. En este ejemplo, el usuario crea el bucket amzn-s3-demo-bucket en la región us-west-1:

```
aws s3 mb s3://amzn-s3-demo-bucket \
    --region us-west-1
```

Salida:

```
make_bucket: s3://amzn-s3-demo-bucket
```

- Para obtener información sobre la API, consulte Mb en la Referencia de comandos de la AWS CLI.

mv

En el siguiente ejemplo de código, se muestra cómo utilizar mv.

AWS CLI

Ejemplo 1: traslado de un archivo local al bucket especificado

El siguiente comando mv mueve un único archivo a un bucket y una clave específicos.

```
aws s3 mv test.txt s3://amzn-s3-demo-bucket/test2.txt
```

Salida:

```
move: test.txt to s3://amzn-s3-demo-bucket/test2.txt
```

Ejemplo 2: traslado de un objeto al bucket y la clave especificados

El siguiente comando mv mueve un único objeto S3 a un bucket y una clave específicos.

```
aws s3 mv s3://amzn-s3-demo-bucket/test.txt s3://amzn-s3-demo-bucket/test2.txt
```

Salida:

```
move: s3://amzn-s3-demo-bucket/test.txt to s3://amzn-s3-demo-bucket/test2.txt
```

Ejemplo 3: traslado de un objeto S3 al directorio local

El siguiente comando mv mueve un único objeto a un archivo específico localmente.

```
aws s3 mv s3://amzn-s3-demo-bucket/test.txt test2.txt
```

Salida:

```
move: s3://amzn-s3-demo-bucket/test.txt to test2.txt
```

Ejemplo 4: traslado de un objeto con su nombre original al bucket especificado

El siguiente comando mv mueve un único objeto a un bucket específico sin perder su nombre original:

```
aws s3 mv s3://amzn-s3-demo-bucket/test.txt s3://amzn-s3-demo-bucket2/
```

Salida:

```
move: s3://amzn-s3-demo-bucket/test.txt to s3://amzn-s3-demo-bucket2/test.txt
```

Ejemplo 5: traslado de todos los objetos y prefijos de un bucket al directorio local

Cuando se pasa con el parámetro `--recursive`, el siguiente comando mv mueve de forma recursiva todos los objetos con un prefijo y un bucket específicos en un directorio concreto. En este ejemplo, el bucket `amzn-s3-demo-bucket` contiene los objetos `test1.txt` y `test2.txt`.

```
aws s3 mv s3://amzn-s3-demo-bucket . \
    --recursive
```

Salida:

```
move: s3://amzn-s3-demo-bucket/test1.txt to test1.txt
move: s3://amzn-s3-demo-bucket/test2.txt to test2.txt
```

Ejemplo 6: traslado de todos los objetos y prefijos de un bucket al directorio local, excepto los archivos .jpg

Cuando se pasa con el parámetro `--recursive`, el siguiente comando `mv` mueve de forma recursiva todos los archivos de un directorio determinado a un bucket y prefijo específicos. También excluye algunos archivos con el parámetro `--exclude`. En este ejemplo, el directorio `myDir` contiene los archivos `test1.txt` y `test2.jpg`.

```
aws s3 mv myDir s3://amzn-s3-demo-bucket/ \
    --recursive \
    --exclude "*.jpg"
```

Salida:

```
move: myDir/test1.txt to s3://amzn-s3-demo-bucket2/test1.txt
```

Ejemplo 7: traslado de todos los objetos y prefijos de un bucket al directorio local, excepto el prefijo especificado

Cuando se pasa con el parámetro `--recursive`, el siguiente comando `--exclude` mueve de forma recursiva todos los objetos de un bucket determinado a otro bucket. También excluye algunos objetos con el parámetro `mv`. En este ejemplo, el bucket `amzn-s3-demo-bucket` contiene los objetos `test1.txt` y `another/test1.txt`.

```
aws s3 mv s3://amzn-s3-demo-bucket/ s3://amzn-s3-demo-bucket2/ \
    --recursive \
    --exclude "amzn-s3-demo-bucket/another/*"
```

Salida:

```
move: s3://amzn-s3-demo-bucket/test1.txt to s3://amzn-s3-demo-bucket2/test1.txt
```

Ejemplo 8: traslado de un objeto al bucket especificado y establecimiento del ACL

En el siguiente comando `mv`, se mueve un único objeto a un bucket y una clave específicos, y se configura ACL en `public-read-write`:

```
aws s3 mv s3://amzn-s3-demo-bucket/test.txt s3://amzn-s3-demo-bucket/test2.txt \
    --acl public-read-write
```

Salida:

```
move: s3://amzn-s3-demo-bucket/test.txt to s3://amzn-s3-demo-bucket/test2.txt
```

Ejemplo 9: traslado de un archivo local al bucket especificado y otorgamiento de permisos

El siguiente comando `mv` ilustra el uso de la opción `--grants` para conceder acceso de lectura a todos los usuarios y el control total a un usuario específico identificado por su dirección de correo electrónico.

```
aws s3 mv file.txt s3://amzn-s3-demo-bucket/ \
    --grants read=uri=http://acs.amazonaws.com/groups/global/
AllUsers full=emailaddress=user@example.com
```

Salida:

```
move: file.txt to s3://amzn-s3-demo-bucket/file.txt
```

Ejemplo 10: traslado de un archivo a un punto de acceso de S3

El siguiente comando `mv` mueve un único archivo denominado `mydoc.txt` al punto de acceso denominado `myaccesspoint` en la clave denominada `mykey`.

```
aws s3 mv mydoc.txt s3://arn:aws:s3:us-west-2:123456789012:accesspoint/
myaccesspoint/mykey
```

Salida:

```
move: mydoc.txt to s3://arn:aws:s3:us-west-2:123456789012:accesspoint/myaccesspoint/
mykey
```

- Para obtener información sobre la API, consulte Mv en la Referencia de comandos de la AWS CLI.

`presign`

En el siguiente ejemplo de código, se muestra cómo utilizar `presign`.

AWS CLI

Ejemplo 1: creación de una URL prefirmada con una vida útil predeterminada de una hora que esté vinculada con un objeto de un bucket de S3

El siguiente comando `presign` genera una URL prefirmada para un bucket y una clave específicos que es válida durante una hora.

```
aws s3 presign s3://amzn-s3-demo-bucket/test2.txt
```

Salida:

```
https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/key?X-Amz-Algorithm=AWS4-
HMAC-SHA256&X-Amz-Credential=AKIAEXAMPLE123456789%2F20210621%2Fus-
west-2%2Fs3%2Faws4_request&X-Amz-Date=20210621T041609Z&X-Amz-Expires=3600&X-Amz-
SignedHeaders=host&X-Amz-
Signature=EXAMBLE1234494d5fba3fed607f98018e1dfc62e2529ae96d844123456
```

Ejemplo 2: creación de una URL prefirmada con una vida útil personalizada que esté vinculada con un objeto de un bucket de S3

El siguiente comando `presign` genera una URL prefirmada para un bucket y una clave específicos que es válida durante una semana.

```
aws s3 presign s3://amzn-s3-demo-bucket/test2.txt \
    --expires-in 604800
```

Salida:

```
https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/key?X-Amz-Algorithm=AWS4-
HMAC-SHA256&X-Amz-Credential=AKIAEXAMPLE123456789%2F20210621%2Fus-
west-2%2Fs3%2Faws4_request&X-Amz-Date=20210621T041609Z&X-Amz-Expires=604800&X-Amz-
SignedHeaders=host&X-Amz-
Signature=EXAMBLE1234494d5fba3fed607f98018e1dfc62e2529ae96d844123456
```

Para obtener más información, consulte Uso compartido de objetos con URL prefirmadas en la Guía para desarrolladores de S3.

- Para obtener detalles de la API, consulte Presign en la Referencia de comandos de la AWS CLI.

`put-bucket-accelerate-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-accelerate-configuration`.

AWS CLI

Establecer la configuración acelerada de un bucket

En el siguiente ejemplo de `put-bucket-accelerate-configuration`, se habilita la configuración acelerada para el bucket especificado.

```
aws s3api put-bucket-accelerate-configuration \
    --bucket amzn-s3-demo-bucket \
    --accelerate-configuration Status=Enabled
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutBucketAccelerateConfiguration en Referencia de comandos de la AWS CLI.

`put-bucket-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-acl`.

AWS CLI

Este ejemplo otorga `full control` a dos usuarios de AWS (user1@example.com y user2@example.com) y permiso de `read` a todos los usuarios:

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --grant-full-
control emailaddress=user1@example.com,emailaddress=user2@example.com --grant-
read uri=http://acs.amazonaws.com/groups/global/AllUsers
```

Consulte http://docs.aws.amazon.com/AmazonS3/latest/API/RESTBucketPUTacl.html para obtener más información sobre las ACL personalizadas (los comandos s3api de ACL, como `put-bucket-acl`, utilizan la misma notación abreviada para el argumentos).

- Para obtener información sobre la API, consulte PutBucketAcl en la Referencia de comandos de la AWS CLI.

`put-bucket-analytics-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-analytics-configuration`.

AWS CLI

Para definir una configuración de análisis de un bucket

En el siguiente ejemplo de `put-bucket-analytics-configuration`, se configura el análisis para el bucket especificado.

```
aws s3api put-bucket-analytics-configuration \
    --bucket amzn-s3-demo-bucket --id 1 \
    --analytics-configuration '{"Id": "1","StorageClassAnalysis": {}}'
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutBucketAnalyticsConfiguration en Referencia de comandos de la AWS CLI.

`put-bucket-cors`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-cors`.

AWS CLI

El siguiente ejemplo habilita solicitudes `PUT`, `POST` y `DELETE` desde www.ejemplo.com, y habilita solicitudes `GET` desde cualquier dominio:

```
aws s3api put-bucket-cors --bucket amzn-s3-demo-bucket --cors-configuration file://
cors.json

cors.json:
{
  "CORSRules": [
    {
      "AllowedOrigins": ["http://www.example.com"],
      "AllowedHeaders": ["*"],
      "AllowedMethods": ["PUT", "POST", "DELETE"],
      "MaxAgeSeconds": 3000,
      "ExposeHeaders": ["x-amz-server-side-encryption"]
    },
    {
      "AllowedOrigins": ["*"],
      "AllowedHeaders": ["Authorization"],
      "AllowedMethods": ["GET"],
      "MaxAgeSeconds": 3000
    }
  ]
}
```

- Para obtener información acerca de la API, consulte PutBucketCors en la Referencia de comandos de la AWS CLI.

`put-bucket-encryption`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-encryption`.

AWS CLI

Configurar el cifrado del lado del servidor de un bucket

En el siguiente ejemplo de `put-bucket-encryption` se establece el cifrado AES256 como predeterminado para el bucket especificado.

```
aws s3api put-bucket-encryption \
    --bucket amzn-s3-demo-bucket \
    --server-side-encryption-configuration '{"Rules":
 [{"ApplyServerSideEncryptionByDefault": {"SSEAlgorithm": "AES256"}}]}'
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutBucketEncryption en la Referencia de comandos de la AWS CLI.

`put-bucket-intelligent-tiering-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-intelligent-tiering-configuration`.

AWS CLI

Para actualizar una configuración de S3 Intelligent-Tiering en un bucket

En el siguiente ejemplo de `put-bucket-intelligent-tiering-configuration`, se actualiza una configuración de S3 Intelligent-Tiering, denominada ExampleConfig, de un bucket. La configuración transferirá los objetos a los que no se haya accedido con el prefijo images a Acceso a archivos después de 90 días y a Acceso a archivos profundos después de 180 días.

```
aws s3api put-bucket-intelligent-tiering-configuration \
    --bucket amzn-s3-demo-bucket \
    --id "ExampleConfig" \
    --intelligent-tiering-configuration file://intelligent-tiering-
configuration.json
```

Contenido de `intelligent-tiering-configuration.json`:

```
{
    "Id": "ExampleConfig",
    "Status": "Enabled",
    "Filter": {
        "Prefix": "images"
        },
    "Tierings": [
        {
            "Days": 90,
            "AccessTier": "ARCHIVE_ACCESS"
        },
        {
            "Days": 180,
            "AccessTier": "DEEP_ARCHIVE_ACCESS"
        }
    ]
```

```
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de la propiedad de objetos en un bucket existente en la Guía del usuario de Amazon S3.

- Para obtener información sobre la API, consulte PutBucketIntelligentTieringConfiguration en Referencia de comandos de la AWS CLI.

`put-bucket-inventory-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-inventory-configuration`.

AWS CLI

Ejemplo 1: establecimiento de una configuración de inventario para un bucket

En el siguiente ejemplo de `put-bucket-inventory-configuration`, se establece un informe de inventario semanal con formato ORC para el bucket `amzn-s3-demo-bucket`.

```
aws s3api put-bucket-inventory-configuration \
    --bucket amzn-s3-demo-bucket \
    --id 1 \
    --inventory-configuration '{"Destination": { "S3BucketDestination":
 { "AccountId": "123456789012", "Bucket": "arn:aws:s3:::amzn-s3-demo-bucket",
 "Format": "ORC" }}, "IsEnabled": true, "Id": "1", "IncludedObjectVersions":
 "Current", "Schedule": { "Frequency": "Weekly" }}'
```

Este comando no genera ninguna salida.

Ejemplo 2: establecimiento de una configuración de inventario para un bucket

En el siguiente ejemplo de `put-bucket-inventory-configuration`, se establece un informe de inventario diario con formato CSV para el bucket `amzn-s3-demo-bucket`.

```
aws s3api put-bucket-inventory-configuration \
    --bucket amzn-s3-demo-bucket \
    --id 2 \
    --inventory-configuration '{"Destination": { "S3BucketDestination":
 { "AccountId": "123456789012", "Bucket": "arn:aws:s3:::amzn-s3-demo-bucket",
```

```
"Format": "CSV" }}, "IsEnabled": true, "Id": "2", "IncludedObjectVersions":
"Current", "Schedule": { "Frequency": "Daily" }}'
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutBucketInventoryConfiguration en Referencia de comandos de la AWS CLI.

`put-bucket-lifecycle-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-lifecycle-configuration`.

AWS CLI

El comando siguiente aplica una configuración del ciclo de vida a un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api put-bucket-lifecycle-configuration --bucket amzn-s3-demo-bucket --
lifecycle-configuration  file://lifecycle.json
```

El archivo `lifecycle.json` es un documento JSON en la carpeta actual que especifica dos reglas:

```
{
    "Rules": [
        {
            "ID": "Move rotated logs to Glacier",
            "Prefix": "rotated/",
            "Status": "Enabled",
            "Transitions": [
                {
                    "Date": "2015-11-10T00:00:00.000Z",
                    "StorageClass": "GLACIER"
                }
            ]
        },
        {
            "Status": "Enabled",
            "Prefix": "",
            "NoncurrentVersionTransitions": [
                {
```

```
                    "NoncurrentDays": 2,
                    "StorageClass": "GLACIER"
                }
            ],
            "ID": "Move old versions to Glacier"
        }
    ]
}
```

La primera regla mueve los archivos con el prefijo `rotated` a Glacier en la fecha especificada. La segunda regla mueve las versiones del objeto antiguas a Glacier cuando ya no están actualizadas. Para obtener más información sobre los formatos de marca temporal permitidos, consulte Especificación de valores de parámetros para la Guía del usuario de la AWS CLI.

- Para obtener información sobre la API, consulte PutBucketLifecycleConfiguration en la Referencia de comandos de la AWS CLI.

`put-bucket-lifecycle`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-lifecycle`.

AWS CLI

El comando siguiente aplica una configuración del ciclo de vida al bucket `amzn-s3-demo-bucket`:

```
aws s3api put-bucket-lifecycle --bucket amzn-s3-demo-bucket --lifecycle-
configuration file://lifecycle.json
```

El archivo `lifecycle.json` es un documento JSON en la carpeta actual que especifica dos reglas:

```
{
  "Rules": [
    {
      "ID": "Move to Glacier after sixty days (objects in logs/2015/)",
      "Prefix": "logs/2015/",
      "Status": "Enabled",
      "Transition": {
        "Days": 60,
        "StorageClass": "GLACIER"
      }
```

```
    },
    {
      "Expiration": {
        "Date": "2016-01-01T00:00:00.000Z"
      },
      "ID": "Delete 2014 logs in 2016.",
      "Prefix": "logs/2014/",
      "Status": "Enabled"
    }
  ]
}
```

La primera regla traslada los archivos a Amazon Glacier después de sesenta días. La segunda regla elimina los archivos de Amazon S3 en la fecha especificada. Para obtener más información sobre los formatos de marca temporal permitidos, consulte Especificación de valores de parámetros para la Guía del usuario de la AWS CLI.

Cada regla del ejemplo anterior especifica una política (`Transition` o `Expiration`) y un prefijo de archivo (nombre de carpeta) a los que se aplica. También puede crear una regla que se aplique a todo un bucket especificando un prefijo en blanco:

```
{
  "Rules": [
    {
      "ID": "Move to Glacier after sixty days (all objects in bucket)",
      "Prefix": "",
      "Status": "Enabled",
      "Transition": {
        "Days": 60,
        "StorageClass": "GLACIER"
      }
    }
  ]
}
```

- Para obtener información sobre la API, consulte PutBucketLifecycle en la Referencia de comandos de la AWS CLI.

`put-bucket-logging`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-logging`.

AWS CLI

Ejemplo 1: Configuración del registro de políticas de bucket

En el siguiente ejemplo de `put-bucket-logging`, se establece la política de registro para amzn-s3-demo-bucket. En primer lugar, conceda al servicio de registro el permiso de entidad principal en la política de bucket mediante el comando `put-bucket-policy`.

```
aws s3api put-bucket-policy \
    --bucket amzn-s3-demo-bucket \
    --policy file://policy.json
```

Contenido de `policy.json`:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "S3ServerAccessLogsPolicy",
            "Effect": "Allow",
            "Principal": {"Service": "logging.s3.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/Logs/*",
            "Condition": {
                "ArnLike": {"aws:SourceARN": "arn:aws:s3:::SOURCE-BUCKET-NAME"},
                "StringEquals": {"aws:SourceAccount": "SOURCE-AWS-ACCOUNT-ID"}
            }
        }
    ]
}
```

Para aplicar la política de registro, use `put-bucket-logging`.

```
aws s3api put-bucket-logging \
    --bucket amzn-s3-demo-bucket \
    --bucket-logging-status file://logging.json
```

Contenido de `logging.json`:

```
{
     "LoggingEnabled": {
```

```
        "TargetBucket": "amzn-s3-demo-bucket",
        "TargetPrefix": "Logs/"
    }
}
```

El comando `put-bucket-policy` es necesario para conceder permisos `s3:PutObject` a la entidad principal del servicio de registro.

Para obtener más información, consulte Registro de acceso al servidor de Amazon S3 en la Guía del usuario de Amazon S3.

Ejemplo 2: Establecimiento de una política de bucket para registrar el acceso a un solo usuario

En el siguiente ejemplo de `put-bucket-logging`, se establece la política de registro para amzn-s3-demo-bucket. El usuario de AWS bob@example.com tendrá el control total sobre los archivos de registro y nadie más tendrá acceso a ellos. En primer lugar, conceda permiso de S3 mediante `put-bucket-acl`.

```
aws s3api put-bucket-acl \
    --bucket amzn-s3-demo-bucket \
    --grant-write URI=http://acs.amazonaws.com/groups/s3/LogDelivery \
    --grant-read-acp URI=http://acs.amazonaws.com/groups/s3/LogDelivery
```

A continuación, aplique la política de registro mediante `put-bucket-logging`.

```
aws s3api put-bucket-logging \
    --bucket amzn-s3-demo-bucket \
    --bucket-logging-status file://logging.json
```

Contenido de `logging.json`:

```
{
    "LoggingEnabled": {
        "TargetBucket": "amzn-s3-demo-bucket",
        "TargetPrefix": "amzn-s3-demo-bucket-logs/",
        "TargetGrants": [
            {
                "Grantee": {
                    "Type": "AmazonCustomerByEmail",
                    "EmailAddress": "bob@example.com"
                },
```

```
                "Permission": "FULL_CONTROL"
            }
        ]
    }
}
```

el comando `put-bucket-acl` es necesario para conceder los permisos necesarios (write y read-acp) al sistema de entrega de registros de S3.

Para obtener más información, consulte Registro de acceso al servidor de Amazon S3 en la Guía para desarrolladores de Amazon S3.

- Para obtener información sobre la API, consulte PutBucketLogging en la Referencia de comandos de la AWS CLI.

`put-bucket-metrics-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-metrics-configuration`.

AWS CLI

Para establecer una configuración de métricas para un bucket

En el siguiente ejemplo de `put-bucket-metrics-configuration` se establece una configuración de métricas para ID 123 para el bucket especificado.

```
aws s3api put-bucket-metrics-configuration \
    --bucket amzn-s3-demo-bucket \
    --id 123 \
    --metrics-configuration '{"Id": "123", "Filter": {"Prefix": "logs"}}'
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutBucketMetricsConfiguration en la Referencia de comandos de la AWS CLI.

`put-bucket-notification-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-notification-configuration`.

AWS CLI

Habilitación de las notificaciones especificadas en un bucket

El siguiente ejemplo de `put-bucket-notification-configuration` se aplica una configuración de notificación a un bucket llamado `amzn-s3-demo-bucket`. El archivo `notification.json` es un documento JSON en la carpeta actual que especifica un tema de SNS y un tipo de evento para supervisar.

```
aws s3api put-bucket-notification-configuration \
    --bucket amzn-s3-demo-bucket \
    --notification-configuration file://notification.json
```

Contenido de `notification.json`:

```
{
    "TopicConfigurations": [
        {
            "TopicArn": "arn:aws:sns:us-west-2:123456789012:s3-notification-topic",
            "Events": [
                "s3:ObjectCreated:*"
            ]
        }
    ]
}
```

El tema de SNS debe tener una política de IAM adjunta que permita a Amazon S3 publicar en él.

```
{
    "Version":"2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SNS:Publish"
            ],
            "Resource": "arn:aws:sns:us-west-2:123456789012::s3-notification-topic",
```

```
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:*:*:amzn-s3-demo-bucket"
                }
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte PutBucketNotificationConfiguration en Referencia de comandos de la AWS CLI.

`put-bucket-notification`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-notification`.

AWS CLI

Aplica una configuración de notificación a un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api put-bucket-notification --bucket amzn-s3-demo-bucket --notification-
configuration file://notification.json
```

El archivo `notification.json` es un documento JSON en la carpeta actual que especifica un tema de SNS y un tipo de evento para supervisar:

```
{
  "TopicConfiguration": {
    "Event": "s3:ObjectCreated:*",
    "Topic": "arn:aws:sns:us-west-2:123456789012:s3-notification-topic"
  }
}
```

El tema de SNS debe tener una política de IAM adjunta que permita a Amazon S3 publicar en él:

```
{
 "Version":"2012-10-17",
 "Id": "example-ID",
 "Statement": [
  {
   "Sid": "example-statement-ID",
```

```
    "Effect": "Allow",
    "Principal": {
      "Service": "s3.amazonaws.com"
    },
    "Action": [
     "SNS:Publish"
    ],
    "Resource": "arn:aws:sns:us-west-2:123456789012:amzn-s3-demo-bucket",
    "Condition": {
       "ArnLike": {
       "aws:SourceArn": "arn:aws:s3:*:*:amzn-s3-demo-bucket"
     }
    }
   }
 ]
}
```

- Para obtener información sobre la API, consulte PutBucketNotification en la Referencia de comandos de la AWS CLI.

`put-bucket-ownership-controls`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-ownership-controls`.

AWS CLI

Para actualizar la configuración de propiedad de un bucket

En el siguiente ejemplo de `put-bucket-ownership-controls`, se actualiza la configuración de propiedad de un bucket.

```
aws s3api put-bucket-ownership-controls \
    --bucket amzn-s3-demo-bucket \
    --ownership-controls="Rules=[{ObjectOwnership=BucketOwnerEnforced}]"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de la propiedad de objetos en un bucket existente en la Guía del usuario de Amazon S3.

- Para obtener información sobre la API, consulte PutBucketOwnershipControls en la Referencia de comandos de la AWS CLI.

put-bucket-policy

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-policy`.

AWS CLI

Este ejemplo permite a todos los usuarios recuperar cualquier objeto en amzn-s3-demo-bucket excepto aquellos en MySecretFolder. También concede un permiso `put` y `delete` al usuario raíz de la cuenta de AWS `1234-5678-9012`:

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://policy.json

policy.json:
{
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": "s3:GetObject",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
      },
      {
         "Effect": "Deny",
         "Principal": "*",
         "Action": "s3:GetObject",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/MySecretFolder/*"
      },
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:root"
         },
         "Action": [
            "s3:DeleteObject",
            "s3:PutObject"
         ],
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
      }

  ]
}
```

- Para obtener información sobre la API, consulte PutBucketPolicy en la Referencia de comandos de la AWS CLI.

`put-bucket-replication`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-replication`.

AWS CLI

Configurar la replicación de un bucket de S

El siguiente ejemplo de `put-bucket-replication` aplica una configuración de replicación al bucket de S3 especificado.

```
aws s3api put-bucket-replication \
    --bucket amzn-s3-demo-bucket1 \
    --replication-configuration file://replication.json
```

Contenido de `replication.json`:

```
{
    "Role": "arn:aws:iam::123456789012:role/s3-replication-role",
    "Rules": [
        {
            "Status": "Enabled",
            "Priority": 1,
            "DeleteMarkerReplication": { "Status": "Disabled" },
            "Filter" : { "Prefix": ""},
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-bucket2"
            }
        }
    ]
}
```

El bucket de destino debe tener habilitado el control de versiones. El rol especificado debe tener permiso para escribir en el bucket de destino y tener una relación de confianza que permita a Amazon S3 asumir el rol.

Ejemplo de política de permisos de roles:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetReplicationConfiguration",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ReplicateObject",
                "s3:ReplicateDelete",
                "s3:ReplicateTags"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket2/*"
        }
    ]
}
```

Ejemplo de política de relación de confianza:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Este es el título del tema en la guía del usuario de la consola de Amazon Simple Storage Service:

- Para obtener información sobre la API, consulte PutBucketReplication en la Referencia de comandos de la AWS CLI.

`put-bucket-request-payment`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-request-payment`.

AWS CLI

Ejemplo 1: habilitar la configuración de “el solicitante paga” para un bucket

El siguiente ejemplo de `put-bucket-request-payment` habilita `requester pays` para el bucket especificado.

```
aws s3api put-bucket-request-payment \
    --bucket amzn-s3-demo-bucket \
    --request-payment-configuration '{"Payer":"Requester"}'
```

Este comando no genera ninguna salida.

Ejemplo 2: deshabilitar la configuración de “el solicitante paga” para un bucket

El siguiente ejemplo de `put-bucket-request-payment` deshabilita `requester pays` para el bucket especificado.

```
aws s3api put-bucket-request-payment \
    --bucket amzn-s3-demo-bucket \
    --request-payment-configuration '{"Payer":"BucketOwner"}'
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutBucketRequestPayment en la Referencia de comandos de la AWS CLI.

put-bucket-tagging

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-tagging`.

AWS CLI

El siguiente comando aplica una configuración de etiquetado a un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api put-bucket-tagging --bucket amzn-s3-demo-bucket --tagging file://
tagging.json
```

El archivo `tagging.json` es un documento JSON en la carpeta actual que especifica etiquetas:

```
{
   "TagSet": [
     {
       "Key": "organization",
       "Value": "marketing"
     }
   ]
}
```

O aplique una configuración de etiquetado a `amzn-s3-demo-bucket` directamente desde la línea de comandos:

```
aws s3api put-bucket-tagging --bucket amzn-s3-demo-bucket --tagging
 'TagSet=[{Key=organization,Value=marketing}]'
```

- Para obtener información sobre la API, consulte PutBucketTagging en la Referencia de comandos de la AWS CLI.

put-bucket-versioning

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-versioning`.

AWS CLI

El siguiente comando habilita el control de versiones en un bucket denominado `amzn-s3-demo-bucket`:

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket --versioning-configuration Status=Enabled
```

El siguiente comando habilita el control de versiones y usa un código mfa

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket --versioning-configuration Status=Enabled --mfa "SERIAL 123456"
```

- Para obtener información sobre la API, consulte PutBucketVersioning en la Referencia de comandos de la AWS CLI.

`put-bucket-website`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-bucket-website`.

AWS CLI

Aplica una configuración de sitio web estática a un bucket llamado `amzn-s3-demo-bucket`:

```
aws s3api put-bucket-website --bucket amzn-s3-demo-bucket --website-configuration file://website.json
```

El archivo `website.json` es un documento JSON en la carpeta actual que especifica las páginas de índice y error del sitio web:

```
{
    "IndexDocument": {
        "Suffix": "index.html"
    },
    "ErrorDocument": {
        "Key": "error.html"
    }
}
```

- Para obtener información sobre la API, consulte PutBucketWebsite en la Referencia de comandos de la AWS CLI.

`put-object-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-object-acl`.

AWS CLI

El comando siguiente concede `full control` a dos usuarios de AWS (user1@example.com y user2@example.com) y permiso de `read` a todos los usuarios:

```
aws s3api put-object-acl --bucket amzn-s3-demo-bucket --key file.txt --grant-full-control emailaddress=user1@example.com,emailaddress=user2@example.com --grant-read uri=http://acs.amazonaws.com/groups/global/AllUsers
```

Consulte http://docs.aws.amazon.com/AmazonS3/latest/API/RESTBucketPUTacl.html para obtener más información sobre las ACL personalizadas (los comandos s3api de ACL, como `put-object-acl`, utilizan la misma notación abreviada para el argumentos).

- Para obtener información acerca de la API, consulte PutObjectAcl en la Referencia de comandos de la AWS CLI.

`put-object-legal-hold`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-object-legal-hold`.

AWS CLI

Para aplicar una retención legal a un objeto

En el siguiente ejemplo de `put-object-legal-hold`, se establece una retención legal sobre el objeto `doc1.rtf`.

```
aws s3api put-object-legal-hold \
    --bucket amzn-s3-demo-bucket-with-object-lock \
    --key doc1.rtf \
    --legal-hold Status=ON
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutObjectLegalHold en la Referencia de comandos de la AWS CLI.

`put-object-lock-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-object-lock-configuration`.

AWS CLI

Para establecer la configuración de bloqueo de objetos en un bucket

En el siguiente ejemplo de `put-object-lock-configuration`, se establece un bloqueo de objetos de 50 días en el bucket especificado.

```
aws s3api put-object-lock-configuration \
    --bucket amzn-s3-demo-bucket-with-object-lock \
    --object-lock-configuration '{ "ObjectLockEnabled": "Enabled", "Rule":
 { "DefaultRetention": { "Mode": "COMPLIANCE", "Days": 50 }}}'
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutObjectLockConfiguration en la Referencia de comandos de la AWS CLI.

`put-object-retention`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-object-retention`.

AWS CLI

Para establecer la configuración de retención de un objeto

En el siguiente ejemplo de `put-object-retention`, se establece una configuración de retención del objeto especificado hasta el 1 de enero de 2025.

```
aws s3api put-object-retention \
    --bucket amzn-s3-demo-bucket-with-object-lock \
    --key doc1.rtf \
    --retention '{ "Mode": "GOVERNANCE", "RetainUntilDate": "2025-01-01T00:00:00" }'
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutObjectRetention en la Referencia de comandos de la AWS CLI.

`put-object-tagging`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-object-tagging`.

AWS CLI

Para establecer una etiqueta en un objeto

En el siguiente ejemplo de `put-object-tagging`, se define una etiqueta con la clave `designation` y el valor `confidential` al objeto especificado.

```
aws s3api put-object-tagging \
    --bucket amzn-s3-demo-bucket \
    --key doc1.rtf \
    --tagging '{"TagSet": [{ "Key": "designation", "Value": "confidential" }]}'
```

Este comando no genera ninguna salida.

En el siguiente ejemplo de `put-object-tagging`, se establecen varios conjuntos de etiquetas en el objeto especificado.

```
aws s3api put-object-tagging \
    --bucket amzn-s3-demo-bucket-example \
    --key doc3.rtf \
    --tagging '{"TagSet": [{ "Key": "designation", "Value": "confidential" },
 { "Key": "department", "Value": "finance" }, { "Key": "team", "Value":
 "payroll" } ]}'
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutObjectTagging en la Referencia de comandos de la AWS CLI.

`put-object`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-object`.

AWS CLI

Ejemplo 1: carga de un objeto en Amazon S3

El ejemplo de comando `put-object` siguiente carga un objeto en Amazon S3.

```
aws s3api put-object \
    --bucket amzn-s3-demo-bucket \
    --key my-dir/MySampleImage.png \
    --body MySampleImage.png
```

Para obtener más información acerca de cómo cargar objetos, consulte Carga de objetos <http://docs.aws.amazon.com/AmazonS3/latest/dev/UploadingObjects.html> en la Guía para desarrolladores de Amazon S3.

Ejemplo 2: carga de un archivo de vídeo en Amazon S3

El ejemplo de comando `put-object` siguiente carga un archivo de vídeo.

```
aws s3api put-object \
    --bucket amzn-s3-demo-bucket \
    --key my-dir/big-video-file.mp4 \
    --body /media/videos/f-sharp-3-data-services.mp4
```

Para obtener más información acerca de cómo cargar objetos, consulte Carga de objetos <http://docs.aws.amazon.com/AmazonS3/latest/dev/UploadingObjects.html> en la Guía para desarrolladores de Amazon S3.

- Para obtener información sobre la API, consulte PutObject en la Referencia de comandos de AWS CLI.

`put-public-access-block`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-public-access-block`.

AWS CLI

Para establecer la configuración de bloqueo de acceso público para un bucket

En el siguiente ejemplo de `put-public-access-block` se establece una configuración de bloqueo de acceso público restrictiva para el bucket especificado.

```
aws s3api put-public-access-block \
    --bucket amzn-s3-demo-bucket \
    --public-access-block-
configuration "BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPub
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutPublicAccessBlock en la Referencia de comandos de la AWS CLI.

`rb`

En el siguiente ejemplo de código, se muestra cómo utilizar `rb`.

AWS CLI

Ejemplo 1: eliminación de un bucket

El siguiente comando `rb` elimina un bucket. En este ejemplo, el bucket del usuario es `amzn-s3-demo-bucket`. Tenga en cuenta que el bucket debe estar vacío para poder eliminar:

```
aws s3 rb s3://amzn-s3-demo-bucket
```

Salida:

```
remove_bucket: amzn-s3-demo-bucket
```

Ejemplo 2: eliminación forzada de un bucket

El siguiente comando `rb` utiliza el parámetro `--force` para eliminar primero todos los objetos del bucket y, a continuación, el propio bucket. En este ejemplo, el bucket del usuario es `amzn-s3-demo-bucket` y los objetos que contiene `amzn-s3-demo-bucket` son `test1.txt` y `test2.txt`:

```
aws s3 rb s3://amzn-s3-demo-bucket \
    --force
```

Salida:

```
delete: s3://amzn-s3-demo-bucket/test1.txt
delete: s3://amzn-s3-demo-bucket/test2.txt
remove_bucket: amzn-s3-demo-bucket
```

- Para obtener información sobre la API, consulte Rb en la Referencia de comandos de la AWS CLI.

`restore-object`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-object`.

AWS CLI

Creación de una solicitud de restauración para un objeto

En el siguiente ejemplo de `restore-object` se restaura el objeto de Amazon S3 Glacier especificado para el bucket `my-glacier-bucket` durante 10 días.

```
aws s3api restore-object \
    --bucket my-glacier-bucket \
    --key doc1.rtf \
    --restore-request Days=10
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte RestoreObject en la Referencia de comandos de la AWS CLI.

`rm`

En el siguiente ejemplo de código, se muestra cómo utilizar `rm`.

AWS CLI

Ejemplo 1: eliminación de un objeto de S

El siguiente comando `rm` elimina un único objeto S3:

```
aws s3 rm s3://amzn-s3-demo-bucket/test2.txt
```

Salida:

```
delete: s3://amzn-s3-demo-bucket/test2.txt
```

Ejemplo 2: eliminación de todo el contenido de un bucket

El siguiente comando `rm` elimina de forma recursiva todos los objetos del bucket y el prefijo especificados al pasarlo con el parámetro `--recursive`. En este ejemplo, el bucket `amzn-s3-demo-bucket` contiene los objetos `test1.txt` y `test2.txt`:

```
aws s3 rm s3://amzn-s3-demo-bucket \
    --recursive
```

Salida:

```
delete: s3://amzn-s3-demo-bucket/test1.txt
delete: s3://amzn-s3-demo-bucket/test2.txt
```

Ejemplo 3: eliminación de todo el contenido de un bucket, excepto los archivos .jpg

Cuando se pasa con el parámetro `--recursive`, el siguiente comando `rm` elimina de forma recursiva todos los objetos de un bucket y prefijo determinados. También excluye algunos objetos con el parámetro `--exclude`. En este ejemplo, el bucket `amzn-s3-demo-bucket` contiene los objetos `test1.txt` y `test2.jpg`:

```
aws s3 rm s3://amzn-s3-demo-bucket/ \
    --recursive \
    --exclude "*.jpg"
```

Salida:

```
delete: s3://amzn-s3-demo-bucket/test1.txt
```

Ejemplo 4: eliminación de todo el contenido de un bucket, excepto los objetos con el prefijo especificado

Cuando se pasa con el parámetro `--recursive`, el siguiente comando `rm` elimina de forma recursiva todos los objetos de un bucket y prefijo determinados. También excluye todos los objetos de un prefijo determinado con el parámetro `--exclude`. En este ejemplo, el bucket `amzn-s3-demo-bucket` contiene los objetos `test1.txt` y `another/test.txt`:

```
aws s3 rm s3://amzn-s3-demo-bucket/ \
    --recursive \
    --exclude "another/*"
```

Salida:

```
delete: s3://amzn-s3-demo-bucket/test1.txt
```

Ejemplo 5: eliminación de un objeto desde un punto de acceso de S

El siguiente comando `rm` elimina un único objeto (`mykey`) del punto de acceso (`myaccesspoint`). :: El siguiente comando `rm` elimina un único objeto (`mykey`) del punto de acceso (`myaccesspoint`).

```
aws s3 rm s3://arn:aws:s3:us-west-2:123456789012:accesspoint/myaccesspoint/mykey
```

Salida:

```
delete: s3://arn:aws:s3:us-west-2:123456789012:accesspoint/myaccesspoint/mykey
```

- Para obtener información sobre la API, consulte Rm en la Referencia de comandos de la AWS CLI.

`select-object-content`

En el siguiente ejemplo de código, se muestra cómo utilizar `select-object-content`.

AWS CLI

Para filtrar el contenido de un objeto de Amazon S3 en función de una instrucción SQL

En el siguiente ejemplo de `select-object-content`, se filtra el objeto `my-data-file.csv` con la instrucción SQL especificada y se envía el resultado a un archivo.

```
aws s3api select-object-content \
    --bucket amzn-s3-demo-bucket \
    --key my-data-file.csv \
    --expression "select * from s3object limit 100" \
    --expression-type 'SQL' \
    --input-serialization '{"CSV": {}, "CompressionType": "NONE"}' \
    --output-serialization '{"CSV": {}}' "output.csv"
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte SelectObjectContent en la Referencia de comandos de la AWS CLI.

sync

En el siguiente ejemplo de código, se muestra cómo utilizar `sync`.

AWS CLI

Ejemplo 1: sincronización de todos los objetos locales con el bucket especificado

El siguiente comando `sync` sincroniza los objetos de un directorio local con el prefijo y el bucket especificados al cargar los archivos locales en S3. Será necesario cargar un archivo local si el tamaño del archivo local es diferente al tamaño del objeto de S3, si la hora de la última modificación del archivo local es posterior a la hora de la última modificación del objeto de S3 o si el archivo local no existe en el bucket y el prefijo especificados. En este ejemplo, el usuario sincroniza el bucket `amzn-s3-demo-bucket` con el directorio local actual. El directorio local actual contiene los archivos `test.txt` y `test2.txt`. El bucket `amzn-s3-demo-bucket` no contiene ningún objeto.

```
aws s3 sync . s3://amzn-s3-demo-bucket
```

Salida:

```
upload: test.txt to s3://amzn-s3-demo-bucket/test.txt
upload: test2.txt to s3://amzn-s3-demo-bucket/test2.txt
```

Ejemplo 2: sincronización de todos los objetos de S3 del bucket de S3 especificado con otro bucket

El siguiente comando `sync` sincroniza los objetos con un prefijo y un bucket específicos que están bajo otro prefijo y bucket determinados al copiar los objetos de S3. Será necesario copiar un objeto de S3 si los tamaños de los dos objetos de S3 son diferentes, si la hora de la última modificación del origen es más reciente que la hora de la última modificación del destino o si el objeto de S3 no existe en el bucket y el prefijo de destino especificados.

En este ejemplo, el usuario sincroniza el bucket `amzn-s3-demo-bucket` con el bucket `amzn-s3-demo-bucket2`. El bucket `amzn-s3-demo-bucket` contiene los objetos `test.txt` y `test2.txt`. El bucket `amzn-s3-demo-bucket2` no contiene ningún objeto:

```
aws s3 sync s3://amzn-s3-demo-bucket s3://amzn-s3-demo-bucket2
```

Salida:

```
copy: s3://amzn-s3-demo-bucket/test.txt to s3://amzn-s3-demo-bucket2/test.txt
copy: s3://amzn-s3-demo-bucket/test2.txt to s3://amzn-s3-demo-bucket2/test2.txt
```

Ejemplo 3: sincronización de todos los objetos de S3 del bucket de S3 especificado con el directorio local

El siguiente comando `sync` sincroniza los archivos de un bucket S3 específico en el directorio local al cargar los objetos S3. Será necesario descargar un objeto de S3 si el tamaño del objeto de S3 es diferente al tamaño del archivo local, si la hora de la última modificación del objeto de S3 es posterior a la hora de la última modificación del archivo local o si el objeto de S3 no existe en el directorio local. Tenga en cuenta que cuando los objetos se descargan desde S3, la hora de la última modificación del archivo local se cambia por la hora de la última modificación del objeto de S3. En este ejemplo, el usuario sincroniza el bucket `amzn-s3-demo-bucket` con el directorio local actual. El bucket `amzn-s3-demo-bucket` contiene los objetos `test.txt` y `test2.txt`. El directorio local actual no tiene archivos:

```
aws s3 sync s3://amzn-s3-demo-bucket .
```

Salida:

```
download: s3://amzn-s3-demo-bucket/test.txt to test.txt
download: s3://amzn-s3-demo-bucket/test2.txt to test2.txt
```

Ejemplo 4: sincronización de todos los objetos locales con el bucket especificado y eliminación de todos los archivos que no coincidan

El siguiente comando `sync` sincroniza los objetos bajo un prefijo y bucket especificados con los archivos de un directorio local cargando los archivos locales en S3. Debido al parámetro `--delete`, se eliminarán todos los archivos que tengan el prefijo y el bucket especificados, pero que no estén en el directorio local. En este ejemplo, el usuario sincroniza el bucket `amzn-s3-demo-bucket` con el directorio local actual. El directorio local actual contiene los archivos `test.txt` y `test2.txt`. El bucket `amzn-s3-demo-bucket` contiene el objeto `test3.txt`:

```
aws s3 sync . s3://amzn-s3-demo-bucket \
    --delete
```

Salida:

```
upload: test.txt to s3://amzn-s3-demo-bucket/test.txt
```

```
upload: test2.txt to s3://amzn-s3-demo-bucket/test2.txt
delete: s3://amzn-s3-demo-bucket/test3.txt
```

Ejemplo 5: sincronización de todos los objetos locales con el bucket especificado, excepto los archivos .jpg

El siguiente comando `sync` sincroniza los objetos bajo un prefijo y bucket especificados con los archivos de un directorio local cargando los archivos locales en S3. Debido al parámetro `--exclude`, todos los archivos que coincidan con el patrón existente tanto en S3 como localmente se excluirán de la sincronización. En este ejemplo, el usuario sincroniza el bucket `amzn-s3-demo-bucket` con el directorio local actual. El directorio local actual contiene los archivos `test.jpg` y `test2.txt`. El bucket `amzn-s3-demo-bucket` contiene el objeto `test.jpg` de un tamaño diferente al `test.jpg` local:

```
aws s3 sync . s3://amzn-s3-demo-bucket \
    --exclude "*.jpg"
```

Salida:

```
upload: test2.txt to s3://amzn-s3-demo-bucket/test2.txt
```

Ejemplo 6: sincronización de todos los objetos locales con el bucket especificado, excepto los archivos del directorio especificado

El siguiente comando `sync` sincroniza los archivos de un directorio local con los objetos con un prefijo y bucket específicos descargando los objetos S3. En este ejemplo, se utiliza el parámetro `--exclude` para excluir un directorio y un prefijo de S3 específicos del comando `sync`. En este ejemplo, el usuario sincroniza el directorio local actual con el bucket `amzn-s3-demo-bucket`. El directorio local actual contiene los archivos `test.txt` y `another/test2.txt`. El bucket `amzn-s3-demo-bucket` contiene los objetos `another/test5.txt` y `test1.txt`:

```
aws s3 sync s3://amzn-s3-demo-bucket/ . \
    --exclude "*another/*"
```

Salida:

```
download: s3://amzn-s3-demo-bucket/test1.txt to test1.txt
```

Ejemplo 7: sincronización de todos los buckets de diferentes regiones

El siguiente comando `sync` sincroniza los archivos entre dos buckets en diferentes regiones:

```
aws s3 sync s3://my-us-west-2-bucket s3://my-us-east-1-bucket \
    --source-region us-west-2 \
    --region us-east-1
```

Salida:

```
download: s3://my-us-west-2-bucket/test1.txt to s3://my-us-east-1-bucket/test1.txt
```

Ejemplo 8: sincronización con un punto de acceso de S

El siguiente comando `sync` sincroniza el directorio actual con el punto de acceso (`myaccesspoint`):

```
aws s3 sync . s3://arn:aws:s3:us-west-2:123456789012:accesspoint/myaccesspoint/
```

Salida:

```
upload: test.txt to s3://arn:aws:s3:us-west-2:123456789012:accesspoint/
myaccesspoint/test.txt
upload: test2.txt to s3://arn:aws:s3:us-west-2:123456789012:accesspoint/
myaccesspoint/test2.txt
```

- Para obtener información sobre la API, consulte Sync en la Referencia de comandos de la AWS CLI.

upload-part-copy

En el siguiente ejemplo de código, se muestra cómo utilizar `upload-part-copy`.

AWS CLI

Para cargar parte de un objeto al copiar los datos de un objeto existente como origen de datos

En el siguiente ejemplo de `upload-part-copy`, se carga una parte al copiar los datos de un objeto existente como origen de datos.

```
aws s3api upload-part-copy \
    --bucket amzn-s3-demo-bucket \
    --key "Map_Data_June.mp4" \
```

```
    --copy-source "amzn-s3-demo-bucket/copy_of_Map_Data_June.mp4" \
    --part-number 1 \
    --upload-
id "bq0tdE1CDpWQYRPLHuNG50xAT6pA5D.m_RiBy0ggOH6b13pVRY7QjvLlf75iFdJqp_2wztk5hvpUM2SesXgrzbeh
```

Salida:

```
{
    "CopyPartResult": {
        "LastModified": "2019-12-13T23:16:03.000Z",
        "ETag": "\"711470fc377698c393d94aed6305e245\""
    }
}
```

- Para obtener información sobre la API, consulte UploadPartCopy en la Referencia AWS CLI de comandos.

`upload-part`

En el siguiente ejemplo de código, se muestra cómo utilizar `upload-part`.

AWS CLI

El siguiente comando carga la primera parte de una carga multiparte iniciada con el comando `create-multipart-upload`:

```
aws s3api upload-part --bucket amzn-s3-demo-bucket --key
 'multipart/01' --part-number 1 --body part01 --upload-id
  "dfRtDYU0WWCCcH43C3WFbkRONycyCpTJJvxu2i5GYkZljF.Yxwh6XG7WfS2vC4to6HiV6Yjlx.cph0gtNBtJ8P3UR
```

La opción body toma el nombre o la ruta de un archivo local para la carga (no utilice el prefijo file://). El tamaño mínimo de parte es de 5 MB. El ID de carga lo devuelve `create-multipart-upload` y también se puede recuperar con `list-multipart-uploads`. El bucket y la clave se especifican al crear la carga multiparte.

Salida:

```
{
    "ETag": "\"e868e0f4719e394144ef36531ee6824c\""
}
```

Guarde el valor de ETag de cada parte para más adelante. Son necesarios para completar la carga multiparte.

- Para obtener información sobre la API, consulte UploadPart en la Referencia de comandos de la AWS CLI.

`website`

En el siguiente ejemplo de código, se muestra cómo utilizar `website`.

AWS CLI

Configuración de un bucket de S3 como sitio web estático

El siguiente comando configura un bucket denominado `amzn-s3-demo-bucket` como sitio web estático. La opción del documento de índice especifica el archivo en `amzn-s3-demo-bucket` al que se dirigirá a los visitantes cuando naveguen a la URL del sitio web. En este caso, el bucket se encuentra en la región us-west-2, por lo que el sitio aparecería en `http://amzn-s3-demo-bucket.s3-website-us-west-2.amazonaws.com`.

Todos los archivos del bucket que aparecen en el sitio estático deben estar configurados para que los visitantes puedan abrirlos. Los permisos de los archivos se configuran de forma independiente desde la configuración del sitio web del bucket.

```
aws s3 website s3://amzn-s3-demo-bucket/ \
    --index-document index.html \
    --error-document error.html
```

Para obtener más información sobre el alojamiento de un sitio web estático en Amazon S3, consulte Alojamiento de un sitio web estático mediante Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

- Para obtener detalles de la API, consulte Website en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon S3 Control que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon S3 Control.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-access-point`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-access-point`.

AWS CLI

Para crear un punto de acceso

En el siguiente ejemplo de `create-access-point`, se crea un punto de acceso denominado `finance-ap` para el bucket `business-records` de la cuenta 123456789012. Antes de ejecutar este ejemplo, reemplace el nombre del punto de acceso, el nombre del bucket y el número de cuenta con valores adecuados para su caso de uso.

```
aws s3control create-access-point \
    --account-id 123456789012 \
    --bucket business-records \
    --name finance-ap
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Crear puntos de acceso en la Guía del usuario de Amazon Simple Storage Service.

- Para obtener información sobre la API, consulte CreateAccessPoint en la Referencia de comandos de la AWS CLI.

`create-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-job`.

AWS CLI

Para crear un trabajo de Operaciones por lotes de Amazon S3

En el siguiente ejemplo de `create-job`, se crea un trabajo de operaciones por lotes de Amazon S3 para etiquetar objetos como `confidential` in the bucket ``employee-records`.

```
aws s3control create-job \
    --account-id 123456789012 \
    --operation '{"S3PutObjectTagging": { "TagSet": [{"Key":"confidential",
 "Value":"true"}] }}' \
    --report '{"Bucket":"arn:aws:s3:::employee-records-logs","Prefix":"batch-op-
create-job",
 "Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \
    --manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820","Fields":
["Bucket","Key"]},"Location":{"ObjectArn":"arn:aws:s3:::employee-records-logs/inv-
report/7a6a9be4-072c-407e-85a2-
ec3e982f773e.csv","ETag":"69f52a4e9f797e987155d9c8f5880897"}}' \
    --priority 42 \
    --role-arn arn:aws:iam::123456789012:role/S3BatchJobRole
```

Salida:

```
{
    "JobId": "93735294-df46-44d5-8638-6356f335324e"
}
```

- Para obtener más información sobre la API, consulte CreateJob en la Referencia de comandos de la AWS CLI.

`delete-access-point-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-access-point-policy`.

AWS CLI

Para eliminar una política de punto de acceso

En el siguiente ejemplo de `delete-access-point-policy`, se elimina la política de puntos de acceso del punto de acceso denominado `finance-ap` en la cuenta 123456789012. Antes

de ejecutar este ejemplo, reemplace el nombre del punto de acceso y el número de cuenta con valores adecuados para su caso de uso.

```
aws s3control delete-access-point-policy \
    --account-id 123456789012 \
    --name finance-ap
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración del acceso a conjuntos de datos compartidos con puntos de acceso en la Guía del usuario de Amazon Simple Storage Service.

- Para obtener información sobre la API, consulte DeleteAccessPointPolicy en la Referencia de comandos de la AWS CLI.

`delete-access-point`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-access-point`.

AWS CLI

Para eliminar un punto de acceso

En el ejemplo siguiente de `delete-access-point`, se elimina un punto de acceso denominado `finance-ap` de la cuenta 123456789012. Antes de ejecutar este ejemplo, reemplace el nombre del punto de acceso y el número de cuenta con valores adecuados para su caso de uso.

```
aws s3control delete-access-point \
    --account-id 123456789012 \
    --name finance-ap
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración del acceso a conjuntos de datos compartidos con puntos de acceso en la Guía del usuario de Amazon Simple Storage Service.

- Para obtener información sobre la API, consulte DeleteAccessPoint en la Referencia de comandos de la AWS CLI.

`delete-public-access-block`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-public-access-block`.

AWS CLI

Para eliminar la configuración de Bloqueo de acceso público de una cuenta

En el siguiente ejemplo de `delete-public-access-block`, se elimina la configuración de bloqueo de acceso público de la cuenta especificada.

```
aws s3control delete-public-access-block \
    --account-id 123456789012
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeletePublicAccessBlock en la Referencia de comandos de la AWS CLI.

`describe-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-job`.

AWS CLI

Para describir un trabajo de Operaciones por lotes de Amazon S3

En el siguiente ejemplo de `describe-job`, se proporcionan los parámetros de configuración y el estado del trabajo de operaciones por lotes especificado.

```
aws s3control describe-job \
    --account-id 123456789012 \
    --job-id 93735294-df46-44d5-8638-6356f335324e
```

Salida:

```
{
    "Job": {
        "TerminationDate": "2019-10-03T21:49:53.944Z",
        "JobId": "93735294-df46-44d5-8638-6356f335324e",
        "FailureReasons": [],
        "Manifest": {
            "Spec": {
                "Fields": [
                    "Bucket",
```

```
                    "Key"
                ],
                "Format": "S3BatchOperations_CSV_20180820"
            },
            "Location": {
                "ETag": "69f52a4e9f797e987155d9c8f5880897",
                "ObjectArn": "arn:aws:s3:::employee-records-logs/inv-
report/7a6a9be4-072c-407e-85a2-ec3e982f773e.csv"
            }
        },
        "Operation": {
            "S3PutObjectTagging": {
                "TagSet": [
                    {
                        "Value": "true",
                        "Key": "confidential"
                    }
                ]
            }
        },
        "RoleArn": "arn:aws:iam::123456789012:role/S3BatchJobRole",
        "ProgressSummary": {
            "TotalNumberOfTasks": 8,
            "NumberOfTasksFailed": 0,
            "NumberOfTasksSucceeded": 8
        },
        "Priority": 42,
        "Report": {
            "ReportScope": "AllTasks",
            "Format": "Report_CSV_20180820",
            "Enabled": true,
            "Prefix": "batch-op-create-job",
            "Bucket": "arn:aws:s3:::employee-records-logs"
        },
        "JobArn": "arn:aws:s3:us-west-2:123456789012:job/93735294-
df46-44d5-8638-6356f335324e",
        "CreationTime": "2019-10-03T21:48:48.048Z",
        "Status": "Complete"
    }
}
```

- Para obtener información sobre la API, consulte DescribeJob en la Referencia de comandos de AWS CLI.

`get-access-point-policy-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-access-point-policy-status`.

AWS CLI

Para recuperar el estado de la política del punto de acceso

En el siguiente ejemplo de `get-access-point-policy-status`, se recupera el estado de la política de puntos de acceso del punto de acceso denominado `finance-ap` en la cuenta 123456789012. El estado de la política del punto de acceso indica si la política del punto de acceso permite el acceso público. Antes de ejecutar este ejemplo, reemplace el nombre del punto de acceso y el número de cuenta con valores adecuados para su caso de uso.

```
aws s3control get-access-point-policy-status \
    --account-id 123456789012 \
    --name finance-ap
```

Salida:

```
{
    "PolicyStatus": {
        "IsPublic": false
    }
}
```

Para obtener más información acerca de cuándo se considera que una política de punto de acceso es pública, consulte la sección Qué significa "pública" en la Guía del usuario de Amazon Simple Storage Service.

- Para obtener información sobre la API, consulte GetAccessPointPolicyStatus en la Referencia de comandos de la AWS CLI.

`get-access-point-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-access-point-policy`.

AWS CLI

Para recuperar una política de punto de acceso

En el siguiente ejemplo de `get-access-point-policy`, se recupera la política del punto de acceso del punto de acceso denominado `finance-ap` en la cuenta 123456789012. Antes de ejecutar este ejemplo, reemplace el nombre del punto de acceso y el número de cuenta con valores adecuados para su caso de uso.

```
aws s3control get-access-point-policy \
    --account-id 123456789012 \
    --name finance-ap
```

Salida:

```
{
    "Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":\"arn:aws:iam::123456789012:role/Admin\"},\"Action\":
\"s3:GetObject\",\"Resource\":\"arn:aws:s3:us-west-2:123456789012:accesspoint/
finance-ap/object/records/*\"}]}"
}
```

Para obtener más información, consulte Administración del acceso a conjuntos de datos compartidos con puntos de acceso en la Guía del usuario de Amazon Simple Storage Service.

- Para obtener información sobre la API, consulte GetAccessPointPolicy en la Referencia de comandos de la AWS CLI.

`get-access-point`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-access-point`.

AWS CLI

Para recuperar los detalles de configuración del punto de acceso

En el siguiente ejemplo de `get-access-point`, se recuperan los detalles de configuración del punto de acceso denominado `finance-ap` en la cuenta 123456789012. Antes de ejecutar este ejemplo, reemplace el nombre del punto de acceso y el número de cuenta con valores adecuados para su caso de uso.

```
aws s3control get-access-point \
    --account-id 123456789012 \
    --name finance-ap
```

Salida:

```
{
    "Name": "finance-ap",
    "Bucket": "business-records",
    "NetworkOrigin": "Internet",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": false,
        "IgnorePublicAcls": false,
        "BlockPublicPolicy": false,
        "RestrictPublicBuckets": false
    },
    "CreationDate": "2020-01-01T00:00:00Z"
}
```

Para obtener más información, consulte Administración del acceso a conjuntos de datos compartidos con puntos de acceso en la Guía del usuario de Amazon Simple Storage Service.

- Para obtener información sobre la API, consulte GetAccessPoint en la Referencia de comandos de la AWS CLI.

`get-multi-region-access-point-routes`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-multi-region-access-point-routes`.

AWS CLI

Para consultar la configuración actual de enrutamiento del punto de acceso de varias regiones

En el siguiente ejemplo de `get-multi-region-access-point-routes`, se devuelve la configuración actual de la ruta del punto de acceso multirregional especificado.

```
aws s3control get-multi-region-access-point-routes \
    --region Region \
    --account-id 111122223333 \
    --mrap MultiRegionAccessPoint_ARN
```

Salida:

```
{
```

```
    "Mrap": "arn:aws:s3::111122223333:accesspoint/0000000000000.mrap",
    "Routes": [
        {
            "Bucket": "amzn-s3-demo-bucket1",
            "Region": "ap-southeast-2",
            "TrafficDialPercentage": 100
        },
        {
            "Bucket": "amzn-s3-demo-bucket2",
            "Region": "us-west-1",
            "TrafficDialPercentage": 0
        }
    ]
}
```

- Para obtener información sobre la API, consulte GetMultiRegionAccessPointRoutes en la Referencia de comandos de la AWS CLI.

`get-public-access-block`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-public-access-block`.

AWS CLI

Para enumerar la configuración de Bloqueo de acceso público de una cuenta

En el siguiente ejemplo de `get-public-access-block`, se muestra la configuración de bloqueo de acceso público de la cuenta especificada.

```
aws s3control get-public-access-block \
    --account-id 123456789012
```

Salida:

```
{
   "PublicAccessBlockConfiguration": {
      "BlockPublicPolicy": true,
      "RestrictPublicBuckets": true,
      "IgnorePublicAcls": true,
      "BlockPublicAcls": true
   }
```

```
}
```

- Para obtener información sobre la API, consulte GetPublicAccessBlock en la Referencia de comandos de la AWS CLI.

`list-access-points`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-access-points`.

AWS CLI

Ejemplo 1: recuperación de una lista de todos los puntos de acceso para una cuenta

En el siguiente ejemplo de `list-access-points`, se muestra una lista de todos los puntos de acceso asociados a los buckets propiedad de la cuenta 123456789012.

```
aws s3control list-access-points \
    --account-id 123456789012
```

Salida:

```
{
    "AccessPointList": [
        {
            "Name": "finance-ap",
            "NetworkOrigin": "Internet",
            "Bucket": "business-records"
        },
        {
            "Name": "managers-ap",
            "NetworkOrigin": "Internet",
            "Bucket": "business-records"
        },
        {
            "Name": "private-network-ap",
            "NetworkOrigin": "VPC",
            "VpcConfiguration": {
                "VpcId": "1a2b3c"
            },
            "Bucket": "business-records"
        },
        {
```

```
            "Name": "customer-ap",
            "NetworkOrigin": "Internet",
            "Bucket": "external-docs"
        },
        {
            "Name": "public-ap",
            "NetworkOrigin": "Internet",
            "Bucket": "external-docs"
        }
    ]
}
```

Ejemplo 2: recuperación de una lista de todos los puntos de acceso para un bucket

En el siguiente ejemplo de `list-access-points`, se recupera una lista de todos los puntos de acceso asociados al bucket `external-docs` propiedad de la cuenta 123456789012.

```
aws s3control list-access-points \
    --account-id 123456789012 \
    --bucket external-docs
```

Salida:

```
{
    "AccessPointList": [
        {
            "Name": "customer-ap",
            "NetworkOrigin": "Internet",
            "Bucket": "external-docs"
        },
        {
            "Name": "public-ap",
            "NetworkOrigin": "Internet",
            "Bucket": "external-docs"
        }
    ]
}
```

Para obtener más información, consulte Administración del acceso a conjuntos de datos compartidos con puntos de acceso en la Guía del usuario de Amazon Simple Storage Service.

- Para obtener información sobre la API, consulte ListAccessPoints en la Referencia de comandos de la AWS CLI.

`list-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-jobs`.

AWS CLI

Para enumerar los trabajos de Operaciones por lotes de Amazon S3 de una cuenta

En el siguiente ejemplo de `list-jobs`, se muestran todos los trabajos de operaciones por lotes recientes de la cuenta especificada.

```
aws s3control list-jobs \
    --account-id 123456789012
```

Salida:

```
{
    "Jobs": [
        {
            "Operation": "S3PutObjectTagging",
            "ProgressSummary": {
                "NumberOfTasksFailed": 0,
                "NumberOfTasksSucceeded": 8,
                "TotalNumberOfTasks": 8
            },
            "CreationTime": "2019-10-03T21:48:48.048Z",
            "Status": "Complete",
            "JobId": "93735294-df46-44d5-8638-6356f335324e",
            "Priority": 42
        },
        {
            "Operation": "S3PutObjectTagging",
            "ProgressSummary": {
                "NumberOfTasksFailed": 0,
                "NumberOfTasksSucceeded": 0,
                "TotalNumberOfTasks": 0
            },
            "CreationTime": "2019-10-03T21:46:07.084Z",
            "Status": "Failed",
            "JobId": "3f3c7619-02d3-4779-97f6-1d98dd313108",
            "Priority": 42
        },
    ]
```

```
}
```

- Para obtener información sobre la API, consulte ListJobs en la Referencia de comandos de la AWS CLI.

`put-access-point-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-access-point-policy`.

AWS CLI

Para definir una política de punto de acceso

En el siguiente ejemplo de `put-access-point-policy`, se coloca la política de puntos de acceso especificada para el punto de acceso `finance-ap` en la cuenta 123456789012. Si el punto de acceso `finance-ap` ya tiene una política, este comando reemplaza la política existente por la especificada en este comando. Antes de ejecutar este ejemplo, reemplace el nombre de la cuenta, el nombre del punto de acceso y las instrucciones de la política con valores adecuados para su caso de uso.

```
aws s3control put-access-point-policy \
    --account-id 123456789012 \
    --name finance-ap \
    --policy file://ap-policy.json
```

Contenido de `ap-policy.json`:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Alice"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/finance-ap/
object/Alice/*"
        }
    ]
```

```
}
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración del acceso a conjuntos de datos compartidos con puntos de acceso en la Guía del usuario de Amazon Simple Storage Service.

- Para obtener información sobre la API, consulte PutAccessPointPolicy en la Referencia de comandos de la AWS CLI.

`put-public-access-block`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-public-access-block`.

AWS CLI

Para editar la configuración de Bloqueo de acceso público de una cuenta

En el siguiente ejemplo de `put-public-access-block`, se cambia la configuración de bloqueo de acceso público de `true` para la cuenta especificada.

```
aws s3control put-public-access-block \
    --account-id 123456789012 \
    --public-access-block-configuration '{"BlockPublicAcls": true,
 "IgnorePublicAcls": true, "BlockPublicPolicy": true, "RestrictPublicBuckets":
 true}'
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutPublicAccessBlock en la Referencia de comandos de la AWS CLI.

`submit-multi-region-access-point-routes`

En el siguiente ejemplo de código, se muestra cómo utilizar `submit-multi-region-access-point-routes`.

AWS CLI

Para actualizar la configuración de enrutamiento del punto de acceso de varias regiones

En el siguiente ejemplo de `submit-multi-region-access-point-routes`, se actualizan los estados de enrutamiento de `amzn-s3-demo-bucket1` y `amzn-s3-demo-bucket2` en la región `ap-southeast-2` para su punto de acceso multirregional.

```
aws s3control submit-multi-region-access-point-routes \
    --region ap-southeast-2 \
    --account-id 111122223333 \
    --mrap MultiRegionAccessPoint_ARN \
    --route-updates Bucket=amzn-s3-demo-
bucket1,TrafficDialPercentage=100 Bucket=amzn-s3-demo-
bucket2,TrafficDialPercentage=0
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte SubmitMultiRegionAccessPointRoutes en la Referencia de comandos de la AWS CLI.

`update-job-priority`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-job-priority`.

AWS CLI

Para actualizar la prioridad de un trabajo de Operaciones por lotes de Amazon S3

En el siguiente ejemplo de `update-job-priority`, se actualiza el trabajo especificado con una prioridad nueva.

```
aws s3control update-job-priority \
    --account-id 123456789012 \
    --job-id 8d9a18fe-c303-4d39-8ccc-860d372da386 \
    --priority 52
```

Salida:

```
{
    "JobId": "8d9a18fe-c303-4d39-8ccc-860d372da386",
    "Priority": 52
}
```

- Para obtener información sobre la API, consulte UpdateJobPriority en la Referencia de comandos de la AWS CLI.

update-job-status

En el siguiente ejemplo de código, se muestra cómo utilizar `update-job-status`.

AWS CLI

Para actualizar el estado de un trabajo de Operaciones por lotes de Amazon S3

En el siguiente ejemplo de `update-job-status`, se cancela el trabajo especificado que espera ser aprobado.

```
aws s3control update-job-status \
    --account-id 123456789012 \
    --job-id 8d9a18fe-c303-4d39-8ccc-860d372da386 \
    --requested-job-status Cancelled
```

Salida:

```
{
    "Status": "Cancelled",
    "JobId": "8d9a18fe-c303-4d39-8ccc-860d372da386"
}
```

En el siguiente ejemplo de `update-job-status`, se confirma y ejecuta el trabajo especificado que espera ser aprobado.

```
aws s3control update-job-status \
    --account-id 123456789012 \
    --job-id 5782949f-3301-4fb3-be34-8d5bab54dbca \
    --requested-job-status Ready

Output::

{
    "Status": "Ready",
    "JobId": "5782949f-3301-4fb3-
be34-8d5bab54dbca"
}
```

En el siguiente ejemplo de `update-job-status`, se cancela el trabajo especificado que se está ejecutando.

```
 aws s3control update-job-status \
    --account-id 123456789012 \
    --job-id 5782949f-3301-4fb3-be34-8d5bab54dbca \
    --requested-job-status Cancelled

Output::
{
         "Status": "Cancelling",
         "JobId": "5782949f-3301-4fb3-be34-8d5bab54dbca"
}
```

- Para obtener información sobre la API, consulte UpdateJobStatus en la Referencia de la API de la AWS CLI.

Ejemplos de Secrets Manager que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Secrets Manager.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`batch-get-secret-value`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-secret-value`.

AWS CLI

Ejemplo 1: recuperación del valor del secreto para un grupo de secretos enumerados por nombre

En el siguiente ejemplo de `batch-get-secret-value`, se obtienen los valores de tres secretos.

```
aws secretsmanager batch-get-secret-value \
    --secret-id-list MySecret1 MySecret2 MySecret3
```

Salida:

```
{
    "SecretValues": [
        {
            "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret1-
a1b2c3",
            "Name": "MySecret1",
            "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
            "SecretString": "{\"username\":\"diego_ramirez\",\"password\":\"EXAMPLE-
PASSWORD\",\"engine\":\"mysql\",\"host\":\"secretsmanagertutorial.cluster.us-
west-2.rds.amazonaws.com\",\"port\":3306,\"dbClusterIdentifier\":
\"secretsmanagertutorial\"}",
            "VersionStages": [
                "AWSCURRENT"
            ],
            "CreatedDate": "1523477145.729"
        },
        {
            "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret2-
a1b2c3",
            "Name": "MySecret2",
            "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
            "SecretString": "{\"username\":\"akua_mansa\",\"password\":\"EXAMPLE-
PASSWORD\"",
            "VersionStages": [
                "AWSCURRENT"
            ],
            "CreatedDate": "1673477781.275"
        },
        {
            "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret3-
a1b2c3",
            "Name": "MySecret3",
            "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLEccccc",
            "SecretString": "{\"username\":\"jie_liu\",\"password\":\"EXAMPLE-
PASSWORD\"",
```

```
            "VersionStages": [
                "AWSCURRENT"
            ],
            "CreatedDate": "1373477721.124"
        }
    ],
    "Errors": []
}
```

Para obtener más información, consulte Retrieve a group of secrets in a batch en la Guía del usuario de AWS Secrets Manager.

Ejemplo 2: recuperación del valor del secreto para un grupo de secretos seleccionado por el filtro

En el siguiente ejemplo de `batch-get-secret-value`, se obtienen los valores de los secretos de la cuenta que incluyen `MySecret` en su nombre. El filtrado por nombres distingue entre mayúsculas y minúsculas.

```
aws secretsmanager batch-get-secret-value \
    --filters Key="name",Values="MySecret"
```

Salida:

```
{
    "SecretValues": [
        {
            "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret1-
a1b2c3",
            "Name": "MySecret1",
            "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
            "SecretString": "{\"username\":\"diego_ramirez\",\"password\":\"EXAMPLE-
PASSWORD\",\"engine\":\"mysql\",\"host\":\"secretsmanagertutorial.cluster.us-
west-2.rds.amazonaws.com\",\"port\":3306,\"dbClusterIdentifier\":
\"secretsmanagertutorial\"}",
            "VersionStages": [
                "AWSCURRENT"
            ],
            "CreatedDate": "1523477145.729"
        },
        {
            "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret2-
a1b2c3",
```

```
            "Name": "MySecret2",
            "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
            "SecretString": "{\"username\":\"akua_mansa\",\"password\":\"EXAMPLE-
PASSWORD\"",
            "VersionStages": [
                "AWSCURRENT"
            ],
            "CreatedDate": "1673477781.275"
        },
        {
            "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret3-
a1b2c3",
            "Name": "MySecret3",
            "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLEccccc",
            "SecretString": "{\"username\":\"jie_liu\",\"password\":\"EXAMPLE-
PASSWORD\"",
            "VersionStages": [
                "AWSCURRENT"
            ],
            "CreatedDate": "1373477721.124"
        }
    ],
    "Errors": []
}
```

Para obtener más información, consulte Retrieve a group of secrets in a batch en la Guía del usuario de AWS Secrets Manager.

- Para obtener detalles sobre la API, consulte BatchGetSecretValue en la Referencia de comandos de la AWS CLI.

`cancel-rotate-secret`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-rotate-secret`.

AWS CLI

Para desactivar la rotación automática de su secreto

En el siguiente ejemplo de `cancel-rotate-secret`, se desactiva la rotación automática de un secreto. Para reanudar la rotación, llame a `rotate-secret`.

```
aws secretsmanager cancel-rotate-secret \
```

```
    --secret-id MyTestSecret
```

Salida:

```
{
  "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-a1b2c3",
  "Name": "MyTestSecret"
}
```

Para obtener más información acerca de Secrets Manager, consulte Rotate a secret en la Guía del usuario de Secrets Manager.

- Para obtener información sobre la API, consulte CancelRotateSecret en la Referencia de comandos de la AWS CLI.

`create-secret`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-secret`.

AWS CLI

Ejemplo 1: creación de un secreto a partir de credenciales de un archivo JSON

En el siguiente ejemplo de `create-secret`, se crea un secreto a partir de las credenciales de un archivo. Para obtener más información, consulte Carga de parámetros de AWS CLI desde un archivo en la Guía del usuario de AWS CLI.

```
aws secretsmanager create-secret \
    --name MyTestSecret \
    --secret-string file://mycreds.json
```

Contenido de `mycreds.json`:

```
{
  "engine": "mysql",
  "username": "saanvis",
  "password": "EXAMPLE-PASSWORD",
  "host": "my-database-endpoint.us-west-2.rds.amazonaws.com",
  "dbname": "myDatabase",
  "port": "3306"
```

```
}
```

Salida:

```
{
  "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-a1b2c3",
  "Name": "MyTestSecret",
  "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Para obtener más información, consulte Creación de un secreto en la Guía del usuario de Secrets Manager.

Ejemplo 2: creación de un secreto

En el siguiente ejemplo de `create-secret` se crea un secreto con dos pares clave-valor. Cuando utiliza ingresa comandos en un shell de comandos, existe el riesgo de que se acceda al historial de comandos o de que las utilidades tengan acceso a sus parámetros de comando. Esto puede ser preocupante si el comando incluye el valor de un secreto. Para obtener más información, consulte Mitigate the risks of using command-line tools to store secrets en la Guía del usuario de Secrets Manager.

```
aws secretsmanager create-secret \
    --name MyTestSecret \
    --description "My test secret created with the CLI." \
    --secret-string "{\"user\":\"diegor\",\"password\":\"EXAMPLE-PASSWORD\"}"
```

Salida:

```
{
  "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-a1b2c3",
  "Name": "MyTestSecret",
  "VersionId": "EXAMPLE1-90ab-cdef-fedc-ba987EXAMPLE"
}
```

Para obtener más información, consulte Creación de un secreto en la Guía del usuario de Secrets Manager.

- Para obtener información sobre la API, consulte CreateSecret en la Referencia de comandos de la AWS CLI.

delete-resource-policy

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-resource-policy`.

AWS CLI

Para eliminar la política basada en recursos asociada a un secreto

En el siguiente ejemplo de `delete-resource-policy` se elimina la política basada en recursos asociada a un secreto.

```
aws secretsmanager delete-resource-policy \
    --secret-id MyTestSecret
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3",
    "Name": "MyTestSecret"
}
```

Para obtener más información, consulte Authentication and access control en la Guía del usuario de Secrets Manager.

- Para obtener detalles sobre la API, consulte DeleteResourcePolicy en la Referencia de comandos de la AWS CLI.

delete-secret

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-secret`.

AWS CLI

Ejemplo 1: Eliminación de un secreto

En el siguiente ejemplo de `delete-secret` se elimina un secreto. Se puede recuperar el secreto con `restore-secret` hasta la fecha y hora del campo de respuesta `DeletionDate`. Para eliminar un secreto que se replica en otras regiones, primero elimine sus réplicas con `remove-regions-from-replication` y, a continuación, llame a `delete-secret`.

```
aws secretsmanager delete-secret \
    --secret-id MyTestSecret \
    --recovery-window-in-days 7
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3",
    "Name": "MyTestSecret",
    "DeletionDate": 1524085349.095
}
```

Para obtener más información, consulte Eliminación de un secreto en la Guía del usuario de Secrets Manager.

Ejemplo 2: Eliminación de un secreto inmediatamente

En el siguiente ejemplo de `delete-secret` se elimina un secreto inmediatamente sin periodo de recuperación. Este secreto no se puede recuperar.

```
aws secretsmanager delete-secret \
    --secret-id MyTestSecret \
    --force-delete-without-recovery
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3",
    "Name": "MyTestSecret",
    "DeletionDate": 1508750180.309
}
```

Para obtener más información, consulte Eliminación de un secreto en la Guía del usuario de Secrets Manager.

- Para obtener información sobre la API, consulte DeleteSecret en la Referencia de comandos de la AWS CLI.

describe-secret

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-secret`.

AWS CLI

Recuperación de los detalles de un secreto

En el siguiente ejemplo `describe-secret`, se muestran detalles de un secreto.

```
aws secretsmanager describe-secret \
    --secret-id MyTestSecret
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
Ca8JGt",
    "Name": "MyTestSecret",
    "Description": "My test secret",
    "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/EXAMPLE1-90ab-cdef-fedc-
ba987EXAMPLE",
    "RotationEnabled": true,
    "RotationLambdaARN": "arn:aws:lambda:us-
west-2:123456789012:function:MyTestRotationLambda",
    "RotationRules": {
        "AutomaticallyAfterDays": 2,
        "Duration": "2h",
        "ScheduleExpression": "cron(0 16 1,15 * ? *)"
    },
    "LastRotatedDate": 1525747253.72,
    "LastChangedDate": 1523477145.729,
    "LastAccessedDate": 1524572133.25,
    "Tags": [
        {
            "Key": "SecondTag",
            "Value": "AnotherValue"
        },
        {
            "Key": "FirstTag",
            "Value": "SomeValue"
        }
    ],
    "VersionIdsToStages": {
```

```
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111": [
            "AWSPREVIOUS"
        ],
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222": [
            "AWSCURRENT"
        ],
        "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333": [
            "AWSPENDING"
        ]
    },
    "CreatedDate": 1521534252.66,
    "PrimaryRegion": "us-west-2",
    "ReplicationStatus": [
        {
            "Region": "eu-west-3",
            "KmsKeyId": "alias/aws/secretsmanager",
            "Status": "InSync",
            "StatusMessage": "Replication succeeded"
        }
    ]
}
```

Para obtener más información, consulte Secreto en la Guía del usuario de Secrets Manager.

- Para obtener información sobre la API, consulte DescribeSecret en la Referencia de comandos de la AWS CLI.

`get-random-password`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-random-password`.

AWS CLI

Para generar una contraseña aleatoria

En el siguiente ejemplo de `get-random-password`, se genera una contraseña aleatoria de 20 caracteres que incluye al menos una letra mayúscula, una minúscula, un número y un signo de puntuación.

```
aws secretsmanager get-random-password \
    --require-each-included-type \
    --password-length 20
```

Salida:

```
{
    "RandomPassword": "EXAMPLE-PASSWORD"
}
```

Para obtener más información, consulte Create and manage secrets en la Guía del usuario de Secrets Manager.

- Para obtener información sobre la API, consulte GetRandomPassword en la Referencia de comandos de la AWS CLI.

`get-resource-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource-policy`.

AWS CLI

Para recuperar la política basada en recursos asociada a un secreto

En el siguiente ejemplo de `get-resource-policy` se recupera la política basada en recursos asociada a un secreto.

```
aws secretsmanager get-resource-policy \
    --secret-id MyTestSecret
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3",
    "Name": "MyTestSecret",
    "ResourcePolicy": "{\n\"Version\":\"2012-10-17\",\n\"Statement\":[{\n\"Effect\":
\"Allow\",\n
    \"Principal\":{\n\"AWS\":\"arn:aws:iam::123456789012:root\"\n},\n\"Action\":
    \"secretsmanager:GetSecretValue\",\n\"Resource\":\"*\"\n}]\n}"
}
```

Para obtener más información, consulte Authentication and access control en la Guía del usuario de Secrets Manager.

- Para obtener información sobre la API, consulte GetResourcePolicy en la Referencia de comandos de la AWS CLI.

`get-secret-value`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-secret-value`.

AWS CLI

Ejemplo 1: Recuperación del valor de secreto cifrado de un secreto

El siguiente ejemplo de `get-secret-value` obtiene el valor de secreto actual.

```
aws secretsmanager get-secret-value \
    --secret-id MyTestSecret
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3",
    "Name": "MyTestSecret",
    "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "SecretString": "{\"user\":\"diegor\",\"password\":\"EXAMPLE-PASSWORD\"}",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": 1523477145.713
}
```

Para obtener más información, consulte Recuperación de un secreto en la Guía del usuario de Secrets Manager.

Ejemplo 2: Recuperación del valor de secreto anterior

El siguiente ejemplo de `get-secret-value` obtiene el valor de secreto anterior:

```
aws secretsmanager get-secret-value \
    --secret-id MyTestSecret
    --version-stage AWSPREVIOUS
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3",
    "Name": "MyTestSecret",
    "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "SecretString": "{\"user\":\"diegor\",\"password\":\"PREVIOUS-EXAMPLE-PASSWORD
\"}",
    "VersionStages": [
        "AWSPREVIOUS"
    ],
    "CreatedDate": 1523477145.713
}
```

Para obtener más información, consulte Recuperación de un secreto en la Guía del usuario de Secrets Manager.

- Para obtener información sobre la API, consulte GetSecretValue en la Referencia de comandos de la AWS CLI.

`list-secret-version-ids`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-secret-version-ids`.

AWS CLI

Para enumerar todas las versiones de secreto asociadas a un secreto

En el siguiente ejemplo de `list-secret-version-ids`, se obtiene una lista de todas las versiones de un secreto.

```
aws secretsmanager list-secret-version-ids \
    --secret-id MyTestSecret
```

Salida:

```
{
  "Versions": [
    {
        "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "VersionStages": [
            "AWSPREVIOUS"
        ],
```

```
        "LastAccessedDate": 1523477145.713,
        "CreatedDate": 1523477145.713
    },
    {
        "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "VersionStages": [
            "AWSCURRENT"
        ],
        "LastAccessedDate": 1523477145.713,
        "CreatedDate": 1523486221.391
    },
    {
        "CreatedDate": 1.51197446236E9,
        "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333;"
    }
    ],
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3",
    "Name": "MyTestSecret"
}
```

Para obtener más información, consulte Version en la Guía del usuario de Secrets Manager.

- Para obtener información sobre la API, consulte ListSecretVersionIds en la Referencia de comandos de la AWS CLI.

`list-secrets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-secrets`.

AWS CLI

Ejemplo 1: Creación de una lista de los secretos de la cuenta

En el siguiente ejemplo de `list-secrets` se obtiene una lista de los secretos de la cuenta.

```
aws secretsmanager list-secrets
```

Salida:

```
{
    "SecretList": [
        {
```

```
            "ARN": "arn:aws:secretsmanager:us-
west-2:123456789012:secret:MyTestSecret-a1b2c3",
            "Name": "MyTestSecret",
            "LastChangedDate": 1523477145.729,
            "SecretVersionsToStages": {
                "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111": [
                    "AWSCURRENT"
                ]
            }
        },
        {
            "ARN": "arn:aws:secretsmanager:us-
west-2:123456789012:secret:AnotherSecret-d4e5f6",
            "Name": "AnotherSecret",
            "LastChangedDate": 1523482025.685,
            "SecretVersionsToStages": {
                "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222": [
                    "AWSCURRENT"
                ]
            }
        }
    ]
}
```

Para obtener más información acerca de Secrets Manager, consulte Encontrar un secreto en la Guía del usuario de Secrets Manager.

Ejemplo 2: Filtrado de la lista de secretos de la cuenta

En el siguiente ejemplo de `list-secrets` se obtiene una lista de los secretos de la cuenta que incluyen `Test` en su nombre. El filtrado por nombres distingue entre mayúsculas y minúsculas.

```
aws secretsmanager list-secrets \
    --filter Key="name",Values="Test"
```

Salida:

```
{
    "SecretList": [
        {
            "ARN": "arn:aws:secretsmanager:us-
west-2:123456789012:secret:MyTestSecret-a1b2c3",
            "Name": "MyTestSecret",
```

```
            "LastChangedDate": 1523477145.729,
            "SecretVersionsToStages": {
                "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111": [
                    "AWSCURRENT"
                ]
            }
        }
    ]
}
```

Para obtener más información acerca de Secrets Manager, consulte Encontrar un secreto en la Guía del usuario de Secrets Manager.

Ejemplo 3: creación de una lista de los secretos de su cuenta administrada por otro servicio

El siguiente ejemplo `list-secrets` devuelve los secretos de su cuenta administrados por Amazon RDS.

```
aws secretsmanager list-secrets \
    --filter Key="owning-service",Values="rds"
```

Salida:

```
{
    "SecretList": [
        {
            "Name": "rds!cluster-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "Tags": [
                {
                    "Value": "arn:aws:rds:us-
west-2:123456789012:cluster:database-1",
                    "Key": "aws:rds:primaryDBClusterArn"
                },
                {
                    "Value": "rds",
                    "Key": "aws:secretsmanager:owningService"
                }
            ],
            "RotationRules": {
                "AutomaticallyAfterDays": 1
            },
            "LastChangedDate": 1673477781.275,
            "LastRotatedDate": 1673477781.26,
```

```
            "SecretVersionsToStages": {
                "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa": [
                    "AWSPREVIOUS"
                ],
                "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb": [
                    "AWSCURRENT",
                    "AWSPENDING"
                ]
            },
            "OwningService": "rds",
            "RotationEnabled": true,
            "CreatedDate": 1673467300.7,
            "LastAccessedDate": 1673395200.0,
            "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:rds!
cluster-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111-a1b2c3",
            "Description": "Secret associated with primary RDS DB cluster:
 arn:aws:rds:us-west-2:123456789012:cluster:database-1"
        }
    ]
}
```

Para obtener más información, consulte Secretos gestionados por otros servicios en la Guía del usuario de Secrets Manager.

- Para obtener información sobre la API, consulte ListSecrets en la Referencia de comandos de la AWS CLI.

`put-resource-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-resource-policy`.

AWS CLI

Para añadir una política basada en recursos a un secreto

En el siguiente ejemplo de `put-resource-policy` se agrega una política de permisos a un secreto, pero primero se comprueba que la política no proporciona un acceso amplio al secreto. La política se lee desde un archivo. Para obtener más información, consulte Carga de parámetros de AWS CLI desde un archivo en la Guía del usuario de AWS CLI.

```
aws secretsmanager put-resource-policy \
    --secret-id MyTestSecret \
    --resource-policy file://mypolicy.json \
```

```
    --block-public-policy
```

Contenido de `mypolicy.json`:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:role/MyRole"
            },
            "Action": "secretsmanager:GetSecretValue",
            "Resource": "*"
        }
    ]
}
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3",
    "Name": "MyTestSecret"
}
```

Para obtener más información, consulte Attach a permissions policy to a secret en la Guía del usuario de Secrets Manager.

- Para obtener detalles sobre la API, consulte PutResourcePolicy en la Referencia de comandos de la AWS CLI.

`put-secret-value`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-secret-value`.

AWS CLI

Ejemplo 1: Almacenamiento de un nuevo valor de secreto en un secreto

En el siguiente ejemplo de `put-secret-value` se crea una nueva versión de un secreto con dos pares clave-valor.

```
aws secretsmanager put-secret-value \
    --secret-id MyTestSecret \
    --secret-string "{\"user\":\"diegor\",\"password\":\"EXAMPLE-PASSWORD\"}"
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-
west-2:123456789012:secret:MyTestSecret-1a2b3c",
    "Name": "MyTestSecret",
    "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "VersionStages": [
        "AWSCURRENT"
    ]
}
```

Para obtener más información, consulte Modificación de un secreto en la Guía del usuario de Secrets Manager.

Ejemplo 2: Almacenamiento de un nuevo valor de secreto a partir de credenciales de un archivo JSON

En el siguiente ejemplo de `put-secret-value` se crea una nueva versión de un secreto a partir de las credenciales de un archivo. Para obtener más información, consulte Carga de parámetros de AWS CLI desde un archivo en la Guía del usuario de AWS CLI.

```
aws secretsmanager put-secret-value \
    --secret-id MyTestSecret \
    --secret-string file://mycreds.json
```

Contenido de `mycreds.json`:

```
{
  "engine": "mysql",
  "username": "saanvis",
  "password": "EXAMPLE-PASSWORD",
  "host": "my-database-endpoint.us-west-2.rds.amazonaws.com",
  "dbname": "myDatabase",
  "port": "3306"
}
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3",
    "Name": "MyTestSecret",
    "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "VersionStages": [
        "AWSCURRENT"
    ]
}
```

Para obtener más información, consulte Modificación de un secreto en la Guía del usuario de Secrets Manager.

- Para obtener información acerca de la API, consulte PutSecretValue en la Referencia de comandos de la AWS CLI.

`remove-regions-from-replication`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-regions-from-replication`.

AWS CLI

Para eliminar un secreto de réplica

En el siguiente ejemplo de `remove-regions-from-replication` se elimina un secreto de réplica de eu-west-3. Para eliminar un secreto principal que se replica en otras regiones, primero elimine las réplicas y, a continuación, llame a `delete-secret`.

```
aws secretsmanager remove-regions-from-replication \
    --secret-id MyTestSecret \
    --remove-replica-regions eu-west-3
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-
west-2:123456789012:secret:MyTestSecret-1a2b3c",
    "ReplicationStatus": []
```

```
}
```

Para obtener más información, consulte Delete a replica secret en la Guía del usuario de Secrets Manager.

- Para obtener información sobre la API, consulte RemoveRegionsFromReplication en la Referencia de comandos de la AWS CLI.

`replicate-secret-to-regions`

En el siguiente ejemplo de código, se muestra cómo utilizar `replicate-secret-to-regions`.

AWS CLI

Para replicar un secreto en otra región

En el siguiente ejemplo de `replicate-secret-to-regions` se replica un secreto en eu-west-3. La réplica se cifra con la clave `aws/secretsmanager` administrada por AWS.

```
aws secretsmanager replicate-secret-to-regions \
    --secret-id MyTestSecret \
    --add-replica-regions Region=eu-west-3
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-
west-2:123456789012:secret:MyTestSecret-1a2b3c",
    "ReplicationStatus": [
        {
            "Region": "eu-west-3",
            "KmsKeyId": "alias/aws/secretsmanager",
            "Status": "InProgress"
        }
    ]
}
```

Para obtener más información, consulte Replicate a secret to another Region en la Guía del usuario de Secrets Manager.

- Para obtener información sobre la API, consulte ReplicateSecretToRegions en la Referencia de comandos de la AWS CLI.

`restore-secret`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-secret`.

AWS CLI

Para restaurar un secreto eliminado previamente

En el siguiente ejemplo de `restore-secret` se restaura un secreto cuya eliminación se había programado previamente.

```
aws secretsmanager restore-secret \
    --secret-id MyTestSecret
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3",
    "Name": "MyTestSecret"
}
```

Para obtener más información, consulte Eliminación de un secreto en la Guía del usuario de Secrets Manager.

- Para obtener información sobre la API, consulte RestoreSecret en la Referencia de comandos de la AWS CLI.

`rotate-secret`

En el siguiente ejemplo de código, se muestra cómo utilizar `rotate-secret`.

AWS CLI

Ejemplo 1: configuración e inicio de la rotación automática de un secreto

En el siguiente ejemplo de `rotate-secret`, se configura e inicia la rotación automática de un secreto. Secrets Manager rota el secreto una vez de forma inmediata y, a continuación, cada ocho horas en un intervalo de dos horas. El resultado muestra el valor de `VersionId` de la nueva versión del secreto creada por la rotación.

```
aws secretsmanager rotate-secret \
    --secret-id MyTestDatabaseSecret \
    --rotation-lambda-arn arn:aws:lambda:us-
west-2:1234566789012:function:SecretsManagerTestRotationLambda \
    --rotation-rules "{\"ScheduleExpression\": \"cron(0 8/8 * * ? *)\", \"Duration
\": \"2h\"}"
```

Salida:

```
{
    "ARN": "aws:arn:secretsmanager:us-
west-2:123456789012:secret:MyTestDatabaseSecret-a1b2c3",
    "Name": "MyTestDatabaseSecret",
    "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Para obtener más información, consulte Rotate secrets en la Guía del usuario de Secrets Manager.

Ejemplo 2: configuración e inicio de la rotación automática en un intervalo de rotación

En el siguiente ejemplo de `rotate-secret`, se configura e inicia la rotación automática de un secreto. Secrets Manager rota el secreto una vez de forma inmediata y, a continuación, cada diez días. El resultado muestra el valor de `VersionId` de la nueva versión del secreto creada por la rotación.

```
aws secretsmanager rotate-secret \
    --secret-id MyTestDatabaseSecret \
    --rotation-lambda-arn arn:aws:lambda:us-
west-2:1234566789012:function:SecretsManagerTestRotationLambda \
    --rotation-rules "{\"ScheduleExpression\": \"rate(10 days)\"}"
```

Salida:

```
{
    "ARN": "aws:arn:secretsmanager:us-
west-2:123456789012:secret:MyTestDatabaseSecret-a1b2c3",
    "Name": "MyTestDatabaseSecret",
    "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Para obtener más información, consulte Rotate secrets en la Guía del usuario de Secrets Manager.

Ejemplo 3: rotación de un secreto inmediatamente

En el siguiente ejemplo de `rotate-secret` se inicia una rotación inmediata. El resultado muestra el valor de `VersionId` de la nueva versión del secreto creada por la rotación. El secreto ya debe tener configurada la rotación.

```
aws secretsmanager rotate-secret \
    --secret-id MyTestDatabaseSecret
```

Salida:

```
{
    "ARN": "aws:arn:secretsmanager:us-
west-2:123456789012:secret:MyTestDatabaseSecret-a1b2c3",
    "Name": "MyTestDatabaseSecret",
    "VersionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Para obtener más información, consulte Rotate secrets en la Guía del usuario de Secrets Manager.

- Para obtener información sobre la API, consulte RotateSecret en la Referencia de comandos de AWS CLI.

`stop-replication-to-replica`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-replication-to-replica`.

AWS CLI

Para promocionar un secreto de réplica en el principal

En el siguiente ejemplo de `stop-replication-to-replica`, se elimina el enlace entre un secreto de réplica y el principal. El secreto de réplica se promociona a secreto principal en la región de réplica. Debe llamar a `stop-replication-to-replica` desde la región de réplica.

```
aws secretsmanager stop-replication-to-replica \
    --secret-id MyTestSecret
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3"
}
```

Para obtener más información, consulte Promote a replica secret en la Guía del usuario de Secrets Manager.

- Para obtener detalles sobre la API, consulte StopReplicationToReplica en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Ejemplo 1: adición de una etiqueta a un secreto

En el siguiente ejemplo de se muestra cómo asociar una etiqueta con sintaxis abreviada.

```
aws secretsmanager tag-resource \
    --secret-id MyTestSecret \
    --tags Key=FirstTag,Value=FirstValue
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tag your secrets en la Guía del usuario de Secrets Manager.

Ejemplo 2: adición de varias etiquetas a un secreto

En el siguiente ejemplo de `tag-resource` se asocian dos etiquetas de clave-valor a un secreto.

```
aws secretsmanager tag-resource \
    --secret-id MyTestSecret \
    --tags '[{"Key": "FirstTag", "Value": "FirstValue"}, {"Key": "SecondTag",
 "Value": "SecondValue"}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tag secrets en la Guía del usuario de Secrets Manager.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar etiquetas de un secreto

En el siguiente ejemplo de `untag-resource` se eliminan dos etiquetas de un secreto. Se eliminan tanto la clave como el valor de cada etiqueta.

```
aws secretsmanager untag-resource \
    --secret-id MyTestSecret \
    --tag-keys '[ "FirstTag", "SecondTag"]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tag secrets en la Guía del usuario de Secrets Manager.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-secret-version-stage`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-secret-version-stage`.

AWS CLI

Ejemplo 1: reversión de un secreto a la versión anterior

En el siguiente ejemplo de `update-secret-version-stage`, se mueve la etiqueta de preparación AWSCURRENT a la versión anterior de un secreto, lo que revierte el secreto a la versión anterior. Para buscar el ID de la versión anterior, utilice `list-secret-version-ids`. Para este ejemplo, la versión con la etiqueta AWSCURRENT es a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 y la versión con la etiqueta AWSPREVIOUS es a1b2c3d4-5678-90ab-cdef-EXAMPLE22222. En este ejemplo, traslada la etiqueta AWSCURRENT de la versión 11111 a la 22222. Como la etiqueta AWSCURRENT se ha eliminado de una versión, `update-secret-`

`version-stage` mueve automáticamente la etiqueta AWSPREVIOUS a esa versión (11111). El efecto es que las versiones AWSCURRENT y AWSPREVIOUS se intercambian.

```
aws secretsmanager update-secret-version-stage \
    --secret-id MyTestSecret \
    --version-stage AWSCURRENT \
    --move-to-version-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
    --remove-from-version-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3",
    "Name": "MyTestSecret"
}
```

Para obtener más información, consulte Version en la Guía del usuario de Secrets Manager.

Ejemplo 2: adición de una etiqueta de preparación asociada a una versión de un secreto

En el siguiente ejemplo de `update-secret-version-stage`, se agrega una etiqueta de preparación a una versión de un secreto. Para revisar los resultados, ejecute `list-secret-version-ids` y visualice el campo de respuesta `VersionStages` de la versión afectada.

```
aws secretsmanager update-secret-version-stage \
    --secret-id MyTestSecret \
    --version-stage STAGINGLABEL1 \
    --move-to-version-id EXAMPLE1-90ab-cdef-fedc-ba987EXAMPLE
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3",
    "Name": "MyTestSecret"
}
```

Para obtener más información, consulte Version en la Guía del usuario de Secrets Manager.

Ejemplo 3: eliminación de una etiqueta de preparación asociada a una versión de un secreto

En el siguiente ejemplo de `update-secret-version-stage`, se elimina una etiqueta de preparación asociada a una versión de un secreto. Para revisar los resultados, ejecute `list-secret-version-ids` y visualice el campo de respuesta `VersionStages` de la versión afectada.

```
aws secretsmanager update-secret-version-stage \
    --secret-id MyTestSecret \
    --version-stage STAGINGLABEL1 \
    --remove-from-version-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3",
    "Name": "MyTestSecret"
}
```

Para obtener más información, consulte Version en la Guía del usuario de Secrets Manager.

- Para obtener información sobre la API, consulte UpdateSecretVersionStage en la Referencia de comandos de la AWS CLI.

`update-secret`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-secret`.

AWS CLI

Ejemplo 1: Actualización de la descripción de un secreto

En el siguiente ejemplo de `update-secret` se actualiza la descripción de un secreto.

```
aws secretsmanager update-secret \
    --secret-id MyTestSecret \
    --description "This is a new description for the secret."
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3",
```

```
    "Name": "MyTestSecret"
}
```

Para obtener más información, consulte Modificación de un secreto en la Guía del usuario de Secrets Manager.

Ejemplo 2: Actualización de la clave de cifrado asociada a un secreto

En el siguiente ejemplo de `update-secret` se actualiza la clave de KMS utilizada para cifrar el valor de secreto. La clave de KMS debe estar en la misma región que el secreto.

```
aws secretsmanager update-secret \
    --secret-id MyTestSecret \
    --kms-key-id arn:aws:kms:us-west-2:123456789012:key/EXAMPLE1-90ab-cdef-fedc-
ba987EXAMPLE
```

Salida:

```
{
    "ARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:MyTestSecret-
a1b2c3",
    "Name": "MyTestSecret"
}
```

Para obtener más información, consulte Modificación de un secreto en la Guía del usuario de Secrets Manager.

- Para obtener información sobre la API, consulte UpdateSecret en la Referencia de comandos de la AWS CLI.

`validate-resource-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `validate-resource-policy`.

AWS CLI

Para validar una política de recursos

En el siguiente ejemplo de `validate-resource-policy`, se comprueba que una política de recursos no conceda un acceso amplio a un secreto. La política se lee desde un archivo en el disco. Para obtener más información, consulte Carga de parámetros de AWS CLI desde un archivo en la Guía del usuario de AWS CLI.

```
aws secretsmanager validate-resource-policy \
    --resource-policy file://mypolicy.json
```

Contenido de `mypolicy.json`:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:role/MyRole"
            },
            "Action": "secretsmanager:GetSecretValue",
            "Resource": "*"
        }
    ]
}
```

Salida:

```
{
    "PolicyValidationPassed": true,
    "ValidationErrors": []
}
```

Para obtener más información, consulte Permissions reference for Secrets Manager en la Guía del usuario de Secrets Manager.

- Para obtener detalles de la API, consulte ValidateResourcePolicy en la Referencia de comandos de la AWS CLI.

Ejemplos de CSPM de Security Hub que utilizan la AWS CLI

Los ejemplos de código siguientes muestran cómo realizar acciones e implementar escenarios comunes mediante la AWS Command Line Interface con CSPM de Security Hub.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`accept-administrator-invitation`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-administrator-invitation`.

AWS CLI

Para aceptar una invitación de una cuenta de administrador

En el siguiente ejemplo de `accept-administrator-invitation`, se acepta la invitación especificada de la cuenta de administrador indicada.

```
aws securityhub accept-invitation \
    --administrator-id 123456789012 \
    --invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

Este comando no genera ninguna salida.

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte AcceptAdministratorInvitation en la Referencia de comandos de la AWS CLI.

`accept-invitation`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-invitation`.

AWS CLI

Para aceptar una invitación de una cuenta de administrador

En el siguiente ejemplo de `accept-invitation`, se acepta la invitación especificada de la cuenta de administrador indicada.

```
aws securityhub accept-invitation \
    --master-id 123456789012 \
    --invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

Este comando no genera ninguna salida.

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener detalles sobre la API, consulte AcceptInvitation en la Referencia de comandos de la AWS CLI.

`batch-delete-automation-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-delete-automation-rules`.

AWS CLI

Para eliminar reglas de automatización

En el siguiente ejemplo de `batch-delete-automation-rules`, se elimina la regla de automatización especificada. Puede eliminar una o más reglas con un solo comando. Solo la cuenta de administrador de Security Hub puede ejecutar este comando.

```
aws securityhub batch-delete-automation-rules \
    --automation-rules-arns '["arn:aws:securityhub:us-
east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"]'
```

Salida:

```
{
    "ProcessedAutomationRules": [
        "arn:aws:securityhub:us-east-1:123456789012:automation-rule/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    ],
    "UnprocessedAutomationRules": []
}
```

Para obtener más información, consulte Deleting automation rules en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte BatchDeleteAutomationRules en la Referencia de comandos de la AWS CLI.

`batch-disable-standards`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-disable-standards`.

AWS CLI

Para deshabilitar un estándar

En el siguiente ejemplo de `batch-disable-standards`, se desactiva el estándar asociado al ARN de suscripción especificado.

```
aws securityhub batch-disable-standards \
    --standards-subscription-arns "arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1"
```

Salida:

```
{
    "StandardsSubscriptions": [
        {
            "StandardsArn": "arn:aws:securityhub:eu-central-1::standards/pci-dss/
v/3.2.1",
            "StandardsInput": { },
            "StandardsStatus": "DELETING",
            "StandardsSubscriptionArn": "arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1"
        }
    ]
}
```

Para obtener más información sobre este estándar, consulte Disabling or enabling a security standard en la Guía del usuario de AWS Security Hub.

- Para obtener detalles sobre la API, consulte BatchDisableStandards en la Referencia de comandos de AWS CLI.

`batch-enable-standards`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-enable-standards`.

AWS CLI

Para habilitar un estándar

En el siguiente ejemplo de `batch-enable-standards`, se habilita el estándar PCI DSS para la cuenta solicitante.

```
aws securityhub batch-enable-standards \
    --standards-subscription-requests '{"StandardsArn":"arn:aws:securityhub:us-
west-1::standards/pci-dss/v/3.2.1"}'
```

Salida:

```
{
    "StandardsSubscriptions": [
        {
            "StandardsArn": "arn:aws:securityhub:us-west-1::standards/pci-dss/
v/3.2.1",
            "StandardsInput": { },
            "StandardsStatus": "PENDING",
            "StandardsSubscriptionArn": "arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1"
        }
    ]
}
```

Para obtener más información sobre este estándar, consulte Disabling or enabling a security standard en la Guía del usuario de AWS Security Hub.

- Para obtener detalles sobre la API, consulte BatchEnableStandards en la Referencia de comandos de la AWS CLI.

`batch-get-automation-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-automation-rules`.

AWS CLI

Para obtener detalles de las reglas de automatización

En el siguiente ejemplo de `batch-get-automation-rules`, se obtiene detalles para la regla de automatización especificada. Puede obtener detalles de una o más reglas de automatización con un solo comando.

```
aws securityhub batch-get-automation-rules \
    --automation-rules-arns '["arn:aws:securityhub:us-
east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"]'
```

Salida:

```
{
    "Rules": [
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-rule/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "RuleStatus": "ENABLED",
            "RuleOrder": 1,
            "RuleName": "Suppress informational findings",
            "Description": "Suppress GuardDuty findings with Informational
 severity",
            "IsTerminal": false,
            "Criteria": {
                "ProductName": [
                    {
                        "Value": "GuardDuty",
                        "Comparison": "EQUALS"
                    }
                ],
                "SeverityLabel": [
                    {
                        "Value": "INFORMATIONAL",
                        "Comparison": "EQUALS"
                    }
                ],
                "WorkflowStatus": [
                    {
                        "Value": "NEW",
                        "Comparison": "EQUALS"
                    }
                ],
                "RecordState": [
                    {
                        "Value": "ACTIVE",
```

```
                        "Comparison": "EQUALS"
                    }
                ]
            },
            "Actions": [
                {
                    "Type": "FINDING_FIELDS_UPDATE",
                    "FindingFieldsUpdate": {
                        "Note": {
                            "Text": "Automatically suppress GuardDuty findings with
 Informational severity",
                            "UpdatedBy": "sechub-automation"
                        },
                        "Workflow": {
                            "Status": "SUPPRESSED"
                        }
                    }
                }
            ],
            "CreatedAt": "2023-05-31T17:56:14.837000+00:00",
            "UpdatedAt": "2023-05-31T17:59:38.466000+00:00",
            "CreatedBy": "arn:aws:iam::123456789012:role/Admin"
        }
    ],
    "UnprocessedAutomationRules": []
}
```

Para obtener más información, consulte Visualización de las reglas de automatización en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte BatchGetAutomationRules en la Referencia de comandos de la AWS CLI.

`batch-get-configuration-policy-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-configuration-policy-associations`.

AWS CLI

Para obtener los detalles de la asociación de configuración de un lote de objetivos

En el siguiente ejemplo de `batch-get-configuration-policy-associations`, se recuperan los detalles de asociación de los destinos especificados. Puede proporcionar los ID de cuenta, los ID de las unidades organizativas o el ID raíz del destino.

```
aws securityhub batch-get-configuration-policy-associations \
    --target '{"OrganizationalUnitId": "ou-6hi7-8j91kl2m"}'
```

Salida:

```
{
    "ConfigurationPolicyId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "TargetId": "ou-6hi7-8j91kl2m",
    "TargetType": "ORGANIZATIONAL_UNIT",
    "AssociationType": "APPLIED",
    "UpdatedAt": "2023-09-26T21:13:01.816000+00:00",
    "AssociationStatus": "SUCCESS",
    "AssociationStatusMessage": "Association applied successfully on this target."
}
```

Para obtener más información, consulte Ver el estado y los detalles de la política de configuración en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte BatchGetConfigurationPolicyAssociations en la Referencia de comandos de la AWS CLI.

`batch-get-security-controls`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-security-controls`.

AWS CLI

Para obtener los detalles del control de seguridad

En el siguiente ejemplo de `batch-get-security-controls`, se obtienen los detalles de los controles de seguridad ACM.1 e IAM.1 de la cuenta de AWS y la región de AWS actuales.

```
aws securityhub batch-get-security-controls \
    --security-control-ids '["ACM.1", "IAM.1"]'
```

Salida:

```
{
    "SecurityControls": [
        {
            "SecurityControlId": "ACM.1",
            "SecurityControlArn": "arn:aws:securityhub:us-
east-2:123456789012:security-control/ACM.1",
            "Title": "Imported and ACM-issued certificates should be renewed after a
 specified time period",
            "Description": "This control checks whether an AWS Certificate Manager
 (ACM) certificate is renewed within the specified time period. It checks both
 imported certificates and certificates provided by ACM. The control fails if the
 certificate isn't renewed within the specified time period. Unless you provide a
 custom parameter value for the renewal period, Security Hub uses a default value of
 30 days.",
            "RemediationUrl": "https://docs.aws.amazon.com/console/securityhub/
ACM.1/remediation",
            "SeverityRating": "MEDIUM",
            "SecurityControlStatus": "ENABLED"
            "UpdateStatus": "READY",
            "Parameters": {
                "daysToExpiration": {
                    "ValueType": CUSTOM,
                    "Value": {
                        "Integer": 15
                    }
                }
            },
            "LastUpdateReason": "Updated control parameter"
        },
        {
            "SecurityControlId": "IAM.1",
            "SecurityControlArn": "arn:aws:securityhub:us-
east-2:123456789012:security-control/IAM.1",
            "Title": "IAM policies should not allow full \"*\" administrative
 privileges",
            "Description": "This AWS control checks whether the default version of
 AWS Identity and Access Management (IAM) policies (also known as customer managed
 policies) do not have administrator access with a statement that has \"Effect\":
 \"Allow\" with \"Action\": \"*\" over \"Resource\": \"*\". It only checks for
 the Customer Managed Policies that you created, but not inline and AWS Managed
 Policies.",
            "RemediationUrl": "https://docs.aws.amazon.com/console/securityhub/
IAM.1/remediation",
```

```
            "SeverityRating": "HIGH",
            "SecurityControlStatus": "ENABLED"
            "UpdateStatus": "READY",
            "Parameters": {}
        }
    ]
}
```

Para obtener más información sobre este estándar, consulte Visualización de los detalles de un control en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte BatchGetSecurityControls en la Referencia de comandos de la AWS CLI.

`batch-get-standards-control-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-get-standards-control-associations`.

AWS CLI

Para obtener el estado de habilitación de un control

En el siguiente ejemplo de `batch-get-standards-control-associations`, se identifica si los controles especificados están habilitados en los estándares indicados.

```
aws securityhub batch-get-standards-control-associations \
    --standards-control-association-ids '[{"SecurityControlId":
 "Config.1","StandardsArn": "arn:aws:securityhub:us-east-1:123456789012:ruleset/cis-
aws-foundations-benchmark/v/1.2.0"}, {"SecurityControlId": "IAM.6","StandardsArn":
 "arn:aws:securityhub:us-east-1:123456789012:standards/aws-foundational-security-
best-practices/v/1.0.0"}]'
```

Salida:

```
{
    "StandardsControlAssociationDetails": [
        {
            "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0",
            "SecurityControlId": "Config.1",
```

```
            "SecurityControlArn": "arn:aws:securityhub:us-
east-1:068873283051:security-control/Config.1",
            "AssociationStatus": "ENABLED",
            "RelatedRequirements": [
                "CIS AWS Foundations 2.5"
            ],
            "UpdatedAt": "2022-10-27T16:07:12.960000+00:00",
            "StandardsControlTitle": "Ensure AWS Config is enabled",
            "StandardsControlDescription": "AWS Config is a web service that
 performs configuration management of supported AWS resources within your account
 and delivers log files to you. The recorded information includes the configuration
 item (AWS resource), relationships between configuration items (AWS resources), and
 any configuration changes between resources. It is recommended to enable AWS Config
 in all regions.",
            "StandardsControlArns": [
                "arn:aws:securityhub:us-east-1:068873283051:control/cis-aws-
foundations-benchmark/v/1.2.0/2.5"
            ]
        },
        {
            "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0",
            "SecurityControlId": "IAM.6",
            "SecurityControlArn": "arn:aws:securityhub:us-
east-1:068873283051:security-control/IAM.6",
            "AssociationStatus": "DISABLED",
            "RelatedRequirements": [],
            "UpdatedAt": "2022-11-22T21:30:35.080000+00:00",
            "UpdatedReason": "test",
            "StandardsControlTitle": "Hardware MFA should be enabled for the root
 user",
            "StandardsControlDescription": "This AWS control checks whether your AWS
 account is enabled to use a hardware multi-factor authentication (MFA) device to
 sign in with root user credentials.",
            "StandardsControlArns": [
                "arn:aws:securityhub:us-east-1:068873283051:control/aws-
foundational-security-best-practices/v/1.0.0/IAM.6"
            ]
        }
    ]
}
```

Para obtener más información, consulte Habilitación de un control en un estándar específico en la Guía del usuario AWS de Security Hub.

- Para obtener más información sobre la API, consulte BatchGetStandardsControlAssociations en la Referencia de comandos de la AWS CLI.

`batch-import-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-import-findings`.

AWS CLI

Para actualizar un hallazgo

En el siguiente ejemplo de `batch-import-findings`, se actualiza un resultado.

```
aws securityhub batch-import-findings \
     --findings '
        [{
            "AwsAccountId": "123456789012",
            "CreatedAt": "2020-05-27T17:05:54.832Z",
            "Description": "Vulnerability in a CloudTrail trail",
            "FindingProviderFields": {
                "Severity": {
                    "Label": "LOW",
                    "Original": "10"
                },
                "Types": [
                    "Software and Configuration Checks/Vulnerabilities/CVE"
                ]
            },
            "GeneratorId": "TestGeneratorId",
            "Id": "Id1",
            "ProductArn": "arn:aws:securityhub:us-
west-1:123456789012:product/123456789012/default",
            "Resources": [
                {
                    "Id": "arn:aws:cloudtrail:us-west-1:123456789012:trail/
TrailName",
                    "Partition": "aws",
                    "Region": "us-west-1",
                    "Type": "AwsCloudTrailTrail"
                }
```

```
            ],
            "SchemaVersion": "2018-10-08",
            "Title": "CloudTrail trail vulnerability",
            "UpdatedAt": "2020-06-02T16:05:54.832Z"
        }]'
```

Salida:

```
{
    "FailedCount": 0,
    "SuccessCount": 1,
    "FailedFindings": []
}
```

Para obtener más información, consulte BatchImportFindings para proveedores de resultados en la Guía del usuario de AWS Security Hub.

- Para obtener detalles sobre la API, consulte BatchImportFindings en la Referencia de comandos de la AWS CLI.

`batch-update-automation-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-update-automation-rules`.

AWS CLI

Para actualizar reglas de automatización

En el siguiente ejemplo de `batch-update-automation-rules`, se actualiza la regla de automatización especificada. Puede actualizar una o más reglas con un solo comando. Solo la cuenta de administrador de Security Hub puede ejecutar este comando.

```
aws securityhub batch-update-automation-rules \
    --update-automation-rules-request-items '[ \
        { \
            "Actions": [{ \
                "Type": "FINDING_FIELDS_UPDATE", \
                "FindingFieldsUpdate": { \
                    "Note": { \
                        "Text": "Known issue that is a risk", \
                        "UpdatedBy": "sechub-automation" \
```

```
                    }, \
                    "Workflow": { \
                        "Status": "NEW" \
                    } \
                } \
            }], \
            "Criteria": { \
                "SeverityLabel": [{ \
                    "Value": "LOW", \
                    "Comparison": "EQUALS" \
                }] \
            }, \
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-rule/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111", \
            "RuleOrder": 1, \
            "RuleStatus": "DISABLED" \
        } \
    ]'
```

Salida:

```
{
    "ProcessedAutomationRules": [
        "arn:aws:securityhub:us-east-1:123456789012:automation-rule/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    ],
    "UnprocessedAutomationRules": []
}
```

Para obtener más información, consulte Edición de reglas de automatización en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte BatchUpdateAutomationRules en la Referencia de comandos de la AWS CLI.

`batch-update-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-update-findings`.

AWS CLI

Ejemplo 1: actualización de un resultado

En el siguiente ejemplo de `batch-update-findings`, se actualizan dos resultados para añadir una nota, cambiar la etiqueta de gravedad y resolverlos.

```
aws securityhub batch-update-findings \
    --finding-identifiers '[{"Id": "arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111", "ProductArn": "arn:aws:securityhub:us-
west-1::product/aws/securityhub"}, {"Id": "arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222", "ProductArn": "arn:aws:securityhub:us-
west-1::product/aws/securityhub"}]' \
    --note '{"Text": "Known issue that is not a risk.", "UpdatedBy": "user1"}' \
    --severity '{"Label": "LOW"}' \
    --workflow '{"Status": "RESOLVED"}'
```

Salida:

```
{
    "ProcessedFindings": [
        {
            "Id": "arn:aws:securityhub:us-west-1:123456789012:subscription/pci-dss/
v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "ProductArn": "arn:aws:securityhub:us-west-1::product/aws/securityhub"
        },
        {
            "Id": "arn:aws:securityhub:us-west-1:123456789012:subscription/pci-dss/
v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "ProductArn": "arn:aws:securityhub:us-west-1::product/aws/securityhub"
        }
    ],
    "UnprocessedFindings": []
}
```

Para obtener más información, consulte BatchUpdateFindings para clientes en la Guía del usuario de AWS Security Hub.

Ejemplo 2: actualización de un resultado con una sintaxis abreviada

En el siguiente ejemplo de `batch-update-findings`, se actualizan dos resultados para añadir una nota, cambiar la etiqueta de gravedad y resolverlos con la sintaxis abreviada.

```
aws securityhub batch-update-findings \
```

```
    --finding-identifiers Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" \
    --note Text="Known issue that is not a risk.",UpdatedBy="user1" \
    --severity Label="LOW" \
    --workflow Status="RESOLVED"
```

Salida:

```
{
    "ProcessedFindings": [
        {
            "Id": "arn:aws:securityhub:us-west-1:123456789012:subscription/pci-dss/
v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "ProductArn": "arn:aws:securityhub:us-west-1::product/aws/securityhub"
        },
        {
            "Id": "arn:aws:securityhub:us-west-1:123456789012:subscription/pci-dss/
v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "ProductArn": "arn:aws:securityhub:us-west-1::product/aws/securityhub"
        }
    ],
    "UnprocessedFindings": []
}
```

Para obtener más información, consulte BatchUpdateFindings para clientes en la Guía del usuario de AWS Security Hub.

- Para obtener detalles sobre la API, consulte BatchUpdateFindings en la Referencia de comandos de la AWS CLI.

`batch-update-standards-control-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-update-standards-control-associations`.

AWS CLI

Para actualizar el estado de habilitación de un control en los estándares habilitados

En el siguiente ejemplo de `batch-update-standards-control-associations`, se desactiva CloudTrail.1 en los estándares especificados.

```
aws securityhub batch-update-standards-control-associations \
    --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
 to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
 "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0",
 "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}]'
```

Este comando no genera ninguna salida si se realiza correctamente.

Para obtener más información, consulte Habilitación de un control en un estándar específico y Habilitación de un control en todos los estándares en la Guía del usuario AWS de Security Hub.

- Para obtener información sobre la API, consulte BatchUpdateStandardsControlAssociations en la Referencia de comandos de la AWS CLI.

`create-action-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-action-target`.

AWS CLI

Para crear una acción personalizada

En el siguiente ejemplo de `create-action-target`, se crea una acción personalizada. Proporciona el nombre, la descripción y el identificador de la acción.

```
aws securityhub create-action-target \
    --name "Send to remediation" \
    --description "Action to send the finding for remediation tracking" \
    --id "Remediation"
```

Salida:

```
{
```

```
    "ActionTargetArn": "arn:aws:securityhub:us-west-1:123456789012:action/custom/
Remediation"
}
```

Para obtener más información, consulte Creating a custom action and associating it with a CloudWatch Events rule en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte CreateActionTarget en la Referencia de comandos de la AWS CLI.

`create-automation-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-automation-rule`.

AWS CLI

Para crear una regla de automatización

En el siguiente ejemplo de `create-automation-rule`, se crea una regla de automatización en la cuenta de AWS y la región de AWS actuales. Security Hub filtra los resultados en función de los criterios especificados y aplica las acciones a los resultados que coinciden. Solo la cuenta de administrador de Security Hub puede ejecutar este comando.

```
aws securityhub create-automation-rule \
    --actions '[{ \
        "Type": "FINDING_FIELDS_UPDATE", \
        "FindingFieldsUpdate": { \
            "Severity": { \
                "Label": "HIGH" \
            }, \
            "Note": { \
                "Text": "Known issue that is a risk. Updated by automation rules", \
                "UpdatedBy": "sechub-automation" \
            } \
        } \
    }]' \
    --criteria '{ \
        "SeverityLabel": [{ \
            "Value": "INFORMATIONAL", \
            "Comparison": "EQUALS" \
        }] \
    }' \
```

```
    --description "A sample rule" \
    --no-is-terminal \
    --rule-name "sample rule" \
    --rule-order 1 \
    --rule-status "ENABLED"
```

Salida:

```
{
    "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-rule/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Para obtener más información, consulte Creación de reglas de automatización en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte CreateAutomationRule en la Referencia de comandos de la AWS CLI.

`create-configuration-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-configuration-policy`.

AWS CLI

Para crear una política de configuración

En el siguiente ejemplo de `create-configuration-policy`, se crea una política de configuración con los ajustes especificados.

```
aws securityhub create-configuration-policy \
    --name "SampleConfigurationPolicy" \
    --description "SampleDescription" \
    --configuration-policy '{"SecurityHub": {"ServiceEnabled":
 true, "EnabledStandardIdentifiers": ["arn:aws:securityhub:eu-
central-1::standards/aws-foundational-security-best-practices/
v/1.0.0","arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"],"SecurityControlsConfiguration":{"DisabledSecurityControlIdentifiers":
 ["CloudTrail.2"], "SecurityControlCustomParameters": [{"SecurityControlId":
 "ACM.1", "Parameters": {"daysToExpiration": {"ValueType": "CUSTOM", "Value":
 {"Integer": 15}}}}]}}}' \
    --tags '{"Environment": "Prod"}'
```

Salida:

```
{
    "Arn": "arn:aws:securityhub:eu-central-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "SampleConfigurationPolicy",
    "Description": "SampleDescription",
    "UpdatedAt": "2023-11-28T20:28:04.494000+00:00",
    "CreatedAt": "2023-11-28T20:28:04.494000+00:00",
    "ConfigurationPolicy": {
        "SecurityHub": {
            "ServiceEnabled": true,
            "EnabledStandardIdentifiers": [
                "arn:aws:securityhub:eu-central-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
            ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Para obtener más información, consulte Usar EventBridge para la respuesta y la corrección automatizadas en la Guía del usuario AWS de Security Hub.

- Para obtener información sobre la API, consulte CreateConfigurationPolicy en la Referencia de comandos de la AWS CLI.

`create-finding-aggregator`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-finding-aggregator`.

AWS CLI

Para habilitar la agregación de hallazgos

En el siguiente ejemplo de `create-finding-aggregator`, se configura la agregación de resultados. Se ejecuta desde Este de EE. UU. (Virginia), que designa Este de EE. UU. (Virginia) como región de agregación. Indica que solo se deben vincular las regiones especificadas y que no se deben vincular automáticamente regiones nuevas. Las regiones vinculadas son Oeste de EE. UU. (Norte de California) y Oeste de EE. UU. (Oregón).

```
aws securityhub create-finding-aggregator \
    --region us-east-1 \
    --region-linking-mode SPECIFIED_REGIONS \
    --regions us-west-1,us-west-2
```

Salida:

```
{
    "FindingAggregatorArn": "arn:aws:securityhub:us-east-1:222222222222:finding-
aggregator/123e4567-e89b-12d3-a456-426652340000",
    "FindingAggregationRegion": "us-east-1",
    "RegionLinkingMode": "SPECIFIED_REGIONS",
    "Regions": "us-west-1,us-west-2"
}
```

Para obtener más información, consulte Habilitación de agregación entre regiones en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte CreateFindingAggregator en la Referencia de comandos de la AWS CLI.

`create-insight`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-insight`.

AWS CLI

Para eliminar un hallazgo personalizado

En el siguiente ejemplo de `create-insight`, se crea información personalizada denominada Critical role Findings que devuelve los resultados esenciales relacionadas con los roles de AWS.

```
aws securityhub create-insight \
    --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' \
    --group-by-attribute "ResourceId" \
    --name "Critical role findings"
```

Salida:

```
{
    "InsightArn": "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/
custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Para obtener más información, consulte Información personalizada en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte CreateInsight en la Referencia de comandos de la AWS CLI.

`create-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-members`.

AWS CLI

Para añadir cuentas como cuentas de miembros

En el siguiente ejemplo de `create-members`, se agregan dos cuentas como cuentas de miembro a la cuenta de administrador solicitante.

```
aws securityhub create-members \
    --account-details '[{"AccountId": "123456789111"}, {"AccountId":
 "123456789222"}]'
```

Salida:

```
{
    "UnprocessedAccounts": []
}
```

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener detalles sobre la API, consulte CreateMembers en la Referencia de comandos de la AWS CLI.

`decline-invitations`

En el siguiente ejemplo de código, se muestra cómo utilizar `decline-invitations`.

AWS CLI

Para rechazar una invitación a ser miembro de la cuenta

En el siguiente ejemplo de `decline-invitations`, se rechaza una invitación para ser una cuenta miembro de la cuenta de administrador especificada. La cuenta de miembro es la cuenta solicitante.

```
aws securityhub decline-invitations \
    --account-ids "123456789012"
```

Salida:

```
{
    "UnprocessedAccounts": []
}
```

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DeclineInvitations en la Referencia de comandos de la AWS CLI.

`delete-action-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-action-target`.

AWS CLI

Para eliminar una acción personalizada

En el siguiente ejemplo de `delete-action-target`, se elimina la acción personalizada identificada por el ARN especificado.

```
aws securityhub delete-action-target \
    --action-target-arn "arn:aws:securityhub:us-west-1:123456789012:action/custom/
Remediation"
```

Salida:

```
{
    "ActionTargetArn": "arn:aws:securityhub:us-west-1:123456789012:action/custom/
Remediation"
}
```

Para obtener más información, consulte Creating a custom action and associating it with a CloudWatch Events rule en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DeleteActionTarget en la Referencia de comandos de la AWS CLI.

`delete-configuration-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-configuration-policy`.

AWS CLI

Eliminación de una política de configuración

En el siguiente ejemplo de `delete-configuration-policy`, se elimina la política de configuración especificada.

```
aws securityhub delete-configuration-policy \
    --identifier "arn:aws:securityhub:eu-central-1:123456789012:configuration-
policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de políticas de configuración en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DeleteConfigurationPolicy en la Referencia de comandos de la AWS CLI.

`delete-finding-aggregator`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-finding-aggregator`.

AWS CLI

Para detener la agregación de hallazgos

En el siguiente ejemplo de `delete-finding-aggregator`, se detiene la agregación de resultados. El comando se ejecuta desde la región de agregación, que es Este de EE. UU. (Virginia).

```
aws securityhub delete-finding-aggregator \
    --region us-east-1 \
    --finding-aggregator-arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Detención de la agregación en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DeleteFindingAggregator en la Referencia de comandos de la AWS CLI.

`delete-insight`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-insight`.

AWS CLI

Para eliminar información personalizada

En el siguiente ejemplo de `delete-insight`, se elimina la información personalizada con el ARN especificado.

```
aws securityhub delete-insight \
    --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/
custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Salida:

```
{
   "InsightArn": "arn:aws:securityhub:eu-
central-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
}
```

Para obtener más información, consulte Información personalizada en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DeleteInsight en la Referencia de comandos de AWS CLI.

`delete-invitations`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-invitations`.

AWS CLI

Para eliminar una invitación a ser miembro de la cuenta

En el siguiente ejemplo de `delete-invitations`, se elimina una invitación para ser una cuenta miembro de la cuenta de administrador especificada. La cuenta de miembro es la cuenta solicitante.

```
aws securityhub delete-invitations \
    --account-ids "123456789012"
```

Salida:

```
{
    "UnprocessedAccounts": []
}
```

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DeleteInvitations en la Referencia de comandos de la AWS CLI.

`delete-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-members`.

AWS CLI

Para eliminar cuentas de miembro

En el siguiente ejemplo de `delete-members`, se eliminan las cuentas de miembro especificadas de la cuenta de administrador solicitante.

```
aws securityhub delete-members \
    --account-ids "123456789111" "123456789222"
```

Salida:

```
{
    "UnprocessedAccounts": []
}
```

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener detalles sobre la API, consulte DeleteMembers en la Referencia de comandos de la AWS CLI.

`describe-action-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-action-targets`.

AWS CLI

Para recuperar detalles sobre las acciones personalizadas

En el siguiente ejemplo de `describe-action-targets`, se recupera información sobre la acción personalizada identificada por el ARN especificado.

```
aws securityhub describe-action-targets \
```

```
    --action-target-arns "arn:aws:securityhub:us-west-1:123456789012:action/custom/
Remediation"
```

Salida:

```
{
    "ActionTargets": [
        {
            "ActionTargetArn": "arn:aws:securityhub:us-west-1:123456789012:action/
custom/Remediation",
            "Description": "Action to send the finding for remediation tracking",
            "Name": "Send to remediation"
        }
    ]
}
```

Para obtener más información, consulte Creating a custom action and associating it with a CloudWatch Events rule en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DescribeActionTargets en la Referencia de comandos de la AWS CLI.

`describe-hub`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-hub`.

AWS CLI

Para obtener información sobre un recurso de hub

En el ejemplo de `describe-hub` siguiente, se devuelve la fecha de suscripción y otros ajustes de configuración del recurso de hub especificado. El recurso de hub se identifica mediante su ARN.

```
aws securityhub describe-hub \
    --hub-arn "arn:aws:securityhub:us-west-1:123456789012:hub/default"
```

Salida:

```
{
```

```
    "HubArn": "arn:aws:securityhub:us-west-1:123456789012:hub/default",
    "SubscribedAt": "2019-11-19T23:15:10.046Z",
    "AutoEnableControls": true,
    "ControlFindingGenerator": "SECURITY_CONTROL"
}
```

Para obtener más información, consulte AWS::SecurityHub::Hub en la Guía del usuario de AWS CloudFormation.

- Para obtener información sobre la API, consulte DescribeHub en la Referencia de comandos de la AWS CLI.

`describe-organization-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-organization-configuration`.

AWS CLI

Para ver cómo se configura Security Hub para una organización

En el siguiente ejemplo de `describe-organization-configuration`, se devuelve información sobre la forma en que se configura una organización en Security Hub. En este ejemplo, la organización utiliza la configuración central. Solo la cuenta de administrador de Security Hub puede ejecutar este comando.

```
aws securityhub describe-organization-configuration
```

Salida:

```
{
    "AutoEnable": false,
    "MemberAccountLimitReached": false,
    "AutoEnableStandards": "NONE",
    "OrganizationConfiguration": {
        "ConfigurationType": "LOCAL",
        "Status": "ENABLED",
        "StatusMessage": "Central configuration has been enabled successfully"
    }
}
```

Para obtener más información, consulte Administración de cuentas de administrador y de miembro de Security Hub con AWS Organizations en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DescribeOrganizationConfiguration en la Referencia de comandos de la AWS CLI.

`describe-products`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-products`.

AWS CLI

Para devolver información sobre las integraciones de productos disponibles

En el siguiente ejemplo de `describe-products`, se devuelven las integraciones de productos disponibles de una en una.

```
aws securityhub describe-products \
    --max-results 1
```

Salida:

```
{
    "NextToken": "U2FsdGVkX18vvPlOqb7RDrWRWVFBJI46MOIAb+nZmRJmR15NoRi2gm13sdQEn3O/
pq/78dGs+bKpgA+7HMPHO0qX33/zoRI+uIG/F9yLNhcOrOWzFUdy36JcXLQji3Rpnn/
cD1SVkGA98qI3zPOSDg==",
    "Products": [
        {
            "ProductArn": "arn:aws:securityhub:us-west-1:123456789333:product/
crowdstrike/crowdstrike-falcon",
            "ProductName": "CrowdStrike Falcon",
            "CompanyName": "CrowdStrike",
            "Description": "CrowdStrike Falcon's single lightweight sensor unifies
 next-gen antivirus, endpoint detection and response, and 24/7 managed hunting, via
 the cloud.",
            "Categories": [
                "Endpoint Detection and Response (EDR)",
                "AV Scanning and Sandboxing",
                "Threat Intelligence Feeds and Reports",
                "Endpoint Forensics",
                "Network Forensics"
            ],
```

```
            "IntegrationTypes": [
                "SEND_FINDINGS_TO_SECURITY_HUB"
            ],
            "MarketplaceUrl": "https://aws.amazon.com/marketplace/seller-profile?
id=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "ActivationUrl": "https://falcon.crowdstrike.com/support/documentation",
            "ProductSubscriptionResourcePolicy": "{\"Version\":
\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
\"123456789333\"},\"Action\":[\"securityhub:BatchImportFindings\"],\"Resource\":
\"arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon\",\"Condition\":{\"StringEquals\":{\"securityhub:TargetAccount
\":\"123456789012\"}}},{\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
\"123456789012\"},\"Action\":[\"securityhub:BatchImportFindings\"],\"Resource
\":\"arn:aws:securityhub:us-west-1:123456789333:product/crowdstrike/crowdstrike-
falcon\",\"Condition\":{\"StringEquals\":{\"securityhub:TargetAccount\":
\"123456789012\"}}}]}"
        }
    ]
}
```

Para obtener más información, consulte Comprensión de las integraciones en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DescribeProducts en la Referencia de comandos de la AWS CLI.

`describe-standards-controls`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-standards-controls`.

AWS CLI

Para solicitar la lista de controles de un estándar habilitado

En el siguiente ejemplo de `describe-standards-controls`, se solicita la lista de controles de la suscripción de la cuenta solicitante a la norma PCI DSS. La solicitud devuelve dos controles a la vez.

```
aws securityhub describe-standards-controls \
    --standards-subscription-arn "arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1" \
    --max-results 2
```

Salida:

```
{
    "Controls": [
        {
            "StandardsControlArn": "arn:aws:securityhub:us-
west-1:123456789012:control/pci-dss/v/3.2.1/PCI.AutoScaling.1",
            "ControlStatus": "ENABLED",
            "ControlStatusUpdatedAt": "2020-05-15T18:49:04.473000+00:00",
            "ControlId": "PCI.AutoScaling.1",
            "Title": "Auto scaling groups associated with a load balancer should use
 health checks",
            "Description": "This AWS control checks whether your Auto Scaling groups
 that are associated with a load balancer are using Elastic Load Balancing health
 checks.",
            "RemediationUrl": "https://docs.aws.amazon.com/console/securityhub/
PCI.AutoScaling.1/remediation",
            "SeverityRating": "LOW",
            "RelatedRequirements": [
                "PCI DSS 2.2"
            ]
        },
        {
            "StandardsControlArn": "arn:aws:securityhub:us-
west-1:123456789012:control/pci-dss/v/3.2.1/PCI.CW.1",
            "ControlStatus": "ENABLED",
            "ControlStatusUpdatedAt": "2020-05-15T18:49:04.498000+00:00",
            "ControlId": "PCI.CW.1",
            "Title": "A log metric filter and alarm should exist for usage of the
 \"root\" user",
            "Description": "This control checks for the CloudWatch metric
 filters using the following pattern { $.userIdentity.type = \"Root\" &&
 $.userIdentity.invokedBy NOT EXISTS && $.eventType != \"AwsServiceEvent\" }
 It checks that the log group name is configured for use with active multi-
region CloudTrail, that there is at least one Event Selector for a Trail with
 IncludeManagementEvents set to true and ReadWriteType set to All, and that there is
 at least one active subscriber to an SNS topic associated with the alarm.",
            "RemediationUrl": "https://docs.aws.amazon.com/console/securityhub/
PCI.CW.1/remediation",
            "SeverityRating": "MEDIUM",
            "RelatedRequirements": [
                "PCI DSS 7.2.1"
            ]
        }
```

```
    ],
    "NextToken": "U2FsdGVkX1+eNkPoZHVl11ip5HUYQPWSWZGmftcmJiHL8JoKEsCDuaKayiPDyLK
+LiTkShveoOdvfxXCkOBaGhohIXhsIedN+LSjQV/
l7kfCfJcq4PziNC1N9xe9aq2pjlLVZnznTfSImrodT5bRNHe4fELCQq/z+5ka
+5Lzmc11axcwTd5lKgQyQqmUVoeriHZhyIiBgWKf7oNYdBVG8OEortVWvSkoUTt
+B2ThcnC7l43kI0UNxlkZ6sc64AsW"
}
```

Para obtener más información sobre este estándar, consulte Visualización de los detalles de un estándar en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DescribeStandardsControls en la Referencia de comandos de la AWS CLI.

`describe-standards`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-standards`.

AWS CLI

Para devolver una lista de los estándares disponibles

En el siguiente ejemplo de `describe-standards`, se devuelve la lista de normas disponibles.

```
aws securityhub describe-standards
```

Salida:

```
{
    "Standards": [
        {
            "StandardsArn": "arn:aws:securityhub:us-west-1::standards/aws-
foundational-security-best-practices/v/1.0.0",
            "Name": "AWS Foundational Security Best Practices v1.0.0",
            "Description": "The AWS Foundational Security Best Practices standard
 is a set of automated security checks that detect when AWS accounts and deployed
 resources do not align to security best practices. The standard is defined by AWS
 security experts. This curated set of controls helps improve your security posture
 in AWS, and cover AWS's most popular and foundational services.",
            "EnabledByDefault": true
        },
```

```
        {
            "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0",
            "Name": "CIS AWS Foundations Benchmark v1.2.0",
            "Description": "The Center for Internet Security (CIS) AWS Foundations
 Benchmark v1.2.0 is a set of security configuration best practices for AWS. This
 Security Hub standard automatically checks for your compliance readiness against a
 subset of CIS requirements.",
            "EnabledByDefault": true
        },
        {
            "StandardsArn": "arn:aws:securityhub:us-west-1::standards/pci-dss/
v/3.2.1",
            "Name": "PCI DSS v3.2.1",
            "Description": "The Payment Card Industry Data Security Standard (PCI
 DSS) v3.2.1 is an information security standard for entities that store, process,
 and/or transmit cardholder data. This Security Hub standard automatically checks
 for your compliance readiness against a subset of PCI DSS requirements.",
            "EnabledByDefault": false
        }
    ]
}
```

Para obtener más información, consulte Descripción de los estándares de seguridad en AWS Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DescribeStandards en la Referencia de comandos de la AWS CLI.

`disable-import-findings-for-product`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-import-findings-for-product`.

AWS CLI

Para dejar de recibir los hallazgos de la integración de un producto

En el siguiente ejemplo de `disable-import-findings-for-product`, se desactiva el flujo de resultados para la suscripción especificada de una integración de productos.

```
aws securityhub disable-import-findings-for-product \
```

```
    --product-subscription-arn "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/crowdstrike-falcon"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Comprensión de las integraciones en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DisableImportFindingsForProduct en la Referencia de comandos de la AWS CLI.

`disable-organization-admin-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-organization-admin-account`.

AWS CLI

Para eliminar una cuenta de administrador de Security Hub

En el siguiente ejemplo de `disable-organization-admin-account`, se revoca la asignación de la cuenta especificada como cuenta de administrador de Security Hub para AWS Organizations.

```
aws securityhub disable-organization-admin-account \
    --admin-account-id 777788889999
```

Este comando no genera ninguna salida.

Para obtener obtener más información, consulte Integración de Security Hub con AWS Organizations en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DisableOrganizationAdminAccount en la Referencia de comandos de la AWS CLI.

`disable-security-hub`

En el siguiente ejemplo de código, se muestra cómo utilizar `disable-security-hub`.

AWS CLI

Para deshabilitar AWS Security Hub

En el siguiente ejemplo de `disable-security-hub`, se deshabilita AWS Security Hub para la cuenta solicitante.

```
aws securityhub disable-security-hub
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deshabilitación de AWS Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DisableSecurityHub en la Referencia de comandos de la AWS CLI.

`disassociate-from-administrator-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-from-administrator-account`.

AWS CLI

Para desvincularse de una cuenta de administrador

En el siguiente ejemplo de `disassociate-from-administrator-account`, se desvincula la cuenta solicitante de su cuenta de administrador actual.

```
aws securityhub disassociate-from-administrator-account
```

Este comando no genera ninguna salida.

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DisassociateFromAdministratorAccount en la Referencia de comandos de AWS CLI.

`disassociate-from-master-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-from-master-account`.

AWS CLI

Para desvincularse de una cuenta de administrador

En el siguiente ejemplo de `disassociate-from-master-account`, se desvincula la cuenta solicitante de su cuenta de administrador actual.

```
aws securityhub disassociate-from-master-account
```

Este comando no genera ninguna salida.

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DisassociateFromMasterAccount en la Referencia de comandos de la AWS CLI.

`disassociate-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-members`.

AWS CLI

Cómo desasociar cuentas miembro

En el siguiente ejemplo de `disassociate-members`, se desvinculan las cuentas de miembro especificadas de la cuenta de administrador solicitante.

```
aws securityhub disassociate-members  \
    --account-ids "123456789111" "123456789222"
```

Este comando no genera ninguna salida.

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte DisassociateMembers en la Referencia de comandos de la AWS CLI.

`enable-import-findings-for-product`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-import-findings-for-product`.

AWS CLI

Para empezar a recibir los hallazgos de la integración de un producto

En el siguiente ejemplo de `enable-import-findings-for-product`, se activa el flujo de resultados de la integración de productos especificada.

```
aws securityhub enable-import-findings-for-product \
    --product-arn "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

Salida:

```
{
    "ProductSubscriptionArn": "arn:aws:securityhub:us-east-1:123456789012:product-subscription/crowdstrike/crowdstrike-falcon"
}
```

Para obtener más información, consulte Comprensión de las integraciones en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte EnableImportFindingsForProduct en la Referencia de comandos de la AWS CLI.

`enable-organization-admin-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-organization-admin-account`.

AWS CLI

Para designar una cuenta de organización como cuenta de administrador de Security Hub

En el siguiente ejemplo de `enable-organization-admin-account`, se designa la cuenta especificada como cuenta de administrador de Security Hub.

```
aws securityhub enable-organization-admin-account \
```

```
    --admin-account-id 777788889999
```

Este comando no genera ninguna salida.

Para obtener obtener más información, consulte Integración de Security Hub con AWS Organizations en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte EnableOrganizationAdminAccount en la Referencia de comandos de la AWS CLI.

`enable-security-hub`

En el siguiente ejemplo de código, se muestra cómo utilizar `enable-security-hub`.

AWS CLI

Para habilitar AWS Security Hub

En el siguiente ejemplo de `enable-security-hub`, se activa AWS Security Hub para la cuenta solicitante. Configura Security Hub para habilitar los estándares predeterminados. En el caso del recurso de hub, asigna el valor `Security` a la etiqueta `Department`.

```
aws securityhub enable-security-hub \
    --enable-default-standards \
    --tags '{"Department": "Security"}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Habilitar y configurar Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre las API, consulte EnableSecurityHub en la Referencia de comandos de la AWS CLI.

`get-administrator-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-administrator-account`.

AWS CLI

Para recuperar información sobre una cuenta de administrador

En el siguiente ejemplo de `get-administrator-account`, se recupera información sobre la cuenta de administrador para la cuenta solicitante.

```
aws securityhub get-administrator-account
```

Salida:

```
{
   "Master": {
      "AccountId": "123456789012",
      "InvitationId": "7ab938c5d52d7904ad09f9e7c20cc4eb",
      "InvitedAt": 2020-06-01T20:21:18.042000+00:00,
      "MemberStatus": "ASSOCIATED"
   }
}
```

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte GetAdministratorAccount en la Referencia de comandos de la AWS CLI.

`get-configuration-policy-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-configuration-policy-association`.

AWS CLI

Para obtener los detalles de la asociación de configuración para un objetivo

En el siguiente ejemplo de `get-configuration-policy-association`, se recuperan los detalles de asociación para el destino especificado. Puede proporcionar un ID de cuenta, un ID de las unidades organizativas o el ID raíz del destino.

```
aws securityhub get-configuration-policy-association \
    --target '{"OrganizationalUnitId": "ou-6hi7-8j91kl2m"}'
```

Salida:

```
{
```

```
    "ConfigurationPolicyId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "TargetId": "ou-6hi7-8j91kl2m",
    "TargetType": "ORGANIZATIONAL_UNIT",
    "AssociationType": "APPLIED",
    "UpdatedAt": "2023-09-26T21:13:01.816000+00:00",
    "AssociationStatus": "SUCCESS",
    "AssociationStatusMessage": "Association applied successfully on this target."
}
```

Para obtener más información, consulte Viewing Security Hub configuration policies en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte GetConfigurationPolicyAssociation en la Referencia de comandos de la AWS CLI.

`get-configuration-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-configuration-policy`.

AWS CLI

Para ver los detalles de la política de configuración

En el siguiente ejemplo de `get-configuration-policy`, se recuperan detalles sobre la política de configuración especificada.

```
aws securityhub get-configuration-policy \
   --identifier "arn:aws:securityhub:eu-central-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Salida:

```
{
    "Arn": "arn:aws:securityhub:eu-central-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Id": "ce5ed1e7-9639-4e2f-9313-fa87fcef944b",
    "Name": "SampleConfigurationPolicy",
    "Description": "SampleDescription",
    "UpdatedAt": "2023-11-28T20:28:04.494000+00:00",
    "CreatedAt": "2023-11-28T20:28:04.494000+00:00",
    "ConfigurationPolicy": {
```

```
        "SecurityHub": {
            "ServiceEnabled": true,
            "EnabledStandardIdentifiers": [
                "arn:aws:securityhub:eu-central-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
            ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Para obtener más información, consulte Viewing Security Hub configuration policies en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte GetConfigurationPolicy en la Referencia de comandos de la AWS CLI.

`get-enabled-standards`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-enabled-standards`.

AWS CLI

Para recuperar información sobre un estándar habilitado

En el siguiente ejemplo de `get-enabled-standards`, se recupera información sobre la normativa PCI DSS.

```
aws securityhub get-enabled-standards \
    --standards-subscription-arn "arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1"
```

Salida:

```
{
    "StandardsSubscriptions": [
        {
            "StandardsArn": "arn:aws:securityhub:us-west-1::standards/pci-dss/
v/3.2.1",
            "StandardsInput": { },
            "StandardsStatus": "READY",
            "StandardsSubscriptionArn": "arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1"
        }
    ]
}
```

Para obtener más información, consulte Descripción de los estándares de seguridad en AWS Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte GetEnabledStandards en la Referencia de comandos de la AWS CLI.

`get-finding-aggregator`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-finding-aggregator`.

AWS CLI

Para recuperar la configuración de agregación de hallazgos actual

En el siguiente ejemplo de `get-finding-aggregator`, se recupera la configuración de agregación de resultados actual.

```
aws securityhub get-finding-aggregator \
```

```
    --finding-aggregator-arn arn:aws:securityhub:us-east-1:222222222222:finding-
aggregator/123e4567-e89b-12d3-a456-426652340000
```

Salida:

```
{
    "FindingAggregatorArn": "arn:aws:securityhub:us-east-1:222222222222:finding-
aggregator/123e4567-e89b-12d3-a456-426652340000",
    "FindingAggregationRegion": "us-east-1",
    "RegionLinkingMode": "SPECIFIED_REGIONS",
    "Regions": "us-west-1,us-west-2"
}
```

Para obtener más información, consulte Visualización de la configuración de agregación en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte GetFindingAggregator en la Referencia de comandos de la AWS CLI.

`get-finding-history`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-finding-history`.

AWS CLI

Para obtener el historial de hallazgos

En el siguiente ejemplo de `get-finding-history`, se obtiene el historial de los últimos 90 días del resultado especificado. En este ejemplo, los resultados se limitan a dos registros del historial de resultados.

```
aws securityhub get-finding-history \
    --finding-identifier Id="arn:aws:securityhub:us-
east-1:123456789012:security-control/S3.17/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-east-1::product/aws/securityhub"
```

Salida:

```
{
    "Records": [
        {
            "FindingIdentifier": {
```

```
                "Id": "arn:aws:securityhub:us-east-1:123456789012:security-control/
S3.17/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
                "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
securityhub"
            },
            "UpdateTime": "2023-06-02T03:15:25.685000+00:00",
            "FindingCreated": false,
            "UpdateSource": {
                "Type": "BATCH_IMPORT_FINDINGS",
                "Identity": "arn:aws:securityhub:us-east-1::product/aws/securityhub"
            },
            "Updates": [
                {
                    "UpdatedField": "Compliance.RelatedRequirements",
                    "OldValue": "[\"NIST.800-53.r5 SC-12(2)\",\"NIST.800-53.r5
 SC-12(3)\",\"NIST.800-53.r5 SC-12(6)\",\"NIST.800-53.r5 CM-3(6)\",\"NIST.800-53.r5
 SC-13\",\"NIST.800-53.r5 SC-28\",\"NIST.800-53.r5 SC-28(1)\",\"NIST.800-53.r5
 SC-7(10)\"]",
                    "NewValue": "[\"NIST.800-53.r5 SC-12(2)\",\"NIST.800-53.r5
 CM-3(6)\",\"NIST.800-53.r5 SC-13\",\"NIST.800-53.r5 SC-28\",\"NIST.800-53.r5
 SC-28(1)\",\"NIST.800-53.r5 SC-7(10)\",\"NIST.800-53.r5 CA-9(1)\",\"NIST.800-53.r5
 SI-7(6)\",\"NIST.800-53.r5 AU-9\"]"
                },
                {
                    "UpdatedField": "LastObservedAt",
                    "OldValue": "2023-06-01T09:15:38.587Z",
                    "NewValue": "2023-06-02T03:15:22.946Z"
                },
                {
                    "UpdatedField": "UpdatedAt",
                    "OldValue": "2023-06-01T09:15:31.049Z",
                    "NewValue": "2023-06-02T03:15:14.861Z"
                },
                {
                    "UpdatedField": "ProcessedAt",
                    "OldValue": "2023-06-01T09:15:41.058Z",
                    "NewValue": "2023-06-02T03:15:25.685Z"
                }
            ]
        },
        {
            "FindingIdentifier": {
                "Id": "arn:aws:securityhub:us-east-1:123456789012:security-control/
S3.17/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
                "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
securityhub"
            },
            "UpdateTime": "2023-05-23T02:06:51.518000+00:00",
            "FindingCreated": "true",
            "UpdateSource": {
                "Type": "BATCH_IMPORT_FINDINGS",
                "Identity": "arn:aws:securityhub:us-east-1::product/aws/securityhub"
            },
            "Updates": []
        }
    ]
}
```

Para obtener más información, consulte Finding history en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte GetFindingHistory en la Referencia de comandos de la AWS CLI.

`get-findings`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-findings`.

AWS CLI

Ejemplo 1: devolución de los resultados generados para un estándar específico

En el siguiente ejemplo de `get-findings`, se devuelven los resultados de la normativa PCI DSS.

```
aws securityhub get-findings \
    --filters '{"GeneratorId":[{"Value": "pci-dss","Comparison":"PREFIX"}]}' \
    --max-items 1
```

Salida:

```
{
    "Findings": [
        {
            "SchemaVersion": "2018-10-08",
            "Id": "arn:aws:securityhub:eu-central-1:123456789012:subscription/pci-
dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
            "ProductArn": "arn:aws:securityhub:us-west-1::product/aws/securityhub",
            "GeneratorId": "pci-dss/v/3.2.1/PCI.Lambda.2",
            "AwsAccountId": "123456789012",
            "Types": [
                "Software and Configuration Checks/Industry and Regulatory
 Standards/PCI-DSS"
            ],
            "FindingProviderFields": {
                "Severity": {
                    "Original": 0,
                    "Label": "INFORMATIONAL"
                },
                "Types": [
                    "Software and Configuration Checks/Industry and Regulatory
 Standards/PCI-DSS"
                ]
            },
            "FirstObservedAt": "2020-06-02T14:02:49.159Z",
            "LastObservedAt": "2020-06-02T14:02:52.397Z",
            "CreatedAt": "2020-06-02T14:02:49.159Z",
            "UpdatedAt": "2020-06-02T14:02:52.397Z",
            "Severity": {
                "Original": 0,
                "Label": "INFORMATIONAL",
                "Normalized": 0
            },
            "Title": "PCI.Lambda.2 Lambda functions should be in a VPC",
            "Description": "This AWS control checks whether a Lambda function is in
 a VPC.",
            "Remediation": {
                "Recommendation": {
                    "Text": "For directions on how to fix this issue, please consult
 the AWS Security Hub PCI DSS documentation.",
                    "Url": "https://docs.aws.amazon.com/console/securityhub/
PCI.Lambda.2/remediation"
                }
            },
            "ProductFields": {
                "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
                "StandardsSubscriptionArn": "arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1",
                "ControlId": "PCI.Lambda.2",
                "RecommendationUrl": "https://docs.aws.amazon.com/console/
securityhub/PCI.Lambda.2/remediation",
```

```
                "RelatedAWSResources:0/name": "securityhub-lambda-inside-
vpc-0e904a3b",
                "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
                "StandardsControlArn": "arn:aws:securityhub:us-
west-1:123456789012:control/pci-dss/v/3.2.1/PCI.Lambda.2",
                "aws/securityhub/SeverityLabel": "INFORMATIONAL",
                "aws/securityhub/ProductName": "Security Hub",
                "aws/securityhub/CompanyName": "AWS",
                "aws/securityhub/FindingId": "arn:aws:securityhub:eu-
central-1::product/aws/securityhub/arn:aws:securityhub:eu-
central-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
        },
            "Resources": [
                {
                    "Type": "AwsAccount",
                    "Id": "AWS::::Account:123456789012",
                    "Partition": "aws",
                    "Region": "us-west-1"
                }
            ],
            "Compliance": {
                "Status": "PASSED",
                "RelatedRequirements": [
                    "PCI DSS 1.2.1",
                    "PCI DSS 1.3.1",
                    "PCI DSS 1.3.2",
                    "PCI DSS 1.3.4"
                ]
            },
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
            },
            "RecordState": "ARCHIVED"
        }
    ],
    "NextToken": "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ=="
}
```

Ejemplo 2: devolución de los resultados de gravedad crítica cuyo estado de flujo de trabajo es NOTIFIED

En el siguiente ejemplo de `get-findings`, se devuelven los resultados cuyo valor en la etiqueta de gravedad es CRITICAL y el estado del flujo de trabajo es NOTIFIED. Los resultados están ordenados de manera descendente por valor de confianza.

```
aws securityhub get-findings \
    --filters '{"SeverityLabel":[{"Value":
 "CRITICAL","Comparison":"EQUALS"}],"WorkflowStatus":
 [{"Value":"NOTIFIED","Comparison":"EQUALS"}]}' \
    --sort-criteria '{ "Field": "Confidence", "SortOrder": "desc"}' \
    --max-items 1
```

Salida:

```
{
    "Findings": [
        {
            "SchemaVersion": "2018-10-08",
            "Id": "arn:aws:securityhub:us-west-1: 123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.13/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
            "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0/rule/1.13",
            "AwsAccountId": "123456789012",
            "Types": [
                "Software and Configuration Checks/Industry and Regulatory
 Standards/CIS AWS Foundations Benchmark"
            ],
            "FindingProviderFields" {
                "Severity": {
                    "Original": 90,
                    "Label": "CRITICAL"
                },
                "Types": [
                    "Software and Configuration Checks/Industry and Regulatory
 Standards/CIS AWS Foundations Benchmark"
                ]
            },
            "FirstObservedAt": "2020-05-21T20:16:34.752Z",
            "LastObservedAt": "2020-06-09T08:16:37.171Z",
            "CreatedAt": "2020-05-21T20:16:34.752Z",
            "UpdatedAt": "2020-06-09T08:16:36.430Z",
            "Severity": {
                "Original": 90,
```

```
                "Label": "CRITICAL",
                "Normalized": 90
            },
            "Title": "1.13 Ensure MFA is enabled for the \"root\" account",
            "Description": "The root account is the most privileged user in an AWS
 account. MFA adds an extra layer of protection on top of a user name and password.
 With MFA enabled, when a user signs in to an AWS website, they will be prompted for
 their user name and password as well as for an authentication code from their AWS
 MFA device.",
            "Remediation": {
                "Recommendation": {
                    "Text": "For directions on how to fix this issue, please consult
 the AWS Security Hub CIS documentation.",
                    "Url": "https://docs.aws.amazon.com/console/securityhub/
standards-cis-1.13/remediation"
                }
            },
            "ProductFields": {
                "StandardsGuideArn": "arn:aws:securityhub:::ruleset/cis-aws-
foundations-benchmark/v/1.2.0",
                "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
west-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
                "RuleId": "1.13",
                "RecommendationUrl": "https://docs.aws.amazon.com/console/
securityhub/standards-cis-1.13/remediation",
                "RelatedAWSResources:0/name": "securityhub-root-account-mfa-
enabled-5pftha",
                "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
                "StandardsControlArn": "arn:aws:securityhub:us-
west-1:123456789012:control/cis-aws-foundations-benchmark/v/1.2.0/1.13",
                "aws/securityhub/SeverityLabel": "CRITICAL",
                "aws/securityhub/ProductName": "Security Hub",
                "aws/securityhub/CompanyName": "AWS",
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-
west-1::product/aws/securityhub/arn:aws:securityhub:us-
west-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0/1.13/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            "Resources": [
                {
                    "Type": "AwsAccount",
                    "Id": "AWS::::Account:123456789012",
                    "Partition": "aws",
                    "Region": "us-west-1"
```

```
                }
            ],
            "Compliance": {
                "Status": "FAILED"
            },
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NOTIFIED"
            },
            "RecordState": "ACTIVE"
        }
    ]
}
```

Para obtener más información, consulte Filtering and grouping findings en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte GetFindings en la Referencia de comandos de la AWS CLI.

`get-insight-results`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-insight-results`.

AWS CLI

Para recuperar los resultados para la información

En el siguiente ejemplo de `get-insight-results`, se devuelve la lista de los resultados de la información con el ARN especificado.

```
aws securityhub get-insight-results \
    --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/
custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Salida:

```
{
    "InsightResults": {
        "GroupByAttribute": "ResourceId",
        "InsightArn": "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
```

```
        "ResultValues": [
            {
                "Count": 10,
                "GroupByAttributeValue": "AWS::::Account:123456789111"
            },
            {
                "Count": 3,
                "GroupByAttributeValue": "AWS::::Account:123456789222"
            }
        ]
    }
}
```

Para obtener más información, consulte Ver y tomar medidas sobre los hallazgos y resultados del conocimiento en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte GetInsightResults en la Referencia de comandos de la AWS CLI.

`get-insights`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-insights`.

AWS CLI

Para recuperar los detalles de la información

En el siguiente ejemplo de `get-insights`, se recuperan los detalles de la configuración para la información con el ARN especificado.

```
aws securityhub get-insights \
    --insight-arns "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/
custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Salida:

```
{
    "Insights": [
        {
            "Filters": {
               "ResourceType": [
                    {
```

```
                        "Comparison": "EQUALS",
                        "Value": "AwsIamRole"
                    }
                ],
                "SeverityLabel": [
                    {
                        "Comparison": "EQUALS",
                        "Value": "CRITICAL"
                    }
                ],
            },
            "GroupByAttribute": "ResourceId",
            "InsightArn": "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
            "Name": "Critical role findings"
        }
    ]
}
```

Para obtener más información, consulte Visualizar información en AWS Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte GetInsights en la Referencia de comandos de la AWS CLI.

`get-invitations-count`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-invitations-count`.

AWS CLI

Para recuperar el número de invitaciones que no se ha aceptado

En el siguiente ejemplo de `get-invitations-count`, se recupera el número de invitaciones que la cuenta solicitante ha rechazado o que no ha respondido.

```
aws securityhub get-invitations-count
```

Salida:

```
{
```

```
  "InvitationsCount": 3
}
```

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte GetInvitationsCount en la Referencia de comandos de la AWS CLI.

`get-master-account`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-master-account`.

AWS CLI

Para recuperar información sobre una cuenta de administrador

En el siguiente ejemplo de `get-master-account`, se recupera información sobre la cuenta de administrador para la cuenta solicitante.

```
aws securityhub get-master-account
```

Salida:

```
{
   "Master": {
      "AccountId": "123456789012",
      "InvitationId": "7ab938c5d52d7904ad09f9e7c20cc4eb",
      "InvitedAt": 2020-06-01T20:21:18.042000+00:00,
      "MemberStatus": "ASSOCIATED"
   }
}
```

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte GetMasterAccount en la Referencia de comandos de la AWS CLI.

`get-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-members`.

AWS CLI

Para recuperar información sobre las cuentas de miembros seleccionadas

En el siguiente ejemplo de `get-members`, se recupera información sobre las cuentas de miembro especificadas.

```
aws securityhub get-members \
    --account-ids "444455556666" "777788889999"
```

Salida:

```
{
    "Members": [
        {
            "AccountId": "123456789111",
            "AdministratorId": "123456789012",
            "InvitedAt": 2020-06-01T20:15:15.289000+00:00,
            "MasterId": "123456789012",
            "MemberStatus": "ASSOCIATED",
            "UpdatedAt": 2020-06-01T20:15:15.289000+00:00
        },
        {
            "AccountId": "123456789222",
            "AdministratorId": "123456789012",
            "InvitedAt": 2020-06-01T20:15:15.289000+00:00,
            "MasterId": "123456789012",
            "MemberStatus": "ASSOCIATED",
            "UpdatedAt": 2020-06-01T20:15:15.289000+00:00
        }
    ],
    "UnprocessedAccounts": [ ]
}
```

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener detalles sobre la API, consulte GetMembers en la Referencia de comandos de la AWS CLI.

`get-security-control-definition`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-security-control-definition`.

AWS CLI

Para obtener los detalles de la definición de control de seguridad

En el siguiente ejemplo de `get-security-control-definition`, se recuperan los detalles de la definición de un control de seguridad de Security Hub. Los detalles incluyen el título del control, la descripción, la disponibilidad regional, los parámetros y otra información.

```
aws securityhub get-security-control-definition \
    --security-control-id ACM.1
```

Salida:

```
{
    "SecurityControlDefinition": {
        "SecurityControlId": "ACM.1",
        "Title": "Imported and ACM-issued certificates should be renewed after a
 specified time period",
        "Description": "This control checks whether an AWS Certificate Manager
 (ACM) certificate is renewed within the specified time period. It checks both
 imported certificates and certificates provided by ACM. The control fails if the
 certificate isn't renewed within the specified time period. Unless you provide a
 custom parameter value for the renewal period, Security Hub uses a default value of
 30 days.",
        "RemediationUrl": "https://docs.aws.amazon.com/console/securityhub/ACM.1/
remediation",
        "SeverityRating": "MEDIUM",
        "CurrentRegionAvailability": "AVAILABLE",
        "ParameterDefinitions": {
            "daysToExpiration": {
                "Description": "Number of days within which the ACM certificate must
 be renewed",
                "ConfigurationOptions": {
                    "Integer": {
                        "DefaultValue": 30,
                        "Min": 14,
                        "Max": 365
                    }
```

```
                }
            }
        }
    }
}
```

Para obtener más información, consulte Personalización de parámetros de control en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte GetSecurityControlDefinition en la Referencia de comandos de la AWS CLI.

`invite-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `invite-members`.

AWS CLI

Para enviar invitaciones a las cuentas de miembros

En el siguiente ejemplo de `invite-members`, se envían invitaciones a las cuentas de miembro especificadas.

```
aws securityhub invite-members \
    --account-ids "123456789111" "123456789222"
```

Salida:

```
{
    "UnprocessedAccounts": []
}
```

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener más información sobre la API, consulte InviteMembers en la Referencia de comandos de la AWS CLI.

`list-automation-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-automation-rules`.

AWS CLI

Para ver una lista de reglas de automatización

En el siguiente ejemplo de `list-automation-rules`, se enumeran las reglas de automatización de una cuenta de AWS. Solo la cuenta de administrador de Security Hub puede ejecutar este comando.

```
aws securityhub list-automation-rules \
    --max-results 3 \
    --next-token NULL
```

Salida:

```
{
    "AutomationRulesMetadata": [
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-rule/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "RuleStatus": "ENABLED",
            "RuleOrder": 1,
            "RuleName": "Suppress informational findings",
            "Description": "Suppress GuardDuty findings with Informational
 severity",
            "IsTerminal": false,
            "CreatedAt": "2023-05-31T17:56:14.837000+00:00",
            "UpdatedAt": "2023-05-31T17:59:38.466000+00:00",
            "CreatedBy": "arn:aws:iam::123456789012:role/Admin"
        },
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-rule/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "RuleStatus": "ENABLED",
            "RuleOrder": 1,
            "RuleName": "sample rule",
            "Description": "A sample rule",
            "IsTerminal": false,
            "CreatedAt": "2023-07-15T23:37:20.223000+00:00",
            "UpdatedAt": "2023-07-15T23:37:20.223000+00:00",
            "CreatedBy": "arn:aws:iam::123456789012:role/Admin"
        },
        {
```

```
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-rule/
a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "RuleStatus": "ENABLED",
            "RuleOrder": 1,
            "RuleName": "sample rule",
            "Description": "A sample rule",
            "IsTerminal": false,
            "CreatedAt": "2023-07-15T23:45:25.126000+00:00",
            "UpdatedAt": "2023-07-15T23:45:25.126000+00:00",
            "CreatedBy": "arn:aws:iam::123456789012:role/Admin"
        }
    ]
}
```

Para obtener más información, consulte Visualización de las reglas de automatización en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte ListAutomationRules en la Referencia de comandos de la AWS CLI.

`list-configuration-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-configuration-policies`.

AWS CLI

Para enumerar los resúmenes de las políticas de configuración

En el siguiente ejemplo de `list-configuration-policies`, se enumera un resumen de las políticas de configuración de la organización.

```
aws securityhub list-configuration-policies \
    --max-items 3
```

Salida:

```
{
    "ConfigurationPolicySummaries": [
        {
            "Arn": "arn:aws:securityhub:eu-central-1:123456789012:configuration-
policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
            "Name": "SampleConfigurationPolicy1",
            "Description": "SampleDescription1",
            "UpdatedAt": "2023-09-26T21:08:36.214000+00:00",
            "ServiceEnabled": true
        },
        {
            "Arn": "arn:aws:securityhub:eu-central-1:123456789012:configuration-
policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "Name": "SampleConfigurationPolicy2",
            "Description": "SampleDescription2"
            "UpdatedAt": "2023-11-28T19:26:25.207000+00:00",
            "ServiceEnabled": true
        },
        {
            "Arn": "arn:aws:securityhub:eu-central-1:123456789012:configuration-
policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "Name": "SampleConfigurationPolicy3",
            "Description": "SampleDescription3",
            "UpdatedAt": "2023-11-28T20:28:04.494000+00:00",
            "ServiceEnabled": true
        }
}
```

Para obtener más información, consulte Viewing Security Hub configuration policies en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte ListConfigurationPolicies en la Referencia de comandos de la AWS CLI.

`list-configuration-policy-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-configuration-policy-associations`.

AWS CLI

Para enumerar las asociaciones de configuración

En el siguiente ejemplo de `list-configuration-policy-associations`, se enumera un resumen de las asociaciones de configuración de la organización. La respuesta incluye asociaciones con políticas de configuración y el comportamiento autoadministrado.

```
aws securityhub list-configuration-policy-associations \
    --filters '{"AssociationType": "APPLIED"}' \
    --max-items 4
```

Salida:

```
{
    "ConfigurationPolicyAssociationSummaries": [
        {
            "ConfigurationPolicyId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "TargetId": "r-1ab2",
            "TargetType": "ROOT",
            "AssociationType": "APPLIED",
            "UpdatedAt": "2023-11-28T19:26:49.417000+00:00",
            "AssociationStatus": "FAILED",
            "AssociationStatusMessage": "Policy association failed because 2
 organizational units or accounts under this root failed."
        },
        {
            "ConfigurationPolicyId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "TargetId": "ou-1ab2-c3de4f5g",
            "TargetType": "ORGANIZATIONAL_UNIT",
            "AssociationType": "APPLIED",
            "UpdatedAt": "2023-09-26T21:14:05.283000+00:00",
            "AssociationStatus": "FAILED",
            "AssociationStatusMessage": "One or more children under this target
 failed association."
        },
        {
            "ConfigurationPolicyId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
            "TargetId": "ou-6hi7-8j91kl2m",
            "TargetType": "ORGANIZATIONAL_UNIT",
            "AssociationType": "APPLIED",
            "UpdatedAt": "2023-09-26T21:13:01.816000+00:00",
            "AssociationStatus": "SUCCESS",
            "AssociationStatusMessage": "Association applied successfully on this
 target."
        },
        {
            "ConfigurationPolicyId": "SELF_MANAGED_SECURITY_HUB",
            "TargetId": "111122223333",
            "TargetType": "ACCOUNT",
            "AssociationType": "APPLIED",
```

```
            "UpdatedAt": "2023-11-28T22:01:26.409000+00:00",
            "AssociationStatus": "SUCCESS"
    }
}
```

Para obtener más información, consulte Visualización de los detalles y el estado de la política de configuración en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte ListConfigurationPolicyAssociations en la Referencia de comandos de la AWS CLI.

`list-enabled-products-for-import`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-enabled-products-for-import`.

AWS CLI

Para devolver la lista de integraciones de productos habilitadas

En el siguiente ejemplo de `list-enabled-products-for-import`, se devuelve la lista de ARN de suscripción para las integraciones de productos habilitadas actualmente.

```
aws securityhub list-enabled-products-for-import
```

Salida:

```
{
    "ProductSubscriptions": [ "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/crowdstrike-falcon", "arn:aws:securityhub:us-west-1:123456789012:product-subscription/aws/securityhub" ]
}
```

Para obtener más información, consulte Comprensión de las integraciones en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte ListEnabledProductsForImport en la Referencia de comandos de la AWS CLI.

`list-finding-aggregators`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-finding-aggregators`.

AWS CLI

Para enumerar los widgets disponibles

En el siguiente ejemplo de `list-finding-aggregators`, se devuelve el ARN de la configuración de agregación de resultados.

```
aws securityhub list-finding-aggregators
```

Salida:

```
{
    "FindingAggregatorArn": "arn:aws:securityhub:us-east-1:222222222222:finding-
aggregator/123e4567-e89b-12d3-a456-426652340000"
}
```

Para obtener más información, consulte Visualización de la configuración de agregación en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte ListFindingAggregators en la Referencia de comandos de la AWS CLI.

`list-invitations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-invitations`.

AWS CLI

Para mostrar una lista de invitaciones

En el siguiente ejemplo de `list-invitations`, se recupera la lista de invitaciones enviadas a la cuenta solicitante.

```
aws securityhub list-invitations
```

Salida:

```
{
    "Invitations": [
        {
            "AccountId": "123456789012",
            "InvitationId": "7ab938c5d52d7904ad09f9e7c20cc4eb",
            "InvitedAt": 2020-06-01T20:21:18.042000+00:00,
            "MemberStatus": "ASSOCIATED"
        }
    ],
}
```

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener detalles sobre la API, consulte ListInvitations en la Referencia de comandos de la AWS CLI.

`list-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-members`.

AWS CLI

Para recuperar una lista de cuentas de miembros

En el siguiente ejemplo de `list-members`, se devuelve la lista de cuentas miembro para la cuenta de administrador solicitante.

```
aws securityhub list-members
```

Salida:

```
{
    "Members": [
        {
            "AccountId": "123456789111",
            "AdministratorId": "123456789012",
            "InvitedAt": 2020-06-01T20:15:15.289000+00:00,
            "MasterId": "123456789012",
            "MemberStatus": "ASSOCIATED",
            "UpdatedAt": 2020-06-01T20:15:15.289000+00:00
```

```
        },
        {
            "AccountId": "123456789222",
            "AdministratorId": "123456789012",
            "InvitedAt": 2020-06-01T20:15:15.289000+00:00,
            "MasterId": "123456789012",
            "MemberStatus": "ASSOCIATED",
            "UpdatedAt": 2020-06-01T20:15:15.289000+00:00
        }
    ],
}
```

Para obtener información, consulte Administración de cuentas de administrador y de miembro en Security Hub en la Guía del usuario de AWS Security Hub.

- Para obtener detalles sobre la API, consulte ListMembers en la Referencia de comandos de la AWS CLI.

`list-organization-admin-accounts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-organization-admin-accounts`.

AWS CLI

Para enumerar las cuentas de administrador de Security Hub

En el siguiente ejemplo de `list-organization-admin-accounts`, se enumeran las cuentas de administrador de Security Hub para una organización.

```
aws securityhub list-organization-admin-accounts
```

Salida:

```
{
    AdminAccounts": [
        { "AccountId": "777788889999" },
        { "Status": "ENABLED" }
    ]
}
```

Para obtener obtener más información, consulte Integración de Security Hub con AWS Organizations en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte ListOrganizationAdminAccounts en la Referencia de comandos de la AWS CLI.

`list-security-control-definitions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-security-control-definitions`.

AWS CLI

Ejemplo 1: lista de todos los controles de seguridad disponibles

En el siguiente ejemplo de `list-security-control-definitions`, se enumeran los controles de seguridad disponibles en todos los estándares de Security Hub. En este ejemplo, los resultados se limitan a tres controles.

```
aws securityhub list-security-control-definitions \
    --max-items 3
```

Salida:

```
{
    "SecurityControlDefinitions": [
        {
            "SecurityControlId": "ACM.1",
            "Title": "Imported and ACM-issued certificates should be renewed after a
 specified time period",
            "Description": "This control checks whether an AWS Certificate Manager
 (ACM) certificate is renewed within the specified time period. It checks both
 imported certificates and certificates provided by ACM. The control fails if the
 certificate isn't renewed within the specified time period. Unless you provide a
 custom parameter value for the renewal period, Security Hub uses a default value of
 30 days.",
            "RemediationUrl": "https://docs.aws.amazon.com/console/securityhub/
ACM.1/remediation",
            "SeverityRating": "MEDIUM",
            "CurrentRegionAvailability": "AVAILABLE",
            "CustomizableProperties": [
                "Parameters"
```

```
            ]
        },
        {
            "SecurityControlId": "ACM.2",
            "Title": "RSA certificates managed by ACM should use a key length of at
 least 2,048 bits",
            "Description": "This control checks whether RSA certificates managed by
 AWS Certificate Manager use a key length of at least 2,048 bits. The control fails
 if the key length is smaller than 2,048 bits.",
            "RemediationUrl": "https://docs.aws.amazon.com/console/securityhub/
ACM.2/remediation",
            "SeverityRating": "HIGH",
            "CurrentRegionAvailability": "AVAILABLE",
            "CustomizableProperties": []
        },
        {
            "SecurityControlId": "APIGateway.1",
            "Title": "API Gateway REST and WebSocket API execution logging should be
 enabled",
            "Description": "This control checks whether all stages of an Amazon
 API Gateway REST or WebSocket API have logging enabled. The control fails if
 the 'loggingLevel' isn't 'ERROR' or 'INFO' for all stages of the API. Unless you
 provide custom parameter values to indicate that a specific log type should be
 enabled, Security Hub produces a passed finding if the logging level is either
 'ERROR' or 'INFO'.",
            "RemediationUrl": "https://docs.aws.amazon.com/console/securityhub/
APIGateway.1/remediation",
            "SeverityRating": "MEDIUM",
            "CurrentRegionAvailability": "AVAILABLE",
            "CustomizableProperties": [
                "Parameters"
            ]
        }
    ],
    "NextToken": "U2FsdGVkX1/UprCPzxVbkDeHikDXbDxfgJZ1w2RG1XWsFPTMTIQPVE0m/
FduIGxS7ObRtAbaUt/8/RCQcg2PU0YXI20hH/GrhoOTgv+TSm0qvQVFhkJepWmqh
+NYawjocVBeos6xzn/8qnbF9IuwGg=="
}
```

Para obtener más información sobre este estándar, consulte Visualización de los detalles de un estándar en la Guía del usuario de AWS Security Hub.

Ejemplo 2: lista de los controles de seguridad disponibles para un estándar específico

En el siguiente ejemplo de `list-security-control-definitions`, se enumeran los controles de seguridad disponibles para CIS AWS Foundations Benchmark versión 1.4.0. En este ejemplo, los resultados se limitan a tres controles.

```
aws securityhub list-security-control-definitions \
    --standards-arn "arn:aws:securityhub:us-east-1::standards/cis-aws-foundations-benchmark/v/1.4.0" \
    --max-items 3
```

Salida:

```
{
    "SecurityControlDefinitions": [
        {
            "SecurityControlId": "CloudTrail.1",
            "Title": "CloudTrail should be enabled and configured with at least one multi-Region trail that includes read and write management events",
            "Description": "This AWS control checks that there is at least one multi-region AWS CloudTrail trail includes read and write management events.",
            "RemediationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.1/remediation",
            "SeverityRating": "HIGH",
            "CurrentRegionAvailability": "AVAILABLE",
            "CustomizableProperties": []
        },
        {
            "SecurityControlId": "CloudTrail.2",
            "Title": "CloudTrail should have encryption at-rest enabled",
            "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
            "RemediationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation",
            "SeverityRating": "MEDIUM",
            "CurrentRegionAvailability": "AVAILABLE",
            "CustomizableProperties": []
        },
        {
            "SecurityControlId": "CloudTrail.4",
            "Title": "CloudTrail log file validation should be enabled",
            "Description": "This AWS control checks whether CloudTrail log file validation is enabled.",
```

```
            "RemediationUrl": "https://docs.aws.amazon.com/console/securityhub/
CloudTrail.4/remediation",
            "SeverityRating": "MEDIUM",
            "CurrentRegionAvailability": "AVAILABLE",
            "CustomizableProperties": []
        }
    ],
    "NextToken": "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAzfQ=="
}
```

Para obtener más información sobre este estándar, consulte Visualización de los detalles de un estándar en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte ListSecurityControlDefinitions en la Referencia de comandos de la AWS CLI.

`list-standards-control-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-standards-control-associations`.

AWS CLI

Para obtener el estado de habilitación de un control en los estándares habilitados

En el siguiente ejemplo de `list-standards-control-associations`, se enumera el estado de activación de CloudTrail.1 en cada estándar habilitado.

```
aws securityhub list-standards-control-associations \
    --security-control-id CloudTrail.1
```

Salida:

```
{
    "StandardsControlAssociationSummaries": [
        {
            "StandardsArn": "arn:aws:securityhub:us-east-2::standards/nist-800-53/
v/5.0.0",
            "SecurityControlId": "CloudTrail.1",
            "SecurityControlArn": "arn:aws:securityhub:us-
east-2:123456789012:security-control/CloudTrail.1",
            "AssociationStatus": "ENABLED",
```

```
            "RelatedRequirements": [
                "NIST.800-53.r5 AC-2(4)",
                "NIST.800-53.r5 AC-4(26)",
                "NIST.800-53.r5 AC-6(9)",
                "NIST.800-53.r5 AU-10",
                "NIST.800-53.r5 AU-12",
                "NIST.800-53.r5 AU-2",
                "NIST.800-53.r5 AU-3",
                "NIST.800-53.r5 AU-6(3)",
                "NIST.800-53.r5 AU-6(4)",
                "NIST.800-53.r5 AU-14(1)",
                "NIST.800-53.r5 CA-7",
                "NIST.800-53.r5 SC-7(9)",
                "NIST.800-53.r5 SI-3(8)",
                "NIST.800-53.r5 SI-4(20)",
                "NIST.800-53.r5 SI-7(8)",
                "NIST.800-53.r5 SA-8(22)"
            ],
            "UpdatedAt": "2023-05-15T17:52:21.304000+00:00",
            "StandardsControlTitle": "CloudTrail should be enabled and configured
 with at least one multi-Region trail that includes read and write management
 events",
            "StandardsControlDescription": "This AWS control checks that there is
 at least one multi-region AWS CloudTrail trail includes read and write management
 events."
        },
        {
            "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0",
            "SecurityControlId": "CloudTrail.1",
            "SecurityControlArn": "arn:aws:securityhub:us-
east-2:123456789012:security-control/CloudTrail.1",
            "AssociationStatus": "ENABLED",
            "RelatedRequirements": [
                "CIS AWS Foundations 2.1"
            ],
            "UpdatedAt": "2020-02-10T21:22:53.998000+00:00",
            "StandardsControlTitle": "Ensure CloudTrail is enabled in all regions",
            "StandardsControlDescription": "AWS CloudTrail is a web service that
 records AWS API calls for your account and delivers log files to you. The recorded
 information includes the identity of the API caller, the time of the API call,
 the source IP address of the API caller, the request parameters, and the response
 elements returned by the AWS service."
        },
```

```
        {
            "StandardsArn": "arn:aws:securityhub:us-east-2::standards/aws-
foundational-security-best-practices/v/1.0.0",
            "SecurityControlId": "CloudTrail.1",
            "SecurityControlArn": "arn:aws:securityhub:us-
east-2:123456789012:security-control/CloudTrail.1",
            "AssociationStatus": "DISABLED",
            "RelatedRequirements": [],
            "UpdatedAt": "2023-05-15T19:31:52.671000+00:00",
            "UpdatedReason": "Alternative compensating controls are in place",
            "StandardsControlTitle": "CloudTrail should be enabled and configured
 with at least one multi-Region trail that includes read and write management
 events",
            "StandardsControlDescription": "This AWS control checks that there is
 at least one multi-region AWS CloudTrail trail includes read and write management
 events."
        },
        {
            "StandardsArn": "arn:aws:securityhub:us-east-2::standards/cis-aws-
foundations-benchmark/v/1.4.0",
            "SecurityControlId": "CloudTrail.1",
            "SecurityControlArn": "arn:aws:securityhub:us-
east-2:123456789012:security-control/CloudTrail.1",
            "AssociationStatus": "ENABLED",
            "RelatedRequirements": [
                "CIS AWS Foundations Benchmark v1.4.0/3.1"
            ],
            "UpdatedAt": "2022-11-10T15:40:36.021000+00:00",
            "StandardsControlTitle": "Ensure CloudTrail is enabled in all regions",
            "StandardsControlDescription": "AWS CloudTrail is a web service that
 records AWS API calls for your account and delivers log files to you. The recorded
 information includes the identity of the API caller, the time of the API call,
 the source IP address of the API caller, the request parameters, and the response
 elements returned by the AWS service. CloudTrail provides a history of AWS API
 calls for an account, including API calls made via the Management Console, SDKs,
 command line tools, and higher-level AWS services (such as CloudFormation)."
        }
    ]
}
```

Para obtener más información, consulte Habilitación de un control en un estándar específico en la Guía del usuario AWS de Security Hub.

- Para obtener información sobre la API, consulte ListStandardsControlAssociations en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para recuperar las etiquetas asignadas a un recurso

En el ejemplo siguiente de `list-tags-for-resource`, se devuelven las etiquetas asignadas al recurso de hub especificado.

```
aws securityhub list-tags-for-resource \
    --resource-arn "arn:aws:securityhub:us-west-1:123456789012:hub/default"
```

Salida:

```
{
    "Tags": {
        "Department" : "Operations",
        "Area" : "USMidwest"
    }
}
```

Para obtener más información, consulte AWS::SecurityHub::Hub en la Guía del usuario de AWS CloudFormation.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`start-configuration-policy-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-configuration-policy-association`.

AWS CLI

Ejemplo 1: desasociación de una política de configuración

En el siguiente ejemplo de `start-configuration-policy-association`, se asocia la política de configuración especificada a la unidad organizativa indicada. Una configuración puede estar asociada a una cuenta de destino, a una unidad organizativa o a la raíz.

```
aws securityhub start-configuration-policy-association \
    --configuration-policy-identifier "arn:aws:securityhub:eu-
central-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333" \
    --target '{"OrganizationalUnitId": "ou-6hi7-8j91kl2m"}'
```

Salida:

```
{
    "ConfigurationPolicyId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "TargetId": "ou-6hi7-8j91kl2m",
    "TargetType": "ORGANIZATIONAL_UNIT",
    "AssociationType": "APPLIED",
    "UpdatedAt": "2023-11-29T17:40:52.468000+00:00",
    "AssociationStatus": "PENDING"
}
```

Para obtener más información, consulte Usar EventBridge para la respuesta y la corrección automatizadas en la Guía del usuario AWS de Security Hub.

Ejemplo 2: asociación de una configuración autoadministrada

En el siguiente ejemplo de `start-configuration-policy-association`, se asocia una configuración autoadministrada a la cuenta especificada.

```
aws securityhub start-configuration-policy-association \
    --configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
    --target '{"OrganizationalUnitId": "123456789012"}'
```

Salida:

```
{
    "ConfigurationPolicyId": "SELF_MANAGED_SECURITY_HUB",
    "TargetId": "123456789012",
    "TargetType": "ACCOUNT",
    "AssociationType": "APPLIED",
    "UpdatedAt": "2023-11-29T17:40:52.468000+00:00",
    "AssociationStatus": "PENDING"
```

```
}
```

Para obtener más información, consulte Usar EventBridge para la respuesta y la corrección automatizadas en la Guía del usuario AWS de Security Hub.

- Para obtener detalles sobre la API, consulte StartConfigurationPolicyAssociation en la Referencia de comandos de la AWS CLI.

`start-configuration-policy-disassociation`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-configuration-policy-disassociation`.

AWS CLI

Ejemplo 1: desasociación de una política de configuración

En el siguiente ejemplo de `start-configuration-policy-disassociation`, se desvincula la política de configuración de la unidad organizativa indicada. Una configuración se puede desasociar de una cuenta de destino, una unidad organizativa o a la raíz.

```
aws securityhub start-configuration-policy-disassociation \
    --configuration-policy-identifier "arn:aws:securityhub:eu-central-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333" \
    --target '{"OrganizationalUnitId": "ou-6hi7-8j91kl2m"}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de políticas de configuración en la Guía del usuario de AWS Security Hub.

Ejemplo 2: asociación de una configuración autoadministrada

En el siguiente ejemplo de `start-configuration-policy-disassociation`, se desvincula una configuración autoadministrada de la cuenta especificada.

```
aws securityhub start-configuration-policy-disassociation \
    --configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
    --target '{"AccountId": "123456789012"}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminación de políticas de configuración en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte StartConfigurationPolicyDisassociation en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para asociar una etiqueta a un recurso

En el ejemplo siguiente de `tag-resource`, se asignan los valores de las etiquetas Department y Area al recurso de hub especificado.

```
aws securityhub tag-resource \
    --resource-arn "arn:aws:securityhub:us-west-1:123456789012:hub/default" \
    --tags '{"Department":"Operations", "Area":"USMidwest"}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte AWS::SecurityHub::Hub en la Guía del usuario de AWS CloudFormation.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar un valor de etiqueta de un recurso

En el siguiente ejemplo de `untag-resource`, se elimina una etiqueta Department de un recurso de hub especificado.

```
aws securityhub untag-resource \
```

```
    --resource-arn "arn:aws:securityhub:us-west-1:123456789012:hub/default" \
    --tag-keys "Department"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte AWS::SecurityHub::Hub en la Guía del usuario de AWS CloudFormation.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-action-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-action-target`.

AWS CLI

Para actualizar una acción personalizada

En el siguiente ejemplo de `update-action-target`, se actualiza el nombre de la acción personalizada identificada por el ARN especificado.

```
aws securityhub update-action-target \
    --action-target-arn "arn:aws:securityhub:us-west-1:123456789012:action/custom/
Remediation" \
    --name "Send to remediation"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creating a custom action and associating it with a CloudWatch Events rule en la Guía del usuario de AWS Security Hub.

- Para obtener información acerca de la API, consulte UpdateActionTarget en la Referencia de comandos de la AWS CLI.

`update-configuration-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-configuration-policy`.

AWS CLI

Para actualizar una política de configuración

En el siguiente ejemplo de `update-configuration-policy`, se actualiza una política de configuración existente para usar los ajustes especificados.

```
aws securityhub update-configuration-policy \
    --identifier "arn:aws:securityhub:eu-central-1:508236694226:configuration-policy/09f37766-57d8-4ede-9d33-5d8b0fecf70e" \
    --name "SampleConfigurationPolicyUpdated" \
    --description "SampleDescriptionUpdated" \
    --configuration-policy '{"SecurityHub": {"ServiceEnabled": true, "EnabledStandardIdentifiers": ["arn:aws:securityhub:eu-central-1::standards/aws-foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":{"DisabledSecurityControlIdentifiers": ["CloudWatch.1"], "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters": {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 21}}}}]}}}' \
    --updated-reason "Disabling CloudWatch.1 and changing parameter value"
```

Salida:

```
{
    "Arn": "arn:aws:securityhub:eu-central-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "SampleConfigurationPolicyUpdated",
    "Description": "SampleDescriptionUpdated",
    "UpdatedAt": "2023-11-28T20:28:04.494000+00:00",
    "CreatedAt": "2023-11-28T20:28:04.494000+00:00",
    "ConfigurationPolicy": {
        "SecurityHub": {
            "ServiceEnabled": true,
            "EnabledStandardIdentifiers": [
                "arn:aws:securityhub:eu-central-1::standards/aws-foundational-security-best-practices/v/1.0.0",
                "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0"
            ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudWatch.1"
                ],
                "SecurityControlCustomParameters": [
                    {
```

```
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 21
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Para obtener más información, consulte Actualización de las políticas de configuración en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte UpdateConfigurationPolicy en la Referencia de comandos de la AWS CLI.

`update-finding-aggregator`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-finding-aggregator`.

AWS CLI

Para actualizar la configuración de agregación de hallazgos actual

En el siguiente ejemplo de `update-finding-aggregator`, se cambia la configuración de agregación de resultados para vincular desde las regiones seleccionadas. El comando se ejecuta desde la región de agregación, que es Este de EE. UU. (Virginia). Las regiones vinculadas son Oeste de EE. UU. (Norte de California) y Oeste de EE. UU. (Oregón).

```
aws securityhub update-finding-aggregator \
    --region us-east-1 \
    --finding-aggregator-arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 \
    --region-linking-mode SPECIFIED_REGIONS \
    --regions us-west-1,us-west-2
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Actualización de la configuración de agregación entre regiones en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte UpdateFindingAggregator en la Referencia de comandos de la AWS CLI.

`update-insight`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-insight`.

AWS CLI

Ejemplo 1: cambio del filtro para obtener información personalizada

En el siguiente ejemplo de `update-insight`, se cambian los filtros para información personalizada. La información actualizada busca hallazgos de gran gravedad relacionados con los roles de AWS.

```
aws securityhub update-insight \
    --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/
custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
    --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' \
    --name "High severity role findings"
```

Ejemplo 2: cambio del atributo de agrupación para obtener información personalizada

En el siguiente ejemplo de `update-insight`, se cambia el atributo de agrupación de la información personalizada con el ARN especificado. El nuevo atributo de agrupación es el ID del recurso.

```
aws securityhub update-insight \
    --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/
custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
    --group-by-attribute "ResourceId" \
    --name "Critical role findings"
```

Salida:

```
{
```

```
    "Insights": [
        {
            "InsightArn": "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
            "Name": "Critical role findings",
            "Filters": {
                "SeverityLabel": [
                    {
                        "Value": "CRITICAL",
                        "Comparison": "EQUALS"
                    }
                ],
                "ResourceType": [
                    {
                        "Value": "AwsIamRole",
                        "Comparison": "EQUALS"
                    }
                ]
            },
            "GroupByAttribute": "ResourceId"
        }
    ]
}
```

Para obtener más información, consulte Información personalizada en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte UpdateInsight en la Referencia de comandos de la AWS CLI.

`update-organization-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-organization-configuration`.

AWS CLI

Para actualizar cómo se configura Security Hub para una organización

En el siguiente ejemplo de `update-organization-configuration`, se especifica que Security Hub debe usar una configuración central para configurar una organización. Después de ejecutar este comando, el administrador delegado de Security Hub puede crear y administrar

políticas de configuración para configurar la organización. El administrador delegado también puede usar este comando para cambiar de la configuración central a la local. Si el tipo de configuración es local, el administrador delegado puede elegir si activar Security Hub automáticamente y los estándares de seguridad predeterminados en las nuevas cuentas de la organización.

```
aws securityhub update-organization-configuration \
    --no-auto-enable \
    --organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administración de cuentas de administrador y de miembro de Security Hub con AWS Organizations en la Guía del usuario de AWS Security Hub.

- Para obtener detalles sobre la API, consulte UpdateOrganizationConfiguration en la Referencia de comandos de la AWS CLI.

`update-security-control`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-security-control`.

AWS CLI

Para actualizar las propiedades de control de seguridad

En el siguiente ejemplo de `update-security-control`, se especifican valores personalizados para un parámetro de control de seguridad de Security Hub.

```
aws securityhub update-security-control \
    --security-control-id ACM.1 \
    --parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":
 15}}}' \
    --last-update-reason "Internal compliance requirement"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Personalización de parámetros de control en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte UpdateSecurityControl en la Referencia de comandos de la AWS CLI.

`update-security-hub-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-security-hub-configuration`.

AWS CLI

Para actualizar la configuración de Security Hub

En el siguiente ejemplo de `update-security-hub-configuration`, se configura Security Hub para activar automáticamente los nuevos controles para los estándares habilitados.

```
aws securityhub update-security-hub-configuration \
    --auto-enable-controls
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Habilitación automática de nuevos controles en la Guía del usuario de AWS Security Hub.

- Para obtener información sobre la API, consulte UpdateSecurityHubConfiguration en la Referencia de comandos de la AWS CLI.

`update-standards-control`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-standards-control`.

AWS CLI

Ejemplo 1: desactivación de un control

En el siguiente ejemplo de `update-standards-control`, se desactiva el control PCI.AutoScaling.1.

```
aws securityhub update-standards-control \
    --standards-control-arn "arn:aws:securityhub:us-west-1:123456789012:control/pci-dss/v/3.2.1/PCI.AutoScaling.1" \
    --control-status "DISABLED" \
    --disabled-reason "Not applicable for my service"
```

Este comando no genera ninguna salida.

Ejemplo 2: activación de un control

En el siguiente ejemplo de `update-standards-control`, se activa el control PCI.AutoScaling.1.

```
aws securityhub update-standards-control \
    --standards-control-arn "arn:aws:securityhub:us-west-1:123456789012:control/pci-dss/v/3.2.1/PCI.AutoScaling.1" \
    --control-status "ENABLED"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Habilitación de controles en la Guía del usuario AWS de Security Hub.

- Para obtener información sobre la API, consulte UpdateStandardsControl en la Referencia de comandos de la AWS CLI.

Ejemplos de Security Lake que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Security Lake.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-aws-log-source`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-aws-log-source`.

AWS CLI

Para añadir un Amazon Web Service compatible de forma nativa como origen de Amazon Security Lake

En el siguiente ejemplo de `create-aws-logsource`, se agregan registros de flujo de VPC como origen de Security Lake en las cuentas y regiones designadas.

```
aws securitylake create-aws-log-source \
    --sources '[{"regions": ["us-east-1"], "accounts": ["123456789012"],
 "sourceName": "SH_FINDINGS", "sourceVersion": "2.0"}]'
```

Salida:

```
{
    "failed": [
        "123456789012"
    ]
}
```

Para obtener más información, consulte Adding an AWS service as a source en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte CreateAwsLogSource en la Referencia de comandos de la AWS CLI.

`create-custom-log-source`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-custom-log-source`.

AWS CLI

Para añadir un origen personalizado como origen de Amazon Security Lake

En el siguiente ejemplo de `create-custom-logsource`, se agrega un origen personalizado como origen de Security Lake en la cuenta de proveedor de registros y en la región designadas.

```
aws securitylake create-custom-log-source \
    --source-name "VPC_FLOW" \
    --event-classes '["DNS_ACTIVITY", "NETWORK_ACTIVITY"]' \
    --configuration '{"crawlerConfiguration": {"roleArn": "arn:aws:glue:eu-
west-2:123456789012:crawler/E1WG1ZNPRXT0D4"},"providerIdentity": {"principal":
 "029189416600","externalId": "123456789012"}}' --region "us-east-1"
```

Salida:

```
{
    "customLogSource": {
        "attributes": {
            "crawlerArn": "arn:aws:glue:eu-west-2:123456789012:crawler/
E1WG1ZNPRXT0D4",
            "databaseArn": "arn:aws:glue:eu-west-2:123456789012:database/
E1WG1ZNPRXT0D4",
            "tableArn": "arn:aws:glue:eu-west-2:123456789012:table/E1WG1ZNPRXT0D4"
        },
        "provider": {
            "location": "amzn-s3-demo-bucket--usw2-az1--x-s3",
            "roleArn": "arn:aws:iam::123456789012:role/AmazonSecurityLake-Provider-
testCustom2-eu-west-2"
        },
        "sourceName": "testCustom2"
        "sourceVersion": "2.0"
    }
}
```

Para obtener más información, consulte Adding a custom source en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte CreateCustomLogSource en la Referencia de comandos de la AWS CLI.

`create-data-lake-exception-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-data-lake-exception-subscription`.

AWS CLI

Para enviar notificaciones sobre las excepciones de Security Lake

En el siguiente ejemplo de `create-data-lake-exception-subscription`, se envían notificaciones de las excepciones de Security Lake a la cuenta especificada mediante el envío de SMS. El mensaje de excepción permanece durante el período de tiempo especificado.

```
aws securitylake create-data-lake-exception-subscription \
    --notification-endpoint "123456789012" \
    --exception-time-to-live 30 \
```

```
    --subscription-protocol "sms"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Troubleshooting Amazon Security Lake en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte CreateDataLakeExceptionSubscription en la Referencia de comandos de la AWS CLI.

`create-data-lake-organization-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-data-lake-organization-configuration`.

AWS CLI

Para configurar Security Lake en las cuentas nuevas de una organización

En el siguiente ejemplo de `create-data-lake-organization-configuration`, se activa Security Lake y la recopilación de los eventos y registros de origen especificados en las nuevas cuentas de la organización.

```
aws securitylake create-data-lake-organization-configuration \
    --auto-enable-new-account '[{"region":"us-east-1","sources":
[{"sourceName":"SH_FINDINGS","sourceVersion": "1.0"}]}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing multiple accounts with AWS Organizations en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte CreateDataLakeOrganizationConfiguration en la Referencia de comandos de la AWS CLI.

`create-data-lake`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-data-lake`.

AWS CLI

Ejemplo 1: configuración del lago de datos en varias regiones

En el siguiente ejemplo de `create-data-lake`, se habilita Amazon Security Lake en varias regiones de AWS y se configura su lago de datos.

```
aws securitylake create-data-lake \
    --configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","lifecycleConfiguration":
 {"expiration":{"days":365},"transitions":
[{"days":60,"storageClass":"ONEZONE_IA"}]}}, {"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-2","lifecycleConfiguration":
 {"expiration":{"days":365},"transitions":
[{"days":60,"storageClass":"ONEZONE_IA"}]}}]' \
    --meta-store-manager-role-arn "arn:aws:iam:us-east-1:123456789012:role/service-
role/AmazonSecurityLakeMetaStoreManager"
```

Salida:

```
{
    "dataLakes": [
        {
            "createStatus": "COMPLETED",
            "dataLakeArn": "arn:aws:securitylake:us-east-1:522481757177:data-lake/
default",
            "encryptionConfiguration": {
                "kmsKeyId": "S3_MANAGED_KEY"
            },
            "lifecycleConfiguration": {
                "expiration": {
                    "days": 365
                },
                "transitions": [
                    {
                        "days": 60,
                        "storageClass": "ONEZONE_IA"
                    }
                ]
            },
            "region": "us-east-1",
            "replicationConfiguration": {
                "regions": [
                    "ap-northeast-3"
                ],
                "roleArn": "arn:aws:securitylake:ap-northeast-3:522481757177:data-
lake/default"
```

```
            },
            "s3BucketArn": "arn:aws:s3:::aws-security-data-lake-us-east-1-
gnevt6s8z7bzby8oi3uiaysbr8v2ml",
            "updateStatus": {
                "exception": {},
                "requestId": "f20a6450-d24a-4f87-a6be-1d4c075a59c2",
                "status": "INITIALIZED"
            }
        },
        {
            "createStatus": "COMPLETED",
            "dataLakeArn": "arn:aws:securitylake:us-east-2:522481757177:data-lake/
default",
            "encryptionConfiguration": {
                "kmsKeyId": "S3_MANAGED_KEY"
            },
            "lifecycleConfiguration": {
                "expiration": {
                    "days": 365
                },
                "transitions": [
                    {
                        "days": 60,
                        "storageClass": "ONEZONE_IA"
                    }
                ]
            },
            "region": "us-east-2",
            "replicationConfiguration": {
                "regions": [
                    "ap-northeast-3"
                ],
                "roleArn": "arn:aws:securitylake:ap-northeast-3:522481757177:data-
lake/default"
            },
            "s3BucketArn": "arn:aws:s3:::aws-security-data-lake-us-east-2-
cehuifzl5rwmhm6m62h7zhvtseogr9",
            "updateStatus": {
                "exception": {},
                "requestId": "f20a6450-d24a-4f87-a6be-1d4c075a59c2",
                "status": "INITIALIZED"
            }
        }
    ]
```

```
}
```

Para obtener más información, consulte Getting started with Amazon Security Lake en la Guía del usuario de Amazon Security Lake.

Ejemplo 2: configuración del lago de datos en una única región

En el siguiente ejemplo de `create-data-lake`, se habilita Amazon Security Lake en una única región de AWS y se configura su lago de datos.

```
aws securitylake create-data-lake \
    --configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"1234abcd-12ab-34cd-56ef-1234567890ab"},"region":"us-
east-2","lifecycleConfiguration": {"expiration":{"days":500},"transitions":
[{"days":30,"storageClass":"GLACIER"}]}}]' \
    --meta-store-manager-role-arn "arn:aws:iam:us-east-1:123456789012:role/service-
role/AmazonSecurityLakeMetaStoreManager"
```

Salida:

```
{
    "dataLakes": [
        {
            "createStatus": "COMPLETED",
            "dataLakeArn": "arn:aws:securitylake:us-east-2:522481757177:data-lake/
default",
            "encryptionConfiguration": {
                "kmsKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
            },
            "lifecycleConfiguration": {
                "expiration": {
                    "days": 500
                },
                "transitions": [
                    {
                        "days": 30,
                        "storageClass": "GLACIER"
                    }
                ]
            },
            "region": "us-east-2",
            "replicationConfiguration": {
```

```
                "regions": [
                    "ap-northeast-3"
                ],
                "roleArn": "arn:aws:securitylake:ap-northeast-3:522481757177:data-
lake/default"
            },
            "s3BucketArn": "arn:aws:s3:::aws-security-data-lake-us-east-2-
cehuifzl5rwmhm6m62h7zhvtseogr9",
            "updateStatus": {
                "exception": {},
                "requestId": "77702a53-dcbf-493e-b8ef-518e362f3003",
                "status": "INITIALIZED"
            }
        }
    ]
}
```

Para obtener más información, consulte Getting started with Amazon Security Lake en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte CreateDataLake en la Referencia de comandos de la AWS CLI.

`create-subscriber-notification`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-subscriber-notification`.

AWS CLI

Para crear una notificación para el suscriptor

En el siguiente ejemplo de `create-subscriber-notification`, se muestra cómo especificar una notificación para el suscriptor para crear una notificación cuando se escriban nuevos datos en el lago de datos.

```
aws securitylake create-subscriber-notification \
    --subscriber-id "12345ab8-1a34-1c34-1bd4-12345ab9012" \
    --configuration '{"httpsNotificationConfiguration":
 {"targetRoleArn":"arn:aws:iam::XXX:role/service-role/RoleName",
 "endpoint":"https://account-management.$3.$2.securitylake.aws.dev/v1/datalake"}}'
```

Salida:

```
{
    "subscriberEndpoint": [
        "https://account-management.$3.$2.securitylake.aws.dev/v1/datalake"
    ]
}
```

Para obtener más información, consulte Subscriber management en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte CreateSubscriberNotification en la Referencia de comandos de la AWS CLI.

`create-subscriber`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-subscriber`.

AWS CLI

Ejemplo 1: creación de un suscriptor con acceso de datos

En el siguiente ejemplo de `create-subscriber`, se crea un suscriptor en Security Lake con acceso a los datos de la región de AWS actual para la identidad de suscriptor especificada para un origen de AWS.

```
aws securitylake create-subscriber \
    --access-types "S3" \
    --sources '[{"awsLogSource": {"sourceName": "VPC_FLOW","sourceVersion":
 "2.0"}}]' \
    --subscriber-name 'opensearch-s3' \
    --subscriber-identity '{"principal": "029189416600","externalId":
 "123456789012"}'
```

Salida:

```
{
    "subscriber": {
        "accessTypes": [
            "S3"
        ],
        "createdAt": "2024-07-17T19:08:26.787000+00:00",
```

```
        "roleArn": "arn:aws:iam::773172568199:role/AmazonSecurityLake-896f218b-
cfba-40be-a255-8b49a65d0407",
        "s3BucketArn": "arn:aws:s3:::aws-security-data-lake-us-east-1-
um632ufwpvxkyz0bc5hkb64atycnf3",
        "sources": [
            {
                "awsLogSource": {
                    "sourceName": "VPC_FLOW",
                    "sourceVersion": "2.0"
                }
            }
        ],
        "subscriberArn": "arn:aws:securitylake:us-
east-1:773172568199:subscriber/896f218b-cfba-40be-a255-8b49a65d0407",
        "subscriberId": "896f218b-cfba-40be-a255-8b49a65d0407",
        "subscriberIdentity": {
            "externalId": "123456789012",
            "principal": "029189416600"
        },
        "subscriberName": "opensearch-s3",
        "subscriberStatus": "ACTIVE",
        "updatedAt": "2024-07-17T19:08:27.133000+00:00"
    }
}
```

Para obtener más información, consulte Creating a subscriber with data access en la Guía del usuario de Amazon Security Lake.

Ejemplo 2: creación de un suscriptor con acceso de consulta

En el siguiente ejemplo de `create-subscriber`, se crea un suscriptor en Security Lake con acceso de consulta en la región de AWS actual para la identidad de suscriptor especificada.

```
aws securitylake create-subscriber \
    --access-types "LAKEFORMATION" \
    --sources '[{"awsLogSource": {"sourceName": "VPC_FLOW","sourceVersion":
 "2.0"}}]' \
    --subscriber-name 'opensearch-s3' \
    --subscriber-identity '{"principal": "029189416600","externalId":
 "123456789012"}'
```

Salida:

```
{
    "subscriber": {
        "accessTypes": [
            "LAKEFORMATION"
        ],
        "createdAt": "2024-07-18T01:05:55.853000+00:00",
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/8c31da49-c224-4f1e-bb12-37ab756d6d8a",
        "resourceShareName": "LakeFormation-V2-NAMENAMENA-123456789012",
        "sources": [
            {
                "awsLogSource": {
                    "sourceName": "VPC_FLOW",
                    "sourceVersion": "2.0"
                }
            }
        ],
        "subscriberArn": "arn:aws:securitylake:us-east-1:123456789012:subscriber/
e762aabb-ce3d-4585-beab-63474597845d",
        "subscriberId": "e762aabb-ce3d-4585-beab-63474597845d",
        "subscriberIdentity": {
            "externalId": "123456789012",
            "principal": "029189416600"
        },
        "subscriberName": "opensearch-s3",
        "subscriberStatus": "ACTIVE",
        "updatedAt": "2024-07-18T01:05:58.393000+00:00"
    }
}
```

Para obtener más información, consulte Creating a subscriber with query access en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte CreateSubscriber en la Referencia de comandos de la AWS CLI.

`delete-aws-log-source`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-aws-log-source`.

AWS CLI

Para eliminar un servicio de AWS compatible de forma nativa

En el siguiente ejemplo de `delete-aws-logsource`, se eliminan registros de flujo de VPC como origen de Security Lake en las cuentas y regiones designadas.

```
aws securitylake delete-aws-log-source \
    --sources '[{"regions": ["us-east-1"], "accounts": ["123456789012"],
 "sourceName": "SH_FINDINGS", "sourceVersion": "2.0"}]'
```

Salida:

```
{
    "failed": [
        "123456789012"
    ]
}
```

Para obtener más información, consulte Removing an AWS service as a source en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte DeleteAwsLogSource en la Referencia de comandos de la AWS CLI.

`delete-custom-log-source`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-custom-log-source`.

AWS CLI

Para eliminar un origen personalizado.

En el siguiente ejemplo de `delete-custom-logsource`, se elimina un origen personalizado en la cuenta de proveedor de registros y la región designadas.

```
aws securitylake delete-custom-log-source \
    --source-name "CustomSourceName"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Deleting a custom source en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte DeleteCustomLogSource en la Referencia de comandos de la AWS CLI.

delete-data-lake-organization-configuration

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-data-lake-organization-configuration`.

AWS CLI

Para detener la recopilación automática de orígenes en las cuentas de los miembros

En el siguiente ejemplo de `delete-data-lake-organization-configuration`, se detiene la recopilación automática de los resultados de AWS Security Hub de las cuentas de los nuevos miembros que se unen a la organización. Solo el administrador delegado de Security Lake puede ejecutar este comando. Impide que las cuentas de los nuevos miembros aporten datos automáticamente al lago de datos.

```
aws securitylake delete-data-lake-organization-configuration \
    --auto-enable-new-account '[{"region":"us-east-1","sources":
[{"sourceName":"SH_FINDINGS"}]}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing multiple accounts with AWS Organizations en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte DeleteDataLakeOrganizationConfiguration en la Referencia de comandos de la AWS CLI.

delete-data-lake

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-data-lake`.

AWS CLI

Para deshabilitar su lago de datos

En el siguiente ejemplo de `delete-data-lake`, se deshabilita el lago de datos en las regiones de AWS especificadas. En las regiones especificadas, los orígenes ya no aportan datos al lago de datos. En el caso de una implementación de Security Lake con AWS Organizations, solo el administrador delegado de Security Lake de la organización puede desactivar Security Lake para las cuentas de la organización.

```
aws securitylake delete-data-lake \
    --regions "ap-northeast-1" "eu-central-1"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Disabling Amazon Security Lake en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte DeleteDataLake en la Referencia de comandos de la AWS CLI.

`delete-subscriber-notification`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-subscriber-notification`.

AWS CLI

Para eliminar una notificación para suscriptores

En el siguiente ejemplo de `delete-subscriber-notification`, se muestra cómo eliminar la notificación para un suscriptor específico de Security Lake.

```
aws securitylake delete-subscriber-notification \
    --subscriber-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Subscriber management en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte DeleteSubscriberNotification en la Referencia de comandos de la AWS CLI.

`delete-subscriber`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-subscriber`.

AWS CLI

Para eliminar un suscriptor

En el siguiente ejemplo de `delete-subscriber`, se muestra cómo eliminar un suscriptor si quiere que deje de consumir datos de Security Lake.

```
aws securitylake delete-subscriber \
    --subscriber-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Subscriber management en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte DeleteSubscriber en la Referencia de comandos de la AWS CLI.

`get-data-lake-exception-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-data-lake-exception-subscription`.

AWS CLI

Para obtener detalles sobre una suscripción de excepción

En el siguiente ejemplo de `get-data-lake-exception-subscription`, se proporcionan detalles sobre una suscripción de excepción a Security Lake. En este ejemplo, se notifica de los errores al usuario de la cuenta de AWS especificada mediante el envío de un SMS. El mensaje de excepción permanece en la cuenta durante el período de tiempo especificado. Una suscripción de excepción notifica un error a un usuario de Security Lake mediante el protocolo preferido del solicitante.

```
aws securitylake get-data-lake-exception-subscription
```

Salida:

```
{
    "exceptionTimeToLive": 30,
    "notificationEndpoint": "123456789012",
    "subscriptionProtocol": "sms"
}
```

Para obtener más información, consulte Troubleshooting data lake status en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte GetDataLakeExceptionSubscription en la Referencia de comandos de la AWS CLI.

`get-data-lake-organization-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-data-lake-organization-configuration`.

AWS CLI

Para obtener detalles sobre la configuración de las nuevas cuentas de la organización

En el siguiente ejemplo de `get-data-lake-organization-configuration`, se recuperan detalles sobre los registros de origen que las nuevas cuentas de la organización enviarán después de incorporarse a Amazon Security Lake.

```
aws securitylake get-data-lake-organization-configuration
```

Salida:

```
{
    "autoEnableNewAccount": [
        {
            "region": "us-east-1",
            "sources": [
                {
                    "sourceName": "VPC_FLOW",
                    "sourceVersion": "1.0"
                },
                {
                    "sourceName": "ROUTE53",
                    "sourceVersion": "1.0"
                },
                {
                    "sourceName": "SH_FINDINGS",
                    "sourceVersion": "1.0"
                }
            ]
        }
```

```
    ]
}
```

Para obtener más información, consulte Managing multiple accounts with AWS Organizations en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte GetDataLakeOrganizationConfiguration en la Referencia de comandos de la AWS CLI.

`get-data-lake-sources`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-data-lake-sources`.

AWS CLI

Para obtener el estado de la recopilación de registros

En el siguiente ejemplo de `get-data-lake-sources`, se obtiene una instantánea de la recopilación de registros de la cuenta especificada en la región de AWS actual. La cuenta tiene Amazon Security Lake activado.

```
aws securitylake get-data-lake-sources \
    --accounts "123456789012"
```

Salida:

```
{
    "dataLakeSources": [
        {
            "account": "123456789012",
            "sourceName": "SH_FINDINGS",
            "sourceStatuses": [
                {
                    "resource": "vpc-1234567890abcdef0",
                    "status": "COLLECTING"
                }
            ]
        },
        {
            "account": "123456789012",
            "sourceName": "VPC_FLOW",
```

```
            "sourceStatuses": [
                {
                    "resource": "vpc-1234567890abcdef0",
                    "status": "NOT_COLLECTING"
                }
            ]
        },
        {
            "account": "123456789012",
            "sourceName": "LAMBDA_EXECUTION",
            "sourceStatuses": [
                {
                    "resource": "vpc-1234567890abcdef0",
                    "status": "COLLECTING"
                }
            ]
        },
        {
            "account": "123456789012",
            "sourceName": "ROUTE53",
            "sourceStatuses": [
                {
                    "resource": "vpc-1234567890abcdef0",
                    "status": "COLLECTING"
                }
            ]
        },
        {
            "account": "123456789012",
            "sourceName": "CLOUD_TRAIL_MGMT",
            "sourceStatuses": [
                {
                    "resource": "vpc-1234567890abcdef0",
                    "status": "COLLECTING"
                }
            ]
        }
    ],
    "dataLakeArn": null
}
```

Para obtener más información, consulte Collecting data from AWS services en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte GetDataLakeSources en la Referencia de comandos de la AWS CLI.

`get-subscriber`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-subscriber`.

AWS CLI

Para recuperar la información de la suscripción

En el siguiente ejemplo de `get-subscriber`, se recupera la información de suscripción del suscriptor de Securiy Lake especificado.

```
aws securitylake get-subscriber \
    --subscriber-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "subscriber": {
        "accessTypes": [
            "LAKEFORMATION"
        ],
        "createdAt": "2024-04-19T15:19:44.421803+00:00",
        "resourceShareArn": "arn:aws:ram:eu-west-2:123456789012:resource-share/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "resourceShareName": "LakeFormation-V3-TKJGBHCKTZ-123456789012",
        "sources": [
            {
                "awsLogSource": {
                    "sourceName": "LAMBDA_EXECUTION",
                    "sourceVersion": "1.0"
                }
            },
            {
                "awsLogSource": {
                    "sourceName": "EKS_AUDIT",
                    "sourceVersion": "2.0"
                }
            },
            {
```

```
                "awsLogSource": {
                    "sourceName": "ROUTE53",
                    "sourceVersion": "1.0"
                }
            },
            {
                "awsLogSource": {
                    "sourceName": "SH_FINDINGS",
                    "sourceVersion": "1.0"
                }
            },
            {
                "awsLogSource": {
                    "sourceName": "VPC_FLOW",
                    "sourceVersion": "1.0"
                }
            },
            {
                "customLogSource": {
                    "attributes": {
                        "crawlerArn": "arn:aws:glue:eu-west-2:123456789012:crawler/
testCustom2",
                        "databaseArn": "arn:aws:glue:eu-
west-2:123456789012:database/amazon_security_lake_glue_db_eu_west_2",
                        "tableArn": "arn:aws:glue:eu-west-2:123456789012:table/
amazon_security_lake_table_eu_west_2_ext_testcustom2"
                    },
                    "provider": {
                        "location": "s3://aws-security-data-lake-eu-
west-2-8ugsus4ztnsfpjbldwbgf4vge98av9/ext/testCustom2/",
                        "roleArn": "arn:aws:iam::123456789012:role/
AmazonSecurityLake-Provider-testCustom2-eu-west-2"
                    },
                    "sourceName": "testCustom2"
                }
            },
            {
                "customLogSource": {
                    "attributes": {
                        "crawlerArn": "arn:aws:glue:eu-west-2:123456789012:crawler/
TestCustom",
                        "databaseArn": "arn:aws:glue:eu-
west-2:123456789012:database/amazon_security_lake_glue_db_eu_west_2",
```

```
                        "tableArn": "arn:aws:glue:eu-west-2:123456789012:table/
amazon_security_lake_table_eu_west_2_ext_testcustom"
                    },
                    "provider": {
                        "location": "s3://aws-security-data-lake-eu-
west-2-8ugsus4ztnsfpjbldwbgf4vge98av9/ext/TestCustom/",
                        "roleArn": "arn:aws:iam::123456789012:role/
AmazonSecurityLake-Provider-TestCustom-eu-west-2"
                    },
                    "sourceName": "TestCustom"
                }
            }
        ],
        "subscriberArn": "arn:aws:securitylake:eu-west-2:123456789012:subscriber/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "subscriberId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "subscriberIdentity": {
            "externalId": "123456789012",
            "principal": "123456789012"
        },
        "subscriberName": "test",
        "subscriberStatus": "ACTIVE",
        "updatedAt": "2024-04-19T15:19:55.230588+00:00"
    }
}
```

Para obtener más información, consulte Subscriber management en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte GetSubscriber en la Referencia de comandos de la AWS CLI.

`list-data-lake-exceptions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-data-lake-exceptions`.

AWS CLI

Para enumerar los problemas que afectan a su lago de datos

En el siguiente ejemplo de `list-data-lake-exceptions`, se enumeran los problemas que han afectado a su lago de datos en los últimos 14 días en las regiones de AWS especificadas.

```
aws securitylake list-data-lake-exceptions \
    --regions "us-east-1" "eu-west-3"
```

Salida:

```
{
    "exceptions": [
        {
            "exception": "The account does not have the required role permissions.
 Update your role permissions to use the new data source version.",
            "region": "us-east-1",
            "timestamp": "2024-02-29T12:24:15.641725+00:00"
        },
        {
            "exception": "The account does not have the required role permissions.
 Update your role permissions to use the new data source version.",
            "region": "eu-west-3",
            "timestamp": "2024-02-29T12:24:15.641725+00:00"
        }
    ]
}
```

Para obtener más información, consulte Troubleshooting Amazon Security Lake en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte ListDataLakeExceptions en la Referencia de comandos de la AWS CLI.

`list-data-lakes`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-data-lakes`.

AWS CLI

Para enumerar el objeto de configuración de Security Lake

En el siguiente ejemplo de `list-data-lakes`, se muestra el objeto de configuración de Amazon Security Lake para la región de AWS especificada. Puede usar este comando para determinar si Security Lake está activado en una o varias regiones especificadas.

```
aws securitylake list-data-lakes \
```

```
    --regions "us-east-1"
```

Salida:

```
{
    "dataLakes": [
        {
            "createStatus": "COMPLETED",
            "dataLakeArn": "arn:aws:securitylake:us-east-1:123456789012:data-lake/
default",
            "encryptionConfiguration": {
                "kmsKeyId": "S3_MANAGED_KEY"
            },
            "lifecycleConfiguration": {
                "expiration": {
                    "days": 365
                },
                "transitions": [
                    {
                        "days": 60,
                        "storageClass": "ONEZONE_IA"
                    }
                ]
            },
            "region": "us-east-1",
            "replicationConfiguration": {
                "regions": [
                    "ap-northeast-3"
                ],
                "roleArn": "arn:aws:securitylake:ap-northeast-3:123456789012:data-
lake/default"
            },
            "s3BucketArn": "arn:aws:s3:::aws-security-data-lake-us-
east-1-1234567890abcdef0",
            "updateStatus": {
                "exception": {
                    "code": "software.amazon.awssdk.services.s3.model.S3Exception",
                    "reason": ""
                },
                "requestId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
                "status": "FAILED"
            }
        }
```

```
    ]
}
```

Para obtener más información, consulte Checking Region status en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte ListDataLakes en la Referencia de comandos de la AWS CLI.

`list-log-sources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-log-sources`.

AWS CLI

Para recuperar los orígenes de registro de Amazon Security Lake

En el siguiente ejemplo de `list-log-sources`, se enumeran los orígenes de registro de Amazon Security Lake en una cuenta específica.

```
aws securitylake list-log-sources \
    --accounts "123456789012"
```

Salida:

```
{
    "account": "123456789012",
    "region": "xy-region-1",
    "sources": [
        {
               "awsLogSource": {
                "sourceName": "VPC_FLOW",
                "sourceVersion": "2.0"
            }
        },
        {
            "awsLogSource": {
                "sourceName": "SH_FINDINGS",
                "sourceVersion": "2.0"
            }
        }
    ]
```

```
}
```

Para obtener más información, consulte Source management en la Guía del usuario de Amazon Security Lake.

- Para obtener detalles de la API, consulte ListLogSources en la Referencia de comandos de la AWS CLI.

`list-subscribers`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-subscribers`.

AWS CLI

Para recuperar los suscriptores de Amazon Security Lake

En el siguiente ejemplo de `list-subscribers`, se enumeran todos los suscriptores de Amazon Security Lake de una cuenta específica.

```
aws securitylake list-subscribers
```

Salida:

```
{
    "subscribers": [
        {
            "accessTypes": [
                "S3"
            ],
            "createdAt": "2024-06-04T15:02:28.921000+00:00",
            "roleArn": "arn:aws:iam::123456789012:role/AmazonSecurityLake-
E1WG1ZNPRXT0D4",
            "s3BucketArn": "amzn-s3-demo-bucket--usw2-az1--x-s3",
            "sources": [
                {
                    "awsLogSource": {
                        "sourceName": "CLOUD_TRAIL_MGMT",
                        "sourceVersion": "2.0"
                    }
                },
                {
                    "awsLogSource": {
                        "sourceName": "LAMBDA_EXECUTION",
```

```
                        "sourceVersion": "1.0"
                    }
                },
                {
                    "customLogSource": {
                        "attributes": {
                            "crawlerArn": "arn:aws:glue:eu-
west-2:123456789012:crawler/E1WG1ZNPRXT0D4",
                            "databaseArn": "arn:aws:glue:eu-
west-2:123456789012:database/E1WG1ZNPRXT0D4",
                            "tableArn": "arn:aws:glue:eu-west-2:123456789012:table/
E1WG1ZNPRXT0D4"
                        },
                        "provider": {
                            "location": "amzn-s3-demo-bucket--usw2-az1--x-s3",
                            "roleArn": "arn:aws:iam::123456789012:role/
AmazonSecurityLake-E1WG1ZNPRXT0D4"
                        },
                        "sourceName": "testCustom2"
                    }
                }
            ],
            "subscriberArn": "arn:aws:securitylake:eu-
west-2:123456789012:subscriber/E1WG1ZNPRXT0D4",
            "subscriberEndpoint": "arn:aws:sqs:eu-
west-2:123456789012:AmazonSecurityLake-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111-Main-
Queue",
            "subscriberId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "subscriberIdentity": {
                "externalId": "ext123456789012",
                "principal": "123456789012"
            },
            "subscriberName": "Test",
            "subscriberStatus": "ACTIVE",
            "updatedAt": "2024-06-04T15:02:35.617000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Subscriber management en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte ListSubscribers en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas para un recurso existente

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran todas las etiquetas del suscriptor de Amazon Security Lake específico. En este ejemplo, la clave de la etiqueta Owner no tiene ningún valor de etiqueta asociado. También puede utilizar esta operación para enumerar las etiquetas de otros recursos de Security Lake existentes.

```
aws securitylake list-tags-for-resource \
    --resource-arn "arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab"
```

Salida:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Cloud"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

Para obtener más información, consulte Tagging Amazon Security Lake resources en la Guía del usuario de Amazon Security Lake.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`register-data-lake-delegated-administrator`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-data-lake-delegated-administrator`.

AWS CLI

Para designar al administrador delegado

En el siguiente ejemplo de `register-data-lake-delegated-administrator`, se designa la cuenta de AWS especificada como administrador de Amazon Security Lake delegado.

```
aws securitylake register-data-lake-delegated-administrator \
    --account-id 123456789012
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing multiple accounts with AWS Organizations en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte RegisterDataLakeDelegatedAdministrator en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para agregar etiquetas a un recurso existente

En el siguiente ejemplo de `tag-resource`, se agregan etiquetas a un recurso de suscriptor existente. Para crear un recurso nuevo y añadirle una o más etiquetas, no utilice esta operación. En su lugar, utilice la operación Create adecuada según el tipo de recurso que desee crear.

```
aws securitylake tag-resource \
    --resource-arn "arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab" \
    --tags key=Environment,value=Cloud
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging Amazon Security Lake resources en la Guía del usuario de Amazon Security Lake.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar etiquetas de un recurso existente

En el siguiente ejemplo de `untag-resource`, se eliminan las etiquetas especificadas de un recurso de suscriptor especificado.

```
aws securitylake untag-resource \
    --resource-arn "arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab" \
    --tags Environment Owner
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging Amazon Security Lake resources en la Guía del usuario de Amazon Security Lake.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-data-lake-exception-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-data-lake-exception-subscription`.

AWS CLI

Para actualizar la suscripción de notificaciones para las excepciones de Security Lake

En el siguiente ejemplo de `update-data-lake-exception-subscription`, se actualiza la suscripción a notificaciones que informa a los usuarios de las excepciones de Security Lake.

```
aws securitylake update-data-lake-exception-subscription \
    --notification-endpoint "123456789012" \
    --exception-time-to-live 30 \
    --subscription-protocol "email"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Troubleshooting Amazon Security Lake en la Guía del usuario de Amazon Security Lake.

- Para obtener información acerca de la API, consulte UpdateDataLakeExceptionSubscription en la Referencia de comandos de la AWS CLI.

`update-data-lake`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-data-lake`.

AWS CLI

Ejemplo 1: actualización de la configuración del lago de datos

En el siguiente ejemplo de `update-data-lake`, se actualiza la configuración de su lago de datos de Amazon Security Lake. Puede utilizar esta operación para especificar la configuración del cifrado de datos, el almacenamiento y la región de acumulación.

```
aws securitylake update-data-lake \
    --configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","lifecycleConfiguration":
 {"expiration":{"days":365},"transitions":
[{"days":60,"storageClass":"ONEZONE_IA"}]}}, {"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-2","lifecycleConfiguration":
 {"expiration":{"days":365},"transitions":
[{"days":60,"storageClass":"ONEZONE_IA"}]}}]' \
    --meta-store-manager-role-arn "arn:aws:iam:us-east-1:123456789012:role/service-
role/AmazonSecurityLakeMetaStoreManager"
```

Salida:

```
{
    "dataLakes": [
        {
            "createStatus": "COMPLETED",
```

```
            "dataLakeArn": "arn:aws:securitylake:us-east-1:522481757177:data-lake/
default",
            "encryptionConfiguration": {
                "kmsKeyId": "S3_MANAGED_KEY"
            },
            "lifecycleConfiguration": {
                "expiration": {
                    "days": 365
                },
                "transitions": [
                    {
                        "days": 60,
                        "storageClass": "ONEZONE_IA"
                    }
                ]
            },
            "region": "us-east-1",
            "replicationConfiguration": {
                "regions": [
                    "ap-northeast-3"
                ],
                "roleArn": "arn:aws:securitylake:ap-northeast-3:522481757177:data-
lake/default"
            },
            "s3BucketArn": "arn:aws:s3:::aws-security-data-lake-us-east-1-
gnevt6s8z7bzby8oi3uiaysbr8v2ml",
            "updateStatus": {
                "exception": {},
                "requestId": "f20a6450-d24a-4f87-a6be-1d4c075a59c2",
                "status": "INITIALIZED"
            }
        },
        {
            "createStatus": "COMPLETED",
            "dataLakeArn": "arn:aws:securitylake:us-east-2:522481757177:data-lake/
default",
            "encryptionConfiguration": {
                "kmsKeyId": "S3_MANAGED_KEY"
            },
            "lifecycleConfiguration": {
                "expiration": {
                    "days": 365
                },
                "transitions": [
```

```
                    {
                        "days": 60,
                        "storageClass": "ONEZONE_IA"
                    }
                ]
            },
            "region": "us-east-2",
            "replicationConfiguration": {
                "regions": [
                    "ap-northeast-3"
                ],
                "roleArn": "arn:aws:securitylake:ap-northeast-3:522481757177:data-
lake/default"
            },
            "s3BucketArn": "arn:aws:s3:::aws-security-data-lake-us-east-2-
cehuifzl5rwmhm6m62h7zhvtseogr9",
            "updateStatus": {
                "exception": {},
                "requestId": "f20a6450-d24a-4f87-a6be-1d4c075a59c2",
                "status": "INITIALIZED"
            }
        }
    ]
}
```

Para obtener más información, consulte Getting started with Amazon Security Lake en la Guía del usuario de Amazon Security Lake.

Ejemplo 2: configuración del lago de datos en una única región

En el siguiente ejemplo de `create-data-lake`, se habilita Amazon Security Lake en una única región de AWS y se configura su lago de datos.

```
aws securitylake create-data-lake \
    --configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"1234abcd-12ab-34cd-56ef-1234567890ab"},"region":"us-
east-2","lifecycleConfiguration": {"expiration":{"days":500},"transitions":
[{"days":30,"storageClass":"GLACIER"}]}}]' \
    --meta-store-manager-role-arn "arn:aws:iam:us-east-1:123456789012:role/service-
role/AmazonSecurityLakeMetaStoreManager"
```

Salida:

```
{
    "dataLakes": [
        {
            "createStatus": "COMPLETED",
            "dataLakeArn": "arn:aws:securitylake:us-east-2:522481757177:data-lake/
default",
            "encryptionConfiguration": {
                "kmsKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
            },
            "lifecycleConfiguration": {
                "expiration": {
                    "days": 500
                },
                "transitions": [
                    {
                        "days": 30,
                        "storageClass": "GLACIER"
                    }
                ]
            },
            "region": "us-east-2",
            "replicationConfiguration": {
                "regions": [
                    "ap-northeast-3"
                ],
                "roleArn": "arn:aws:securitylake:ap-northeast-3:522481757177:data-
lake/default"
            },
            "s3BucketArn": "arn:aws:s3:::aws-security-data-lake-us-east-2-
cehuifzl5rwmhm6m62h7zhvtseogr9",
            "updateStatus": {
                "exception": {},
                "requestId": "77702a53-dcbf-493e-b8ef-518e362f3003",
                "status": "INITIALIZED"
            }
        }
    ]
}
```

Para obtener más información, consulte Getting started with Amazon Security Lake en la Guía del usuario de Amazon Security Lake.

- Para obtener detalles sobre la API, consulte UpdateDataLake en la Referencia de comandos de la AWS CLI.

`update-subscriber-notification`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-subscriber-notification`.

AWS CLI

Para actualizar una notificación de suscriptor

En el siguiente ejemplo de `update-subscriber-notification`, se muestra cómo se puede actualizar el método de notificación de un suscriptor.

```
aws securitylake update-subscriber-notification \
    --subscriber-id "12345ab8-1a34-1c34-1bd4-12345ab9012" \
    --configuration '{"httpsNotificationConfiguration":
 {"targetRoleArn":"arn:aws:iam::XXX:role/service-role/RoleName",
 "endpoint":"https://account-management.$3.$2.securitylake.aws.dev/v1/datalake"}}'
```

Salida:

```
{
    "subscriberEndpoint": [
        "https://account-management.$3.$2.securitylake.aws.dev/v1/datalake"
    ]
}
```

Para obtener más información, consulte Subscriber management en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte UpdateSubscriberNotification en la Referencia de comandos de la AWS CLI.

`update-subscriber`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-subscriber`.

AWS CLI

Para actualizar un suscriptor de Amazon Security Lake.

En el siguiente ejemplo de `update-subscriber`, se actualizan los orígenes de acceso a los datos de Security Lake para un suscriptor de Security Lake específico.

```
aws securitylake update-subscriber \
    --subscriber-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "subscriber": {
        "accessTypes": [
            "LAKEFORMATION"
        ],
        "createdAt": "2024-04-19T15:19:44.421803+00:00",
        "resourceShareArn": "arn:aws:ram:eu-west-2:123456789012:resource-share/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "resourceShareName": "LakeFormation-V3-TKJGBHCKTZ-123456789012",
        "sources": [
            {
                "awsLogSource": {
                    "sourceName": "LAMBDA_EXECUTION",
                    "sourceVersion": "1.0"
                }
            },
            {
                "awsLogSource": {
                    "sourceName": "EKS_AUDIT",
                    "sourceVersion": "2.0"
                }
            },
            {
                "awsLogSource": {
                    "sourceName": "ROUTE53",
                    "sourceVersion": "1.0"
                }
            },
            {
                "awsLogSource": {
                    "sourceName": "SH_FINDINGS",
                    "sourceVersion": "1.0"
                }
            },
            {
```

```
                "awsLogSource": {
                    "sourceName": "VPC_FLOW",
                    "sourceVersion": "1.0"
                }
            },
            {
                "customLogSource": {
                    "attributes": {
                        "crawlerArn": "arn:aws:glue:eu-west-2:123456789012:crawler/
E1WG1ZNPRXT0D4",
                        "databaseArn": "arn:aws:glue:eu-
west-2:123456789012:database/E1WG1ZNPRXT0D4",
                        "tableArn": "arn:aws:glue:eu-west-2:123456789012:table/
E1WG1ZNPRXT0D4"
                    },
                    "provider": {
                        "location": "amzn-s3-demo-bucket--usw2-az1--x-s3",
                        "roleArn": "arn:aws:iam::123456789012:role/
AmazonSecurityLake-E1WG1ZNPRXT0D4"
                    },
                    "sourceName": "testCustom2"
                }
            }
        ],
        "subscriberArn": "arn:aws:securitylake:eu-west-2:123456789012:subscriber/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "subscriberId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "subscriberIdentity": {
            "externalId": "123456789012",
            "principal": "123456789012"
        },
        "subscriberName": "test",
        "subscriberStatus": "ACTIVE",
        "updatedAt": "2024-07-18T20:47:37.098000+00:00"
    }
}
```

Para obtener más información, consulte Subscriber management en la Guía del usuario de Amazon Security Lake.

- Para obtener información sobre la API, consulte UpdateSubscriber en la Referencia de comandos de la AWS CLI.

AWS Serverless Application Repository Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS Serverless Application Repository.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`put-application-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-application-policy`.

AWS CLI

Ejemplo 1: cómo compartir una aplicación públicamente

En el siguiente ejemplo de `put-application-policy`, se comparte una aplicación públicamente, de modo que cualquier persona puede encontrarla e implementarla en Repositorio de aplicaciones sin servidor de AWS.

```
aws serverlessrepo put-application-policy \
    --application-id arn:aws:serverlessrepo:us-east-1:123456789012:applications/my-test-application \
    --statements Principals='*',Actions=Deploy
```

Salida:

```
{
    "Statements": [
        {
            "Actions": [
                "Deploy"
```

```
            ],
            "Principals": [
                ""
            ],
            "StatementId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
        }
    ]
}
```

Ejemplo 2: cómo compartir una aplicación de forma privada

En el siguiente ejemplo de `put-application-policy`, se comparte una aplicación de forma privada, de modo solo cuentas AWS específicas pueden encontrar e implementar su aplicación en Repositorio de aplicaciones sin servidor de AWS.

```
aws serverlessrepo put-application-policy \
    --application-id arn:aws:serverlessrepo:us-east-1:123456789012:applications/my-test-application \
    --statements Principals=111111111111,222222222222,Actions=Deploy
```

Salida:

```
{
    "Statements": [
        {
            "Actions": [
                "Deploy"
            ],
            "Principals": [
                "111111111111",
                "222222222222"
            ],
            "StatementId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
        }
    ]
}
```

Para obtener más información, consulte Sharing an Application Through the Console en la Guía para desarrolladores de Repositorio de aplicaciones sin servidor de AWS.

- Para obtener información sobre la API, consulte PutApplicationPolicy en la Referencia de comandos de la AWS CLI.

Ejemplos de Service Catalog que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Service Catalog.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`accept-portfolio-share`

En el siguiente ejemplo de código, se muestra cómo utilizar `accept-portfolio-share`.

AWS CLI

Para aceptar compartir una cartera

En el siguiente ejemplo de `accept-portfolio-share`, se acepta una oferta, realizada por otro usuario, para compartir la cartera especificada.

```
aws servicecatalog accept-portfolio-share \
    --portfolio-id port-2s6wuabcdefghijk
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte AcceptPortfolioShare en la Referencia de comandos de la AWS CLI.

`associate-principal-with-portfolio`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-principal-with-portfolio`.

AWS CLI

Para asociar una entidad principal a una cartera

En el siguiente ejemplo de `associate-principal-with-portfolio`, se asocia un usuario a la cartera especificada.

```
aws servicecatalog associate-principal-with-portfolio \
    --portfolio-id port-2s6abcdefwdh4 \
    --principal-arn arn:aws:iam::123456789012:user/usertest \
    --principal-type IAM
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte AssociatePrincipalWithPortfolio en la Referencia de comandos de la AWS CLI.

`associate-product-with-portfolio`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-product-with-portfolio`.

AWS CLI

Para asociar un producto a una cartera

En el siguiente ejemplo de `associate-product-with-portfolio`, se asocia un producto determinado a la cartera especificada.

```
aws servicecatalog associate-product-with-portfolio
     --product-id prod-3p5abcdef3oyk
     --portfolio-id port-2s6abcdef5wdh4
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte AssociateProductWithPortfolio en la Referencia de comandos de la AWS CLI.

`associate-tag-option-with-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-tag-option-with-resource`.

AWS CLI

Para asociar una TagOption a un recurso

En el siguiente ejemplo de `associate-tag-option-with-resource`, se asocia la TagOption especificada con el recurso especificado.

```
aws servicecatalog associate-tag-option-with-resource \
    --resource-id port-2s6abcdq5wdh4 \
    --tag-option-id tag-p3abc2pkpz5qc
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte AssociateTagOptionWithResource en la Referencia de comandos de la AWS CLI.

`copy-product`

En el siguiente ejemplo de código, se muestra cómo utilizar `copy-product`.

AWS CLI

Para copiar un producto

En el siguiente ejemplo de `copy-product`, se hace una copia del producto especificado con un archivo JSON para pasar los parámetros.

```
aws servicecatalog copy-product --cli-input-json file://copy-product-input.json
```

Contenido de `copy-product-input.json`:

```
{
    "SourceProductArn": "arn:aws:catalog:us-west-2:123456789012:product/prod-
tcabcd3syn2xy",
    "TargetProductName": "copy-of-myproduct",
    "CopyOptions": [
        "CopyTags"
    ]
}
```

Salida:

```
{
    "CopyProductToken": "copyproduct-abc5defgjkdji"
}
```

- Para obtener información sobre la API, consulte CopyProduct en la Referencia de comandos de la AWS CLI.

`create-portfolio-share`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-portfolio-share`.

AWS CLI

Para compartir una cartera con una cuenta

En el siguiente ejemplo de `create-portfolio-share`, se comparte la cartera especificada con la cuenta especificada.

```
aws servicecatalog create-portfolio-share \
    --portfolio-id port-2s6abcdef5wdh4 \
    --account-id 794123456789
```

Este comando no genera ningún resultado.

- Para obtener información sobre la API, consulte CreatePortfolioShare en la Referencia de comandos de la AWS CLI.

`create-portfolio`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-portfolio`.

AWS CLI

Para crear una cartera

En el siguiente ejemplo de `create-portfolio`, se crea una cartera.

```
aws servicecatalog create-portfolio  \
    --provider-name my-provider \
    --display-name my-portfolio
```

Salida:

```
{
    "PortfolioDetail": {
        "ProviderName": "my-provider",
        "DisplayName": "my-portfolio",
        "CreatedTime": 1571337221.555,
        "ARN": "arn:aws:catalog:us-east-2:123456789012:portfolio/
port-2s6xmplq5wdh4",
        "Id": "port-2s6xmplq5wdh4"
    }
}
```

- Para obtener información sobre la API, consulte CreatePortfolio en la Referencia de comandos de la AWS CLI.

`create-product`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-product`.

AWS CLI

Para crear un producto

En el siguiente ejemplo de `create-product`, se crea un producto con un archivo JSON para pasar los parámetros.

```
aws servicecatalog create-product \
    --cli-input-json file://create-product-input.json
```

Contenido de `create-product-input.json`:

```
{
    "AcceptLanguage": "en",
    "Name": "test-product",
    "Owner": "test-owner",
    "Description": "test-description",
    "Distributor": "test-distributor",
    "SupportDescription": "test-support",
    "SupportEmail": "test@amazon.com",
    "SupportUrl": "https://aws.amazon.com",
```

```
    "ProductType": "CLOUD_FORMATION_TEMPLATE",
    "Tags": [
        {
            "Key": "region",
            "Value": "us-east-1"
        }
    ],
    "ProvisioningArtifactParameters": {
        "Name": "test-version-name",
        "Description": "test-version-description",
        "Info": {
            "LoadTemplateFromURL": "https://s3-us-west-1.amazonaws.com/
cloudformation-templates-us-west-1/my-cfn-template.template"
        },
        "Type": "CLOUD_FORMATION_TEMPLATE"
    }
}
```

Salida:

```
{
    "Tags": [
        {
            "Key": "region",
            "Value": "us-east-1"
        }
    ],
    "ProductViewDetail": {
        "CreatedTime": 1576025036.0,
        "ProductARN": "arn:aws:catalog:us-west-2:1234568542028:product/
prod-3p5abcdef3oyk",
        "Status": "CREATED",
        "ProductViewSummary": {
            "Type": "CLOUD_FORMATION_TEMPLATE",
            "Distributor": "test-distributor",
            "SupportUrl": "https://aws.amazon.com",
            "SupportEmail": "test@amazon.com",
            "Id": "prodview-abcd42wvx45um",
            "SupportDescription": "test-support",
            "ShortDescription": "test-description",
            "Owner": "test-owner",
            "Name": "test-product2",
            "HasDefaultPath": false,
```

```
            "ProductId": "prod-3p5abcdef3oyk"
        }
    },
    "ProvisioningArtifactDetail": {
        "CreatedTime": 1576025036.0,
        "Active": true,
        "Id": "pa-pq3p5lil12a34",
        "Description": "test-version-description",
        "Name": "test-version-name",
        "Type": "CLOUD_FORMATION_TEMPLATE"
    }
}
```

- Para obtener información sobre la API, consulte CreateProduct en la Referencia de comandos de la AWS CLI.

`create-provisioning-artifact`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-provisioning-artifact`.

AWS CLI

Para crear un artefacto de aprovisionamiento

En el siguiente ejemplo de `create-provisioning-artifact`, se crea un artefacto de aprovisionamiento con un archivo JSON para pasar los parámetros.

```
aws servicecatalog create-provisioning-artifact \
   --cli-input-json file://create-provisioning-artifact-input.json
```

Contenido de `create-provisioning-artifact-input.json`:

```
{
    "ProductId": "prod-nfi2abcdefghi",
    "Parameters": {
        "Name": "test-provisioning-artifact",
        "Description": "test description",
        "Info": {
            "LoadTemplateFromURL": "https://s3-us-west-1.amazonaws.com/
cloudformation-templates-us-west-1/my-cfn-template.template"
        },
        "Type": "CLOUD_FORMATION_TEMPLATE"
```

```
    }
}
```

Salida:

```
{
    "Info": {
        "TemplateUrl": "https://s3-us-west-1.amazonaws.com/cloudformation-templates-
us-west-1/my-cfn-template.template"
    },
    "Status": "CREATING",
    "ProvisioningArtifactDetail": {
        "Id": "pa-bb4abcdefwnaio",
        "Name": "test-provisioning-artifact",
        "Description": "test description",
        "Active": true,
        "Type": "CLOUD_FORMATION_TEMPLATE",
        "CreatedTime": 1576022545.0
    }
}
```

- Para obtener información sobre la API, consulte CreateProvisioningArtifact en la Referencia de comandos de la AWS CLI.

`create-tag-option`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-tag-option`.

AWS CLI

Para crear una TagOption

En el siguiente ejemplo de `create-tag-option`, se crea una TagOption.

```
aws servicecatalog create-tag-option
    --key 1234
    --value name
```

Salida:

```
{
```

```
    "TagOptionDetail": {
    "Id": "tag-iabcdn4fzjjms",
    "Value": "name",
    "Active": true,
    "Key": "1234"
    }
}
```

- Para obtener información sobre la API, consulte CreateTagOption en la Referencia de comandos de la AWS CLI.

`delete-portfolio-share`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-portfolio-share`.

AWS CLI

Para dejar de compartir una cartera con una cuenta

En el siguiente ejemplo de `delete-portfolio-share`, se deja de compartir la cartera con la cuenta especificada.

```
aws servicecatalog delete-portfolio-share \
    --portfolio-id port-2s6abcdq5wdh4 \
    --account-id 123456789012
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeletePortfolioShare en la Referencia de comandos de la AWS CLI.

`delete-portfolio`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-portfolio`.

AWS CLI

Para eliminar una cartera

En el siguiente ejemplo de `delete-portfolio`, se elimina la cartera especificada.

```
aws servicecatalog delete-portfolio \
```

```
    --id port-abcdlx4gox4do
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeletePortfolio en la Referencia de comandos de la AWS CLI.

`delete-product`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-product`.

AWS CLI

Para eliminar un producto

En el siguiente ejemplo de `delete-product`, se elimina el producto especificado.

```
aws servicecatalog delete-product \
    --id prod-abcdcek6yhbxi
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteProduct en la Referencia de comandos de la AWS CLI.

`delete-provisioning-artifact`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-provisioning-artifact`.

AWS CLI

Para eliminar un artefacto de aprovisionamiento

En el siguiente ejemplo de `delete-provisioning-artifact`, se elimina el artefacto de aprovisionamiento especificado.

```
aws servicecatalog delete-provisioning-artifact \
    --product-id prod-abc2uebuplcpw \
    --provisioning-artifact-id pa-pqabcddii7ouc
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteProvisioningArtifact en la Referencia de comandos de la AWS CLI.

`delete-tag-option`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-tag-option`.

AWS CLI

Para eliminar una TagOption

En el siguiente ejemplo de `delete-tag-option`, se elimina la TagOption especificada.

```
aws servicecatalog delete-tag-option \
    --id tag-iabcdn4fzjjms
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteTagOption en la Referencia de comandos de la AWS CLI.

`describe-copy-product-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-copy-product-status`.

AWS CLI

Para describir el estado de la operación de copia del producto

En el siguiente ejemplo de `describe-copy-product-status`, se muestra el estado actual de la operación de copia asíncrona del producto especificada.

```
aws servicecatalog describe-copy-product-status \
    --copy-product-token copyproduct-znn5tf5abcd3w
```

Salida:

```
{
    "CopyProductStatus": "SUCCEEDED",
    "TargetProductId": "prod-os6hog7abcdt2"
```

```
}
```

- Para obtener información sobre la API, consulte DescribeCopyProductStatus en la Referencia de comandos de la AWS CLI.

`describe-portfolio`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-portfolio`.

AWS CLI

Para describir una cartera

En el siguiente ejemplo de `describe-portfolio`, se muestran los detalles de la cartera especificada.

```
aws servicecatalog describe-portfolio \
    --id port-2s6abcdq5wdh4
```

Salida:

```
{
    "TagOptions": [],
    "PortfolioDetail": {
        "ARN": "arn:aws:catalog:us-west-2:687558541234:portfolio/
port-2s6abcdq5wdh4",
        "Id": "port-2s6wuzyq5wdh4",
        "CreatedTime": 1571337221.555,
        "DisplayName": "my-portfolio",
        "ProviderName": "my-provider"
    },
    "Tags": []
}
```

- Para obtener información sobre la API, consulte DescribePortfolio en la Referencia de comandos de la AWS CLI.

`describe-product-as-admin`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-product-as-admin`.

AWS CLI

Para describir un producto como administrador

En el siguiente ejemplo de `describe-product-as-admin`, se muestran los detalles del producto especificado mediante los privilegios de administrador.

```
aws servicecatalog describe-product-as-admin \
    --id prod-abcdcek6yhbxi
```

Salida:

```
{
    "TagOptions": [],
    "ProductViewDetail": {
        "ProductARN": "arn:aws:catalog:us-west-2:687558542028:product/prod-
abcdcek6yhbxi",
        "ProductViewSummary": {
            "SupportEmail": "test@amazon.com",
            "Type": "CLOUD_FORMATION_TEMPLATE",
            "Distributor": "test-distributor",
            "ShortDescription": "test-description",
            "Owner": "test-owner",
            "Id": "prodview-wi3l2j4abc6vc",
            "SupportDescription": "test-support",
            "ProductId": "prod-abcdcek6yhbxi",
            "HasDefaultPath": false,
            "Name": "test-product3",
            "SupportUrl": "https://aws.amazon.com"
        },
        "CreatedTime": 1577136715.0,
        "Status": "CREATED"
    },
    "ProvisioningArtifactSummaries": [
        {
            "CreatedTime": 1577136715.0,
            "Description": "test-version-description",
            "ProvisioningArtifactMetadata": {
                "SourceProvisioningArtifactId": "pa-abcdxkkiv5fcm"
            },
            "Name": "test-version-name-3",
            "Id": "pa-abcdxkkiv5fcm"
        }
```

```
    ],
    "Tags": [
        {
            "Value": "iad",
            "Key": "region"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte DescribeProductAsAdmin en la Referencia de comandos de la AWS CLI.

`describe-provisioned-product`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-provisioned-product`.

AWS CLI

Para describir un producto aprovisionado

En el siguiente ejemplo de `describe-provisioned-product`, se muestran los detalles del producto de aprovisionamiento especificado.

```
aws servicecatalog describe-provisioned-product \
    --id pp-dpom27bm4abcd
```

Salida:

```
{
    "ProvisionedProductDetail": {
        "Status": "ERROR",
        "CreatedTime": 1577222793.358,
        "Arn": "arn:aws:servicecatalog:us-west-2:123456789012:stack/mytestppname3/
pp-dpom27bm4abcd",
        "Id": "pp-dpom27bm4abcd",
        "StatusMessage": "AmazonCloudFormationException  Parameters: [KeyName]
 must have values (Service: AmazonCloudFormation; Status Code: 400; Error Code:
 ValidationError; Request ID: 5528602a-a9ef-427c-825c-f82c31b814f5)",
        "IdempotencyToken": "527c5358-2a1a-4b9e-b1b9-7293b0ddff42",
        "LastRecordId": "rec-tfuawdjovzxge",
        "Type": "CFN_STACK",
        "Name": "mytestppname3"
```

```
    },
    "CloudWatchDashboards": []
}
```

- Para obtener información sobre la API, consulte DescribeProvisionedProduct en la Referencia de comandos de la AWS CLI.

`describe-provisioning-artifact`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-provisioning-artifact`.

AWS CLI

Para describir un artefacto de aprovisionamiento

En el siguiente ejemplo de `describe-provisioning-artifact`, se muestran los detalles del artefacto de aprovisionamiento especificado.

```
aws servicecatalog describe-provisioning-artifact \
    --provisioning-artifact-id pa-pcz347abcdcfm \
    --product-id prod-abcdfz3syn2rg
```

Salida:

```
{
    "Info": {
        "TemplateUrl": "https://awsdocs.s3.amazonaws.com/servicecatalog/
myexampledevelopment-environment.template"
    },
    "ProvisioningArtifactDetail": {
        "Id": "pa-pcz347abcdcfm",
        "Active": true,
        "Type": "CLOUD_FORMATION_TEMPLATE",
        "Description": "updated description",
        "CreatedTime": 1562097906.0,
        "Name": "updated name"
    },
    "Status": "AVAILABLE"
}
```

- Para obtener información sobre la API, consulte DescribeProvisioningArtifact en la Referencia de comandos de la AWS CLI.

describe-tag-option

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-tag-option`.

AWS CLI

Para describir una TagOption

En el siguiente ejemplo de `describe-tag-option`, se muestran los detalles de la TagOption especificada.

```
aws servicecatalog describe-tag-option \
    --id tag-p3tej2abcd5qc
```

Salida:

```
{
    "TagOptionDetail": {
        "Active": true,
        "Id": "tag-p3tej2abcd5qc",
        "Value": "value-3",
        "Key": "1234"
    }
}
```

- Para obtener información sobre la API, consulte DescribeTagOption en la Referencia de comandos de la AWS CLI.

disassociate-principal-from-portfolio

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-principal-from-portfolio`.

AWS CLI

Para desasociar una entidad principal de una cartera

En el siguiente ejemplo de `disassociate-principal-from-portfolio`, se desvincula la entidad principal especificada de la cartera.

```
aws servicecatalog disassociate-principal-from-portfolio \
    --portfolio-id port-2s6abcdq5wdh4 \
```

```
    --principal-arn arn:aws:iam::123456789012:group/myendusers
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DisassociatePrincipalFromPortfolio en la Referencia de comandos de la AWS CLI.

`disassociate-product-from-portfolio`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-product-from-portfolio`.

AWS CLI

Para desasociar un producto de una cartera

En el siguiente ejemplo de `disassociate-product-from-portfolio`, se desvincula el producto especificado de la cartera.

```
aws servicecatalog disassociate-product-from-portfolio \
    --product-id prod-3p5abcdmu3oyk \
    --portfolio-id port-2s6abcdq5wdh4
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DisassociateProductFromPortfolio en la Referencia de comandos de la AWS CLI.

`disassociate-tag-option-from-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-tag-option-from-resource`.

AWS CLI

Para desasociar una TagOption de un recurso

En el siguiente ejemplo de `disassociate-tag-option-from-resource`, se desvincula la `TagOption` especificada del recurso.

```
aws servicecatalog disassociate-tag-option-from-resource \
     --resource-id port-2s6abcdq5wdh4 \
```

```
    --tag-option-id tag-p3abc2pkpz5qc
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DisassociateTagOptionFromResource en la Referencia de comandos de la AWS CLI.

`list-accepted-portfolio-shares`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-accepted-portfolio-shares`.

AWS CLI

Para enumerar las carpetas de la cartera compartidas

En el siguiente ejemplo de `list-accepted-portfolio-shares`, se enumeran todas las carteras que esta cuenta ha aceptado compartir, incluidas únicamente las carteras predeterminadas de Service Catalog.

```
aws servicecatalog list-accepted-portfolio-shares \
    --portfolio-share-type "AWS_SERVICECATALOG"
```

Salida:

```
{
    "PortfolioDetails": [
        {
            "ARN": "arn:aws:catalog:us-west-2:123456789012:portfolio/port-
d2abcd5dpkuma",
            "Description": "AWS Service Catalog Reference blueprints for often-used
 AWS services such as EC2, S3, RDS, VPC and EMR.",
            "CreatedTime": 1574456190.687,
            "ProviderName": "AWS Service Catalog",
            "DisplayName": "Reference Architectures",
            "Id": "port-d2abcd5dpkuma"
        },
        {
            "ARN": "arn:aws:catalog:us-west-2:123456789012:portfolio/port-
abcdefaua7zpu",
            "Description": "AWS well-architected blueprints for high reliability
 applications.",
            "CreatedTime": 1574461496.092,
            "ProviderName": "AWS Service Catalog",
```

```
            "DisplayName": "High Reliability Architectures",
            "Id": "port-abcdefaua7zpu"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListAcceptedPortfolioShares en la Referencia de comandos de la AWS CLI.

`list-portfolio-access`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-portfolio-access`.

AWS CLI

Para enumerar las cuentas con acceso a una cartera

En el siguiente ejemplo de `list-portfolio-access`, se enumeran las cuentas de AWS que tienen acceso a la cartera especificada.

```
aws servicecatalog list-portfolio-access \
    --portfolio-id port-2s6abcdq5wdh4
```

Salida:

```
{
    "AccountIds": [
        "123456789012"
    ]
}
```

- Para obtener información sobre la API, consulte ListPortfolioAccess en la Referencia de comandos de la AWS CLI.

`list-portfolios-for-product`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-portfolios-for-product`.

AWS CLI

Para asociar las carteras asociadas a un producto

En el siguiente ejemplo de `list-portfolios-for-product`, se enumeran las carteras asociadas a un producto determinado.

```
aws servicecatalog list-portfolios-for-product \
    --product-id prod-abcdfz3syn2rg
```

Salida:

```
{
    "PortfolioDetails": [
        {
            "CreatedTime": 1571337221.555,
            "Id": "port-2s6abcdq5wdh4",
            "ARN": "arn:aws:catalog:us-west-2:123456789012:portfolio/
port-2s6abcdq5wdh4",
            "DisplayName": "my-portfolio",
            "ProviderName": "my-provider"
        },
        {
            "CreatedTime": 1559665256.348,
            "Id": "port-5abcd3e5st4ei",
            "ARN": "arn:aws:catalog:us-west-2:123456789012:portfolio/
port-5abcd3e5st4ei",
            "DisplayName": "test",
            "ProviderName": "provider-name"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte ListPortfoliosForProduct en la Referencia de comandos de la AWS CLI.

`list-portfolios`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-portfolios`.

AWS CLI

Para enumerar carteras

En el siguiente ejemplo de `list-portfolios`, se enumeran las carteras de Service Catalog de la región actual.

```
aws servicecatalog list-portfolios
```

Salida:

```
{
    "PortfolioDetails": [
        {
           "CreatedTime": 1559665256.348,
           "ARN": "arn:aws:catalog:us-east-2:123456789012:portfolio/
port-5pzcxmplst4ei",
           "DisplayName": "my-portfolio",
           "Id": "port-5pzcxmplst4ei",
           "ProviderName": "my-user"
        }
    ]
}
```

- Para obtener detalles de la API, consulte ListPortfolios en la Referencia de comandos de la AWS CLI.

`list-principals-for-portfolio`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-principals-for-portfolio`.

AWS CLI

Para enumerar todas las entidades principales de una cartera

En el siguiente ejemplo de `list-principals-for-portfolio`, se enumeran todas las entidades principales de la cartera especificada.

```
aws servicecatalog list-principals-for-portfolio \
    --portfolio-id port-2s6abcdq5wdh4
```

Salida:

```
{
    "Principals": [
        {
            "PrincipalARN": "arn:aws:iam::123456789012:user/usertest",
            "PrincipalType": "IAM"
```

```
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListPrincipalsForPortfolio en la Referencia de comandos de la AWS CLI.

`list-provisioning-artifacts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-provisioning-artifacts`.

AWS CLI

Para enumerar todos los artefactos de aprovisionamiento de un producto

En el siguiente ejemplo de `list-provisioning-artifacts`, se enumeran los artefactos de aprovisionamiento del producto especificado.

```
aws servicecatalog list-provisioning-artifacts \
    --product-id prod-nfi2abcdefgcpw
```

Salida:

```
{
    "ProvisioningArtifactDetails": [
        {
            "Id": "pa-abcdef54ipm6z",
            "Description": "test-version-description",
            "Type": "CLOUD_FORMATION_TEMPLATE",
            "CreatedTime": 1576021147.0,
            "Active": true,
            "Name": "test-version-name"
        },
        {
            "Id": "pa-bb4zyxwwnaio",
            "Description": "test description",
            "Type": "CLOUD_FORMATION_TEMPLATE",
            "CreatedTime": 1576022545.0,
            "Active": true,
            "Name": "test-provisioning-artifact-2"
        }
    ]
```

```
}
```

- Para obtener información sobre la API, consulte ListProvisioningArtifacts en la Referencia de comandos de la AWS CLI.

`list-resources-for-tag-option`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resources-for-tag-option`.

AWS CLI

Para enumerar los recursos asociados a una TagOption

En el siguiente ejemplo de `list-resources-for-tag-option`, se enumeran los recursos asociados a la `TagOption` especificada.

```
aws servicecatalog list-resources-for-tag-option \
    --tag-option-id tag-p3tej2abcd5qc
```

Salida:

```
{
    "ResourceDetails": [
        {
            "ARN": "arn:aws:catalog:us-west-2:123456789012:product/prod-
abcdfz3syn2rg",
            "Name": "my product",
            "Description": "description",
            "CreatedTime": 1562097906.0,
            "Id": "prod-abcdfz3syn2rg"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListResourcesForTagOption en la Referencia de comandos de la AWS CLI.

`list-tag-options`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tag-options`.

AWS CLI

En el siguiente ejemplo de `list-tag-options`, se enumeran todos los valores de `TagOptions`.

```
aws servicecatalog list-tag-options
```

Salida:

```
{
    "TagOptionDetails": [
        {
            "Value": "newvalue",
            "Active": true,
            "Id": "tag-iabcdn4fzjjms",
            "Key": "1234"
        },
        {
            "Value": "value1",
            "Active": true,
            "Id": "tag-e3abcdvmwvrzy",
            "Key": "key"
        }
    ]
}
```

- Para obtener detalles de la API, consulte ListTagOptions en la Referencia de comandos de la AWS CLI.

`provision-product`

En el siguiente ejemplo de código, se muestra cómo utilizar `provision-product`.

AWS CLI

Para aprovisionar un producto

En el siguiente ejemplo de `provision-product`, se aprovisiona el producto especificado mediante el artefacto de aprovisionamiento indicado.

```
aws servicecatalog provision-product \
    --product-id prod-abcdfz3syn2rg \
```

```
    --provisioning-artifact-id pa-abc347pcsccfm \
    --provisioned-product-name "mytestppname3"
```

Salida:

```
{
    "RecordDetail": {
        "RecordId": "rec-tfuawdabcdege",
        "CreatedTime": 1577222793.362,
        "ProvisionedProductId": "pp-abcd27bm4mldq",
        "PathId": "lpv2-abcdg3jp6t5k6",
        "RecordErrors": [],
        "ProductId": "prod-abcdfz3syn2rg",
        "UpdatedTime": 1577222793.362,
        "RecordType": "PROVISION_PRODUCT",
        "ProvisionedProductName": "mytestppname3",
        "ProvisioningArtifactId": "pa-pcz347abcdcfm",
        "RecordTags": [],
        "Status": "CREATED",
        "ProvisionedProductType": "CFN_STACK"
    }
}
```

- Para obtener detalles de la API, consulte ProvisionProduct en la Referencia de comandos de la AWS CLI.

`reject-portfolio-share`

En el siguiente ejemplo de código, se muestra cómo utilizar `reject-portfolio-share`.

AWS CLI

Para no compartir una cartera

En el siguiente ejemplo de `reject-portfolio-share`, se rechaza el recurso compartido de una cartera determinada.

```
aws servicecatalog reject-portfolio-share \
    --portfolio-id port-2s6wuabcdefghijk
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte RejectPortfolioShare en la Referencia de comandos de la AWS CLI.

`scan-provisioned-products`

En el siguiente ejemplo de código, se muestra cómo utilizar `scan-provisioned-products`.

AWS CLI

Para ver una lista de todos los productos aprovisionados disponibles

En el siguiente ejemplo de `scan-provisioned-products`, se enumeran los productos aprovisionados disponibles.

```
aws servicecatalog scan-provisioned-products
```

Salida:

```
{
    "ProvisionedProducts": [
        {
            "Status": "ERROR",
            "Arn": "arn:aws:servicecatalog:us-west-2:123456789012:stack/
mytestppname3/pp-abcd27bm4mldq",
            "StatusMessage": "AmazonCloudFormationException  Parameters: [KeyName]
 must have values (Service: AmazonCloudFormation; Status Code: 400; Error Code:
 ValidationError; Request ID: 5528602a-a9ef-427c-825c-f82c31b814f5)",
            "Id": "pp-abcd27bm4mldq",
            "Type": "CFN_STACK",
            "IdempotencyToken": "527c5358-2a1a-4b9e-b1b9-7293b0ddff42",
            "CreatedTime": 1577222793.358,
            "Name": "mytestppname3",
            "LastRecordId": "rec-tfuawdabcdxge"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ScanProvisionedProducts en la Referencia de comandos de la AWS CLI.

`search-products-as-admin`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-products-as-admin`.

AWS CLI

Para buscar productos con privilegios de administrador

En el siguiente ejemplo de `search-products-as-admin`, se buscan productos con privilegios de administrador con un ID de cartera como filtro.

```
aws servicecatalog search-products-as-admin \
    --portfolio-id port-5abcd3e5st4ei
```

Salida:

```
{
    "ProductViewDetails": [
        {
            "ProductViewSummary": {
                "Name": "my product",
                "Owner": "owner name",
                "Type": "CLOUD_FORMATION_TEMPLATE",
                "ProductId": "prod-abcdfz3syn2rg",
                "HasDefaultPath": false,
                "Id": "prodview-abcdmyuzv2dlu",
                "ShortDescription": "description"
            },
            "ProductARN": "arn:aws:catalog:us-west-2:123456789012:product/prod-
abcdfz3syn2rg",
            "CreatedTime": 1562097906.0,
            "Status": "CREATED"
        }
    ]
}
```

- Para obtener información sobre la API, consulte SearchProductsAsAdmin en la Referencia de comandos de la AWS CLI.

`search-provisioned-products`

En el siguiente ejemplo de código, se muestra cómo utilizar `search-provisioned-products`.

AWS CLI

Para buscar productos aprovisionados

En el siguiente ejemplo de `search-provisioned-products`, se buscan productos aprovisionados que coincidan con el ID de producto especificado mediante un archivo JSON para pasar los parámetros.

```
aws servicecatalog search-provisioned-products \
    --cli-input-json file://search-provisioned-products-input.json
```

Contenido de `search-provisioned-products-input.json`:

```
{
    "Filters": {
        "SearchQuery": [
            "prod-tcjvfz3syn2rg"
        ]
    }
}
```

Salida:

```
{
    "ProvisionedProducts": [
        {
            "ProvisioningArtifactId": "pa-pcz347abcdcfm",
            "Name": "mytestppname3",
            "CreatedTime": 1577222793.358,
            "Id": "pp-abcd27bm4mldq",
            "Status": "ERROR",
            "UserArn": "arn:aws:iam::123456789012:user/cliuser",
            "StatusMessage": "AmazonCloudFormationException  Parameters: [KeyName]
 must have values (Service: AmazonCloudFormation; Status Code: 400; Error Code:
 ValidationError; Request ID: 5528602a-a9ef-427c-825c-f82c31b814f5)",
            "Arn": "arn:aws:servicecatalog:us-west-2:123456789012:stack/
mytestppname3/pp-abcd27bm4mldq",
            "Tags": [
                {
                    "Value": "arn:aws:catalog:us-west-2:123456789012:product/prod-
abcdfz3syn2rg",
                    "Key": "aws:servicecatalog:productArn"
                },
```

```
                {
                    "Value": "arn:aws:iam::123456789012:user/cliuser",
                    "Key": "aws:servicecatalog:provisioningPrincipalArn"
                },
                {
                    "Value": "value-3",
                    "Key": "1234"
                },
                {
                    "Value": "pa-pcz347abcdcfm",
                    "Key": "aws:servicecatalog:provisioningArtifactIdentifier"
                },
                {
                    "Value": "arn:aws:catalog:us-west-2:123456789012:portfolio/
port-2s6abcdq5wdh4",
                    "Key": "aws:servicecatalog:portfolioArn"
                },
                {
                    "Value": "arn:aws:servicecatalog:us-west-2:123456789012:stack/
mytestppname3/pp-abcd27bm4mldq",
                    "Key": "aws:servicecatalog:provisionedProductArn"
                }
            ],
            "IdempotencyToken": "527c5358-2a1a-4b9e-b1b9-7293b0ddff42",
            "UserArnSession": "arn:aws:iam::123456789012:user/cliuser",
            "Type": "CFN_STACK",
            "LastRecordId": "rec-tfuawdabcdxge",
            "ProductId": "prod-abcdfz3syn2rg"
        }
    ],
    "TotalResultsCount": 1
}
```

- Para obtener información sobre la API, consulte SearchProvisionedProducts en la Referencia de comandos de la AWS CLI.

`update-portfolio`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-portfolio`.

AWS CLI

Para actualizar una cartera

En el siguiente ejemplo de `update-portfolio`, se actualiza el nombre de la cartera especificada.

```
aws servicecatalog update-portfolio \
    --id port-5abcd3e5st4ei \
    --display-name "New portfolio name"
```

Salida:

```
{
    "PortfolioDetail": {
        "DisplayName": "New portfolio name",
        "ProviderName": "provider",
        "ARN": "arn:aws:catalog:us-west-2:123456789012:portfolio/
port-5abcd3e5st4ei",
        "Id": "port-5abcd3e5st4ei",
        "CreatedTime": 1559665256.348
    },
    "Tags": []
}
```

- Para obtener información sobre la API, consulte UpdatePortfolio en la Referencia de comandos de la AWS CLI.

`update-product`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-product`.

AWS CLI

Para actualizar un producto

En el siguiente ejemplo de `update-product`, se actualiza el nombre y el propietario de la cartera especificada.

```
aws servicecatalog update-product \
    --id prod-os6abc7drqlt2 \
    --name "New product name" \
    --owner "Updated product owner"
```

Salida:

```
{
    "Tags": [
        {
            "Value": "iad",
            "Key": "region"
        }
    ],
    "ProductViewDetail": {
        "ProductViewSummary": {
            "Owner": "Updated product owner",
            "ProductId": "prod-os6abc7drqlt2",
            "Distributor": "test-distributor",
            "SupportUrl": "https://aws.amazon.com",
            "Name": "New product name",
            "ShortDescription": "test-description",
            "HasDefaultPath": false,
            "Id": "prodview-6abcdgrfhvidy",
            "SupportDescription": "test-support",
            "SupportEmail": "test@amazon.com",
            "Type": "CLOUD_FORMATION_TEMPLATE"
        },
        "Status": "CREATED",
        "ProductARN": "arn:aws:catalog:us-west-2:123456789012:product/prod-
os6abc7drqlt2",
        "CreatedTime": 1577136255.0
    }
}
```

- Para obtener información sobre la API, consulte UpdateProduct en la Referencia de comandos de la AWS CLI.

`update-provisioning-artifact`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-provisioning-artifact`.

AWS CLI

Para actualizar un artefacto de aprovisionamiento

En el siguiente ejemplo de `update-provisioning-artifact`, se actualiza el nombre y la descripción del artefacto de aprovisionamiento especificado con un archivo JSON para pasar los parámetros.

```
aws servicecatalog update-provisioning-artifact \
    --cli-input-json file://update-provisioning-artifact-input.json
```

Contenido de `update-provisioning-artifact-input.json`:

```
{
    "ProductId": "prod-abcdfz3syn2rg",
    "ProvisioningArtifactId": "pa-pcz347abcdcfm",
    "Name": "updated name",
    "Description": "updated description"
}
```

Salida:

```
{
    "Info": {
        "TemplateUrl": "https://awsdocs.s3.amazonaws.com/servicecatalog/
myexampledevelopment-environment.template"
    },
    "Status": "AVAILABLE",
    "ProvisioningArtifactDetail": {
        "Active": true,
        "Description": "updated description",
        "Id": "pa-pcz347abcdcfm",
        "Name": "updated name",
        "Type": "CLOUD_FORMATION_TEMPLATE",
        "CreatedTime": 1562097906.0
    }
}
```

- Para obtener información sobre la API, consulte UpdateProvisioningArtifact en la Referencia de comandos de la AWS CLI.

`update-tag-option`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-tag-option`.

AWS CLI

Para actualizar una TagOption

En el siguiente ejemplo de `update-tag-option`, se actualiza el valor `TagOption` mediante el archivo JSON especificado.

```
aws servicecatalog update-tag-option --cli-input-json file://update-tag-option-input.json
```

Contenido de `update-tag-option-input.json`:

```
{
    "Id": "tag-iabcdn4fzjjms",
    "Value": "newvalue",
    "Active": true
}
```

Salida:

```
{
    "TagOptionDetail": {
        "Value": "newvalue",
        "Key": "1234",
        "Active": true,
        "Id": "tag-iabcdn4fzjjms"
    }
}
```

- Para obtener información sobre la API, consulte UpdateTagOption en la Referencia de la API de la AWS CLI.

Ejemplos de Service Quotas que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Service Quotas.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`get-aws-default-service-quota`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-aws-default-service-quota`.

AWS CLI

Para describir una cuota de servicio predeterminada

En el siguiente ejemplo de `get-aws-default-service-quota`, se muestran los detalles de la cuota especificada.

```
aws service-quotas get-aws-default-service-quota \
    --service-code ec2 \
    --quota-code L-1216C47A
```

Salida:

```
{
    "Quota": {
        "ServiceCode": "ec2",
        "ServiceName": "Amazon Elastic Compute Cloud (Amazon EC2)",
        "QuotaArn": "arn:aws:servicequotas:us-east-2::ec2/L-1216C47A",
        "QuotaCode": "L-1216C47A",
        "QuotaName": "Running On-Demand Standard (A, C, D, H, I, M, R, T, Z)
 instances",
        "Value": 5.0,
        "Unit": "None",
        "Adjustable": true,
        "GlobalQuota": false,
        "UsageMetric": {
            "MetricNamespace": "AWS/Usage",
            "MetricName": "ResourceCount",
            "MetricDimensions": {
                "Class": "Standard/OnDemand",
                "Resource": "vCPU",
                "Service": "EC2",
```

```
                "Type": "Resource"
            },
            "MetricStatisticRecommendation": "Maximum"
        }
    }
}
```

- Para obtener información sobre la API, consulte GetAwsDefaultServiceQuota en la Referencia de comandos de la AWS CLI.

`get-requested-service-quota-change`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-requested-service-quota-change`.

AWS CLI

Para describir una solicitud de un aumento de la cuota de servicio

En el siguiente ejemplo de `get-requested-service-quota-change`, se describe la solicitud de incremento de la cuota especificada.

```
aws service-quotas get-requested-service-quota-change \
    --request-id d187537d15254312a9609aa51bbf7624u7W49tP0
```

Salida:

```
{
    "RequestedQuota": {
        "Id": "d187537d15254312a9609aa51bbf7624u7W49tPO",
        "CaseId": "6780195351",
        "ServiceCode": "ec2",
        "ServiceName": "Amazon Elastic Compute Cloud (Amazon EC2)",
        "QuotaCode": "L-20F13EBD",
        "QuotaName": "Running Dedicated c5n Hosts",
        "DesiredValue": 2.0,
        "Status": "CASE_OPENED",
        "Created": 1580446904.067,
        "LastUpdated": 1580446953.265,
        "Requester": "{\"accountId\":\"123456789012\",\"callerArn\":
\"arn:aws:iam::123456789012:root\"}",
        "QuotaArn": "arn:aws:servicequotas:us-east-2:123456789012:ec2/L-20F13EBD",
```

```
        "GlobalQuota": false,
        "Unit": "None"
    }
}
```

- Para obtener información sobre la API, consulte GetRequestedServiceQuotaChange en la Referencia de comandos de la AWS CLI.

`get-service-quota`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-quota`.

AWS CLI

Para describir una cuota de servicio

En el siguiente ejemplo de `get-service-quota`, se muestran los detalles de la cuota especificada.

```
aws service-quotas get-service-quota \
    --service-code ec2 \
    --quota-code L-1216C47A
```

Salida:

```
{
    "Quota": {
        "ServiceCode": "ec2",
        "ServiceName": "Amazon Elastic Compute Cloud (Amazon EC2)",
        "QuotaArn": "arn:aws:servicequotas:us-east-2:123456789012:ec2/L-1216C47A",
        "QuotaCode": "L-1216C47A",
        "QuotaName": "Running On-Demand Standard (A, C, D, H, I, M, R, T, Z)
 instances",
        "Value": 1920.0,
        "Unit": "None",
        "Adjustable": true,
        "GlobalQuota": false,
        "UsageMetric": {
            "MetricNamespace": "AWS/Usage",
            "MetricName": "ResourceCount",
            "MetricDimensions": {
                "Class": "Standard/OnDemand",
```

```
                "Resource": "vCPU",
                "Service": "EC2",
                "Type": "Resource"
            },
            "MetricStatisticRecommendation": "Maximum"
        }
    }
}
```

- Para obtener información sobre la API, consulte GetServiceQuota en la Referencia de comandos de la AWS CLI.

`list-aws-default-service-quotas`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-aws-default-service-quotas`.

AWS CLI

Para enumerar las cuotas predeterminadas de un servicio

En el siguiente ejemplo de `list-aws-default-service-quotas`, se enumeran los valores predeterminados de las cuotas del servicio especificado.

```
aws service-quotas list-aws-default-service-quotas \
    --service-code xray
```

Salida:

```
{
    "Quotas": [
        {
            "ServiceCode": "xray",
            "ServiceName": "AWS X-Ray",
            "QuotaArn": "arn:aws:servicequotas:us-west-2::xray/L-C6B6F05D",
            "QuotaCode": "L-C6B6F05D",
            "QuotaName": "Indexed annotations per trace",
            "Value": 50.0,
            "Unit": "None",
            "Adjustable": false,
            "GlobalQuota": false
        },
```

```
        {
            "ServiceCode": "xray",
            "ServiceName": "AWS X-Ray",
            "QuotaArn": "arn:aws:servicequotas:us-west-2::xray/L-D781C0FD",
            "QuotaCode": "L-D781C0FD",
            "QuotaName": "Segment document size",
            "Value": 64.0,
            "Unit": "Kilobytes",
            "Adjustable": false,
            "GlobalQuota": false
        },
        {
            "ServiceCode": "xray",
            "ServiceName": "AWS X-Ray",
            "QuotaArn": "arn:aws:servicequotas:us-west-2::xray/L-998BFF16",
            "QuotaCode": "L-998BFF16",
            "QuotaName": "Trace and service graph retention in days",
            "Value": 30.0,
            "Unit": "None",
            "Adjustable": false,
            "GlobalQuota": false
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListAwsDefaultServiceQuotas en la Referencia de comandos de la AWS CLI.

`list-requested-service-quota-change-history-by-quota`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-requested-service-quota-change-history-by-quota`.

AWS CLI

Para enumerar sus solicitudes de aumento de cuota

En el siguiente ejemplo de `list-requested-service-quota-change-history-by-quota`, se enumeran las solicitudes de incremento de la cuota especificada.

```
aws service-quotas list-requested-service-quota-change-history-by-quota \
    --service-code ec2 \
```

```
    --quota-code L-20F13EBD
```

Salida:

```
{
    "RequestedQuotas": [
        {
            "Id": "d187537d15254312a9609aa51bbf7624u7W49tPO",
            "CaseId": "6780195351",
            "ServiceCode": "ec2",
            "ServiceName": "Amazon Elastic Compute Cloud (Amazon EC2)",
            "QuotaCode": "L-20F13EBD",
            "QuotaName": "Running Dedicated c5n Hosts",
            "DesiredValue": 2.0,
            "Status": "CASE_OPENED",
            "Created": 1580446904.067,
            "LastUpdated": 1580446953.265,
            "Requester": "{\"accountId\":\"123456789012\",\"callerArn\":
\"arn:aws:iam::123456789012:root\"}",
            "QuotaArn": "arn:aws:servicequotas:us-east-2:123456789012:ec2/
L-20F13EBD",
            "GlobalQuota": false,
            "Unit": "None"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListRequestedServiceQuotaChangeHistoryByQuota en la Referencia de comandos de la AWS CLI.

`list-requested-service-quota-change-history`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-requested-service-quota-change-history`.

AWS CLI

Para enumerar sus solicitudes de aumento de cuota

En el siguiente ejemplo de `list-requested-service-quota-change-history`, se enumeran las solicitudes de incremento de cuota del servicio especificado.

```
aws service-quotas list-requested-service-quota-change-history \
    --service-code ec2
```

Salida:

```
{
    "RequestedQuotas": [
        {
            "Id": "d187537d15254312a9609aa51bbf7624u7W49tPO",
            "CaseId": "6780195351",
            "ServiceCode": "ec2",
            "ServiceName": "Amazon Elastic Compute Cloud (Amazon EC2)",
            "QuotaCode": "L-20F13EBD",
            "QuotaName": "Running Dedicated c5n Hosts",
            "DesiredValue": 2.0,
            "Status": "CASE_OPENED",
            "Created": 1580446904.067,
            "LastUpdated": 1580446953.265,
            "Requester": "{\"accountId\":\"123456789012\",\"callerArn\":
\"arn:aws:iam::123456789012:root\"}",
            "QuotaArn": "arn:aws:servicequotas:us-east-2:123456789012:ec2/
L-20F13EBD",
            "GlobalQuota": false,
            "Unit": "None"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListRequestedServiceQuotaChangeHistory en la Referencia de comandos de la AWS CLI.

`list-service-quotas`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-service-quotas`.

AWS CLI

Para enumerar las cuotas de un servicio

En el siguiente ejemplo de `list-service-quotas`, se muestran detalles sobre las cuotas de AWS CloudFormation.

```
aws service-quotas list-service-quotas \
    --service-code cloudformation
```

Salida:

```
{
    "Quotas": [
        {
            "ServiceCode": "cloudformation",
            "ServiceName": "AWS CloudFormation",
            "QuotaArn": "arn:aws:servicequotas:us-
east-2:123456789012:cloudformation/L-87D14FB7",
            "QuotaCode": "L-87D14FB7",
            "QuotaName": "Output count in CloudFormation template",
            "Value": 60.0,
            "Unit": "None",
            "Adjustable": false,
            "GlobalQuota": false
        },
        {
            "ServiceCode": "cloudformation",
            "ServiceName": "AWS CloudFormation",
            "QuotaArn": "arn:aws:servicequotas:us-
east-2:123456789012:cloudformation/L-0485CB21",
            "QuotaCode": "L-0485CB21",
            "QuotaName": "Stack count",
            "Value": 200.0,
            "Unit": "None",
            "Adjustable": true,
            "GlobalQuota": false
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListServiceQuotas en la Referencia de comandos de la AWS CLI.

`list-services`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-services`.

AWS CLI

Para enumerar los servicios disponibles

El siguiente comando muestra los servicios que están disponibles en Service Quotas.

```
aws service-quotas list-services
```

Salida:

```
{
    "Services": [
        {
            "ServiceCode": "AWSCloudMap",
            "ServiceName": "AWS Cloud Map"
        },
        {
            "ServiceCode": "access-analyzer",
            "ServiceName": "Access Analyzer"
        },
        {
            "ServiceCode": "acm",
            "ServiceName": "AWS Certificate Manager (ACM)"
        },

        ...truncated...

        {
            "ServiceCode": "xray",
            "ServiceName": "AWS X-Ray"
        }
    ]
}
```

Puede añadir el parámetro `--query` para filtrar la visualización según la información que le interese. El siguiente ejemplo muestra solo los códigos de servicio.

```
aws service-quotas list-services \
    --query Services[*].ServiceCode
```

Salida:

```
[
    "AWSCloudMap",
    "access-analyzer",
    "acm",
    "acm-pca",
    "amplify",
    "apigateway",
    "application-autoscaling",
        ...truncated...
    "xray"
]
```

- Para obtener información sobre la API, consulte ListServices en la Referencia de comandos de la AWS CLI.

`request-service-quota-increase`

En el siguiente ejemplo de código, se muestra cómo utilizar `request-service-quota-increase`.

AWS CLI

Para solicitar un aumento de la cuota de servicio

En el siguiente ejemplo de `request-service-quota-increase`, se solicita un incremento de la cuota del servicio especificada.

```
aws service-quotas request-service-quota-increase \
    --service-code ec2 \
    --quota-code L-20F13EBD \
    --desired-value 2
```

Salida:

```
{
    "RequestedQuota": {
        "Id": "d187537d15254312a9609aa51bbf7624u7W49tPO",
        "ServiceCode": "ec2",
        "ServiceName": "Amazon Elastic Compute Cloud (Amazon EC2)",
        "QuotaCode": "L-20F13EBD",
        "QuotaName": "Running Dedicated c5n Hosts",
        "DesiredValue": 2.0,
```

```
        "Status": "PENDING",
        "Created": 1580446904.067,
        "Requester": "{\"accountId\":\"123456789012\",\"callerArn\":
\"arn:aws:iam::123456789012:root\"}",
        "QuotaArn": "arn:aws:servicequotas:us-east-2:123456789012:ec2/L-20F13EBD",
        "GlobalQuota": false,
        "Unit": "None"
    }
}
```

- Para obtener información sobre la API, consulte RequestServiceQuotaIncrease en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon SES que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon SES.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`delete-identity`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-identity`.

AWS CLI

Para eliminar una identidad

En el siguiente ejemplo, se utiliza el comando `delete-identity` para eliminar una identidad de la lista de identidades verificadas con Amazon SES:

```
aws ses delete-identity --identity user@example.com
```

Para obtener más información sobre las identidades verificadas, consulte Verificación de direcciones de correo electrónico y dominios en Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener detalles sobre la API, consulte DeleteIdentity en la Referencia de comandos de la AWS CLI.

`get-identity-dkim-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-identity-dkim-attributes`.

AWS CLI

Para obtener los atributos Easy DKIM de Amazon SES para una lista de identidades

En el siguiente ejemplo, se utiliza el comando `get-identity-dkim-attributes` para recuperar los atributos Easy DKIM de Amazon SES de una lista de identidades:

```
aws ses get-identity-dkim-attributes --identities "example.com" "user@example.com"
```

Salida:

```
{
   "DkimAttributes": {
       "example.com": {
           "DkimTokens": [
               "EXAMPLEjcs5xoyqytjsotsijas7236gr",
               "EXAMPLEjr76cvoc6mysspnioorxsn6ep",
               "EXAMPLEkbmkqkhlm2lyz77ppkulerm4k"
           ],
           "DkimEnabled": true,
           "DkimVerificationStatus": "Success"
       },
       "user@example.com": {
           "DkimEnabled": false,
           "DkimVerificationStatus": "NotStarted"
       }
   }
```

```
}
```

Si llama a este comando con una identidad que nunca ha enviado para su verificación, esa identidad no aparecerá en el resultado.

Para obtener más información sobre Easy DKIM, consulte Easy DKIM in Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener información sobre la API, consulte GetIdentityDkimAttributes en la Referencia de comandos de la AWS CLI.

`get-identity-notification-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-identity-notification-attributes`.

AWS CLI

Para obtener los atributos de notificación de Amazon SES para una lista de identidades

En el siguiente ejemplo, se utiliza el comando `get-identity-notification-attributes` para recuperar los atributos de notificación de Amazon SES de una lista de identidades:

```
aws ses get-identity-notification-attributes --
identities "user1@example.com" "user2@example.com"
```

Salida:

```
{
   "NotificationAttributes": {
       "user1@example.com": {
           "ForwardingEnabled": false,
           "ComplaintTopic": "arn:aws:sns:us-east-1:EXAMPLE65304:MyTopic",
           "BounceTopic": "arn:aws:sns:us-east-1:EXAMPLE65304:MyTopic",
           "DeliveryTopic": "arn:aws:sns:us-east-1:EXAMPLE65304:MyTopic"
       },
       "user2@example.com": {
           "ForwardingEnabled": true
       }
   }
}
```

Este comando devuelve el estado del reenvío de comentarios por correo electrónico y, si corresponde, los nombres de recursos de Amazon (ARN) de los temas de Amazon SNS a los que se envían las notificaciones de devolución, queja y entrega.

Si llama a este comando con una identidad que nunca ha enviado para su verificación, esa identidad no aparecerá en el resultado.

Para obtener más información acerca de las notificaciones, consulte Using Notifications With Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener detalles sobre la API, consulte GetIdentityNotificationAttributes en la Referencia de comandos de la AWS CLI.

`get-identity-verification-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-identity-verification-attributes`.

AWS CLI

Para obtener el estado de verificación de Amazon SES de una lista de identidades

En el siguiente ejemplo, se utiliza el comando `get-identity-verification-attributes` para recuperar el estado de verificación de Amazon SES de una lista de identidades:

```
aws ses get-identity-verification-attributes --
identities "user1@example.com" "user2@example.com"
```

Salida:

```
{
   "VerificationAttributes": {
       "user1@example.com": {
           "VerificationStatus": "Success"
       },
       "user2@example.com": {
           "VerificationStatus": "Pending"
       }
   }
}
```

Si llama a este comando con una identidad que nunca ha enviado para su verificación, esa identidad no aparecerá en el resultado.

Para obtener más información sobre las identidades verificadas, consulte Verificación de direcciones de correo electrónico y dominios en Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener detalles sobre la API, consulte GetIdentityVerificationAttributes en la Referencia de comandos de la AWS CLI.

`get-send-quota`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-send-quota`.

AWS CLI

Para obtener los límites de envío de Amazon SES

En el siguiente ejemplo, se utiliza el comando `get-send-quota` para devolver los límites de envío de Amazon SES:

```
aws ses get-send-quota
```

Salida:

```
{
   "Max24HourSend": 200.0,
   "SentLast24Hours": 1.0,
   "MaxSendRate": 1.0
}
```

Max24HourSend es la cuota de envío, que es el número máximo de correos electrónicos que puede enviar en un periodo de 24 horas. La cuota de envío refleja un período de tiempo acumulativo. Cada vez que intenta enviar un correo electrónico, Amazon SES comprueba la cantidad de correos electrónicos que envió en las 24 horas anteriores. Siempre que el número total de mensajes de correo electrónico que haya enviado sea inferior a su cuota, se aceptará su solicitud de envío y se enviará su correo electrónico.

SentLast24Hours es el número de correos electrónicos que ha enviado en las últimas 24 horas.

MaxSendRate es el número máximo de correos electrónicos que puede enviar por segundo.

Tenga en cuenta que los límites de envío se basan en los destinatarios en lugar de en los mensajes. Por ejemplo, un correo electrónico que tenga 10 destinatarios se contabiliza como 10 en la cuota de envío.

Para obtener más información, consulte Administración de los límites de envío de Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener detalles sobre la API, consulte GetSendQuota en la Referencia de comandos de la AWS CLI.

`get-send-statistics`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-send-statistics`.

AWS CLI

Para obtener las estadísticas de envío de Amazon SES

En el siguiente ejemplo, se utiliza el comando `get-send-statistics` para devolver las estadísticas de envío de Amazon SES.

```
aws ses get-send-statistics
```

Salida:

```
{
   "SendDataPoints": [
       {
           "Complaints": 0,
           "Timestamp": "2013-06-12T19:32:00Z",
           "DeliveryAttempts": 2,
           "Bounces": 0,
           "Rejects": 0
       },
       {
           "Complaints": 0,
           "Timestamp": "2013-06-12T00:47:00Z",
           "DeliveryAttempts": 1,
           "Bounces": 0,
```

```
            "Rejects": 0
        }
    ]
}
```

El resultado es una lista de puntos de datos correspondiente a las últimas dos semanas de actividad de envío. Cada punto de datos de la lista contiene las estadísticas de un intervalo de 15 minutos.

En este ejemplo, solo hay dos puntos de datos, porque los únicos correos electrónicos que el usuario ha enviado en las últimas dos semanas han tenido lugar en dos intervalos de 15 minutos.

Para obtener más información, consulte Monitoring Your Amazon SES Usage Statistics in the en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener información sobre la API, consulte GetSendStatistics en la Referencia de comandos de la AWS CLI.

`list-identities`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-identities`.

AWS CLI

Para mostrar todas las identidades (de las direcciones de correo electrónico y de los dominios) para una cuenta de AWS específica

En el siguiente ejemplo, se utiliza el comando `list-identities` para mostrar todas las identidades que se han enviado para su verificación con Amazon SES:

```
aws ses list-identities
```

Salida:

```
{
    "Identities": [
      "user@example.com",
      "example.com"
    ]
}
```

La lista que se devuelve contiene todas las identidades, independientemente del estado de la verificación (verificada, pendiente de verificación, error, etc.).

En este ejemplo, se devuelven las direcciones de correo electrónico y los dominios porque no especificamos el parámetro de tipo de identidad.

Para obtener más información sobre la verificación, consulte Verificación de direcciones de correo electrónico y dominios en Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener detalles sobre la API, consulte ListIdentities en la Referencia de comandos de la AWS CLI.

`send-email`

En el siguiente ejemplo de código, se muestra cómo utilizar `send-email`.

AWS CLI

Para enviar un correo electrónico formateado con Amazon SES

En el siguiente ejemplo, se utiliza el comando `send-email` para enviar un correo electrónico formateado:

```
aws ses send-email --from sender@example.com --destination file://destination.json
 --message file://message.json
```

Salida:

```
{
   "MessageId": "EXAMPLEf3a5efcd1-51adec81-d2a4-4e3f-9fe2-5d85c1b23783-000000"
}
```

El destino y el mensaje son estructuras de datos de JSON guardadas en archivos .json en el directorio actual. Estos archivos son los siguientes:

`destination.json`:

```
{
  "ToAddresses":  ["recipient1@example.com", "recipient2@example.com"],
  "CcAddresses":  ["recipient3@example.com"],
  "BccAddresses": []
```

```
}
```

`message.json`:

```
{
   "Subject": {
       "Data": "Test email sent using the AWS CLI",
       "Charset": "UTF-8"
   },
   "Body": {
       "Text": {
           "Data": "This is the message body in text format.",
           "Charset": "UTF-8"
       },
       "Html": {
           "Data": "This message body contains HTML formatting. It can, for example,
 contain links like this one: <a class=\"ulink\" href=\"http://docs.aws.amazon.com/
ses/latest/DeveloperGuide\" target=\"_blank\">Amazon SES Developer Guide</a>.",
           "Charset": "UTF-8"
       }
   }
}
```

Sustituya las direcciones de correo electrónico del remitente y del destinatario por las que desee utilizar. Tenga en cuenta que la dirección de correo electrónico del remitente se debe verificar con Amazon SES. Hasta que se le conceda el acceso de producción a Amazon SES, también debe verificar la dirección de correo electrónico de cada destinatario, a menos que el destinatario sea el simulador de bandeja de correo de Amazon SES. Para obtener más información sobre la verificación, consulte Verificación de direcciones de correo electrónico y dominios en Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

El ID del mensaje en el resultado indica que la llamada para enviar el correo electrónico se ha realizado correctamente.

Si no recibe el correo electrónico, marque la casilla de correo no deseado.

Para obtener más información sobre el envío de correo electrónico formateado, consulte Envío de correo electrónico formateado con la API de Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener más información sobre la API, consulte SendEmail en la Referencia de comandos de la AWS CLI.

`send-raw-email`

En el siguiente ejemplo de código, se muestra cómo utilizar `send-raw-email`.

AWS CLI

Para enviar un correo electrónico sin procesar con Amazon SES

En el siguiente ejemplo, se utiliza el comando `send-raw-email` para enviar un correo electrónico con un TXT adjunto:

```
aws ses send-raw-email --raw-message file://message.json
```

Salida:

```
{
   "MessageId": "EXAMPLEf3f73d99b-c63fb06f-d263-41f8-a0fb-d0dc67d56c07-000000"
}
```

El mensaje sin procesar es una estructura de datos JSON guardada en un archivo denominado `message.json` en el directorio actual. Contiene lo siguiente:

```
{
   "Data": "From: sender@example.com\nTo: recipient@example.com\nSubject: Test email
 sent using the AWS CLI (contains an attachment)\nMIME-Version: 1.0\nContent-type:
 Multipart/Mixed; boundary=\"NextPart\"\n\n--NextPart\nContent-Type: text/plain
\n\nThis is the message body.\n\n--NextPart\nContent-Type: text/plain;\nContent-
Disposition: attachment; filename=\"attachment.txt\"\n\nThis is the text in the
 attachment.\n\n--NextPart--"
}
```

Como puede ver, “Datos” es una cadena larga que contiene todo el contenido sin procesar del correo electrónico en formato MIME, incluido un archivo adjunto llamado attachment.txt.

Sustituya sender@example.com y recipient@example.com por las direcciones que desee utilizar. Tenga en cuenta que la dirección de correo electrónico del remitente se debe verificar con Amazon SES. Hasta que se le conceda el acceso de producción a Amazon SES, también debe verificar la dirección de correo electrónico del destinatario, a menos que el destinatario sea el simulador de bandeja de correo de Amazon SES. Para obtener más información sobre la verificación, consulte Verificación de direcciones de correo electrónico y dominios en Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

El ID del mensaje en el resultado indica que la llamada a send-raw-email se ha realizado correctamente.

Si no recibe el correo electrónico, marque la casilla de correo no deseado.

Para obtener más información sobre el envío de correo electrónico sin procesar, consulte Envío de correo electrónico sin procesar con la API de Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener detalles sobre la API, consulte SendRawEmail en la Referencia de comandos de la AWS CLI.

`set-identity-dkim-enabled`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-identity-dkim-enabled`.

AWS CLI

Para activar o desactivar Easy DKIM para una identidad verificada de Amazon SES

En el siguiente ejemplo, se usa el comando `set-identity-dkim-enabled` para desactivar DKIM para una dirección de correo electrónico:

```
aws ses set-identity-dkim-enabled --identity user@example.com --no-dkim-enabled
```

Para obtener más información sobre Easy DKIM, consulte Easy DKIM in Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener información sobre la API, consulte SetIdentityDkimEnabled en la Referencia de comandos de la AWS CLI.

`set-identity-feedback-forwarding-enabled`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-identity-feedback-forwarding-enabled`.

AWS CLI

Para habilitar o deshabilitar la devolución y el envío de comentarios por correo electrónico para una identidad verificada de Amazon SES

En el siguiente ejemplo, se utiliza el comando `set-identity-feedback-forwarding-enabled` para permitir que una dirección de correo electrónico verificada reciba notificaciones de devoluciones y quejas por correo electrónico:

```
aws ses set-identity-feedback-forwarding-enabled --identity user@example.com --
forwarding-enabled
```

Debe recibir notificaciones de devoluciones y reclamaciones a través de Amazon SNS o de reenvío de comentarios de correo electrónico, para poder deshabilitar el reenvío de comentarios de correo electrónico si selecciona un tema de Amazon SNS tanto para notificaciones de devolución como de reclamaciones.

Para obtener más información acerca de las notificaciones, consulte Using Notifications With Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener información sobre la API, consulte SetIdentityFeedbackForwardingEnabled en la Referencia de comandos de la AWS CLI.

`set-identity-notification-topic`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-identity-notification-topic`.

AWS CLI

Para configurar el tema de Amazon SNS donde Amazon SES publicará notificaciones de devoluciones, reclamaciones o entregas para una identidad verificada

En el siguiente ejemplo, se utiliza el comando `set-identity-notification-topic` para especificar el tema de Amazon SNS en el que una dirección de correo electrónico verificada recibirá las notificaciones de devolución:

```
aws ses set-identity-notification-topic --identity user@example.com --notification-
type Bounce --sns-topic arn:aws:sns:us-east-1:EXAMPLE65304:MyTopic
```

Para obtener más información acerca de las notificaciones, consulte Using Notifications With Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para ver los detalles de la API, consulte SetIdentityNotificationTopic en la Referencia de comandos de la AWS CLI.

`verify-domain-dkim`

En el siguiente ejemplo de código, se muestra cómo utilizar `verify-domain-dkim`.

AWS CLI

Para generar los tokens DKIM de un dominio verificado para la firma de DKIM con Amazon SES

En el siguiente ejemplo, se utiliza el comando `verify-domain-dkim` para generar tokens DKIM para un dominio que se ha verificado con Amazon SES:

```
aws ses verify-domain-dkim --domain example.com
```

Salida:

```
{
   "DkimTokens": [
       "EXAMPLEq76owjnks3lnluwg65scbemvw",
       "EXAMPLEi3dnsj67hstzaj673klariwx2",
       "EXAMPLEwfbtcukvimehexktmdtaz6naj"
   ]
}
```

Para configurar DKIM, debe usar los tokens DKIM devueltos para actualizar la configuración de DNS de su dominio con registros CNAME que apunten hacia claves públicas de DKIM alojadas en Amazon SES. Para obtener más información, consulte Easy DKIM in Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener información sobre la API, consulte VerifyDomainDkim en la Referencia de comandos de la AWS CLI.

`verify-domain-identity`

En el siguiente ejemplo de código, se muestra cómo utilizar `verify-domain-identity`.

AWS CLI

Para verificar un dominio con Amazon SES

En el siguiente ejemplo, se usa el comando `verify-domain-identity` para verificar un dominio:

```
aws ses verify-domain-identity --domain example.com
```

Salida:

```
{
   "VerificationToken": "eoEmxw+YaYhb3h3iVJHuXMJXqeu1q1/wwmvjuEXAMPLE"
}
```

Para completar la verificación del dominio, debe agregar un registro TXT con el token de verificación devuelto a la configuración de DNS del dominio. Para obtener más información, consulte Verificación de dominios en Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener detalles sobre la API, consulte VerifyDomainIdentity en la Referencia de comandos de la AWS CLI.

`verify-email-identity`

En el siguiente ejemplo de código, se muestra cómo utilizar `verify-email-identity`.

AWS CLI

Para verificar una dirección de correo electrónico con Amazon SES

En el siguiente ejemplo, se usa el comando `verify-email-identity` para verificar una dirección de correo electrónico:

```
aws ses verify-email-identity --email-address user@example.com
```

Antes de poder enviar un correo electrónico mediante Amazon SES, debe verificar la dirección o el dominio desde el que envía el correo electrónico para demostrar que es de su propiedad. Si todavía no tiene acceso de producción, también deberá verificar las direcciones de correo electrónico a las que envíe correos electrónicos, excepto las proporcionadas por el simulador de buzón de correo de Amazon SES.

Después de llamar a verify-email-identity, la dirección de correo electrónico recibirá un correo electrónico de verificación. El usuario debe hacer clic en el enlace del correo electrónico para completar el proceso de verificación.

Para obtener más información, consulte Verificación de direcciones de correo electrónico en Amazon SES, en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener detalles sobre la API, consulte VerifyEmailIdentity en la Referencia de comandos de la AWS CLI.

Ejemplos de Shield que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Shield.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-drt-log-bucket`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-drt-log-bucket`.

AWS CLI

Para autorizar al DRT acceder al bucket de Amazon S3

En el siguiente ejemplo de `associate-drt-log-bucket`, se crea una asociación entre el DRT y el bucket de S3 especificado. Esto permite que el DRT acceda al bucket en nombre de la cuenta.

```
aws shield associate-drt-log-bucket \
    --log-bucket flow-logs-for-website-lb
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración del soporte de AWS Shield Response Team (SRT) para responder a eventos DDoS en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener detalles sobre la API, consulte AssociateDrtLogBucket en la Referencia de comandos de la AWS CLI.

`associate-drt-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-drt-role`.

AWS CLI

Para autorizar al DRT a mitigar los posibles ataques en su nombre

En el siguiente ejemplo de `associate-drt-role`, se crea una asociación entre el DRT y el rol especificado. El DRT puede usar el rol para acceder a la cuenta y administrarla.

```
aws shield associate-drt-role \
    --role-arn arn:aws:iam::123456789012:role/service-role/DrtRole
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración del soporte de AWS Shield Response Team (SRT) para responder a eventos DDoS en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener información sobre la API, consulte AssociateDrtRole en la Referencia de comandos de la AWS CLI.

`create-protection`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-protection`.

AWS CLI

Para habilitar la protección AWS Shield Avanzado para un solo recurso de AWS

En el siguiente ejemplo de `create-protection`, se habilita la protección Shield Avanzado para la distribución de AWS CloudFront especificada.

```
aws shield create-protection \
    --name "Protection for CloudFront distribution" \
    --resource-arn arn:aws:cloudfront::123456789012:distribution/E198WC25FXOWY8
```

Salida:

```
{
    "ProtectionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Para obtener más información, consulte Cómo agregar y configurar protecciones de recursos con Shield Advanced en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener información sobre la API, consulte CreateProtection en la Referencia de comandos de la AWS CLI.

`create-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-subscription`.

AWS CLI

Para habilitar la protección AWS Shield Avanzado para una cuenta

En el siguiente ejemplo de `create-subscription`, se habilita la protección Shield Avanzado para la cuenta.

```
aws shield create-subscription
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de AWS Shield Advanced en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener información sobre la API, consulte CreateSubscription en la Referencia de comandos de la AWS CLI.

`delete-protection`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-protection`.

AWS CLI

Para eliminar la protección AWS Shield Avanzado de un recurso de AWS

En el siguiente ejemplo de `delete-protection`, se elimina la protección AWS Shield Avanzado especificada.

```
aws shield delete-protection \
    --protection-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Eliminar la protección de AWS Shield Avanzado desde un recurso de AWS en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener información sobre la API, consulte DeleteProtection en la Referencia de comandos de la AWS CLI.

`describe-attack`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-attack`.

AWS CLI

Para recuperar una descripción detallada de un ataque

En el siguiente ejemplo de `describe-attack`, se muestran los detalles del ataque DDoS con el ID de ataque especificado. Puede obtener los ID de ataque ejecutando el comando `list-attacks`.

```
aws shield describe-attack --attack-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

Salida:

```
{
    "Attack": {
        "AttackId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "ResourceArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/testElb",
        "SubResources": [
            {
                "Type": "IP",
```

```
                "Id": "192.0.2.2",
                "AttackVectors": [
                    {
                        "VectorType": "SYN_FLOOD",
                        "VectorCounters": [
                            {
                                "Name": "SYN_FLOOD_BPS",
                                "Max": 982184.0,
                                "Average": 982184.0,
                                "Sum": 11786208.0,
                                "N": 12,
                                "Unit": "BPS"
                            }
                        ]
                    }
                ],
                "Counters": []
            },
            {
                "Type": "IP",
                "Id": "192.0.2.3",
                "AttackVectors": [
                    {
                        "VectorType": "SYN_FLOOD",
                        "VectorCounters": [
                            {
                                "Name": "SYN_FLOOD_BPS",
                                "Max": 982184.0,
                                "Average": 982184.0,
                                "Sum": 9821840.0,
                                "N": 10,
                                "Unit": "BPS"
                            }
                        ]
                    }
                ],
                "Counters": []
            },
            {
                "Type": "IP",
                "Id": "192.0.2.4",
                "AttackVectors": [
                    {
                        "VectorType": "SYN_FLOOD",
```

```
                    "VectorCounters": [
                        {
                            "Name": "SYN_FLOOD_BPS",
                            "Max": 982184.0,
                            "Average": 982184.0,
                            "Sum": 7857472.0,
                            "N": 8,
                            "Unit": "BPS"
                        }
                    ]
                }
            ],
            "Counters": []
        },
        {
            "Type": "IP",
            "Id": "192.0.2.5",
            "AttackVectors": [
                {
                    "VectorType": "SYN_FLOOD",
                    "VectorCounters": [
                        {
                            "Name": "SYN_FLOOD_BPS",
                            "Max": 982184.0,
                            "Average": 982184.0,
                            "Sum": 1964368.0,
                            "N": 2,
                            "Unit": "BPS"
                        }
                    ]
                }
            ],
            "Counters": []
        },
        {
            "Type": "IP",
            "Id": "2001:DB8::bcde:4321:8765:0:0",
            "AttackVectors": [
                {
                    "VectorType": "SYN_FLOOD",
                    "VectorCounters": [
                        {
                            "Name": "SYN_FLOOD_BPS",
                            "Max": 982184.0,
```

```
                            "Average": 982184.0,
                            "Sum": 1964368.0,
                            "N": 2,
                            "Unit": "BPS"
                        }
                    ]
                }
            ],
            "Counters": []
        },
        {
            "Type": "IP",
            "Id": "192.0.2.6",
            "AttackVectors": [
                {
                    "VectorType": "SYN_FLOOD",
                    "VectorCounters": [
                        {
                            "Name": "SYN_FLOOD_BPS",
                            "Max": 982184.0,
                            "Average": 982184.0,
                            "Sum": 1964368.0,
                            "N": 2,
                            "Unit": "BPS"
                        }
                    ]
                }
            ],
            "Counters": []
        }
    ],
    "StartTime": 1576024927.457,
    "EndTime": 1576025647.457,
    "AttackCounters": [],
    "AttackProperties": [
        {
            "AttackLayer": "NETWORK",
            "AttackPropertyIdentifier": "SOURCE_IP_ADDRESS",
            "TopContributors": [
                {
                    "Name": "198.51.100.5",
                    "Value": 2024475682
                },
                {
```

```
                        "Name": "198.51.100.8",
                        "Value": 1311380863
                    },
                    {
                        "Name": "203.0.113.4",
                        "Value": 900599855
                    },
                    {
                        "Name": "198.51.100.4",
                        "Value": 769417366
                    },
                    {
                        "Name": "203.1.113.13",
                        "Value": 757992847
                    }
                ],
                "Unit": "BYTES",
                "Total": 92773354841
            },
            {
                "AttackLayer": "NETWORK",
                "AttackPropertyIdentifier": "SOURCE_COUNTRY",
                "TopContributors": [
                    {
                        "Name": "United States",
                        "Value": 80938161764
                    },
                    {
                        "Name": "Brazil",
                        "Value": 9929864330
                    },
                    {
                        "Name": "Netherlands",
                        "Value": 1635009446
                    },
                    {
                        "Name": "Mexico",
                        "Value": 144832971
                    },
                    {
                        "Name": "Japan",
                        "Value": 45369000
                    }
                ],
```

```
                "Unit": "BYTES",
                "Total": 92773354841
            },
            {
                "AttackLayer": "NETWORK",
                "AttackPropertyIdentifier": "SOURCE_ASN",
                "TopContributors": [
                    {
                        "Name": "12345",
                        "Value": 74953625841
                    },
                    {
                        "Name": "12346",
                        "Value": 4440087595
                    },
                    {
                        "Name": "12347",
                        "Value": 1635009446
                    },
                    {
                        "Name": "12348",
                        "Value": 1221230000
                    },
                    {
                        "Name": "12349",
                        "Value": 1199425294
                    }
                ],
                "Unit": "BYTES",
                "Total": 92755479921
            }
        ],
        "Mitigations": []
    }
}
```


Para obtener más información, consulte Visibilidad de los eventos de DDoS en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener información sobre la API, consulte DescribeAttack en la Referencia de comandos de la AWS CLI.

`describe-drt-access`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-drt-access`.

AWS CLI

Para obtener una descripción de las autorizaciones de las que dispone el DRT para mitigar los ataques en su nombre

En el siguiente ejemplo de `describe-drt-access`, se recuperan las autorizaciones de rol y bucket de S3 de las que dispone el DRT, que le permiten responder a posibles ataques en su nombre.

```
aws shield describe-drt-access
```

Salida:

```
{
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/DrtRole",
    "LogBucketList": [
        "flow-logs-for-website-lb"
    ]
}
```

Para obtener más información, consulte Configuración del soporte de AWS Shield Response Team (SRT) para responder a eventos DDoS en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener información sobre la API, consulte DescribeDrtAccess en la Referencia de comandos de la AWS CLI.

`describe-emergency-contact-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-emergency-contact-settings`.

AWS CLI

Para recuperar las direcciones de correo electrónico de emergencia que tenga archivadas con el DRT

En el siguiente ejemplo de `describe-emergency-contact-settings`, se recuperan las direcciones de correo electrónico archivadas en el DRT de la cuenta. Estas son las direcciones con las que debe contactar el DRT al responder a un presunto ataque.

```
aws shield describe-emergency-contact-settings
```

Salida:

```
{
    "EmergencyContactList": [
        {
            "EmailAddress": "ops@example.com"
        },
        {
            "EmailAddress": "ddos-notifications@example.com"
       }
    ]
}
```

Para obtener más información, consulte Cómo funcionan AWS Shield y Shield Advanced<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html> en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener información sobre la API, consulte DescribeEmergencyContactSettings en la Referencia de comandos de la AWS CLI.

`describe-protection`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-protection`.

AWS CLI

Para recuperar los detalles de una protección AWS Shield Avanzado

En el siguiente ejemplo de `describe-protection`, se muestran detalles sobre la protección Shield Avanzado con el ID especificado. Puede obtener los ID de protección ejecutando el comando `list-protections`.

```
aws shield describe-protection \
    --protection-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "Protection": {
        "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "Name": "1.2.3.4",
        "ResourceArn": "arn:aws:ec2:us-west-2:123456789012:eip-allocation/
eipalloc-0ac1537af40742a6d"
    }
}
```

Para obtener más información, consulte Cómo agregar y configurar protecciones de recursos con Shield Advanced en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener detalles sobre la API, consulte DescribeProtection en la Referencia de comandos de la AWS CLI.

`describe-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-subscription`.

AWS CLI

Para recuperar los detalles de la protección AWS Shield Avanzado de la cuenta

En el siguiente ejemplo de `describe-subscription`, se muestran detalles sobre la protección Shield Avanzado proporcionada para la cuenta.

```
aws shield describe-subscription
```

Salida:

```
{
    "Subscription": {
        "StartTime": 1534368978.0,
        "EndTime": 1597613778.0,
        "TimeCommitmentInSeconds": 63244800,
        "AutoRenew": "ENABLED",
        "Limits": [
            {
                "Type": "GLOBAL_ACCELERATOR",
                "Max": 1000
```

```
            },
            {
                "Type": "ROUTE53_HOSTED_ZONE",
                "Max": 1000
            },
            {
                "Type": "CF_DISTRIBUTION",
                "Max": 1000
            },
            {
                "Type": "ELB_LOAD_BALANCER",
                "Max": 1000
            },
            {
                "Type": "EC2_ELASTIC_IP_ALLOCATION",
                "Max": 1000
            }
        ]
    }
}
```

Para obtener más información, consulte Cómo funcionan AWS Shield y Shield Advanced en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener información sobre la API, consulte DescribeSubscription en la Referencia de comandos de la AWS CLI.

`disassociate-drt-log-bucket`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-drt-log-bucket`.

AWS CLI

Para eliminar la autorización para que el DRT obtenga acceso a un bucket de Amazon S3 en su nombre

En el siguiente ejemplo de `disassociate-drt-log-bucket`, se elimina la asociación entre el DRT y el bucket de S3 especificado. Una vez completado este comando, el DRT ya no podrá acceder al bucket en nombre de la cuenta.

```
aws shield disassociate-drt-log-bucket \
    --log-bucket flow-logs-for-website-lb
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración del soporte de AWS Shield Response Team (SRT) para responder a eventos DDoS en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener información sobre la API, consulte DisassociateDrtLogBucket en la Referencia de la comandos de la AWS CLI.

`disassociate-drt-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-drt-role`.

AWS CLI

Para eliminar la autorización para que el DRT mitigue posibles ataques en su nombre

En el siguiente ejemplo de `disassociate-drt-role`, se elimina la asociación entre el DRT y la cuenta. Tras esta llamada, el DRT ya no podrá acceder a su cuenta ni administrarla.

```
aws shield disassociate-drt-role
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración del soporte de AWS Shield Response Team (SRT) para responder a eventos DDoS en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener información sobre la API, consulte DisassociateDrtRole en la Referencia de comandos de la AWS CLI.

`get-subscription-state`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-subscription-state`.

AWS CLI

Para recuperar el estado actual de la suscripción a AWS Shield Avanzado de la cuenta

En el siguiente ejemplo de `get-subscription-state`, se recupera el estado de la protección Shield Avanzado para la cuenta.

```
aws shield get-subscription-state
```

Salida:

```
{
    "SubscriptionState": "ACTIVE"
}
```

Para obtener más información, consulte Cómo funcionan AWS Shield y Shield Advanced en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener información sobre la API, consulte GetSubscriptionState en la Referencia de comandos de la AWS CLI.

`list-attacks`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-attacks`.

AWS CLI

Para recuperar los resúmenes de los ataques de AWS Shield Avanzado

En el siguiente ejemplo de `list-attacks`, se recuperan resúmenes de los ataques de la distribución de AWS CloudFront especificada durante el período de tiempo especificado. La respuesta incluye los ID de ataque que puede proporcionar al comando `describe-attack` para obtener información detallada sobre un ataque.

```
aws shield list-attacks \
    --resource-arns arn:aws:cloudfront::12345678910:distribution/E1PXMP22ZVFAOR \
    --start-time FromInclusive=1529280000,ToExclusive=1529300000
```

Salida:

```
{
    "AttackSummaries": [
        {
            "AttackId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "ResourceArn": "arn:aws:cloudfront::123456789012:distribution/
E1PXMP22ZVFAOR",
            "StartTime": 1529280000.0,
```

```
            "EndTime": 1529449200.0,
            "AttackVectors": [
                {
                    "VectorType": "SYN_FLOOD"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Visibilidad de los eventos de DDoS en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener información sobre la API, consulte ListAttacks en la Referencia de comandos de la AWS CLI.

`list-protections`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-protections`.

AWS CLI

Para recuperar los resúmenes de protección de AWS Shield Avanzado

En el siguiente ejemplo de `list-protections`, se recuperan resúmenes de las protecciones que están habilitadas para la cuenta.

```
aws shield list-protections
```

Salida:

```
{
    "Protections": [
        {
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "Name": "Protection for CloudFront distribution",
            "ResourceArn": "arn:aws:cloudfront::123456789012:distribution/
E198WC25FXOWY8"
        }
    ]
}
```

Para obtener más información, consulte Cómo agregar y configurar protecciones de recursos con Shield Advanced en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener información sobre la API, consulte ListProtections en la Referencia de comandos de la AWS CLI.

`update-emergency-contact-settings`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-emergency-contact-settings`.

AWS CLI

Para definir las direcciones de correo electrónico de emergencia que tenga archivadas con el DRT

En el siguiente ejemplo de `update-emergency-contact-settings`, se definen dos direcciones de correo electrónico con las que el DRT debe contactar cuando responda a un presunto ataque.

```
aws shield update-emergency-contact-settings \
        --emergency-contact-list EmailAddress=ops@example.com EmailAddress=ddos-notifications@example.com
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Cómo funcionan AWS Shield y Shield Advanced en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener información sobre la API, consulte UpdateEmergencyContactSettings en la Referencia de comandos de la AWS CLI.

`update-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-subscription`.

AWS CLI

Para modificar la suscripción a AWS Shield Avanzado de la cuenta

En el siguiente ejemplo de `update-subscription`, se permite la renovación automática de la suscripción a AWS Shield Avanzado de la cuenta.

```
aws shield update-subscription \
    --auto-renew ENABLED
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Cómo funcionan AWS Shield y Shield Advanced en la Guía para desarrolladores de AWS Shield Avanzado.

- Para obtener detalles sobre la API, consulte UpdateSubscription en la Referencia de comandos de la AWS CLI.

Ejemplos de Signer que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Signer.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`cancel-signing-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-signing-profile`.

AWS CLI

Para eliminar un perfil de firma

En el siguiente ejemplo de `cancel-signing-profile`, se elimina un perfil de firma existente de AWS Signer.

```
aws signer cancel-signing-profile \
```

```
    --profile-name MyProfile1
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte CancelSigningProfile en la Referencia de comandos de la AWS CLI.

`describe-signing-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-signing-job`.

AWS CLI

Para mostrar los detalles de un trabajo de firma

En el siguiente ejemplo de `describe-signing-job`, se muestran los detalles del trabajo de firma especificado.

```
aws signer describe-signing-job \
    --job-id 2065c468-73e2-4385-a6c9-0123456789abc
```

Salida:

```
{
    "status": "Succeeded",
    "completedAt": 1568412037,
    "platformId": "AmazonFreeRTOS-Default",
    "signingMaterial": {
        "certificateArn": "arn:aws:acm:us-
west-2:123456789012:certificate/6a55389b-306b-4e8c-a95c-0123456789abc"
    },
    "statusReason": "Signing Succeeded",
    "jobId": "2065c468-73e2-4385-a6c9-0123456789abc",
    "source": {
        "s3": {
            "version": "PNyFaUTgsQh5ZdMCcoCe6pT1gOpgB_M4",
            "bucketName": "signer-source",
            "key": "MyCode.rb"
        }
    },
    "profileName": "MyProfile2",
    "signedObject": {
        "s3": {
```

```
            "bucketName": "signer-destination",
            "key": "signed-2065c468-73e2-4385-a6c9-0123456789abc"
        }
    },
    "requestedBy": "arn:aws:iam::123456789012:user/maria",
    "createdAt": 1568412036
}
```

- Para obtener información sobre la API, consulte DescribeSigningJob en la Referencia de comandos de la AWS CLI.

`get-signing-platform`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-signing-platform`.

AWS CLI

Para mostrar los detalles de una plataforma de firma

En el siguiente ejemplo de `get-signing-platform`, se muestran los detalles de la plataforma de firma especificada.

```
aws signer get-signing-platform \
    --platform-id AmazonFreeRTOS-TI-CC3220SF
```

Salida:

```
{
    "category": "AWS",
    "displayName": "Amazon FreeRTOS SHA1-RSA CC3220SF-Format",
    "target": "SHA1-RSA-TISHA1",
    "platformId": "AmazonFreeRTOS-TI-CC3220SF",
    "signingConfiguration": {
        "encryptionAlgorithmOptions": {
            "defaultValue": "RSA",
            "allowedValues": [
                "RSA"
            ]
        },
        "hashAlgorithmOptions": {
            "defaultValue": "SHA1",
            "allowedValues": [
```

```
                "SHA1"
            ]
        }
    },
    "maxSizeInMB": 16,
    "partner": "AmazonFreeRTOS",
    "signingImageFormat": {
        "defaultFormat": "JSONEmbedded",
        "supportedFormats": [
            "JSONEmbedded"
        ]
    }
}
```

- Para obtener información sobre la API, consulte GetSigningPlatform en la Referencia de comandos de la AWS CLI.

`get-signing-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-signing-profile`.

AWS CLI

Para mostrar los detalles de un perfil de firma

En el siguiente ejemplo de `get-signing-profile`, se muestran los detalles del perfil de firma especificado.

```
aws signer get-signing-profile \
    --profile-name MyProfile3
```

Salida:

```
{
    "platformId": "AmazonFreeRTOS-TI-CC3220SF",
    "profileName": "MyProfile3",
    "status": "Active",
    "signingMaterial": {
        "certificateArn": "arn:aws:acm:us-
west-2:123456789012:certificate/6a55389b-306b-4e8c-a95c-0123456789abc"
    }
}
```

- Para obtener información sobre la API, consulte GetSigningProfile en la Referencia de comandos de la AWS CLI.

`list-signing-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-signing-jobs`.

AWS CLI

Para enumerar todos los trabajos de firma

En el siguiente ejemplo de `list-signing-jobs`, se muestran los detalles de todos los trabajos de firma de la cuenta.

```
aws signer list-signing-jobs
```

En este ejemplo, se devuelven dos trabajos, uno correcto y otro erróneo.

```
{
    "jobs": [
        {
            "status": "Succeeded",
            "signingMaterial": {
                "certificateArn": "arn:aws:acm:us-
west-2:123456789012:certificate/6a55389b-306b-4e8c-a95c-0123456789abc"
            },
            "jobId": "2065c468-73e2-4385-a6c9-0123456789abc",
            "source": {
                "s3": {
                    "version": "PNyFaUTgsQh5ZdMCcoCe6pT1gOpgB_M4",
                    "bucketName": "signer-source",
                    "key": "MyCode.rb"
                }
            },
            "signedObject": {
                "s3": {
                    "bucketName": "signer-destination",
                    "key": "signed-2065c468-73e2-4385-a6c9-0123456789abc"
                }
            },
            "createdAt": 1568412036
        },
```

```
        {
            "status": "Failed",
            "source": {
                "s3": {
                    "version": "PNyFaUTgsQh5ZdMCcoCe6pT1gOpgB_M4",
                    "bucketName": "signer-source",
                    "key": "MyOtherCode.rb"
                }
            },
            "signingMaterial": {
                "certificateArn": "arn:aws:acm:us-
west-2:123456789012:certificate/6a55389b-306b-4e8c-a95c-0123456789abc"
            },
            "createdAt": 1568402690,
            "jobId": "74d9825e-22fc-4a0d-b962-0123456789abc"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListSigningJobs en la Referencia de comandos de la AWS CLI.

`list-signing-platforms`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-signing-platforms`.

AWS CLI

Para enumerar todas las plataformas de firma

En el siguiente ejemplo de `list-signing-platforms`, se muestran los detalles de todas las plataformas de firma disponibles.

```
aws signer list-signing-platforms
```

Salida:

```
{
    "platforms": [
        {
            "category": "AWS",
            "displayName": "AWS IoT Device Management SHA256-ECDSA ",
```

```
            "target": "SHA256-ECDSA",
            "platformId": "AWSIoTDeviceManagement-SHA256-ECDSA",
            "signingConfiguration": {
                "encryptionAlgorithmOptions": {
                    "defaultValue": "ECDSA",
                    "allowedValues": [
                        "ECDSA"
                    ]
                },
                "hashAlgorithmOptions": {
                    "defaultValue": "SHA256",
                    "allowedValues": [
                        "SHA256"
                    ]
                }
            },
            "maxSizeInMB": 2048,
            "partner": "AWSIoTDeviceManagement",
            "signingImageFormat": {
                "defaultFormat": "JSONDetached",
                "supportedFormats": [
                    "JSONDetached"
                ]
            }
        },
        {
            "category": "AWS",
            "displayName": "Amazon FreeRTOS SHA1-RSA CC3220SF-Format",
            "target": "SHA1-RSA-TISHA1",
            "platformId": "AmazonFreeRTOS-TI-CC3220SF",
            "signingConfiguration": {
                "encryptionAlgorithmOptions": {
                    "defaultValue": "RSA",
                    "allowedValues": [
                        "RSA"
                    ]
                },
                "hashAlgorithmOptions": {
                    "defaultValue": "SHA1",
                    "allowedValues": [
                        "SHA1"
                    ]
                }
            },
```

```
            "maxSizeInMB": 16,
            "partner": "AmazonFreeRTOS",
            "signingImageFormat": {
                "defaultFormat": "JSONEmbedded",
                "supportedFormats": [
                    "JSONEmbedded"
                ]
            }
        },
        {
            "category": "AWS",
            "displayName": "Amazon FreeRTOS SHA256-ECDSA",
            "target": "SHA256-ECDSA",
            "platformId": "AmazonFreeRTOS-Default",
            "signingConfiguration": {
                "encryptionAlgorithmOptions": {
                    "defaultValue": "ECDSA",
                    "allowedValues": [
                        "ECDSA"
                    ]
                },
                "hashAlgorithmOptions": {
                    "defaultValue": "SHA256",
                    "allowedValues": [
                        "SHA256"
                    ]
                }
            },
            "maxSizeInMB": 16,
            "partner": "AmazonFreeRTOS",
            "signingImageFormat": {
                "defaultFormat": "JSONEmbedded",
                "supportedFormats": [
                    "JSONEmbedded"
                ]
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListSigningPlatforms en la Referencia de comandos de la AWS CLI.

`list-signing-profiles`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-signing-profiles`.

AWS CLI

Para enumerar todos los perfiles de firma

En el siguiente ejemplo de `list-signing-profiles`, se muestran los detalles de todos los perfiles de firma de la cuenta.

```
aws signer list-signing-profiles
```

Salida:

```
{
    "profiles": [
        {
            "platformId": "AmazonFreeRTOS-TI-CC3220SF",
            "profileName": "MyProfile4",
            "status": "Active",
            "signingMaterial": {
                "certificateArn": "arn:aws:acm:us-
west-2:123456789012:certificate/6a55389b-306b-4e8c-a95c-0123456789abc"
            }
        },
        {
            "platformId": "AWSIoTDeviceManagement-SHA256-ECDSA",
            "profileName": "MyProfile5",
            "status": "Active",
            "signingMaterial": {
                "certificateArn": "arn:aws:acm:us-
west-2:123456789012:certificate/6a55389b-306b-4e8c-a95c-0123456789abc"
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListSigningProfiles en la Referencia de comandos de la AWS CLI.

`put-signing-profile`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-signing-profile`.

AWS CLI

Para crear un perfil de firma

En el siguiente ejemplo de `put-signing-profile`, se crea un perfil de firma con el certificado y la plataforma especificados.

```
aws signer put-signing-profile \
    --profile-name MyProfile6 \
    --signing-material certificateArn=arn:aws:acm:us-
west-2:123456789012:certificate/6a55389b-306b-4e8c-a95c-0123456789abc \
    --platform AmazonFreeRTOS-TI-CC3220SF
```

Salida:

```
{
    "arn": "arn:aws:signer:us-west-2:123456789012:/signing-profiles/MyProfile6"
}
```

- Para obtener información sobre la API, consulte PutSigningProfile en la Referencia de comandos de la AWS CLI.

`start-signing-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-signing-job`.

AWS CLI

Para iniciar un trabajo de firma

En el siguiente ejemplo de `start-signing-job`, se inicia un trabajo de firma en el código que se encuentra en el origen especificado. Utiliza el perfil especificado para firmar y coloca el código firmado en el destino especificado.

```
aws signer start-signing-job \
    --source 's3={bucketName=signer-
source,key=MyCode.rb,version=PNyFaUTgsQh5ZdMCcoCe6pT1gOpgB_M4}' \
```

```
    --destination 's3={bucketName=signer-destination,prefix=signed-}' \
    --profile-name MyProfile7
```

El resultado es el ID del trabajo de firma.

```
{
    "jobId": "2065c468-73e2-4385-a6c9-0123456789abc"
}
```

- Para obtener información sobre la API, consulte StartSigningJob en la Referencia de comandos de la AWS CLI.

Ejemplos de Snowball Edge que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes mediante la AWS Command Line Interface con Snowball Edge.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`get-snowball-usage`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-snowball-usage`.

AWS CLI

Para obtener información sobre el límite del servicio Snowball para la cuenta

En el siguiente ejemplo de `get-snowball-usage`, se muestra información sobre el límite de servicio de Snowball para su cuenta, así como el número de Snowball que está usando su cuenta.

```
aws snowball get-snowball-usage
```

Salida:

```
{
    "SnowballLimit": 1,
    "SnowballsInUse": 0
}
```

Para obtener más información, consulte AWS Snowball Edge Limits en la Guía para desarrolladores de AWS Snowball.

- Para obtener información sobre la API, consulte GetSnowballUsage en la Referencia de comandos de la AWS CLI.

`list-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-jobs`.

AWS CLI

Para mostrar los trabajos actuales de Snowball en su cuenta

En el siguiente ejemplo de `list-jobs`, se muestra una matriz de objetos `JobListEntry`. En este ejemplo, se enumera un solo trabajo.

```
aws snowball list-jobs
```

Salida:

```
{
    "JobListEntries": [
        {
            "CreationDate": 2016-09-27T14:50Z,
             "Description": "Important Photos 2016-08-11",
             "IsMaster": TRUE,
             "JobId": "ABCd1e324fe-022f-488e-a98b-3b0566063db1",
             "JobState": "Complete",
             "JobType": "IMPORT",
             "SnowballType": "EDGE"
        }
   ]
```

```
}
```

Para obtener más información, consulte Jobs for AWS Snowball Edge devices en la Guía para desarrolladores de AWS Snowball.

- Para obtener información sobre la API, consulte ListJobs en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon SNS que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon SNS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica a través de llamadas a varias funciones dentro del servicio o combinado con otros Servicios de AWS.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones
- Escenarios

Acciones

`add-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-permission`.

AWS CLI

Para añadir un permiso a un tema

En el siguiente ejemplo de `add-permission`, se agrega el permiso para que la cuenta de AWS `987654321098` utilice la acción `Publish` con el tema especificado en la cuenta de AWS `123456789012`.

```
aws sns add-permission \
    --topic-arn arn:aws:sns:us-west-2:123456789012:MyTopic \
    --label Publish-Permission \
    --aws-account-id 987654321098 \
    --action-name Publish
```

Este comando no genera ninguna salida.

- Para obtener más información sobre la API, consulte AddPermission en la Referencia de comandos de la AWS CLI.

`check-if-phone-number-is-opted-out`

En el siguiente ejemplo de código, se muestra cómo utilizar `check-if-phone-number-is-opted-out`.

AWS CLI

Comprobar que se ha cancelado la recepción de mensajes SMS en un número de teléfono

El siguiente ejemplo de `check-if-phone-number-is-opted-out` comprueba si el número de teléfono especificado está excluido de la recepción de mensajes SMS de la cuenta de AWS actual.

```
aws sns check-if-phone-number-is-opted-out \
    --phone-number +1555550100
```

Salida:

```
{
    "isOptedOut": false
}
```

- Para obtener detalles sobre la API, consulte CheckIfPhoneNumberIsOptedOut en la Referencia de comandos de la AWS CLI.

`confirm-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `confirm-subscription`.

AWS CLI

Confirmar una suscripción

El siguiente comando `confirm-subscription` completa el proceso de confirmación que se inició al suscribirse a un tema de SNS denominado `my-topic`. El parámetro --token proviene del mensaje de confirmación enviado al punto de conexión de notificación especificado en la llamada de suscripción.

```
aws sns confirm-subscription \
    --topic-arn arn:aws:sns:us-west-2:123456789012:my-topic \
    --
token 2336412f37fb687f5d51e6e241d7700ae02f7124d8268910b858cb4db727ceeb2474bb937929d3bdd7ce5d
```

Salida:

```
{
    "SubscriptionArn": "arn:aws:sns:us-west-2:123456789012:my-
topic:8a21d249-4329-4871-acc6-7be709c6ea7f"
}
```

- Para obtener detalles sobre la API, consulte ConfirmSubscription en la Referencia del comando de la AWS CLI.

`create-platform-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-platform-application`.

AWS CLI

Para crear una aplicación de plataforma

En el siguiente ejemplo de `create-platform-application`, se crea una aplicación de la plataforma Google Firebase con la credencial de plataforma especificada.

```
aws sns create-platform-application \
    --name MyApplication \
    --platform GCM \
    --attributes PlatformCredential=EXAMPLEabcd12345jklm67890stuv12345bcdef
```

Salida:

```
{
    "PlatformApplicationArn": "arn:aws:sns:us-west-2:123456789012:app/GCM/
MyApplication"
}
```

- Para obtener información sobre la API, consulte CreatePlatformApplication en la Referencia de comandos de la AWS CLI.

`create-topic`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-topic`.

AWS CLI

Creación de un tema de SNS

En el siguiente ejemplo de `create-topic` se crea un tema de SNS denominado `my-topic`.

```
aws sns create-topic \
    --name my-topic
```

Salida:

```
{
    "ResponseMetadata": {
        "RequestId": "1469e8d7-1642-564e-b85d-a19b4b341f83"
    },
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
}
```

Para obtener más información, consulte Uso de la interfaz de la línea de comandos de AWS con Amazon SQS y Amazon SNS en la Guía del usuario de la interfaz de la línea de comandos de AWS.

- Para obtener detalles sobre la API, consulte CreateTopic en la Referencia del comando de la AWS CLI.

`delete-endpoint`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-endpoint`.

AWS CLI

Para eliminar un punto de conexión de aplicación de plataforma

En el siguiente ejemplo de `delete-endpoint`, se elimina el punto de conexión de la aplicación de la plataforma especificado.

```
aws sns delete-endpoint \
    --endpoint-arn arn:aws:sns:us-west-2:123456789012:endpoint/GCM/
MyApplication/12345678-abcd-9012-efgh-345678901234
```

Este comando no genera ninguna salida.

- Para obtener detalles sobre la API, consulte DeleteEndpoint en la Referencia de comandos de la AWS CLI.

`delete-platform-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-platform-application`.

AWS CLI

Para eliminar una aplicación de plataforma

En el siguiente ejemplo de `delete-platform-application`, se elimina la aplicación de la plataforma especificada.

```
aws sns delete-platform-application \
    --platform-application-arn arn:aws:sns:us-west-2:123456789012:app/ADM/
MyApplication
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeletePlatformApplication en la Referencia de comandos de la AWS CLI.

`delete-topic`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-topic`.

AWS CLI

Eliminación de un tema de SNS

El siguiente ejemplo de `delete-topic` elimina el tema de SNS especificado.

```
aws sns delete-topic \
    --topic-arn "arn:aws:sns:us-west-2:123456789012:my-topic"
```

Este comando no genera ninguna salida.

- Para obtener detalles sobre la API, consulte DeleteTopic en la Referencia del comando de la AWS CLI.

`get-endpoint-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-endpoint-attributes`.

AWS CLI

Para enumerar los atributos de punto de conexión de la aplicación de plataforma

En el siguiente ejemplo de `get-endpoint-attributes`, se enumeran los atributos del punto de conexión de la aplicación de la plataforma especificado.

```
aws sns get-endpoint-attributes \
    --endpoint-arn arn:aws:sns:us-west-2:123456789012:endpoint/GCM/
MyApplication/12345678-abcd-9012-efgh-345678901234
```

Salida:

```
{
    "Attributes": {
        "Enabled": "true",
        "Token": "EXAMPLE12345..."
    }
}
```

- Para obtener información sobre la API, consulte GetEndpointAttributes en la Referencia de comandos de la AWS CLI.

`get-platform-application-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-platform-application-attributes`.

AWS CLI

Para enumerar los atributos de la aplicación de plataforma

En el siguiente ejemplo de `get-platform-application-attributes`, se enumeran los atributos de la aplicación de la plataforma especificada.

```
aws sns get-platform-application-attributes \
    --platform-application-arn arn:aws:sns:us-west-2:123456789012:app/MPNS/
MyApplication
```

Salida:

```
{
    "Attributes": {
        "Enabled": "true",
        "SuccessFeedbackSampleRate": "100"
    }
}
```

- Para obtener información sobre la API, consulte GetPlatformApplicationAttributes en la Referencia de comandos de la AWS CLI.

`get-sms-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-sms-attributes`.

AWS CLI

Mostrar los atributos predeterminados de los mensajes SMS

En el siguiente ejemplo de `get-sms-attributes`, se muestran los atributos predeterminados para enviar mensajes SMS.

```
aws sns get-sms-attributes
```

Salida:

```
{
    "attributes": {
        "DefaultSenderID": "MyName"
    }
}
```

- Para obtener detalles sobre la API, consulte GetSMSAttributes en la Referencia de comandos de la AWS CLI.

`get-subscription-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-subscription-attributes`.

AWS CLI

Para recuperar los atributos de suscripción de un tema

En el siguiente ejemplo de `get-subscription-attributes`, se muestran los atributos de la suscripción especificada. Puede obtener el `subscription-arn` del resultado del comando `list-subscriptions`.

```
aws sns get-subscription-attributes \
    --subscription-arn "arn:aws:sns:us-west-2:123456789012:my-
topic:8a21d249-4329-4871-acc6-7be709c6ea7f"
```

Salida:

```
{
    "Attributes": {
        "Endpoint": "my-email@example.com",
        "Protocol": "email",
        "RawMessageDelivery": "false",
        "ConfirmationWasAuthenticated": "false",
        "Owner": "123456789012",
        "SubscriptionArn": "arn:aws:sns:us-west-2:123456789012:my-
topic:8a21d249-4329-4871-acc6-7be709c6ea7f",
        "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
    }
```

```
}
```

- Para obtener información sobre la API, consulte GetSubscriptionAttributes en la Referencia de comandos de la AWS CLI.

`get-topic-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-topic-attributes`.

AWS CLI

Recuperación de los atributos de un tema

En el siguiente ejemplo de `get-topic-attributes`, se muestran los atributos del tema especificado.

```
aws sns get-topic-attributes \
    --topic-arn "arn:aws:sns:us-west-2:123456789012:my-topic"
```

Salida:

```
{
    "Attributes": {
        "SubscriptionsConfirmed": "1",
        "DisplayName": "my-topic",
        "SubscriptionsDeleted": "0",
        "EffectiveDeliveryPolicy": "{\"http\":{\"defaultHealthyRetryPolicy\":
{\"minDelayTarget\":20,\"maxDelayTarget\":20,\"numRetries\":3,\"numMaxDelayRetries
\":0,\"numNoDelayRetries\":0,\"numMinDelayRetries\":0,\"backoffFunction\":\"linear
\"},\"disableSubscriptionOverrides\":false}}",
        "Owner": "123456789012",
        "Policy": "{\"Version\":\"2008-10-17\",\"Id\":\"__default_policy_ID\",
\"Statement\":[{\"Sid\":\"__default_statement_ID\",\"Effect\":\"Allow\",\"Principal
\":{\"AWS\":\"*\"},\"Action\":[\"SNS:Subscribe\",\"SNS:ListSubscriptionsByTopic
\",\"SNS:DeleteTopic\",\"SNS:GetTopicAttributes\",\"SNS:Publish\",
\"SNS:RemovePermission\",\"SNS:AddPermission\",\"SNS:SetTopicAttributes\"],
\"Resource\":\"arn:aws:sns:us-west-2:123456789012:my-topic\",\"Condition\":
{\"StringEquals\":{\"AWS:SourceOwner\":\"0123456789012\"}}}]}",
        "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic",
        "SubscriptionsPending": "0"
    }
}
```

- Para obtener detalles sobre la API, consulte GetTopicAttributes en la Referencia del comando de la AWS CLI.

`list-endpoints-by-platform-application`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-endpoints-by-platform-application`.

AWS CLI

Para enumerar los puntos de conexión de una aplicación de plataforma

En el siguiente ejemplo de `list-endpoints-by-platform-application`, se enumeran los puntos de conexión y los atributos de los puntos de conexión de la aplicación de la plataforma especificada.

```
aws sns list-endpoints-by-platform-application \
    --platform-application-arn arn:aws:sns:us-west-2:123456789012:app/GCM/
MyApplication
```

Salida:

```
{
    "Endpoints": [
        {
            "Attributes": {
                "Token": "EXAMPLE12345...,
                "Enabled": "true"
            },
            "EndpointArn": "arn:aws:sns:us-west-2:123456789012:endpoint/GCM/
MyApplication/12345678-abcd-9012-efgh-345678901234"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListEndpointsByPlatformApplication en la Referencia de comandos de la AWS CLI.

`list-phone-numbers-opted-out`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-phone-numbers-opted-out`.

AWS CLI

Mostrar exclusiones de mensajes SMS

El siguiente ejemplo de `list-phone-numbers-opted-out` muestra los números de teléfono excluidos de la recepción de mensajes SMS.

```
aws sns list-phone-numbers-opted-out
```

Salida:

```
{
    "phoneNumbers": [
        "+15555550100"
    ]
}
```

- Para obtener detalles sobre la API, consulte ListPhoneNumbersOptedOut en la Referencia de comandos de la AWS CLI.

`list-platform-applications`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-platform-applications`.

AWS CLI

Para enumerar las aplicaciones de plataforma

En el siguiente ejemplo de `list-platform-applications`, se enumeran las aplicaciones de plataforma para ADM y MPNS.

```
aws sns list-platform-applications
```

Salida:

```
{
    "PlatformApplications": [
        {
            "PlatformApplicationArn": "arn:aws:sns:us-west-2:123456789012:app/ADM/
MyApplication",
            "Attributes": {
                "SuccessFeedbackSampleRate": "100",
```

```
                "Enabled": "true"
            }
        },
        {
            "PlatformApplicationArn": "arn:aws:sns:us-west-2:123456789012:app/MPNS/
MyOtherApplication",
            "Attributes": {
                "SuccessFeedbackSampleRate": "100",
                "Enabled": "true"
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListPlatformApplications en la Referencia de comandos de la AWS CLI.

`list-subscriptions-by-topic`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-subscriptions-by-topic`.

AWS CLI

Para enumerar las suscripciones asociadas a un tema

En el siguiente ejemplo de `list-subscriptions-by-topic`, se recupera una lista de las suscripciones de SNS asociadas al tema especificado.

```
aws sns list-subscriptions-by-topic \
    --topic-arn "arn:aws:sns:us-west-2:123456789012:my-topic"
```

Salida:

```
{
    "Subscriptions": [
        {
            "Owner": "123456789012",
            "Endpoint": "my-email@example.com",
            "Protocol": "email",
            "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic",
            "SubscriptionArn": "arn:aws:sns:us-west-2:123456789012:my-
topic:8a21d249-4329-4871-acc6-7be709c6ea7f"
```

```
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListSubscriptionsByTopic en la Referencia de comandos de la AWS CLI.

`list-subscriptions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-subscriptions`.

AWS CLI

Mostrar las suscripciones de SNS

En el siguiente ejemplo de `list-subscriptions`, se muestra una lista de las suscripciones de SNS de la cuenta de AWS.

```
aws sns list-subscriptions
```

Salida:

```
{
    "Subscriptions": [
        {
            "Owner": "123456789012",
            "Endpoint": "my-email@example.com",
            "Protocol": "email",
            "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic",
            "SubscriptionArn": "arn:aws:sns:us-west-2:123456789012:my-
topic:8a21d249-4329-4871-acc6-7be709c6ea7f"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte ListSubscriptions en la Referencia del comando de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un tema

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran las etiquetas de un tema de Amazon SNS específico.

```
aws sns list-tags-for-resource \
    --resource-arn arn:aws:sns:us-west-2:123456789012:MyTopic
```

Salida:

```
{
    "Tags": [
        {
            "Key": "Team",
            "Value": "Alpha"
        }
    ]
}
```

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-topics`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-topics`.

AWS CLI

Mostrar los temas de SNS

En el siguiente ejemplo de `list-topics`, se muestran todos los temas de SNS de la cuenta de AWS.

```
aws sns list-topics
```

Salida:

```
{
    "Topics": [
```

```
        {
            "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
        }
    ]
}
```

- Para obtener detalles sobre la API, consulte ListTopics en la Referencia del comando de la AWS CLI.

`opt-in-phone-number`

En el siguiente ejemplo de código, se muestra cómo utilizar `opt-in-phone-number`.

AWS CLI

Para optar por recibir mensajes SMS

El siguiente ejemplo de `opt-in-phone-number`, se permite que el número de teléfono especificado reciba mensajes SMS.

```
aws sns opt-in-phone-number \
    --phone-number +15555550100
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte OptInPhoneNumber en la Referencia de comandos de la AWS CLI.

`publish`

En el siguiente ejemplo de código, se muestra cómo utilizar `publish`.

AWS CLI

Ejemplo 1: publicar un mensaje en un tema

En el siguiente ejemplo de `publish` se publica el mensaje especificado en el tema de SNS especificado. El mensaje proviene de un archivo de texto que le permite incluir saltos de línea.

```
aws sns publish \
    --topic-arn "arn:aws:sns:us-west-2:123456789012:my-topic" \
```

```
    --message file://message.txt
```

Contenido de `message.txt`:

```
Hello World
Second Line
```

Salida:

```
{
    "MessageId": "123a45b6-7890-12c3-45d6-111122223333"
}
```

Ejemplo 2: publicar un mensaje SMS en un número de teléfono

En el siguiente ejemplo de `publish`, se publica el mensaje `Hello world!` en el número de teléfono `+1-555-555-0100`.

```
aws sns publish \
    --message "Hello world!" \
    --phone-number +1-555-555-0100
```

Salida:

```
{
    "MessageId": "123a45b6-7890-12c3-45d6-333322221111"
}
```

- Para obtener detalles sobre la API, consulte Publish en la Referencia del comando de la AWS CLI.

`put-data-protection-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-data-protection-policy`.

AWS CLI

Para definir la política de protección de datos

Ejemplo 1: cómo impedir que los publicadores publiquen mensajes que incluyan CreditCardNumber

En el siguiente ejemplo de `put-data-protection-policy`, se impide a los publicadores publicar mensajes con CreditCardNumber.

```
aws sns put-data-protection-policy \
    --resource-arn arn:aws:sns:us-east-1:123456789012:mytopic \
    --data-protection-policy "{\"Name\":\"data_protection_policy\",\"Description
\":\"Example data protection policy\",\"Version\":\"2021-06-01\",\"Statement
\":[{\"DataDirection\":\"Inbound\",\"Principal\":[\"*\"],\"DataIdentifier\":
[\"arn:aws:dataprotection::aws:data-identifier/CreditCardNumber\"],\"Operation\":
{\"Deny\":{}}}]}"
```

Este comando no genera ninguna salida.

Ejemplo 2: cómo cargar parámetros de un archivo

En el siguiente ejemplo de `put-data-protection-policy`, se cargan parámetros de un archivo.

```
aws sns put-data-protection-policy \
    --resource-arn arn:aws:sns:us-west-2:123456789012:MyTopic \
    --data-protection-policy file://policy.json
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutDataProtectionPolicy en la Referencia de comandos de la AWS CLI.

`remove-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-permission`.

AWS CLI

Para eliminar un permiso de un tema

En el siguiente ejemplo de `remove-permission`, se retira el permiso `Publish-Permission` del tema especificado.

```
aws sns remove-permission \
    --topic-arn arn:aws:sns:us-west-2:123456789012:MyTopic \
    --label Publish-Permission
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte RemovePermission en la Referencia de comandos de la AWS CLI.

`set-endpoint-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-endpoint-attributes`.

AWS CLI

Para definir los atributos de punto de conexión

En el siguiente ejemplo de `set-endpoint-attributes`, se desactiva el punto de conexión de la aplicación de la plataforma especificado.

```
aws sns set-endpoint-attributes \
    --endpoint-arn arn:aws:sns:us-west-2:123456789012:endpoint/GCM/
MyApplication/12345678-abcd-9012-efgh-345678901234 \
    --attributes Enabled=false
```

Salida:

```
{
    "Attributes": {
        "Enabled": "false",
        "Token": "EXAMPLE12345..."
    }
}
```

- Para obtener información sobre la API, consulte SetEndpointAttributes en la Referencia de comandos de la AWS CLI.

`set-platform-application-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-platform-application-attributes`.

AWS CLI

Para definir los atributos de una aplicación de plataforma

En el siguiente ejemplo de `set-platform-application-attributes`, se establece el atributo `EventDeliveryFailure` de la aplicación de plataforma especificada en el ARN del tema de Amazon SNS especificado.

```
aws sns set-platform-application-attributes \
    --platform-application-arn arn:aws:sns:us-west-2:123456789012:app/GCM/
MyApplication \
    --attributes EventDeliveryFailure=arn:aws:sns:us-
west-2:123456789012:AnotherTopic
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte SetPlatformApplicationAttributes en la Referencia de comandos de la AWS CLI.

`set-sms-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-sms-attributes`.

AWS CLI

Establecimiento de los atributos de los mensajes SMS

En el siguiente ejemplo de `set-sms-attributes`, se establece el ID de remitente predeterminado para los mensajes SMS a `MyName`.

```
aws sns set-sms-attributes \
    --attributes DefaultSenderID=MyName
```

Este comando no genera ninguna salida.

- Para obtener detalles sobre la API, consulte SetSMSAttributes en la Referencia de comandos de la AWS CLI.

`set-subscription-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-subscription-attributes`.

AWS CLI

Establecimiento de los atributos de suscripción

En el siguiente ejemplo de `set-subscription-attributes`, se establece el atributo `RawMessageDelivery` en una suscripción de SQS.

```
aws sns set-subscription-attributes \
    --subscription-arn arn:aws:sns:us-
east-1:123456789012:mytopic:f248de18-2cf6-578c-8592-b6f1eaa877dc \
    --attribute-name RawMessageDelivery \
    --attribute-value true
```

Este comando no genera ninguna salida.

En el siguiente ejemplo de `set-subscription-attributes`, se establece un atributo `FilterPolicy` en una suscripción de SQS.

```
aws sns set-subscription-attributes \
    --subscription-arn arn:aws:sns:us-
east-1:123456789012:mytopic:f248de18-2cf6-578c-8592-b6f1eaa877dc \
    --attribute-name FilterPolicy \
    --attribute-value "{ \"anyMandatoryKey\": [\"any\", \"of\", \"these\"] }"
```

Este comando no genera ninguna salida.

En el siguiente ejemplo de `set-subscription-attributes`, se elimina el atributo `FilterPolicy` de una suscripción de SQS.

```
aws sns set-subscription-attributes \
    --subscription-arn arn:aws:sns:us-
east-1:123456789012:mytopic:f248de18-2cf6-578c-8592-b6f1eaa877dc \
    --attribute-name FilterPolicy \
    --attribute-value "{}"
```

Este comando no genera ninguna salida.

- Para obtener detalles sobre la API, consulte SetSubscriptionAttributes en la Referencia de comandos de la AWS CLI.

`set-topic-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-topic-attributes`.

AWS CLI

Establecimiento de un atributo para un tema

En el ejemplo de `set-topic-attributes` siguiente, se establece el atributo `DisplayName` del tema especificado.

```
aws sns set-topic-attributes \
    --topic-arn arn:aws:sns:us-west-2:123456789012:MyTopic \
    --attribute-name DisplayName \
    --attribute-value MyTopicDisplayName
```

Este comando no genera ninguna salida.

- Para obtener detalles sobre la API, consulte SetTopicAttributes en la Referencia de comandos de la AWS CLI.

`subscribe`

En el siguiente ejemplo de código, se muestra cómo utilizar `subscribe`.

AWS CLI

Suscripción a un tema

El siguiente comando `subscribe` suscribe una dirección de correo electrónico al tema especificado.

```
aws sns subscribe \
    --topic-arn arn:aws:sns:us-west-2:123456789012:my-topic \
    --protocol email \
    --notification-endpoint my-email@example.com
```

Salida:

```
{
    "SubscriptionArn": "pending confirmation"
}
```

- Para obtener detalles sobre la API, consulte Subscribe en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Añadir una etiqueta a un tema

El siguiente ejemplo de `tag-resource` añade una etiqueta de metadatos al tema de Amazon SNS especificado.

```
aws sns tag-resource \
    --resource-arn arn:aws:sns:us-west-2:123456789012:MyTopic \
    --tags Key=Team,Value=Alpha
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`unsubscribe`

En el siguiente ejemplo de código, se muestra cómo utilizar `unsubscribe`.

AWS CLI

Cancelación de la suscripción a un tema

En el siguiente ejemplo de `unsubscribe`, se elimina la suscripción especificada de un tema.

```
aws sns unsubscribe \
    --subscription-arn arn:aws:sns:us-west-2:0123456789012:my-
topic:8a21d249-4329-4871-acc6-7be709c6ea7f
```

Este comando no genera ninguna salida.

- Para obtener detalles sobre la API, consulte Unsubscribe en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar una etiqueta de un tema

En el siguiente ejemplo de `untag-resource`, se eliminan las etiquetas con las claves especificadas del tema de Amazon SNS indicado.

```
aws sns untag-resource \
    --resource-arn arn:aws:sns:us-west-2:123456789012:MyTopic \
    --tag-keys Team
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

Escenarios

Creación de un punto de conexión de la plataforma para notificaciones push

El siguiente ejemplo de código indica cómo crear un punto de enlace de la plataforma para las notificaciones push de Amazon SNS.

AWS CLI

Creación de un punto de conexión de aplicación de plataforma

En el siguiente ejemplo de `create-platform-endpoint`, se crea un punto de conexión para la aplicación de plataforma especificada mediante el token especificado.

```
aws sns create-platform-endpoint \
    --platform-application-arn arn:aws:sns:us-west-2:123456789012:app/GCM/
MyApplication \
    --token EXAMPLE12345...
```

Salida:

```
{
      "EndpointArn": "arn:aws:sns:us-west-2:1234567890:endpoint/GCM/
MyApplication/12345678-abcd-9012-efgh-345678901234"
```

```
}
```

Ejemplos de Amazon SQS usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon SQS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-permission`.

AWS CLI

Para añadir un permiso a una cola

Este ejemplo permite a la cuenta de AWS especificada enviar mensajes a la cola indicada.

Comando:

```
aws sqs add-permission --queue-url https://sqs.us-east-1.amazonaws.com/80398EXAMPLE/
MyQueue --label SendMessagesFromMyQueue --aws-account-ids 12345EXAMPLE --
actions SendMessage
```

Salida:

```
None.
```

- Para obtener más información sobre la API, consulte AddPermission en la Referencia de comandos de la AWS CLI.

`cancel-message-move-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-message-move-task`.

AWS CLI

Para cancelar una tarea de traslado de mensajes

En el siguiente ejemplo de `cancel-message-move-task`, se cancela la tarea de traslado de mensajes especificada.

```
aws sqs cancel-message-move-task \
    --task-handle AQEB6nR4...HzlvZQ==
```

Salida:

```
{
    "ApproximateNumberOfMessagesMoved": 102
}
```

Para obtener más información, consulte Amazon SQS API permissions: Actions and resource reference en la Guía para desarrolladores.

- Para obtener más información sobre la API, consulte CancelMessageMoveTask en la Referencia de comandos de la AWS CLI.

`change-message-visibility-batch`

En el siguiente ejemplo de código, se muestra cómo utilizar `change-message-visibility-batch`.

AWS CLI

Para cambiar la visibilidad del tiempo de espera de varios mensajes en un lote

En este ejemplo, se cambia la visibilidad del tiempo de espera de dos mensajes especificados a 10 horas (10 horas * 60 minutos * 60 segundos).

Comando:

```
aws sqs change-message-visibility-batch --queue-url https://sqs.us-east-1.amazonaws.com/80398EXAMPLE/MyQueue --entries file://change-message-visibility-batch.json
```

Archivo de entrada (change-message-visibility-batch.json):

```
[
  {
    "Id": "FirstMessage",
        "ReceiptHandle": "AQEBhz2q...Jf3kaw==",
        "VisibilityTimeout": 36000
  },
  {
    "Id": "SecondMessage",
        "ReceiptHandle": "AQEBkTUH...HifSnw==",
        "VisibilityTimeout": 36000
  }
]
```

Salida:

```
{
  "Successful": [
    {
      "Id": "SecondMessage"
    },
    {
      "Id": "FirstMessage"
    }
  ]
}
```

- Para obtener detalles sobre la API, consulte ChangeMessageVisibilityBatch en la Referencia de comandos de la AWS CLI.

`change-message-visibility`

En el siguiente ejemplo de código, se muestra cómo utilizar `change-message-visibility`.

AWS CLI

Cambio de la visibilidad del tiempo de espera de un mensaje

En este ejemplo, se cambia la visibilidad del tiempo de espera del mensaje especificado a 10 horas (10 horas * 60 minutos * 60 segundos).

Comando:

```
aws sqs change-message-visibility --queue-url https://sqs.us-east-1.amazonaws.com/80398EXAMPLE/MyQueue --receipt-handle AQEBTpyI...t6HyQg== --visibility-timeout 36000
```

Salida:

```
None.
```

- Para obtener información sobre de la API, consulte ChangeMessageVisibility en la Referencia de comandos de la AWS CLI.

`create-queue`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-queue`.

AWS CLI

Para crear una cola

En este ejemplo, se crea una cola con el nombre especificado, se establece el período de retención de mensajes en 3 días (3 días * 24 horas * 60 minutos * 60 segundos) y se establece la cola de mensajes fallidos en la cola especificada con un recuento máximo de 1000 mensajes recibidos.

Comando:

```
aws sqs create-queue --queue-name MyQueue --attributes file://create-queue.json
```

Archivo de entrada (create-queue.json):

```
{
```

```
  "RedrivePolicy": "{\"deadLetterTargetArn\":\"arn:aws:sqs:us-
east-1:80398EXAMPLE:MyDeadLetterQueue\",\"maxReceiveCount\":\"1000\"}",
  "MessageRetentionPeriod": "259200"
}
```

Salida:

```
{
  "QueueUrl": "https://queue.amazonaws.com/80398EXAMPLE/MyQueue"
}
```

- Para obtener información sobre la API, consulte CreateQueue en la Referencia de comandos de la AWS CLI.

`delete-message-batch`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-message-batch`.

AWS CLI

Eliminación de varios mensajes en un lote

En este ejemplo, se eliminan los mensajes especificados.

Comando:

```
aws sqs delete-message-batch --queue-url https://sqs.us-
east-1.amazonaws.com/80398EXAMPLE/MyQueue --entries file://delete-message-batch.json
```

Archivo de entrada (delete-message-batch.json):

```
[
  {
        "Id": "FirstMessage",
        "ReceiptHandle": "AQEB1mgl...Z4GuLw=="
  },
  {
    "Id": "SecondMessage",
        "ReceiptHandle": "AQEBLsYM...VQubAA=="
  }
]
```

Salida:

```
{
  "Successful": [
    {
      "Id": "FirstMessage"
    },
    {
      "Id": "SecondMessage"
    }
  ]
}
```

- Para obtener información sobre la API, consulte DeleteMessageBatch en la Referencia de comandos de la AWS CLI.

`delete-message`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-message`.

AWS CLI

Eliminación de un mensaje

En este ejemplo, se elimina el mensaje especificado.

Comando:

```
aws sqs delete-message --queue-url https://sqs.us-east-1.amazonaws.com/80398EXAMPLE/MyQueue --receipt-handle AQEBRXTo...q2doVA==
```

Salida:

```
None.
```

- Para obtener información sobre la API, consulte DeleteMessage en la Referencia de comandos de la AWS CLI.

`delete-queue`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-queue`.

AWS CLI

Para eliminar una cola

En este ejemplo, se elimina la cola especificada.

Comando:

```
aws sqs delete-queue --queue-url https://sqs.us-east-1.amazonaws.com/80398EXAMPLE/MyNewerQueue
```

Salida:

```
None.
```

- Para obtener información sobre la API, consulte DeleteQueue en la Referencia de comandos de la AWS CLI.

`get-queue-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-queue-attributes`.

AWS CLI

Obtención de los atributos de una cola

En este ejemplo, se obtienen todos los atributos de la cola especificada.

Comando:

```
aws sqs get-queue-attributes --queue-url https://sqs.us-east-1.amazonaws.com/80398EXAMPLE/MyQueue --attribute-names All
```

Salida:

```
{
  "Attributes": {
    "ApproximateNumberOfMessagesNotVisible": "0",
    "RedrivePolicy": "{\"deadLetterTargetArn\":\"arn:aws:sqs:us-east-1:80398EXAMPLE:MyDeadLetterQueue\",\"maxReceiveCount\":1000}",
    "MessageRetentionPeriod": "345600",
    "ApproximateNumberOfMessagesDelayed": "0",
```

```
    "MaximumMessageSize": "262144",
    "CreatedTimestamp": "1442426968",
    "ApproximateNumberOfMessages": "0",
    "ReceiveMessageWaitTimeSeconds": "0",
    "DelaySeconds": "0",
    "VisibilityTimeout": "30",
    "LastModifiedTimestamp": "1442426968",
    "QueueArn": "arn:aws:sqs:us-east-1:80398EXAMPLE:MyNewQueue"
  }
}
```

En este ejemplo, se obtienen únicamente los atributos de tamaño máximo de mensaje y tiempo de espera de visibilidad de la cola especificada.

Comando:

```
aws sqs get-queue-attributes --queue-url https://sqs.us-
east-1.amazonaws.com/80398EXAMPLE/MyNewQueue --attribute-
names MaximumMessageSize VisibilityTimeout
```

Salida:

```
{
  "Attributes": {
    "VisibilityTimeout": "30",
    "MaximumMessageSize": "262144"
  }
}
```

- Para obtener información sobre la API, consulte GetQueueAttributes en la Referencia de comandos de la AWS CLI.

`get-queue-url`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-queue-url`.

AWS CLI

Obtención de la URL de una cola

En este ejemplo, se obtiene la URL de la cola especificada.

Comando:

```
aws sqs get-queue-url --queue-name MyQueue
```

Salida:

```
{
  "QueueUrl": "https://queue.amazonaws.com/80398EXAMPLE/MyQueue"
}
```

- Para obtener información sobre la API, consulte GetQueueUrl en la Referencia de comandos de la AWS CLI.

`list-dead-letter-source-queues`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-dead-letter-source-queues`.

AWS CLI

Para enumerar las colas de origen de mensajes fallidos

En este ejemplo, se muestran las colas asociadas a la cola de origen de mensajes fallidos especificada.

Comando:

```
aws sqs list-dead-letter-source-queues --queue-url https://sqs.us-
east-1.amazonaws.com/80398EXAMPLE/MyDeadLetterQueue
```

Salida:

```
{
  "queueUrls": [
    "https://queue.amazonaws.com/80398EXAMPLE/MyQueue",
    "https://queue.amazonaws.com/80398EXAMPLE/MyOtherQueue"
  ]
}
```

- Para obtener información sobre la API, consulte ListDeadLetterSourceQueues en la Referencia de comandos de la AWS CLI.

`list-message-move-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-message-move-tasks`.

AWS CLI

Para enumerar las tareas de traslado de mensajes

En el siguiente ejemplo de `list-message-move-tasks`, se enumeran las dos tareas de traslado de mensajes más recientes de la cola especificada.

```
aws sqs list-message-move-tasks \
    --source-arn arn:aws:sqs:us-west-2:80398EXAMPLE:MyQueue \
    --max-results 2
```

Salida:

```
{
    "Results": [
        {
            "TaskHandle": "AQEB6nR4...HzlvZQ==",
            "Status": "RUNNING",
            "SourceArn": "arn:aws:sqs:us-west-2:80398EXAMPLE:MyQueue1",
            "DestinationArn": "arn:aws:sqs:us-west-2:80398EXAMPLE:MyQueue2",
            "MaxNumberOfMessagesPerSecond": 50,
            "ApproximateNumberOfMessagesMoved": 203,
            "ApproximateNumberOfMessagesToMove": 30,
            "StartedTimestamp": 1442428276921
        },

        {
            "Status": "COMPLETED",
            "SourceArn": "arn:aws:sqs:us-west-2:80398EXAMPLE:MyQueue1",
            "DestinationArn": "arn:aws:sqs:us-west-2:80398EXAMPLE:MyQueue2",
            "ApproximateNumberOfMessagesMoved": 29,
            "ApproximateNumberOfMessagesToMove": 0,
            "StartedTimestamp": 1342428272093
        }
    ]
}
```

Para obtener más información, consulte Amazon SQS API permissions: Actions and resource reference en la Guía para desarrolladores.

- Para obtener información sobre la API, consulte ListMessageMoveTasks en la Referencia de comandos de la AWS CLI.

`list-queue-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-queue-tags`.

AWS CLI

Para enumerar todas las etiquetas de asignación de costos de una cola

En el siguiente ejemplo de `list-queue-tags`, se muestran todas las etiquetas de asignación de costos asociadas a la cola especificada.

```
aws sqs list-queue-tags \
    --queue-url https://sqs.us-west-2.amazonaws.com/123456789012/MyQueue
```

Salida:

```
{
    "Tags": {
        "Team": "Alpha"
    }
}
```

Para obtener más información, consulte Listing Cost Allocation Tags en la Guía para desarrolladores de Amazon Simple Queue Service.

- Para obtener información sobre la API, consulte ListQueueTags en la Referencia de comandos de la AWS CLI.

`list-queues`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-queues`.

AWS CLI

Creación de una lista de las colas

En este ejemplo, se enumeran todas las colas.

Comando:

```
aws sqs list-queues
```

Salida:

```
{
  "QueueUrls": [
    "https://queue.amazonaws.com/80398EXAMPLE/MyDeadLetterQueue",
    "https://queue.amazonaws.com/80398EXAMPLE/MyQueue",
    "https://queue.amazonaws.com/80398EXAMPLE/MyOtherQueue",
    "https://queue.amazonaws.com/80398EXAMPLE/TestQueue1",
        "https://queue.amazonaws.com/80398EXAMPLE/TestQueue2"
  ]
}
```

En este ejemplo, solo se muestran las colas que comienzan por "My".

Comando:

```
aws sqs list-queues --queue-name-prefix My
```

Salida:

```
{
  "QueueUrls": [
    "https://queue.amazonaws.com/80398EXAMPLE/MyDeadLetterQueue",
    "https://queue.amazonaws.com/80398EXAMPLE/MyQueue",
    "https://queue.amazonaws.com/80398EXAMPLE/MyOtherQueue"
  ]
}
```

- Para obtener información sobre la API, consulte ListQueues en la Referencia de comandos de la AWS CLI.

`purge-queue`

En el siguiente ejemplo de código, se muestra cómo utilizar `purge-queue`.

AWS CLI

Para purgar una cola

En este ejemplo, se eliminan los mensajes de la cola especificada.

Comando:

```
aws sqs purge-queue --queue-url https://sqs.us-east-1.amazonaws.com/80398EXAMPLE/MyNewQueue
```

Salida:

```
None.
```

- Para obtener información sobre la API, consulte PurgeQueue en la Referencia de comandos de la AWS CLI.

`receive-message`

En el siguiente ejemplo de código, se muestra cómo utilizar `receive-message`.

AWS CLI

Recepción de un mensaje

En este ejemplo, se reciben hasta 10 mensajes disponibles y se devuelven todos los atributos disponibles.

Comando:

```
aws sqs receive-message --queue-url https://sqs.us-east-1.amazonaws.com/80398EXAMPLE/MyQueue --attribute-names All --message-attribute-names All --max-number-of-messages 10
```

Salida:

```
{
  "Messages": [
    {
      "Body": "My first message.",
      "ReceiptHandle": "AQEBzbVv...fqNzFw==",
      "MD5OfBody": "1000f835...a35411fa",
      "MD5OfMessageAttributes": "9424c491...26bc3ae7",
```

```
      "MessageId": "d6790f8d-d575-4f01-bc51-40122EXAMPLE",
      "Attributes": {
        "ApproximateFirstReceiveTimestamp": "1442428276921",
        "SenderId": "AIDAIAZKMSNQ7TEXAMPLE",
        "ApproximateReceiveCount": "5",
        "SentTimestamp": "1442428276921"
      },
      "MessageAttributes": {
        "PostalCode": {
          "DataType": "String",
          "StringValue": "ABC123"
        },
        "City": {
          "DataType": "String",
          "StringValue": "Any City"
        }
      }
    }
  ]
}
```

En este ejemplo, se recibe el siguiente mensaje disponible y se devuelven únicamente los atributos SenderId y SentTimestamp, así como el atributo de mensaje PostalCode.

Comando:

```
aws sqs receive-message --queue-url https://sqs.us-
east-1.amazonaws.com/80398EXAMPLE/MyQueue --attribute-names SenderId SentTimestamp
 --message-attribute-names PostalCode
```

Salida:

```
{
  "Messages": [
    {
      "Body": "My first message.",
      "ReceiptHandle": "AQEB6nR4...HzlvZQ==",
      "MD5OfBody": "1000f835...a35411fa",
      "MD5OfMessageAttributes": "b8e89563...e088e74f",
      "MessageId": "d6790f8d-d575-4f01-bc51-40122EXAMPLE",
      "Attributes": {
        "SenderId": "AIDAIAZKMSNQ7TEXAMPLE",
```

```
        "SentTimestamp": "1442428276921"
      },
      "MessageAttributes": {
        "PostalCode": {
          "DataType": "String",
          "StringValue": "ABC123"
        }
      }
    }
  ]
}
```

- Para obtener información sobre la API, consulte ReceiveMessage en la Referencia de comandos de la AWS CLI.

`remove-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-permission`.

AWS CLI

Para eliminar un permiso

En este ejemplo, se quita el permiso con la etiqueta especificada de la cola indicada.

Comando:

```
aws sqs remove-permission --queue-url https://sqs.us-
east-1.amazonaws.com/80398EXAMPLE/MyQueue --label SendMessagesFromMyQueue
```

Salida:

```
None.
```

- Para obtener información sobre la API, consulte RemovePermission en la Referencia de comandos de la AWS CLI.

`send-message-batch`

En el siguiente ejemplo de código, se muestra cómo utilizar `send-message-batch`.

AWS CLI

Envío de varios mensajes por lotes

En este ejemplo, se envían 2 mensajes con los cuerpos de los mensajes, los períodos de retraso y los atributos de los mensajes especificados a la cola especificada.

Comando:

```
aws sqs send-message-batch --queue-url https://sqs.us-
east-1.amazonaws.com/80398EXAMPLE/MyQueue --entries file://send-message-batch.json
```

Archivo de entrada (send-message-batch.json):

```
[
  {
    "Id": "FuelReport-0001-2015-09-16T140731Z",
        "MessageBody": "Fuel report for account 0001 on 2015-09-16 at 02:07:31 PM.",
        "DelaySeconds": 10,
        "MessageAttributes": {
          "SellerName": {
            "DataType": "String",
                "StringValue": "Example Store"
      },
          "City": {
        "DataType": "String",
        "StringValue": "Any City"
      },
          "Region": {
            "DataType": "String",
                "StringValue": "WA"
      },
          "PostalCode": {
            "DataType": "String",
                "StringValue": "99065"
          },
          "PricePerGallon": {
            "DataType": "Number",
                "StringValue": "1.99"
      }
        }
  },
  {
```

```
    "Id": "FuelReport-0002-2015-09-16T140930Z",
        "MessageBody": "Fuel report for account 0002 on 2015-09-16 at 02:09:30 PM.",
        "DelaySeconds": 10,
        "MessageAttributes": {
          "SellerName": {
            "DataType": "String",
                "StringValue": "Example Fuels"
      },
          "City": {
        "DataType": "String",
        "StringValue": "North Town"
      },
          "Region": {
            "DataType": "String",
                "StringValue": "WA"
      },
          "PostalCode": {
            "DataType": "String",
                "StringValue": "99123"
          },
          "PricePerGallon": {
            "DataType": "Number",
                "StringValue": "1.87"
      }
        }
  }
]
```

Salida:

```
{
  "Successful": [
    {
      "MD5OfMessageBody": "203c4a38...7943237e",
      "MD5OfMessageAttributes": "10809b55...baf283ef",
      "Id": "FuelReport-0001-2015-09-16T140731Z",
      "MessageId": "d175070c-d6b8-4101-861d-adeb3EXAMPLE"
    },
    {
      "MD5OfMessageBody": "2cf0159a...c1980595",
      "MD5OfMessageAttributes": "55623928...ae354a25",
      "Id": "FuelReport-0002-2015-09-16T140930Z",
      "MessageId": "f9b7d55d-0570-413e-b9c5-a9264EXAMPLE"
```

```
    }
  ]
}
```

- Para obtener información sobre de la API, consulte SendMessageBatch en la Referencia de comandos de la AWS CLI

`send-message`

En el siguiente ejemplo de código, se muestra cómo utilizar `send-message`.

AWS CLI

Cómo enviar un mensaje

En este ejemplo, se envía un mensaje con el cuerpo del mensaje, el período de retraso y los atributos del mensaje especificados a la cola especificada.

Comando:

```
aws sqs send-message --queue-url https://sqs.us-east-1.amazonaws.com/80398EXAMPLE/MyQueue --message-body "Information about the largest city in Any Region." --delay-seconds 10 --message-attributes file://send-message.json
```

Archivo de entrada (send-message.json):

```
{
  "City": {
    "DataType": "String",
    "StringValue": "Any City"
  },
  "Greeting": {
    "DataType": "Binary",
    "BinaryValue": "Hello, World!"
  },
  "Population": {
    "DataType": "Number",
    "StringValue": "1250800"
  }
}
```

Salida:

```
{
  "MD5OfMessageBody": "51b0a325...39163aa0",
  "MD5OfMessageAttributes": "00484c68...59e48f06",
  "MessageId": "da68f62c-0c07-4bee-bf5f-7e856EXAMPLE"
}
```

- Para obtener información sobre de la API, consulte SendMessage en la Referencia de comandos de la AWS CLI.

`set-queue-attributes`

En el siguiente ejemplo de código, se muestra cómo utilizar `set-queue-attributes`.

AWS CLI

Fijación de los atributos de una cola

Este ejemplo establece la cola especificada en un retraso de entrega de 10 segundos, un tamaño máximo de mensaje de 128 KB (128 KB * 1024 bytes), un período de retención de mensajes de 3 días (3 días * 24 horas * 60 minutos * 60 segundos), un tiempo de espera de recepción de mensajes de 20 segundos y un tiempo de espera de visibilidad predeterminado de 60 segundos. En este ejemplo, también se asocia la cola de mensajes fallidos especificada a un recuento máximo de 1000 mensajes recibidos.

Comando:

```
aws sqs set-queue-attributes --queue-url https://sqs.us-
east-1.amazonaws.com/80398EXAMPLE/MyNewQueue --attributes file://set-queue-
attributes.json
```

Archivo de entrada (set-queue-attributes.json):

```
{
  "DelaySeconds": "10",
  "MaximumMessageSize": "131072",
  "MessageRetentionPeriod": "259200",
  "ReceiveMessageWaitTimeSeconds": "20",
  "RedrivePolicy": "{\"deadLetterTargetArn\":\"arn:aws:sqs:us-
east-1:80398EXAMPLE:MyDeadLetterQueue\",\"maxReceiveCount\":\"1000\"}",
  "VisibilityTimeout": "60"
}
```

Salida:

```
None.
```

- Para obtener información sobre la API, consulte SetQueueAttributes en la Referencia del comando de la AWS CLI.

`start-message-move-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-message-move-task`.

AWS CLI

Ejemplo 1: *inicio de una tarea de traslado de mensajes*

En el siguiente ejemplo de `start-message-move-task`, se inicia una tarea de traslado de mensajes para redirigir los mensajes de la cola de mensajes fallidos especificada a la cola de origen.

```
aws sqs start-message-move-task \
    --source-arn arn:aws:sqs:us-west-2:80398EXAMPLE:MyQueue
```

Salida:

```
{
    "TaskHandle": "AQEB6nR4...HzlvZQ=="
}
```

Para obtener más información, consulte Título del tema en la Nombre de la guía.

Ejemplo 2: *Inicio de una tarea de traslado de mensajes con una velocidad máxima*

En el siguiente ejemplo de `start-message-move-task`, se inicia una tarea de traslado de mensajes para redirigir los mensajes de la cola de mensajes fallidos especificada a la cola de destino designada a una velocidad máxima de 50 mensajes por segundo.

```
aws sqs start-message-move-task \
    --source-arn arn:aws:sqs:us-west-2:80398EXAMPLE:MyQueue1 \
    --destination-arn arn:aws:sqs:us-west-2:80398EXAMPLE:MyQueue2 \
    --max-number-of-messages-per-second 50
```

Salida:

```
{
    "TaskHandle": "AQEB6nR4...HzlvZQ=="
}
```

Para obtener más información, consulte Amazon SQS API permissions: Actions and resource reference en la Guía para desarrolladores.

- Para obtener información sobre la API, consulte StartMessageMoveTask en la Referencia de comandos de la AWS CLI.

`tag-queue`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-queue`.

AWS CLI

Para añadir etiquetas de asignación de costos a una cola

En el siguiente ejemplo de `tag-queue`, se añade una etiqueta de asignación de costos a la cola de Amazon SQS especificada.

```
aws sqs tag-queue \
    --queue-url https://sqs.us-west-2.amazonaws.com/123456789012/MyQueue \
    --tags Priority=Highest
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adding Cost Allocation Tags en la Guía para desarrolladores de Amazon Simple Queue Service.

- Para obtener información sobre la API, consulte TagQueue en la Referencia de comandos de la AWS CLI.

`untag-queue`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-queue`.

AWS CLI

Para eliminar etiquetas de asignación de costos de una cola

En el siguiente ejemplo de `untag-queue`, se añade una etiqueta de asignación de costos a la cola de Amazon SQS especificada.

```
aws sqs untag-queue \
    --queue-url https://sqs.us-west-2.amazonaws.com/123456789012/MyQueue \
    --tag-keys "Priority"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Adding Cost Allocation Tags en la Guía para desarrolladores de Amazon Simple Queue Service.

- Para obtener detalles sobre la API, consulte UntagQueue en la Referencia de comandos de la AWS CLI.

Ejemplos de Storage Gateway que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes utilizando AWS Command Line Interface con Storage Gateway.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`describe-gateway-information`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-gateway-information`.

AWS CLI

Para describir una puerta de enlace

Este comando `describe-gateway-information` devuelve metadatos acerca de la puerta de enlace especificada. Para especificar la puerta de enlace que desea describir, utilice el nombre de recurso de Amazon (ARN) de la puerta de enlace en el comando.

En este ejemplo se especifica una puerta de enlace con el ID `sgw-12A3456B` la cuenta `123456789012`:

```
aws storagegateway describe-gateway-information --gateway-
arn "arn:aws:storagegateway:us-west-2:123456789012:gateway/sgw-12A3456B"
```

Este comando devuelve un bloque JSON que contiene los metadatos de una puerta de enlace, por ejemplo, su nombre, las interfaces de red, la zona horaria configurada y el estado (es decir, si se está ejecutando o no la puerta de enlace).

- Para obtener información sobre la API, consulte DescribeGatewayInformation en la Referencia de comandos de la AWS CLI.

`list-file-shares`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-file-shares`.

AWS CLI

Para enumerar los archivos compartidos

En el siguiente ejemplo de `command-name`, se genera una lista de los widgets disponibles en la cuenta de AWS.

```
aws storagegateway list-file-shares \
    --gateway-arn arn:aws:storagegateway:us-east-1:209870788375:gateway/sgw-FB02E292
```

Salida:

```
{
    "FileShareInfoList": [
        {
            "FileShareType": "NFS",
            "FileShareARN": "arn:aws:storagegateway:us-east-1:111122223333:share/
share-2FA12345",
            "FileShareId": "share-2FA12345",
```

```
            "FileShareStatus": "AVAILABLE",
            "GatewayARN": "arn:aws:storagegateway:us-east-1:111122223333:gateway/
sgw-FB0AAAAA"
        }
    ],
    "Marker": null
}
```

Para obtener más información, consulte ListFileShares en la Referencia de la API del servicio AWS Storage Gateway.

- Para obtener detalles de la API, consulte ListFileShares en la Referencia de comandos de la AWS CLI.

`list-gateways`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-gateways`.

AWS CLI

Para enumerar las puertas de enlace de una cuenta

El siguiente comando `list-gateways` muestra todas las puertas de enlace definidas para una cuenta:

```
aws storagegateway list-gateways
```

Este comando genera un bloque JSON que contiene una lista de ARN (Nombre de recurso de Amazon) de la puerta de enlace.

- Para obtener información sobre la API, consulte ListGateways en la Referencia de comandos de la AWS CLI.

`list-volumes`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-volumes`.

AWS CLI

Para enumerar los volúmenes configurados para una puerta de enlace

El siguiente comando `list-volumes` devuelve una lista de los volúmenes configurados para la puerta de enlace especificada. Para especificar la puerta de enlace que desea describir, utilice el nombre de recurso de Amazon (ARN) de la puerta de enlace en el comando.

En este ejemplo se especifica una puerta de enlace con el ID `sgw-12A3456B` la cuenta `123456789012`:

```
aws storagegateway list-volumes --gateway-arn "arn:aws:storagegateway:us-
west-2:123456789012:gateway/sgw-12A3456B"
```

Este comando genera un bloque JSON que contiene una lista de volúmenes que incluye el tipo y el ARN de cada volumen.

- Para obtener información sobre la API, consulte ListVolumes en la Referencia de comandos de la AWS CLI.

`refresh-cache`

En el siguiente ejemplo de código, se muestra cómo utilizar `refresh-cache`.

AWS CLI

Para actualizar la caché de archivos compartidos

En el siguiente ejemplo de `refresh-cache`, se actualiza la caché del recurso de archivos compartidos especificado.

```
aws storagegateway refresh-cache \
    --file-share-arn arn:aws:storagegateway:us-east-1:111122223333:share/
share-2FA12345
```

Salida:

```
{
    "FileShareARN": "arn:aws:storagegateway:us-east-1:111122223333:share/
share-2FA12345",
    "NotificationId": "4954d4b1-abcd-ef01-1234-97950a7d3483"
}
```

Para obtener más información, consulte ListFileShares en la Referencia de la API del servicio AWS Storage Gateway.

- Para obtener información sobre la API, consulte RefreshCache en la Referencia de comandos de la AWS CLI.

AWS STS Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS STS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`assume-role-with-saml`

En el siguiente ejemplo de código, se muestra cómo utilizar `assume-role-with-saml`.

AWS CLI

Para obtener credenciales a corto plazo para un rol autenticado con SAML

El siguiente comando `assume-role-with-saml` recupera un conjunto de credenciales a corto plazo para el rol de IAM `TestSaml`. La solicitud de este ejemplo se autentica mediante la aserción SAML proporcionada por el proveedor de identidades al autenticarse en él.

```
aws sts assume-role-with-saml \
    --role-arn arn:aws:iam::123456789012:role/TestSaml \
    --principal-arn arn:aws:iam::123456789012:saml-provider/SAML-test \
    --saml-
assertion "VERYLONGENCODEDASSERTIONEXAMPLExzYW1sOkF1ZGllbmNlPmJsYW5rPC9zYW1sOkF1ZGllbmNlPjwv
+PHNhbWw6TmFtZUlEIEZvcm1hdD0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOm5hbWVpZC1mb3JtYXQ6dHJhbnN
+PHNhbWw6U3ViamVjdENvbmZpcm1hdGlvbiBNZXRob2Q9InVybjpvYXNpczpuYW1lczp0YzpTQU1MOjIuMDpjbTpiZWF
```

Salida:


```
{
    "Issuer": "https://integ.example.com/idp/shibboleth</Issuer",
    "AssumedRoleUser": {
        "Arn": "arn:aws:sts::123456789012:assumed-role/TestSaml",
        "AssumedRoleId": "ARO456EXAMPLE789:TestSaml"
    },
    "Credentials": {
        "AccessKeyId": "ASIAV3ZUEFP6EXAMPLE",
        "SecretAccessKey": "8P+SQvWIuLnKhh8d++jpw0nNmQRBZvNEXAMPLEKEY",
        "SessionToken": "IQoJb3JpZ2luX2VjEOz////////////////////
wEXAMPLEtMSJHMEUCIDoKK3JH9uGQE1z0sINr5M4jk
+Na8KHDcCYRVjJCZEvOAiEA3OvJGtw1EcViOleS2vhs8VdCKFJQWPQrmGdeehM4IC1NtBmUpp2wUE8phUZampKsburED
+xo0rKwT38xVqr7ZD0u0iPPkUL64lIZbqBAz
+scqKmlzm8FDrypNC9Yjc8fPOLn9FX9KSYvKTr4rvx3iSIlTJabIQwj2ICCR/oLxBA==",
        "Expiration": "2019-11-01T20:26:47Z"
    },
    "Audience": "https://signin.aws.amazon.com/saml",
    "SubjectType": "transient",
    "PackedPolicySize": "6",
    "NameQualifier": "SbdGOnUkh1i4+EXAMPLExL/jEvs=",
    "Subject": "SamlExample"
}
```


Para obtener más información, consulte Solicitud de credenciales de seguridad temporales en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte AssumeRoleWithSaml en la Referencia de comandos de la AWS CLI.

`assume-role-with-web-identity`

En el siguiente ejemplo de código, se muestra cómo utilizar `assume-role-with-web-identity`.

AWS CLI

Cómo obtener credenciales a corto plazo para un rol autenticado con Web Identity (OAuth 2."0)

El siguiente comando `assume-role-with-web-identity` recupera un conjunto de credenciales a corto plazo para el rol de IAM `app1`. La solicitud se autentica mediante el token de identidad web proporcionado por el proveedor de identidad web especificado. Se aplican

dos políticas adicionales a la sesión para restringir aún más lo que el usuario puede hacer. Las credenciales devueltas caducan una hora después de haberse generado.

```
aws sts assume-role-with-web-identity \
    --duration-seconds 3600 \
    --role-session-name "app1" \
    --provider-id "www.amazon.com" \
    --policy-arns "arn:aws:iam::123456789012:policy/
q=webidentitydemopolicy1","arn:aws:iam::123456789012:policy/webidentitydemopolicy2"
 \
    --role-arn arn:aws:iam::123456789012:role/FederatedWebIdentityRole \
    --web-identity-token "Atza
%7CIQEBLjAsAhRFiXuWpUXuRvQ9PZL3GMFcYevydwIUFAHZwXZXXXXXXXXJnrulxKDHwy87oGKPznh0D6bEQZTSCzyoC
CrKqjG7nPBjNIL016GGvuS5gSvPRUxWES3VYfm1wl7WTI7jn-Pcb6M-
buCgHhFOzTQxod27L9CqnOLio7N3gZAGpsp6n1-
AJBOCJckcyXe2c6uD0srOJeZlKUm2eTDVMf8IehDVI0r1QOnTV6KzzAI3OY87Vd_cVMQ"
```

Salida:

```
{
    "SubjectFromWebIdentityToken": "amzn1.account.AF6RHO7KZU5XRVQJGXK6HB56KR2A",
    "Audience": "client.5498841531868486423.1548@apps.example.com",
    "AssumedRoleUser": {
        "Arn": "arn:aws:sts::123456789012:assumed-role/FederatedWebIdentityRole/
app1",
        "AssumedRoleId": "AROACLKWSDQRAOEXAMPLE:app1"
    },
    "Credentials": {
        "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYzEXAMPLEKEY",
        "SessionToken": "AQoEXAMPLEH4aoAH0gNCAPyJxz4BlCFFxWNE1OPTgk5TthT
+FvwqnKwRcOIfrRh3c/LTo6UDdyJwOOvEVPvLXCrrrUtdnniCEXAMPLE/
IvU1dYUg2RVAJBanLiHb4IgRmpRV3zrkuWJOgQs8IZZaIv2BXIa2R4OlgkBN9bkUDNCJiBeb/
AXlzBBko7b15fjrBs2+cTQtpZ3CYWFXG8C5zqx37wnOE49mRl/+OtkIKGO7fAE",
        "Expiration": "2020-05-19T18:06:10+00:00"
    },
    "Provider": "www.amazon.com"
}
```

Para obtener más información, consulte Solicitud de credenciales de seguridad temporales en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte AssumeRoleWithWebIdentity en la Referencia de comandos de la AWS CLI.

`assume-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `assume-role`.

AWS CLI

Cómo asumir un rol

El siguiente comando `assume-role` recupera un conjunto de credenciales a corto plazo para el rol de IAM `s3-access-example`.

```
aws sts assume-role \
    --role-arn arn:aws:iam::123456789012:role/xaccounts3access \
    --role-session-name s3-access-example
```

Salida:

```
{
    "AssumedRoleUser": {
        "AssumedRoleId": "AROA3XFRBF535PLBIFPI4:s3-access-example",
        "Arn": "arn:aws:sts::123456789012:assumed-role/xaccounts3access/s3-access-
example"
    },
    "Credentials": {
        "SecretAccessKey": "9drTJvcXLB89EXAMPLELB8923FB892xMFI",
        "SessionToken": "AQoXdzELDDY//////////
wEaoAK1wvxJY12r2IrDFT2IvAzTCn3zHoZ7YNtpiQLF0MqZye/qwjzP2iEXAMPLEbw/
m3hsj8VBTkPORGvr9jM5sgP+w9IZWZnU+LWhmg
+a5fDi2oTGUYcdg9uexQ4mtCHIHfi4citgqZTgco40Yqr4lIlo4V2b2Dyauk0eYFNebHtYlFVgAUj
+7Indz3LU0aTWk1WKIjHmmMCIoTkyYp/k7kUG7moeEYKSitwQIi6Gjn+nyzM
+PtoA3685ixzv0R7i5rjQi0YE0lf1oeie3bDiNHncmzosRM6SFiPzSvp6h/32xQuZsjcypmwsPSDtTPYcs0+YN/8BRi2
IcrxSpnWEXAMPLEXSDFTAQAM6Dl9zR0tXoybnlrZIwMLlMi1Kcgo5OytwU=",
        "Expiration": "2016-03-15T00:05:07Z",
        "AccessKeyId": "ASIAJEXAMPLEXEG2JICEA"
    }
}
```

El resultado del comando contiene una clave de acceso, una clave secreta y un token de sesión que puede utilizar para autenticarse con AWS.

Para el uso de la CLI de AWS, puede configurar un perfil con nombre asociado a un rol. Cuando utilice el perfil, la CLI de AWS llamará a assume-role y administrará las credenciales por usted. Para obtener más información, consulte Uso de un rol de IAM en la CLI de AWS en la Guía del usuario de la CLI de AWS.

- Para obtener información sobre la API, consulte AssumeRole en la Referencia de comandos de la AWS CLI.

`assume-root`

En el siguiente ejemplo de código, se muestra cómo utilizar `assume-root`.

AWS CLI

Lanzamiento de una sesión privilegiada

El comando `assume-root` siguiente recupera un conjunto de credenciales a corto plazo que puede utilizar para eliminar una política de bucket de Amazon S3 mal configurada para una cuenta de miembro de la organización.

```
aws sts assume-root \
    --duration-seconds 900 \
    --target-principal 111122223333 \
    --task-policy-arn arn=arn:aws:iam::aws:policy/root-task/S3UnlockBucketPolicy
```

Salida:

```
{
    "Credentials": {
        "SecretAccessKey": "9drTJvcXLB89EXAMPLELB8923FB892xMFI",
        "SessionToken": "AQoXdzELDDY//////////
wEaoAK1wvxJY12r2IrDFT2IvAzTCn3zHoZ7YNtpiQLF0MqZye/qwjzP2iEXAMPLEbw/
m3hsj8VBTkPORGvr9jM5sgP+w9IZWZnU+LWhmg
+a5fDi2oTGUYcdg9uexQ4mtCHIHfi4citgqZTgco40Yqr4lIlo4V2b2Dyauk0eYFNebHtYlFVgAUj
+7Indz3LU0aTWk1WKIjHmmMCIoTkyYp/k7kUG7moeEYKSitwQIi6Gjn+nyzM
+PtoA3685ixzv0R7i5rjQi0YE0lf1oeie3bDiNHncmzosRM6SFiPzSvp6h/32xQuZsjcypmwsPSDtTPYcs0+YN/8BRi2
IcrxSpnWEXAMPLEXSDFTAQAM6Dl9zR0tXoybnlrZIwMLlMi1Kcgo5OytwU=",
        "Expiration": "2024-11-15T00:05:07Z",
        "AccessKeyId": "ASIAJEXAMPLEXEG2JICEA"
    },
    "SourceIdentity": "Alice",
```

```
}
```

El resultado del comando contiene una clave de acceso, una clave secreta y un token de sesión que puede utilizar para realizar acciones con privilegios en la cuenta de miembro. Para obtener más información, consulte Realización de una tarea con privilegios en una cuenta de miembro de AWS Organizations en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte AssumeRoot en la Referencia de comandos de la AWS CLI.

`decode-authorization-message`

En el siguiente ejemplo de código, se muestra cómo utilizar `decode-authorization-message`.

AWS CLI

Cómo decodificar un mensaje de autorización codificado devuelto en respuesta a una solicitud

En el siguiente ejemplo de `decode-authorization-message`, se decodifica información adicional sobre el estado de autorización de una solicitud de un mensaje codificado que regresa como respuesta a una solicitud de Amazon Web Services.

```
aws sts decode-authorization-message \
    --encoded-message EXAMPLEWodyRNrtlQARDip-
eTA6i6DrlUhHhPQrLWB_lAbl5pAKxl9mPDLexYcGBreyIKQC1BGBIpBKr3dFDkwqeO7e2NMk5j_hmzAiChJN-8oy3Ewi
Ojau7BMjOTWwOtHPhV_Zaz87yENdipr745EjQwRd5LaoL3vN8_5ZfA9UiBMKDgVh1gjqZJFUiQoubv78V1RbHNYnK44E
pOu3FZjwYStfvTb3GHs3-6rLribGO9jZOktkfE6vqxlFzLyeDr4P2ihC1wty9tArCvvGzIAUNmARQJ2VVWPxioqgoqCz
JWP5pwe_mAyqh0NLw-r1S56YC_90onj9A80sNrHlI-
tIiNd7tgNTYzDuPQYD2FMDBnp82V9eVmYGtPp5NIeSpuf3fOHanFuBZgENxZQZ2dlH3xJGMTtYayzZrRXjiq_SfX9zeB
FaoPIb8LmmKVBLpIB0iFhU9sEHPqKHVPi6jdxXqKaZaFGvYVmVOiuQdNQKuyk0p067POFrZECLjjOtNPBOZCcuEKEXAM
```

Salida:

```
{
    "DecodedMessage": "{\"allowed\":false,\"explicitDeny\":true,\"matchedStatements
\":{\"items\":[{\"statementId\":\"VisualEditor0\",\"effect\":\"DENY\",\"principals
\":{\"items\":[{\"value\":\"AROA123456789EXAMPLE\"}]},\"principalGroups
\":{\"items\":[]},\"actions\":{\"items\":[{\"value\":\"ec2:RunInstances
\"}]},\"resources\":{\"items\":[{\"value\":\"*\"}]},\"conditions\":{\"items
\":[]}}]},\"failures\":{\"items\":[]},\"context\":{\"principal\":{\"id\":
\"AROA123456789EXAMPLE:Ana\",\"arn\":\"arn:aws:sts::111122223333:assumed-role/
Developer/Ana\"},\"action\":\"RunInstances\",\"resource\":\"arn:aws:ec2:us-
```

```
east-1:111122223333:instance/*\",\"conditions\":{\"items\":[{\"key\":
\"ec2:MetadataHttpPutResponseHopLimit\",\"values\":{\"items\":[{\"value\":
\"2\"}]}},{\"key\":\"ec2:InstanceMarketType\",\"values\":{\"items\":[{\"value
\":\"on-demand\"}]}},{\"key\":\"aws:Resource\",\"values\":{\"items\":[{\"value
\":\"instance/*\"}]}},{\"key\":\"aws:Account\",\"values\":{\"items\":[{\"value
\":\"111122223333\"}]}},{\"key\":\"ec2:AvailabilityZone\",\"values\":{\"items\":
[{\"value\":\"us-east-1f\"}]}},{\"key\":\"ec2:ebsOptimized\",\"values\":{\"items
\":[{\"value\":\"false\"}]}},{\"key\":\"ec2:IsLaunchTemplateResource\",\"values
\":{\"items\":[{\"value\":\"false\"}]}},{\"key\":\"ec2:InstanceType\",\"values\":
{\"items\":[{\"value\":\"t2.micro\"}]}},{\"key\":\"ec2:RootDeviceType\",\"values
\":{\"items\":[{\"value\":\"ebs\"}]}},{\"key\":\"aws:Region\",\"values\":{\"items
\":[{\"value\":\"us-east-1\"}]}},{\"key\":\"ec2:MetadataHttpEndpoint\",\"values
\":{\"items\":[{\"value\":\"enabled\"}]}},{\"key\":\"aws:Service\",\"values\":
{\"items\":[{\"value\":\"ec2\"}]}},{\"key\":\"ec2:InstanceID\",\"values\":{\"items
\":[{\"value\":\"*\"}]}},{\"key\":\"ec2:MetadataHttpTokens\",\"values\":{\"items
\":[{\"value\":\"required\"}]}},{\"key\":\"aws:Type\",\"values\":{\"items\":
[{\"value\":\"instance\"}]}},{\"key\":\"ec2:Tenancy\",\"values\":{\"items\":
[{\"value\":\"default\"}]}},{\"key\":\"ec2:Region\",\"values\":{\"items\":[{\"value
\":\"us-east-1\"}]}},{\"key\":\"aws:ARN\",\"values\":{\"items\":[{\"value\":
\"arn:aws:ec2:us-east-1:111122223333:instance/*\"}]}}]}}}"
}
```

Para obtener más información, consulte Lógica de evaluación de políticas en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte DecodeAuthorizationMessage en la Referencia de comandos de la AWS CLI.

`get-caller-identity`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-caller-identity`.

AWS CLI

Para obtener detalles sobre la identidad de IAM actual

El siguiente comando `get-caller-identity` muestra información sobre la identidad de IAM utilizada para autenticar la solicitud. La persona que llama es un usuario de IAM.

```
aws sts get-caller-identity
```

Salida:

```
{
    "UserId": "AIDASAMPLEUSERID",
    "Account": "123456789012",
    "Arn": "arn:aws:iam::123456789012:user/DevAdmin"
}
```

- Para obtener información sobre la API, consulte GetCallerIdentity en la Referencia de comandos de la AWS CLI.

`get-federation-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-federation-token`.

AWS CLI

Cómo devolver un conjunto de credenciales de seguridad temporales utilizando credenciales de clave de acceso de usuario de IAM

En el siguiente ejemplo de `get-federation-token`, se devuelve un conjunto de credenciales de seguridad temporales (que consiste en un ID de clave de acceso, una clave de acceso secreta y un token de seguridad). Debe llamar a la operación `GetFederationToken` utilizando las credenciales de seguridad de largo plazo de un usuario de IAM.

```
aws sts get-federation-token \
    --name Bob \
    --policy file://myfile.json \
    --policy-arns arn=arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess \
    --duration-seconds 900
```

Contenidos de `myfile.json`:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:Describe*",
            "Resource": "*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": "elasticloadbalancing:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:ListMetrics",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "autoscaling:Describe*",
            "Resource": "*"
        }
    ]
}
```

Salida:

```
{
    "Credentials": {
        "AccessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
        "SessionToken": "EXAMPLEpZ2luX2VjEGoaCXVzLXdlc3QtMiJIMEYCIQC/
W9pL5ArQyDD5JwFL3/h5+WGopQ24GEXweNctwhi9sgIhAMkg
+MZE35iWM8s4r5Lr25f9rSTVPFH98G42QQunWMTfKq0DCOP/////////
wEQAxoMNDUyOTI1MTcwNTA3Igxuy3AOpuuoLsk3MJwqgQPg8QOd9HuoClUxq26wnc/nm
+eZLjHDyGf2KUAHK2DuaS/nrGSEXAMPLE",
        "Expiration": "2023-12-20T02:06:07+00:00"
    },
    "FederatedUser": {
        "FederatedUserId": "111122223333:Bob",
        "Arn": "arn:aws:sts::111122223333:federated-user/Bob"
    },
    "PackedPolicySize": 36
}
```

Para obtener más información, consulte Solicitud de credenciales de seguridad temporales en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetFederationToken en la Referencia de comandos de la AWS CLI.

`get-session-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-session-token`.

AWS CLI

Cómo obtener un conjunto de credenciales a corto plazo para una identidad de IAM

El siguiente comando `get-session-token` recupera un conjunto de credenciales a corto plazo para la identidad de IAM que realiza la llamada. Las credenciales resultantes se pueden utilizar para las solicitudes donde la política requiere la autenticación multifactor (MFA). Las credenciales caducan 15 minutos después de haberse generado.

```
aws sts get-session-token \
    --duration-seconds 900 \
    --serial-number "YourMFADeviceSerialNumber" \
    --token-code 123456
```

Salida:

```
{
    "Credentials": {
        "AccessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYzEXAMPLEKEY",
        "SessionToken": "AQoEXAMPLEH4aoAH0gNCAPyJxz4BlCFFxWNE1OPTgk5TthT
+FvwqnKwRcOIfrRh3c/LTo6UDdyJwOOvEVPvLXCrrrUtdnniCEXAMPLE/
IvU1dYUg2RVAJBanLiHb4IgRmpRV3zrkuWJOgQs8IZZaIv2BXIa2R4OlgkBN9bkUDNCJiBeb/
AXlzBBko7b15fjrBs2+cTQtpZ3CYWFXG8C5zqx37wnOE49mRl/+OtkIKGO7fAE",
        "Expiration": "2020-05-19T18:06:10+00:00"
    }
}
```

Para obtener más información, consulte Solicitud de credenciales de seguridad temporales en la Guía del usuario de AWS IAM.

- Para obtener información sobre la API, consulte GetSessionToken en la Referencia de comandos de la AWS CLI.

Soporte Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Soporte.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-attachments-to-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-attachments-to-set`.

AWS CLI

Para añadir un archivo adjunto a un conjunto

En el siguiente ejemplo de `add-attachments-to-set`, se agrega una imagen a un conjunto que, a continuación, puede especificar para un caso de soporte en su cuenta de AWS.

```
aws support add-attachments-to-set \
    --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE" \
    --attachments fileName=troubleshoot-screenshot.png,data=base64-encoded-string
```

Salida:

```
{
    "attachmentSetId": "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE",
    "expiryTime": "2020-05-14T17:04:40.790+0000"
```

```
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS.

- Para obtener detalles sobre la API, consulte AddAttachmentsToSet en la Referencia de comandos de la AWS CLI.

`add-communication-to-case`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-communication-to-case`.

AWS CLI

Para agregar una comunicación a un caso

En el siguiente ejemplo de `add-communication-to-case`, se agregan comunicaciones a un caso de soporte en su cuenta de AWS.

```
aws support add-communication-to-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --communication-body "I'm attaching a set of images to this case." \
    --cc-email-addresses "myemail@example.com" \
    --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE"
```

Salida:

```
{
    "result": true
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS.

- Para obtener información sobre la API, consulte AddCommunicationToCase en la Referencia de comandos de la AWS CLI.

`create-case`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-case`.

AWS CLI

Creación de un caso

En el siguiente ejemplo de `create-case` se crea un caso de soporte para su cuenta de AWS.

```
aws support create-case \
    --category-code "using-aws" \
    --cc-email-addresses "myemail@example.com" \
    --communication-body "I want to learn more about an AWS service." \
    --issue-type "technical" \
    --language "en" \
    --service-code "general-info" \
    --severity-code "low" \
    --subject "Question about my account"
```

Salida:

```
{
    "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47"
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS.

- Para obtener información sobre la API, consulte CreateCase en la Referencia de comandos de la AWS CLI.

`describe-attachment`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-attachment`.

AWS CLI

Descripción de un archivo adjunto

El siguiente ejemplo de `describe-attachment` devuelve información sobre el archivo adjunto con el ID especificado.

```
aws support describe-attachment \
```

```
    --attachment-id "attachment-KBnjRNrePd9D6Jx0-Mm00xZuDEaL2JAj_0-
gJv9qqDooTipsz3V1Nb19rCfkZneeQeDPgp8X1iVJyHH7UuhZDdNeqGoduZsPrAhyMakqlc60-
iJjL5HqyYGiT1FG8EXAMPLE"
```

Salida:

```
{
    "attachment": {
        "fileName": "troubleshoot-screenshot.png",
        "data": "base64-blob"
    }
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS.

- Para obtener información sobre la API, consulte DescribeAttachment en la Referencia de comandos de la AWS CLI.

`describe-cases`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-cases`.

AWS CLI

Descripción de un caso

En el siguiente ejemplo de `describe-cases` se devuelve información sobre el caso de soporte especificado en su cuenta de AWS.

```
aws support describe-cases \
    --display-id "1234567890" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --include-resolved-cases \
    --language "en" \
    --no-include-communications \
    --max-item 1
```

Salida:

```
{
    "cases": [
```

```
        {
            "status": "resolved",
            "ccEmailAddresses": [],
            "timeCreated": "2020-03-23T21:31:47.774Z",
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "severityCode": "low",
            "language": "en",
            "categoryCode": "using-aws",
            "serviceCode": "general-info",
            "submittedBy": "myemail@example.com",
            "displayId": "1234567890",
            "subject": "Question about my account"
        }
    ]
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS.

- Para obtener información sobre la API, consulte DescribeCases en la Referencia de comandos de la AWS CLI.

`describe-communications`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-communications`.

AWS CLI

Descripción de la última comunicación de un caso

En el siguiente ejemplo de `describe-communications` se devuelve la última comunicación del caso de soporte especificado en su cuenta de AWS.

```
aws support describe-communications \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --max-item 1
```

Salida:

```
{
    "communications": [
```

```
        {
            "body": "I want to learn more about an AWS service.",
            "attachmentSet": [],
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "timeCreated": "2020-05-12T23:12:35.000Z",
            "submittedBy": "Amazon Web Services"
        }
    ],
    "NextToken": "eyJuZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQEXAMPLE=="
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS.

- Para obtener información sobre la API, consulte DescribeCommunications en la Referencia de comandos de la AWS CLI.

`describe-services`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-services`.

AWS CLI

Creación de una lista de los servicios y las categorías de servicios de AWS

En el siguiente ejemplo de `describe-services` se enumeran las categorías de servicios disponibles para solicitar información general.

```
aws support describe-services \
    --service-code-list "general-info"
```

Salida:

```
{
    "services": [
        {
            "code": "general-info",
            "name": "General Info and Getting Started",
            "categories": [
                {
                    "code": "charges",
                    "name": "How Will I Be Charged?"
```

```
                },
                {
                    "code": "gdpr-queries",
                    "name": "Data Privacy Query"
                },
                {
                    "code": "reserved-instances",
                    "name": "Reserved Instances"
                },
                {
                    "code": "resource",
                    "name": "Where is my Resource?"
                },
                {
                    "code": "using-aws",
                    "name": "Using AWS & Services"
                },
                {
                    "code": "free-tier",
                    "name": "Free Tier"
                },
                {
                    "code": "security-and-compliance",
                    "name": "Security & Compliance"
                },
                {
                    "code": "account-structure",
                    "name": "Account Structure"
                }
            ]
        }
    ]
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS.

- Para obtener información sobre la API, consulte DescribeServices en la Referencia de comandos de la AWS CLI.

`describe-severity-levels`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-severity-levels`.

AWS CLI

Creación de una lista de los niveles de gravedad disponibles

En el siguiente ejemplo de `describe-severity-levels` se enumeran los niveles de gravedad disponibles para un caso de soporte.

```
aws support describe-severity-levels
```

Salida:

```
{
    "severityLevels": [
        {
            "code": "low",
            "name": "Low"
        },
        {
            "code": "normal",
            "name": "Normal"
        },
        {
            "code": "high",
            "name": "High"
        },
        {
            "code": "urgent",
            "name": "Urgent"
        },
        {
            "code": "critical",
            "name": "Critical"
        }
    ]
}
```

Para obtener más información, consulte Elección de la gravedad en la Guía del usuario de soporte de AWS.

- Para obtener información sobre la API, consulte DescribeSeverityLevels en la Referencia de comandos de la AWS CLI.

`describe-trusted-advisor-check-refresh-statuses`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-trusted-advisor-check-refresh-statuses`.

AWS CLI

Para enumerar los estados de actualización de las comprobaciones de AWS Trusted Advisor

En el siguiente ejemplo de `describe-trusted-advisor-check-refresh-statuses`, se muestran los estados de actualización de dos comprobaciones de Trusted Advisor: Permisos de bucket de Amazon S3 y Uso de IAM.

```
aws support describe-trusted-advisor-check-refresh-statuses \
    --check-id "Pfx0RwqBli" "zXCkfM1nI3"
```

Salida:

```
{
    "statuses": [
        {
            "checkId": "Pfx0RwqBli",
            "status": "none",
            "millisUntilNextRefreshable": 0
        },
        {
            "checkId": "zXCkfM1nI3",
            "status": "none",
            "millisUntilNextRefreshable": 0
        }
    ]
}
```

Para obtener más información, consulte AWS Trusted Advisor en la Guía del usuario de AWS Support.

- Para obtener información sobre la API, consulte DescribeTrustedAdvisorCheckRefreshStatuses en la Referencia de comandos de la AWS CLI.

`describe-trusted-advisor-check-result`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-trusted-advisor-check-result`.

AWS CLI

Para enumerar los resultados de una comprobación de AWS Trusted Advisor

En el siguiente ejemplo de `describe-trusted-advisor-check-result`, se muestran los resultados de la comprobación de Uso de IAM.

```
aws support describe-trusted-advisor-check-result \
    --check-id "zXCkfM1nI3"
```

Salida:

```
{
    "result": {
        "checkId": "zXCkfM1nI3",
        "timestamp": "2020-05-13T21:38:05Z",
        "status": "ok",
        "resourcesSummary": {
            "resourcesProcessed": 1,
            "resourcesFlagged": 0,
            "resourcesIgnored": 0,
            "resourcesSuppressed": 0
        },
        "categorySpecificSummary": {
            "costOptimizing": {
                "estimatedMonthlySavings": 0.0,
                "estimatedPercentMonthlySavings": 0.0
            }
        },
        "flaggedResources": [
            {
                "status": "ok",
                "resourceId": "47DEQpj8HBSa-_TImW-5JCeuQeRkm5NMpJWZEXAMPLE",
                "isSuppressed": false
            }
        ]
    }
}
```

Para obtener más información, consulte AWS Trusted Advisor en la Guía del usuario de AWS Support.

- Para obtener información sobre la API, consulte DescribeTrustedAdvisorCheckResult en la Referencia de comandos de la AWS CLI.

`describe-trusted-advisor-check-summaries`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-trusted-advisor-check-summaries`.

AWS CLI

Para enumerar los resúmenes de las comprobaciones de AWS Trusted Advisor

En el siguiente ejemplo de `describe-trusted-advisor-check-summaries`, se muestran los resultados de dos comprobaciones de Trusted Advisor: Permisos de bucket de Amazon S3 y Uso de IAM.

```
aws support describe-trusted-advisor-check-summaries \
    --check-ids "Pfx0RwqBli" "zXCkfM1nI3"
```

Salida:

```
{
    "summaries": [
        {
            "checkId": "Pfx0RwqBli",
            "timestamp": "2020-05-13T21:38:12Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 44,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
```

```
            }
        },
        {
            "checkId": "zXCkfM1nI3",
            "timestamp": "2020-05-13T21:38:05Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 1,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        }
    ]
}
```

Para obtener más información, consulte AWS Trusted Advisor en la Guía del usuario de AWS Support.

- Para obtener información sobre la API, consulte DescribeTrustedAdvisorCheckSummaries en la Referencia de comandos de la AWS CLI.

`describe-trusted-advisor-checks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-trusted-advisor-checks`.

AWS CLI

Para enumerar las comprobaciones de AWS Trusted Advisor disponibles

En el siguiente ejemplo de `describe-trusted-advisor-checks`, se enumeran las comprobaciones de Trusted Advisor disponibles en su cuenta de AWS. Esta información incluye el nombre, el ID, la descripción, la categoría y los metadatos del cheque. Tenga en cuenta que el resultado se abrevia para que se pueda leer.

```
aws support describe-trusted-advisor-checks \
    --language "en"
```

Salida:

```
{
    "checks": [
        {
            "id": "zXCkfM1nI3",
            "name": "IAM Use",
            "description": "Checks for your use of AWS Identity and Access
 Management (IAM). You can use IAM to create users, groups, and roles in AWS, and
 you can use permissions to control access to AWS resources. \n<br>\n<br>\n<b>Alert
 Criteria</b><br>\nYellow: No IAM users have been created for this account.\n<br>
\n<br>\n<b>Recommended Action</b><br>\nCreate one or more IAM users and groups in
 your account. You can then create additional users whose permissions are limited
 to perform specific tasks in your AWS environment. For more information, see <a
 href=\"https://docs.aws.amazon.com/IAM/latest/UserGuide/IAMGettingStarted.html\"
 target=\"_blank\">Getting Started</a>. \n<br><br>\n<b>Additional Resources</b><br>
\n<a href=\"https://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_Introduction.html\"
 target=\"_blank\">What Is IAM?</a>",
            "category": "security",
            "metadata": []
        }
    ]
}
```

Para obtener más información, consulte AWS Trusted Advisor en la Guía del usuario de AWS Support.

- Para obtener información sobre la API, consulte DescribeTrustedAdvisorChecks en la Referencia de comandos de la AWS CLI.

`refresh-trusted-advisor-check`

En el siguiente ejemplo de código, se muestra cómo utilizar `refresh-trusted-advisor-check`.

AWS CLI

Para actualizar una comprobación de AWS Trusted Advisor

En el siguiente ejemplo de `refresh-trusted-advisor-check`, se actualiza la comprobación Permisos del bucket de Amazon S3 de Trusted Advisor en su cuenta de AWS.

```
aws support refresh-trusted-advisor-check \
    --check-id "Pfx0RwqBli"
```

Salida:

```
{
    "status": {
        "checkId": "Pfx0RwqBli",
        "status": "enqueued",
        "millisUntilNextRefreshable": 3599992
    }
}
```

Para obtener más información, consulte AWS Trusted Advisor en la Guía del usuario de AWS Support.

- Para ver los detalles de la API, consulte RefreshTrustedAdvisorCheck en la Referencia de comandos de la AWS CLI.

`resolve-case`

En el siguiente ejemplo de código, se muestra cómo utilizar `resolve-case`.

AWS CLI

Resolución de un caso de soporte

En el siguiente ejemplo de `resolve-case` se resuelve un caso de soporte en su cuenta de AWS.

```
aws support resolve-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Salida:

```
{
    "finalCaseStatus": "resolved",
    "initialCaseStatus": "work-in-progress"
```

```
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS.

- Para obtener información sobre la API, consulte ResolveCase en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon SWF que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon SWF.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`count-closed-workflow-executions`

En el siguiente ejemplo de código, se muestra cómo utilizar `count-closed-workflow-executions`.

AWS CLI

Recuento de ejecuciones de flujo de trabajo cerradas

Puede utilizar `swf count-closed-workflow-executions` para recuperar el número de ejecuciones de flujo de trabajo cerradas de un dominio determinado. Puede especificar filtros para contar clases de ejecuciones específicas.

Los argumentos `--domain` y `--close-time-filter` o `--start-time-filter` son obligatorios. Todos los demás argumentos son opcionales.

```
aws swf count-closed-workflow-executions \
    --domain DataFrobtzz \
    --close-time-filter "{ \"latestDate\" : 1377129600, \"oldestDate\" :
 1370044800 }"
```

Salida:

```
{
    "count": 2,
    "truncated": false
}
```

Si el valor de truncated es `true`, count representa el número máximo que puede devolver Amazon SWF. Los demás resultados se truncan.

Para reducir el número de resultados devueltos, puede:

modificar los valores `--close-time-filter` o `--start-time-filter` para reducir el intervalo de tiempo en el que se busca. Cada valor se excluye mutuamente: puede especificar solo uno en una solicitud. Utilice los argumentos `--close-status-filter`, `--execution-filter`, `--tag-filter` o `--type-filter` para filtrar aún más los resultados. Sin embargo, estos argumentos también se excluyen mutuamente.

Consulte CountClosedWorkflowExecutions en la Referencia de la API de Amazon Simple Workflow Service.

- Para obtener información sobre la API, consulte CountClosedWorkflowExecutions en la Referencia de comandos de la AWS CLI.

`count-open-workflow-executions`

En el siguiente ejemplo de código, se muestra cómo utilizar `count-open-workflow-executions`.

AWS CLI

Recuento de ejecuciones de flujo de trabajo pendientes

Puede utilizar `swf count-open-workflow-executions` para recuperar el número de ejecuciones de flujo de trabajo pendientes de un dominio determinado. Puede especificar filtros para contar clases de ejecuciones específicas.

Solo se necesitan los argumentos `--domain` y `--start-time-filter`. Todos los demás argumentos son opcionales.

```
aws swf count-open-workflow-executions \
    --domain DataFrobtzz \
    --start-time-filter "{ \"latestDate\" : 1377129600, \"oldestDate\" :
 1370044800 }"
```

Salida:

```
{
    "count": 4,
    "truncated": false
}
```

Si el valor de truncated es `true`, count representa el número máximo que puede devolver Amazon SWF. Los demás resultados se truncan.

Para reducir el número de resultados devueltos, puede:

modificar los valores `--start-time-filter` para reducir el intervalo de tiempo en el que se busca. Utilice los argumentos `--close-status-filter`, `--execution-filter`, `--tag-filter` o `--type-filter` para filtrar aún más los resultados. Cada uno se excluye mutuamente: puede especificar solo uno en una solicitud.

Para obtener más información, consulte CountOpenWorkflowExecutions en la Referencia de la API de Amazon Simple Workflow Service.

- Para obtener información sobre la API, consulte CountOpenWorkflowExecutions en la Referencia de comandos de la AWS CLI.

`deprecate-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `deprecate-domain`.

AWS CLI

Para dar de baja un dominio

Para dar de baja un dominio (aunque todavía podrá verlo, no podrá crear nuevas ejecuciones de flujo de trabajo ni tipos de registro en él), use `swf deprecate-domain`. Solo tiene un parámetro necesario, `--name`, que toma el nombre del dominio que se va a descartar.

```
aws swf deprecate-domain \
    --name MyNeatNewDomain ""
```

Al igual que ocurre con `register-domain`, no se devuelve ningún resultado. Si usa `list-domains` para ver los dominios registrados, sin embargo, verá que el dominio se ha retirado y ya no aparece entre los datos devueltos.

```
aws swf list-domains \
    --registration-status REGISTERED
        {
            "domainInfos": [
                {
                    "status": "REGISTERED",
                    "name": "DataFrobotz"
                },
                {
                    "status": "REGISTERED",
                    "name": "erontest"
                }
            ]
        }
```

Si usa `--registration-status DEPRECATED` con `list-domains`, verá el dominio obsoleto.

```
aws swf list-domains \
    --registration-status DEPRECATED
        {
            "domainInfos": [
                {
                    "status": "DEPRECATED",
                    "name": "MyNeatNewDomain"
                }
            ]
        }
```

También puede usar `describe-domain` para obtener información sobre un dominio obsoleto.

```
aws swf describe-domain \
    --name MyNeatNewDomain
        {
            "domainInfo": {
```

```
            "status": "DEPRECATED",
            "name": "MyNeatNewDomain"
        },
        "configuration": {
            "workflowExecutionRetentionPeriodInDays": "0"
        }
    }
```

Consulte DeprecateDomain en la Referencia de la API de Amazon Simple Workflow Service.

- Para obtener más información sobre la API, consulte DeprecateDomain en la Referencia de comandos de la AWS CLI.

`describe-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-domain`.

AWS CLI

Para obtener información sobre un dominio

Para obtener información detallada acerca de un dominio en particular, use el comando `swf describe-domain`. Hay un parámetro necesario: `--name`, que lleva el nombre del dominio sobre el que desee información.

```
aws swf describe-domain \
    --name DataFrobotz
    {
        "domainInfo": {
            "status": "REGISTERED",
            "name": "DataFrobotz"
        },
        "configuration": {
            "workflowExecutionRetentionPeriodInDays": "1"
        }
    }
```

También puede usar `describe-domain` para obtener información sobre los dominios obsoletos.

```
aws swf describe-domain \
    --name MyNeatNewDomain
    {
```

```
            "domainInfo": {
                "status": "DEPRECATED",
                "name": "MyNeatNewDomain"
            },
            "configuration": {
                "workflowExecutionRetentionPeriodInDays": "0"
            }
        }
```

Consulte DescribeDomain en la Referencia de la API de Amazon Simple Workflow Service.

- Para obtener más información sobre la API, consulte DescribeDomain en la Referencia de comandos de la AWS CLI.

`list-activity-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-activity-types`.

AWS CLI

Lista de tipos de actividad

Para obtener una lista de los tipos de actividad de un dominio, utilice `swf list-activity-types`. Solo se necesitan los argumentos `--domain` y `--registration-status`.

```
aws swf list-activity-types \
    --domain DataFrobtzz \
    --registration-status REGISTERED
```

Salida:

```
{
    "typeInfos": [
        {
            "status": "REGISTERED",
            "creationDate": 1371454150.451,
            "activityType": {
                "version": "1",
                "name": "confirm-user-email"
            },
            "description": "subscribe confirm-user-email activity"
        },
```

```
        {
            "status": "REGISTERED",
            "creationDate": 1371454150.709,
            "activityType": {
                "version": "1",
                "name": "confirm-user-phone"
            },
            "description": "subscribe confirm-user-phone activity"
        },
        {
            "status": "REGISTERED",
            "creationDate": 1371454149.871,
            "activityType": {
                "version": "1",
                "name": "get-subscription-info"
            },
            "description": "subscribe get-subscription-info activity"
        },
        {
            "status": "REGISTERED",
            "creationDate": 1371454150.909,
            "activityType": {
                "version": "1",
                "name": "send-subscription-success"
            },
            "description": "subscribe send-subscription-success activity"
        },
        {
            "status": "REGISTERED",
            "creationDate": 1371454150.085,
            "activityType": {
                "version": "1",
                "name": "subscribe-user-sns"
            },
            "description": "subscribe subscribe-user-sns activity"
        }
    ]
}
```

Puede usar el argumento `--name` para seleccionar solo los tipos de actividad que tengan un nombre determinado:

```
aws swf list-activity-types \
```

```
    --domain DataFrobtzz \
    --registration-status REGISTERED \
    --name "send-subscription-success"
```

Salida:

```
{
    "typeInfos": [
        {
            "status": "REGISTERED",
            "creationDate": 1371454150.909,
            "activityType": {
                "version": "1",
                "name": "send-subscription-success"
            },
            "description": "subscribe send-subscription-success activity"
        }
    ]
}
```

Para recuperar los resultados en las páginas, puede establecer el argumento `--maximum-page-size`. Si se devuelven más resultados de los que caben en una página de resultados, se devolverá un nextPageToken en el conjunto de resultados:

```
aws swf list-activity-types \
    --domain DataFrobtzz \
    --registration-status REGISTERED \
    --maximum-page-size 2
```

Salida:

```
{
    "nextPageToken": "AAAAKgAAAAEAAAAAAAAAA1Gp1BelJq
+PmHvAnDxJYbup8+0R4LVtbXLDl7QNY7C3OpHo9Sz06D/GuFz1OyC73umBQ1tOPJ/gC/
aYpzDMqUIWIA1T9W0s2DryyZX4OC/6Lhk9/
o5kdsuWMSBkHhgaZjgwp3WJINIFJFdaSMxY2vYAX7AtRtpcqJuBDDRE9RaRqDGYqIYUMltarkiqpSY1ZVveBasBvlvyU
WGAaqehiDz7/JzLT/wWNNUMOd+Nhe",
    "typeInfos": [
        {
            "status": "REGISTERED",
            "creationDate": 1371454150.451,
            "activityType": {
```

```
                "version": "1",
                "name": "confirm-user-email"
            },
            "description": "subscribe confirm-user-email activity"
        },
        {
            "status": "REGISTERED",
            "creationDate": 1371454150.709,
            "activityType": {
                "version": "1",
                "name": "confirm-user-phone"
            },
            "description": "subscribe confirm-user-phone activity"
        }
    ]
}
```

Puede pasar el valor nextPageToken a la siguiente llamada a `list-activity-types` en el argumento `--next-page-token` y recuperar la siguiente página de resultados:

```
aws swf list-activity-types \
    --domain DataFrobtzz \
    --registration-status REGISTERED \
    --maximum-page-size 2 \
    --next-page-token "AAAAKgAAAAEAAAAAAAAAA1Gp1BelJq
+PmHvAnDxJYbup8+0R4LVtbXLDl7QNY7C3OpHo9Sz06D/GuFz1OyC73umBQ1tOPJ/gC/
aYpzDMqUIWIA1T9W0s2DryyZX4OC/6Lhk9/
o5kdsuWMSBkHhgaZjgwp3WJINIFJFdaSMxY2vYAX7AtRtpcqJuBDDRE9RaRqDGYqIYUMltarkiqpSY1ZVveBasBvlvyU
WGAaqehiDz7/JzLT/wWNNUMOd+Nhe"
```

Salida:

```
{
    "nextPageToken": "AAAAKgAAAAEAAAAAAAAAAw+7LZ4GRZPzTqBHsp2wBxWB8m1sgLCclgCuq3J+h/
m3+vOfFqtkcjLwV5cc4OjNAzTCuq/
XcylPumGwkjbajtqpZpbqOcVNfjFxGoi0LB2Olbvv0krbUISBvlpFPmSWpDSZJsxg5UxCcweteSlFn1PNSZ/
MoinBZo8OTkjMuzcsTuKOzH9wCaR8ITcALJ3SaqHU3pyIRS5hPmFA3OLIc8zaAepjlaujo6hntNSCruB4"
    "typeInfos": [
        {
            "status": "REGISTERED",
            "creationDate": 1371454149.871,
            "activityType": {
                "version": "1",
```

```
                "name": "get-subscription-info"
            },
            "description": "subscribe get-subscription-info activity"
        },
        {
            "status": "REGISTERED",
            "creationDate": 1371454150.909,
            "activityType": {
                "version": "1",
                "name": "send-subscription-success"
            },
            "description": "subscribe send-subscription-success activity"
        }
    ]
}
```

Si aún quedan más resultados por devolver, se devolverá nextPageToken con los resultados. Cuando no haya más páginas de resultados a devolver, nextPageToken no aparecerá en el conjunto de resultados.

Puede utilizar el argumento `--reverse-order` para revertir el orden de los resultados devueltos. Esto también afecta a los resultados paginados.

```
aws swf list-activity-types \
    --domain DataFrobtzz \
    --registration-status REGISTERED \
    --maximum-page-size 2 \
    --reverse-order
```

Salida:

```
{
    "nextPageToken": "AAAAKgAAAAEAAAAAAAAAAwXcpu5ePSyQkrC
+8WMbmSrenuZC2ZkIXQYBPB/b9xIOVkj+bMEFhGj0KmmJ4rF7iddhjf7UMYCsfGkEn7mk
+yMCgVc1JxDWmB0EH46bhcmcLmYNQihMDmUWocpr7To6/R7CLu0St1gkFayxOidJXErQW0zdNfQaIWAnF/
cwioBbXlkz1fQzmDeU3M5oYGMPQIrUqkPq7pMEW0q0lK5eDN97NzFYdZZ/rlcLDWPZhUjY",
    "typeInfos": [
        {
            "status": "REGISTERED",
            "creationDate": 1371454150.085,
            "activityType": {
                "version": "1",
```

```
                "name": "subscribe-user-sns"
            },
            "description": "subscribe subscribe-user-sns activity"
        },
        {
            "status": "REGISTERED",
            "creationDate": 1371454150.909,
            "activityType": {
                "version": "1",
                "name": "send-subscription-success"
            },
            "description": "subscribe send-subscription-success activity"
        }
    ]
}
```

Consulte ListActivityTypes en la Referencia de la API de Amazon Simple Workflow Service.

- Para obtener información sobre la API, consulte ListActivityTypes en la Referencia de comandos de la AWS CLI.

`list-domains`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-domains`.

AWS CLI

Ejemplo 1: enumeración de los dominios registrados

El siguiente comando `list-domains` enumera los dominios de SWF `REGISTERED` que ha registrado en su cuenta.

```
aws swf list-domains \
    --registration-status REGISTERED
```

Salida:

```
{
  "domainInfos": [
    {
      "status": "REGISTERED",
      "name": "DataFrobotz"
```

```
    },
    {
      "status": "REGISTERED",
      "name": "erontest"
    }
  ]
}
```

Para obtener más información, consulte ListDomains en la Referencia de la API de Amazon Simple Workflow Service.

Ejemplo 2: enumeración de los dominios obsoletos

El siguiente comando `list-domains` enumera los dominios de SWF `DEPRECATED` que ha registrado en su cuenta. Los dominios obsoletos son dominios que no pueden registrar nuevos flujos de trabajo ni actividades, pero que pueden consultarse.

```
aws swf list-domains \
    --registration-status DEPRECATED
```

Salida:

```
{
  "domainInfos": [
    {
      "status": "DEPRECATED",
      "name": "MyNeatNewDomain"
    }
  ]
}
```

Para obtener más información, consulte ListDomains en la Referencia de la API de Amazon Simple Workflow Service.

Ejemplo 3: enumeración de la primera página de dominios registrados

El siguiente comando `list-domains` enumera los dominios de SWF `REGISTERED` de la primera página que ha registrado en su cuenta con la opción `--maximum-page-size`.

```
aws swf list-domains \
    --registration-status REGISTERED \
```

```
    --maximum-page-size 1
```

Salida:

```
{
    "domainInfos": [
        {
            "status": "REGISTERED",
            "name": "DataFrobotz"
        }
    ],
"nextPageToken": "AAAAKgAAAAEAAAAAAAAAA2QJKNtidVgd49TTeNwYcpD
+QKT2ynuEbibcQWe2QKrslMGe63gpS0MgZGpcpoKttL4OCXRFn98Xif557it
+wSZUsvUDtImjDLvguyuyyFdIZtvIxIKEOPm3k2r4OjAGaFsGOuVbrKljvla7wdU7FYH3OlkNCP8b7PBj9SBkUyGoiAg
}
```

Para obtener más información, consulte ListDomains en la Referencia de la API de Amazon Simple Workflow Service.

Ejemplo 4: enumeración de la única página de dominios registrados especificada

El siguiente comando `list-domains` enumera los dominios de SWF `REGISTERED` de la primera página que ha registrado en su cuenta con la opción `--maximum-page-size`.

Cuando realice la llamada de nuevo, indicando en esta ocasión el valor de `nextPageToken` en el argumento `--next-page-token`, obtendrá otra página de resultados.

```
aws swf list-domains \
    --registration-status REGISTERED \
    --maximum-page-size 1 \
    --next-page-token "AAAAKgAAAAEAAAAAAAAAA2QJKNtidVgd49TTeNwYcpD
+QKT2ynuEbibcQWe2QKrslMGe63gpS0MgZGpcpoKttL4OCXRFn98Xif557it
+wSZUsvUDtImjDLvguyuyyFdIZtvIxIKEOPm3k2r4OjAGaFsGOuVbrKljvla7wdU7FYH3OlkNCP8b7PBj9SBkUyGoiAg
```

Salida:

```
{
    "domainInfos": [
        {
            "status": "REGISTERED",
            "name": "erontest"
        }
```

```
    ]
}
```

Cuando no haya más páginas de resultados que recuperar, `nextPageToken` no aparecerá en los resultados.

Para obtener más información, consulte ListDomains en la Referencia de la API de Amazon Simple Workflow Service.

- Para obtener información sobre la API, consulte ListDomains en la Referencia de comandos de la AWS CLI.

`list-workflow-types`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-workflow-types`.

AWS CLI

Para enumerar tipos de flujo de trabajo

Para obtener una lista de los tipos de flujo de trabajo de un dominio, utilice `swf list-workflow-types`. Solo se necesitan los argumentos `--domain` y `--registration-status`. A continuación, se muestra un ejemplo sencillo.

```
aws swf list-workflow-types \
    --domain DataFrobtzz \
    --registration-status REGISTERED
```

Salida:

```
{
    "typeInfos": [
        {
            "status": "REGISTERED",
            "creationDate": 1371454149.598,
            "description": "DataFrobtzz subscribe workflow",
            "workflowType": {
                "version": "v3",
                "name": "subscribe"
            }
        }
    ]
```

```
}
```

Del mismo modo que con `list-activity-types`, puede usar el argumento `--name` para seleccionar solo los tipos de flujo de trabajo con un nombre concreto y usar el argumento `--maximum-page-size` en coordinación con `--next-page-token` para paginar los resultados. Para invertir el orden en el que se devuelven los resultados, utilice `--reverse-order`.

Consulte ListWorkflowTypes en la Referencia de la API de Amazon Simple Workflow Service.

- Para obtener información sobre la API, consulte ListWorkflowTypes en la Referencia de comandos de la AWS CLI.

`register-domain`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-domain`.

AWS CLI

Registro de un dominio

Puede usar la AWS CLI para registrar nuevos dominios. Utilice el comando `swf register-domain`. Existen dos parámetros obligatorios: `--name`, que toma el nombre de dominio, y `--workflow-execution-retention-period-in-days`, que toma un número entero para especificar el número de días que deben conservarse los datos de ejecución de flujo de trabajo en este dominio, hasta un período máximo de 90 días (para obtener más información, consulte las Preguntas frecuentes sobre SWF <https://aws.amazon.com/swf/faqs/#retain_limit>). Los datos de ejecución de flujo de trabajo no se conservarán después de que haya transcurrido el número especificado de días.

```
aws swf register-domain \
    --name MyNeatNewDomain \
    --workflow-execution-retention-period-in-days 0
    ""
```

Al registrar un dominio, no se devuelve nada (""), pero puede utilizar `swf list-domains` o `swf describe-domain` para ver el nuevo dominio.

```
aws swf list-domains \
    --registration-status REGISTERED
        {
```

```
            "domainInfos": [
                {
                    "status": "REGISTERED",
                    "name": "DataFrobotz"
                },
                {
                    "status": "REGISTERED",
                    "name": "MyNeatNewDomain"
                },
                {
                    "status": "REGISTERED",
                    "name": "erontest"
                }
            ]
        }
```

Uso de `swf describe-domain`:

```
aws swf describe-domain --
name MyNeatNewDomain
{
    "domainInfo": {
        "status": "REGISTERED",
        "name": "MyNeatNewDomain"
    },
    "configuration": {
        "workflowExecutionRetentionPeriodInDays": "0"

  }
}
```

Consulte RegisterDomain en la Referencia de la API de Amazon Simple Workflow Service.

- Para obtener información sobre la API, consulte RegisterDomain en la Referencia de comandos de la AWS CLI.

`register-workflow-type`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-workflow-type`.

AWS CLI

Registro de un tipo de flujo de trabajo

Para registrar un tipo de flujo de trabajo con la AWS CLI, utilice el comando `swf register-workflow-type`.

```
aws swf register-workflow-type \
    --domain DataFrobtzz \
    --name "MySimpleWorkflow" \
    --workflow-version "v1"
```

Si se ejecuta correctamente, este comando no genera ningún resultado.

En caso de error (por ejemplo, si intenta registrar el mismo tipo de flujo de trabajo dos veces o especifica un dominio que no existe), obtendrá una respuesta en JSON.

```
{
    "message": "WorkflowType=[name=MySimpleWorkflow, version=v1]",
    "__type": "com.amazonaws.swf.base.model#TypeAlreadyExistsFault"
}
```

`--domain`, `--name` y `--workflow-version` son obligatorios. También puede configurar la descripción del flujo de trabajo, los tiempos de espera y la política de flujo de trabajo secundario.

Para obtener más información, consulte RegisterWorkflowType en la Referencia de la API de Amazon Simple Workflow Service.

- Para obtener información sobre la API, consulte RegisterWorkflowType en la Referencia de comandos de la AWS CLI.

Ejemplos de Systems Manager que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Systems Manager.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`add-tags-to-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-tags-to-resource`.

AWS CLI

Ejemplo 1: adición de etiquetas a un periodo de mantenimiento

En el siguiente ejemplo de `add-tags-to-resource` se agrega una etiqueta al periodo de mantenimiento especificado.

```
aws ssm add-tags-to-resource \
    --resource-type "MaintenanceWindow" \
    --resource-id "mw-03eb9db428EXAMPLE" \
    --tags "Key=Stack,Value=Production"
```

Este comando no genera ninguna salida.

Ejemplo 2: adición de etiquetas a un parámetro

En el siguiente ejemplo de `add-tags-to-resource` se agregan dos etiquetas al parámetro especificado.

```
aws ssm add-tags-to-resource \
    --resource-type "Parameter" \
    --resource-id "My-Parameter" \
    --tags '[{"Key":"Region","Value":"East"},{"Key":"Environment",
 "Value":"Production"}]'
```

Este comando no genera ninguna salida.

Ejemplo 3: adición de etiquetas a un documento de SSM

En el siguiente ejemplo de `add-tags-to-resource` se agrega una etiqueta al documento especificado.

```
aws ssm add-tags-to-resource \
    --resource-type "Document" \
    --resource-id "My-Document" \
    --tags "Key=Quarter,Value=Q322"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de recursos de Systems Manager en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte AddTagsToResource en la Referencia de comandos de la AWS CLI.

`associate-ops-item-related-item`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-ops-item-related-item`.

AWS CLI

Para asociar un elemento relacionado

En el siguiente ejemplo de `associate-ops-item-related-item`, se asocia un elemento relacionado con el OpsItem.

```
aws ssm associate-ops-item-related-item \
    --ops-item-id "oi-649fExample" \
    --association-type "RelatesTo" \
    --resource-type "AWS::SSMIncidents::IncidentRecord" \
    --resource-uri "arn:aws:ssm-incidents::111122223333:incident-record/Example-Response-Plan/c2bde883-f7d5-343a-b13a-bf5fe9ea689f"
```

Salida:

```
{
    "AssociationId": "61d7178d-a30d-4bc5-9b4e-a9e74EXAMPLE"
}
```

Para obtener más información, consulte Working with Incident Manager incidents in OpsCenter en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte AssociateOpsItemRelatedItem en la Referencia de comandos de la AWS CLI.

`cancel-command`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-command`.

AWS CLI

Ejemplo 1: cancelación de un comando para todas las instancias

En el siguiente ejemplo de `cancel-command` se intenta cancelar el comando especificado que ya se está ejecutando en todas las instancias.

```
aws ssm cancel-command \
    --command-id "662add3d-5831-4a10-b64a-f2ff3EXAMPLE"
```

Este comando no genera ninguna salida.

Ejemplo 2: cancelación de un comando para instancias específicas

En el siguiente ejemplo de `cancel-command` se intenta cancelar un comando únicamente en la instancia especificada.

```
aws ssm cancel-command \
    --command-id "662add3d-5831-4a10-b64a-f2ff3EXAMPLE"
    --instance-ids "i-02573cafcfEXAMPLE"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Etiquetado de parámetros de Systems Manager en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte CancelCommand en la Referencia de comandos de la AWS CLI.

`cancel-maintenance-window-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `cancel-maintenance-window-execution`.

AWS CLI

Para cancelar una ejecución del período de mantenimiento

En este ejemplo de `cancel-maintenance-window-execution`, se detiene la ejecución del período de mantenimiento especificada que ya está en curso.

```
aws ssm cancel-maintenance-window-execution \
```

```
    --window-execution-id j2l8d5b5c-mw66-tk4d-r3g9-1d4d1EXAMPLE
```

Salida:

```
{
    "WindowExecutionId": "j2l8d5b5c-mw66-tk4d-r3g9-1d4d1EXAMPLE"
}
```

Para obtener más información, consulte Tutoriales de Maintenance Windows de Systems Manager (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener más información sobre la API, consulte CancelMaintenanceWindowExecution en Referencia de comandos de la AWS CLI.

`create-activation`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-activation`.

AWS CLI

Creación de la activación de una instancia administrada

En el siguiente ejemplo de `create-activation` se crea la activación de una instancia administrada.

```
aws ssm create-activation \
    --default-instance-name "HybridWebServers" \
    --iam-role "HybridWebServersRole" \
    --registration-limit 5
```

Salida:

```
{
    "ActivationId": "5743558d-563b-4457-8682-d16c3EXAMPLE",
    "ActivationCode": "dRmgnYaFv567vEXAMPLE"
}
```

Para obtener más información, consulte Paso 4: crear una activación híbrida para un entorno híbrido y multinube en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte CreateActivation en la Referencia de comandos de la AWS CLI.

`create-association-batch`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-association-batch`.

AWS CLI

Creación de varias asociaciones

En este ejemplo se asocia un documento de configuración a varias instancias. El resultado devuelve una lista de operaciones correctas y con errores, si corresponde.

Comando:

```
aws ssm create-association-batch --entries "Name=AWS-
UpdateSSMAgent,InstanceId=i-1234567890abcdef0" "Name=AWS-
UpdateSSMAgent,InstanceId=i-9876543210abcdef0"
```

Salida:

```
{
  "Successful": [
      {
          "Name": "AWS-UpdateSSMAgent",
          "InstanceId": "i-1234567890abcdef0",
          "AssociationVersion": "1",
          "Date": 1550504725.007,
          "LastUpdateAssociationDate": 1550504725.007,
          "Status": {
              "Date": 1550504725.007,
              "Name": "Associated",
              "Message": "Associated with AWS-UpdateSSMAgent"
          },
          "Overview": {
              "Status": "Pending",
              "DetailedStatus": "Creating"
          },
          "DocumentVersion": "$DEFAULT",
          "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
          "Targets": [
              {
                  "Key": "InstanceIds",
                  "Values": [
                      "i-1234567890abcdef0"
                  ]
```

```
                }
            ]
        },
        {
            "Name": "AWS-UpdateSSMAgent",
            "InstanceId": "i-9876543210abcdef0",
            "AssociationVersion": "1",
            "Date": 1550504725.057,
            "LastUpdateAssociationDate": 1550504725.057,
            "Status": {
                "Date": 1550504725.057,
                "Name": "Associated",
                "Message": "Associated with AWS-UpdateSSMAgent"
            },
            "Overview": {
                "Status": "Pending",
                "DetailedStatus": "Creating"
            },
            "DocumentVersion": "$DEFAULT",
            "AssociationId": "9c9f7f20-5154-4fed-a83e-0123456789ab",
            "Targets": [
                {
                    "Key": "InstanceIds",
                    "Values": [
                        "i-9876543210abcdef0"
                    ]
                }
            ]
        }
    ],
    "Failed": []
}
```

- Para obtener información sobre la API, consulte CreateAssociationBatch en la Referencia de comandos de la AWS CLI.

`create-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-association`.

AWS CLI

Ejemplo 1: asociación de un documento mediante los ID de instancia

En este ejemplo se asocia un documento de configuración a una instancia mediante los ID de instancia.

```
aws ssm create-association \
    --instance-id "i-0cb2b964d3e14fd9f" \
    --name "AWS-UpdateSSMAgent"
```

Salida:

```
{
    "AssociationDescription": {
        "Status": {
            "Date": 1487875500.33,
            "Message": "Associated with AWS-UpdateSSMAgent",
            "Name": "Associated"
        },
        "Name": "AWS-UpdateSSMAgent",
        "InstanceId": "i-0cb2b964d3e14fd9f",
        "Overview": {
            "Status": "Pending",
            "DetailedStatus": "Creating"
        },
        "AssociationId": "b7c3266e-a544-44db-877e-b20d3a108189",
        "DocumentVersion": "$DEFAULT",
        "LastUpdateAssociationDate": 1487875500.33,
        "Date": 1487875500.33,
        "Targets": [
            {
                "Values": [
                    "i-0cb2b964d3e14fd9f"
                ],
                "Key": "InstanceIds"
            }
        ]
    }
}
```

Para obtener más información, consulte CreateAssociation en la Referencia de la API de AWS Systems Manager.

Ejemplo 2: asociación de un documento mediante destinos

En este ejemplo, se asocia un documento de configuración a una instancia mediante destinos.

```
aws ssm create-association \
    --name "AWS-UpdateSSMAgent" \
    --targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f"
```

Salida:

```
{
    "AssociationDescription": {
        "Status": {
            "Date": 1487875500.33,
            "Message": "Associated with AWS-UpdateSSMAgent",
            "Name": "Associated"
        },
        "Name": "AWS-UpdateSSMAgent",
        "InstanceId": "i-0cb2b964d3e14fd9f",
        "Overview": {
            "Status": "Pending",
            "DetailedStatus": "Creating"
        },
        "AssociationId": "b7c3266e-a544-44db-877e-b20d3a108189",
        "DocumentVersion": "$DEFAULT",
        "LastUpdateAssociationDate": 1487875500.33,
        "Date": 1487875500.33,
        "Targets": [
            {
                "Values": [
                    "i-0cb2b964d3e14fd9f"
                ],
                "Key": "InstanceIds"
            }
        ]
    }
}
```

Para obtener más información, consulte CreateAssociation en la Referencia de la API de AWS Systems Manager.

Ejemplo 3: creación de una asociación que solo se ejecuta una vez

En este ejemplo se crea una nueva asociación que solo se ejecuta una vez en la fecha y hora especificadas. Las asociaciones creadas con una fecha en el pasado o en el presente (cuando se procesan, la fecha queda en el pasado) se ejecutan inmediatamente.

```
aws ssm create-association \
    --name "AWS-UpdateSSMAgent" \
    --targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f" \
    --schedule-expression "at(2020-05-14T15:55:00)"  \
    --apply-only-at-cron-interval
```

Salida:

```
{
    "AssociationDescription": {
        "Status": {
            "Date": 1487875500.33,
            "Message": "Associated with AWS-UpdateSSMAgent",
            "Name": "Associated"
        },
        "Name": "AWS-UpdateSSMAgent",
        "InstanceId": "i-0cb2b964d3e14fd9f",
        "Overview": {
            "Status": "Pending",
            "DetailedStatus": "Creating"
        },
        "AssociationId": "b7c3266e-a544-44db-877e-b20d3a108189",
        "DocumentVersion": "$DEFAULT",
        "LastUpdateAssociationDate": 1487875500.33,
        "Date": 1487875500.33,
        "Targets": [
            {
                "Values": [
                    "i-0cb2b964d3e14fd9f"
                ],
                "Key": "InstanceIds"
            }
        ]
    }
}
```

Para obtener más información, consulte CreateAssociation en la Referencia de la API de AWS Systems Manager o Referencia: expresiones cron y rate para Systems Manager en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte CreateAssociation en la Referencia de comandos de la AWS CLI.

`create-document`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-document`.

AWS CLI

Creación de un documento

En el siguiente ejemplo de `create-document` se crea un documento de Systems Manager.

```
aws ssm create-document \
    --content file://exampleDocument.yml \
    --name "Example" \
    --document-type "Automation" \
    --document-format YAML
```

Salida:

```
{
    "DocumentDescription": {
        "Hash": "fc2410281f40779e694a8b95975d0f9f316da8a153daa94e3d9921102EXAMPLE",
        "HashType": "Sha256",
        "Name": "Example",
        "Owner": "29884EXAMPLE",
        "CreatedDate": 1583256349.452,
        "Status": "Creating",
        "DocumentVersion": "1",
        "Description": "Document Example",
        "Parameters": [
            {
                "Name": "AutomationAssumeRole",
                "Type": "String",
                "Description": "(Required) The ARN of the role that allows
 Automation to perform the actions on your behalf. If no role is specified, Systems
 Manager Automation uses your IAM permissions to execute this document.",
                "DefaultValue": ""
            },
            {
                "Name": "InstanceId",
                "Type": "String",
                "Description": "(Required) The ID of the Amazon EC2 instance.",
                "DefaultValue": ""
            }
```

```
        ],
        "PlatformTypes": [
            "Windows",
            "Linux"
        ],
        "DocumentType": "Automation",
        "SchemaVersion": "0.3",
        "LatestVersion": "1",
        "DefaultVersion": "1",
        "DocumentFormat": "YAML",
        "Tags": []
    }
}
```

Para obtener más información, consulte Crear contenido en el documento de SSM en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte CreateDocument en la Referencia de comandos de la AWS CLI.

`create-maintenance-window`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-maintenance-window`.

AWS CLI

Ejemplo 1: creación de un periodo de mantenimiento

En el siguiente ejemplo de `create-maintenance-window` se crea un nuevo periodo de mantenimiento que, cada cinco minutos durante un máximo de dos horas (según sea necesario), impide que se inicien nuevas tareas una hora después de que finalice el periodo de mantenimiento, permite los destinos no asociados (instancias que no ha registrado con el periodo de mantenimiento) e indica, mediante el uso de etiquetas personalizadas, que su creador tiene la intención de utilizarlo en un tutorial.

```
aws ssm create-maintenance-window \
    --name "My-Tutorial-Maintenance-Window" \
    --schedule "rate(5 minutes)" \
    --duration 2 --cutoff 1 \
    --allow-unassociated-targets \
    --tags "Key=Purpose,Value=Tutorial"
```

Salida:

```
{
    "WindowId": "mw-0c50858d01EXAMPLE"
}
```

Ejemplo 2: creación de un periodo de mantenimiento que se ejecuta solo una vez

En el siguiente ejemplo de `create-maintenance-window` se crea un nuevo periodo de mantenimiento que solo se ejecuta una vez en la fecha y hora especificadas.

```
aws ssm create-maintenance-window \
    --name My-One-Time-Maintenance-Window \
    --schedule "at(2020-05-14T15:55:00)" \
    --duration 5 \
    --cutoff 2 \
    --allow-unassociated-targets \
    --tags "Key=Environment,Value=Production"
```

Salida:

```
{
    "WindowId": "mw-01234567890abcdef"
}
```

Para obtener más información, consulte Maintenance Windows en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte CreateMaintenanceWindow en la Referencia de comandos de la AWS CLI.

`create-ops-item`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-ops-item`.

AWS CLI

Creación de un OpsItems

En el siguiente ejemplo de `create-ops-item` se utiliza la clave /aws/resources en OperationalData para crear un OpsItem con un recurso relacionado de Amazon DynamoDB.

```
aws ssm create-ops-item \
    --title "EC2 instance disk full" \
    --description "Log clean up may have failed which caused the disk to be full" \
    --priority 2 \
    --source ec2 \
    --operational-data '{"/aws/resources":{"Value":"[{\"arn
\": \"arn:aws:dynamodb:us-west-2:12345678:table/OpsItems
\"}]","Type":"SearchableString"}}' \
    --notifications Arn="arn:aws:sns:us-west-2:12345678:TestUser"
```

Salida:

```
{
    "OpsItemId": "oi-1a2b3c4d5e6f"
}
```

Para obtener más información, consulte Creación de OpsItems en la Guía del usuario AWS Systems Manager.

- Para obtener información sobre la API, consulte CreateOpsItem en la Referencia de comandos de la AWS CLI.

`create-patch-baseline`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-patch-baseline`.

AWS CLI

Ejemplo 1: creación de una línea de base de revisiones con aprobación automática

En el siguiente ejemplo de `create-patch-baseline` se crea una línea de base de revisiones para Windows Server que aprueba las revisiones de un entorno de producción siete días después de que Microsoft las publique.

```
aws ssm create-patch-baseline \
    --name "Windows-Production-Baseline-AutoApproval" \
    --operating-system "WINDOWS" \
    --approval-
rules "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=MSRC_SEVERITY,Values=[Critical,Impo
{Key=CLASSIFICATION,Values=[SecurityUpdates,Updates,UpdateRollups,CriticalUpdates]}]},Approv
 \
```

```
    --description "Baseline containing all updates approved for Windows Server
 production systems"
```

Salida:

```
{
    "BaselineId": "pb-045f10b4f3EXAMPLE"
}
```

Ejemplo 2: creación de una línea de base de revisiones con una fecha límite de aprobación

En el siguiente ejemplo de `create-patch-baseline` se crea una línea de base de revisiones para Windows Server que aprueba todas las revisiones de un entorno de producción que se publicaron el 7 de julio del 2020 o antes.

```
aws ssm create-patch-baseline \
    --name "Windows-Production-Baseline-AutoApproval" \
    --operating-system "WINDOWS" \
    --approval-
rules "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=MSRC_SEVERITY,Values=[Critical,Impo
{Key=CLASSIFICATION,Values=[SecurityUpdates,Updates,UpdateRollups,CriticalUpdates]}]},Approv
 \
    --description "Baseline containing all updates approved for Windows Server
 production systems"
```

Salida:

```
{
    "BaselineId": "pb-045f10b4f3EXAMPLE"
}
```

Ejemplo 3: creación de una línea de base de revisiones con las reglas de aprobación almacenadas en un archivo JSON

En el siguiente ejemplo de `create-patch-baseline` se crea una línea de base de revisiones para Amazon Linux 2017.09 que aprueba las revisiones de un entorno de producción siete días después de su publicación, especifica las reglas de aprobación para la línea de base de revisiones y especifica un repositorio personalizado para las revisiones.

```
aws ssm create-patch-baseline \
    --cli-input-json file://my-amazon-linux-approval-rules-and-repo.json
```

Contenido de `my-amazon-linux-approval-rules-and-repo.json`:

```
{
    "Name": "Amazon-Linux-2017.09-Production-Baseline",
    "Description": "My approval rules patch baseline for Amazon Linux 2017.09
 instances",
    "OperatingSystem": "AMAZON_LINUX",
    "Tags": [
        {
            "Key": "Environment",
            "Value": "Production"
        }
    ],
    "ApprovalRules": {
        "PatchRules": [
            {
                "ApproveAfterDays": 7,
                "EnableNonSecurity": true,
                "PatchFilterGroup": {
                    "PatchFilters": [
                        {
                            "Key": "SEVERITY",
                            "Values": [
                                "Important",
                                "Critical"
                            ]
                        },
                        {
                            "Key": "CLASSIFICATION",
                            "Values": [
                                "Security",
                                "Bugfix"
                            ]
                        },
                        {
                            "Key": "PRODUCT",
                            "Values": [
                                "AmazonLinux2017.09"
                            ]
                        }
                    ]
                }
            }
        ]
```

```
    },
    "Sources": [
        {
            "Name": "My-AL2017.09",
            "Products": [
                "AmazonLinux2017.09"
            ],
            "Configuration": "[amzn-main] \nname=amzn-main-Base
\nmirrorlist=http://repo./$awsregion./$awsdomain//$releasever/main/mirror.list //
nmirrorlist_expire=300//nmetadata_expire=300 \npriority=10 \nfailovermethod=priority
 \nfastestmirror_enabled=0 \ngpgcheck=1 \ngpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-
KEY-amazon-ga \nenabled=1 \nretries=3 \ntimeout=5\nreport_instanceid=yes"
        }
    ]
}
```

Ejemplo 4: creación de una línea de base de revisiones que especifica las revisiones aprobadas y rechazadas

En el siguiente ejemplo de `create-patch-baseline` se especifican de forma explícita las revisiones que se deben aprobar y rechazar como excepción a las reglas de aprobación predeterminadas.

```
aws ssm create-patch-baseline \
    --name "Amazon-Linux-2017.09-Alpha-Baseline" \
    --description "My custom approve/reject patch baseline for Amazon Linux 2017.09
 instances" \
    --operating-system "AMAZON_LINUX" \
    --approved-patches "CVE-2018-1234567,example-pkg-EE-2018*.amzn1.noarch" \
    --approved-patches-compliance-level "HIGH" \
    --approved-patches-enable-non-security \
    --tags "Key=Environment,Value=Alpha"
```

Para obtener más información, consulte Creación de una línea de base de revisiones personalizada en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte CreatePatchBaseline en la Referencia de comandos de la AWS CLI.

`create-resource-data-sync`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-resource-data-sync`.

AWS CLI

Para crear una sincronización de datos de recursos

En este ejemplo, se crea una sincronización de datos de recursos. No se obtienen resultados si el comando se ejecuta satisfactoriamente.

Comando:

```
aws ssm create-resource-data-sync --sync-name "ssm-resource-data-sync" --s3-destination "BucketName=ssm-bucket,Prefix=inventory,SyncFormat=JsonSerDe,Region=us-east-1"
```

- Para obtener información sobre la API, consulte CreateResourceDataSync en la Referencia de comandos de la AWS CLI.

`delete-activation`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-activation`.

AWS CLI

Eliminación de la activación de una instancia administrada

En el siguiente ejemplo de `delete-activation` se elimina la activación de una instancia administrada.

```
aws ssm delete-activation \
    --activation-id "aa673477-d926-42c1-8757-1358cEXAMPLE"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Setting Up AWS Systems Manager for Hybrid Environments en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DeleteActivation en la Referencia de comandos de la AWS CLI.

`delete-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-association`.

AWS CLI

Ejemplo 1: eliminación de una asociación mediante el ID de asociación

En el siguiente ejemplo de `delete-association` se elimina la asociación del ID de asociación especificado. No se obtienen resultados si el comando se ejecuta satisfactoriamente.

```
aws ssm delete-association \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Edición y creación de una nueva versión de una asociación en la Guía del usuario de AWS Systems Manager.

Ejemplo 2: eliminación de una asociación

En el siguiente ejemplo de `delete-association` se elimina la asociación entre una instancia y un documento. No se obtienen resultados si el comando se ejecuta satisfactoriamente.

```
aws ssm delete-association \
    --instance-id "i-1234567890abcdef0" \
    --name "AWS-UpdateSSMAgent"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Trabajo con asociaciones en Systems Manager en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DeleteAssociation en la Referencia de comandos de la AWS CLI.

`delete-document`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-document`.

AWS CLI

Eliminación de un documento

En el siguiente ejemplo de `delete-document` se elimina un documento de Systems Manager.

```
aws ssm delete-document \
```

```
    --name "Example"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Crear contenido en el documento de SSM en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DeleteDocument en la Referencia de comandos de la AWS CLI.

`delete-inventory`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-inventory`.

AWS CLI

Para eliminar un tipo de inventario personalizado

En este ejemplo, se elimina un esquema de inventario personalizado.

Comando:

```
aws ssm delete-inventory --type-name "Custom:RackInfo" --schema-delete-
option "DeleteSchema"
```

Salida:

```
{
  "DeletionId": "d72ac9e8-1f60-4d40-b1c6-bf8c78c68c4d",
  "TypeName": "Custom:RackInfo",
  "DeletionSummary": {
      "TotalCount": 1,
      "RemainingCount": 1,
      "SummaryItems": [
          {
              "Version": "1.0",
              "Count": 1,
              "RemainingCount": 1
          }
      ]
  }
}
```

Para deshabilitar un tipo de inventario personalizado

En este ejemplo, se desactiva un esquema de inventario personalizado.

Comando:

```
aws ssm delete-inventory --type-name "Custom:RackInfo" --schema-delete-
option "DisableSchema"
```

Salida:

```
{
  "DeletionId": "6961492a-8163-44ec-aa1e-923364dd0850",
  "TypeName": "Custom:RackInformation",
  "DeletionSummary": {
      "TotalCount": 0,
      "RemainingCount": 0,
      "SummaryItems": []
  }
}
```

- Para obtener información sobre la API, consulte DeleteInventory en la Referencia de comandos de la AWS CLI.

`delete-maintenance-window`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-maintenance-window`.

AWS CLI

Eliminación de un periodo de mantenimiento

En este ejemplo de `delete-maintenance-window` se elimina el periodo de mantenimiento especificado.

```
aws ssm delete-maintenance-window \
    --window-id "mw-1a2b3c4d5e6f7g8h9"
```

Salida:

```
{
```

```
    "WindowId":"mw-1a2b3c4d5e6f7g8h9"
}
```

Para obtener más información, consulte Eliminar un período de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DeleteMaintenanceWindow en la Referencia de comandos de la AWS CLI.

`delete-parameter`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-parameter`.

AWS CLI

Eliminación de un parámetro

En el siguiente ejemplo de `delete-parameter` se elimina el parámetro único especificado.

```
aws ssm delete-parameter \
    --name "MyParameter"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Uso de Parameter Store en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DeleteParameter en la Referencia de comandos de la AWS CLI.

`delete-parameters`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-parameters`.

AWS CLI

Para eliminar una lista de parámetros

En el siguiente ejemplo de `delete-parameters`, se eliminan los parámetros especificados.

```
aws ssm delete-parameters \
    --names "MyFirstParameter" "MySecondParameter" "MyInvalidParameterName"
```

Salida:

```
{
    "DeletedParameters": [
        "MyFirstParameter",
        "MySecondParameter"
    ],
    "InvalidParameters": [
        "MyInvalidParameterName"
    ]
}
```

Para obtener más información, consulte Uso de Parameter Store en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DeleteParameters en la Referencia de comandos de la AWS CLI.

`delete-patch-baseline`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-patch-baseline`.

AWS CLI

Eliminación de una línea de base de revisiones

En el siguiente ejemplo de `delete-patch-baseline` se elimina la línea de base de revisiones especificada.

```
aws ssm delete-patch-baseline \
    --baseline-id "pb-045f10b4f382baeda"
```

Salida:

```
{
    "BaselineId": "pb-045f10b4f382baeda"
}
```

Para obtener más información, consulte Actualización o eliminación de una línea de base de revisiones (consola) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DeletePatchBaseline en la Referencia de comandos de la AWS CLI.

`delete-resource-data-sync`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-resource-data-sync`.

AWS CLI

Para eliminar una sincronización de datos de recursos

En este ejemplo, se elimina una sincronización de datos de recursos. No se obtienen resultados si el comando se ejecuta satisfactoriamente.

Comando:

```
aws ssm delete-resource-data-sync --sync-name "ssm-resource-data-sync"
```

- Para obtener información sobre la API, consulte DeleteResourceDataSync en la Referencia de comandos de la AWS CLI.

`deregister-managed-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-managed-instance`.

AWS CLI

Anulación del registro de una instancia administrada

En el siguiente ejemplo de `deregister-managed-instance` se anula el registro de la instancia administrada especificada.

```
aws ssm deregister-managed-instance \
    --instance-id 'mi-08ab247cdfEXAMPLE'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Anulación del registro de nodos administrados en un entorno híbrido y multinube en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DeregisterManagedInstance en la Referencia de comandos de la AWS CLI.

deregister-patch-baseline-for-patch-group

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-patch-baseline-for-patch-group`.

AWS CLI

Anulación del registro de un grupo de revisiones de una línea de base de revisiones

En el siguiente ejemplo de `deregister-patch-baseline-for-patch-group` se anula el registro del grupo de revisiones especificado de la línea de base de revisiones.

```
aws ssm deregister-patch-baseline-for-patch-group \
    --patch-group "Production" \
    --baseline-id "pb-0ca44a362fEXAMPLE"
```

Salida:

```
{
  "PatchGroup":"Production",
  "BaselineId":"pb-0ca44a362fEXAMPLE"
}
```

Para obtener más información, consulte Añadir un grupo de revisiones a una línea de base de revisiones en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DeregisterPatchBaselineForPatchGroup en la Referencia de comandos de la AWS CLI.

deregister-target-from-maintenance-window

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-target-from-maintenance-window`.

AWS CLI

Eliminación de un destino de un periodo de mantenimiento

En el siguiente ejemplo de `deregister-target-from-maintenance-window`, se elimina el destino especificado del periodo de mantenimiento especificado.

```
aws ssm deregister-target-from-maintenance-window \
```

```
    --window-id "mw-ab12cd34ef56gh78" \
    --window-target-id "1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
```

Salida:

```
{
    "WindowId":"mw-ab12cd34ef56gh78",
    "WindowTargetId":"1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

Para obtener más información, consulte Actualizar un período de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DeregisterTargetFromMaintenanceWindow en la Referencia de comandos de la AWS CLI.

`deregister-task-from-maintenance-window`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-task-from-maintenance-window`.

AWS CLI

Eliminación de una tarea de un periodo de mantenimiento

En el siguiente ejemplo de `deregister-task-from-maintenance-window` se elimina la tarea especificada del periodo de mantenimiento especificado.

```
aws ssm deregister-task-from-maintenance-window \
    --window-id "mw-ab12cd34ef56gh78" \
    --window-task-id "1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d5e6c"
```

Salida:

```
{
    "WindowTaskId":"1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d5e6c",
    "WindowId":"mw-ab12cd34ef56gh78"
}
```

Para obtener más información, consulte Tutoriales de Maintenance Windows de Systems Manager (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DeregisterTaskFromMaintenanceWindow en la Referencia de comandos de la AWS CLI.

`describe-activations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-activations`.

AWS CLI

Descripción de las activaciones

En el siguiente ejemplo de `describe-activations` se muestran detalles sobre las activaciones de su cuenta de AWS.

```
aws ssm describe-activations
```

Salida:

```
{
    "ActivationList": [
        {
            "ActivationId": "5743558d-563b-4457-8682-d16c3EXAMPLE",
            "Description": "Example1",
            "IamRole": "HybridWebServersRole,
            "RegistrationLimit": 5,
            "RegistrationsCount": 5,
            "ExpirationDate": 1584316800.0,
            "Expired": false,
            "CreatedDate": 1581954699.792
        },
        {
            "ActivationId": "3ee0322b-f62d-40eb-b672-13ebfEXAMPLE",
            "Description": "Example2",
            "IamRole": "HybridDatabaseServersRole",
            "RegistrationLimit": 5,
            "RegistrationsCount": 5,
            "ExpirationDate": 1580515200.0,
            "Expired": true,
            "CreatedDate": 1578064132.002
        },
    ]
}
```

Para obtener más información, consulte Paso 4: crear una activación híbrida para un entorno híbrido y multinube en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeActivations en la Referencia de comandos de la AWS CLI.

`describe-association-execution-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-association-execution-targets`.

AWS CLI

Obtención de detalles de la ejecución de una asociación

En el siguiente ejemplo de `describe-association-execution-targets` se describe la ejecución de la asociación especificada.

```
aws ssm describe-association-execution-targets \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab" \
    --execution-id "7abb6378-a4a5-4f10-8312-0123456789ab"
```

Salida:

```
{
    "AssociationExecutionTargets": [
        {
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "AssociationVersion": "1",
            "ExecutionId": "7abb6378-a4a5-4f10-8312-0123456789ab",
            "ResourceId": "i-1234567890abcdef0",
            "ResourceType": "ManagedInstance",
            "Status": "Success",
            "DetailedStatus": "Success",
            "LastExecutionDate": 1550505538.497,
            "OutputSource": {
                "OutputSourceId": "97fff367-fc5a-4299-aed8-0123456789ab",
                "OutputSourceType": "RunCommand"
            }
        }
    ]
}
```

Para obtener más información, consulte Visualización de los historiales de asociación en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeAssociationExecutionTargets en la Referencia de comandos de la AWS CLI.

`describe-association-executions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-association-executions`.

AWS CLI

Ejemplo 1: obtención de detalles de todas las ejecuciones de una asociación

En el siguiente ejemplo de `describe-association-executions` se describen todas las ejecuciones de la asociación especificada.

```
aws ssm describe-association-executions \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab"
```

Salida:

```
{
    "AssociationExecutions": [
        {
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "AssociationVersion": "1",
            "ExecutionId": "474925ef-1249-45a2-b93d-0123456789ab",
            "Status": "Success",
            "DetailedStatus": "Success",
            "CreatedTime": 1550505827.119,
            "ResourceCountByStatus": "{Success=1}"
        },
        {
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "AssociationVersion": "1",
            "ExecutionId": "7abb6378-a4a5-4f10-8312-0123456789ab",
            "Status": "Success",
            "DetailedStatus": "Success",
            "CreatedTime": 1550505536.843,
            "ResourceCountByStatus": "{Success=1}"
        },
```

```
        ...
    ]
}
```

Para obtener más información, consulte Visualización de los historiales de asociación en la Guía del usuario de AWS Systems Manager.

Ejemplo 2: obtención de detalles de todas las ejecuciones de una asociación después de una fecha y hora específicas

En el siguiente ejemplo de `describe-association-executions` se describen todas las ejecuciones de una asociación después de la fecha y hora especificadas.

```
aws ssm describe-association-executions \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab" \
    --filters "Key=CreatedTime,Value=2019-02-18T16:00:00Z,Type=GREATER_THAN"
```

Salida:

```
{
    "AssociationExecutions": [
        {
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "AssociationVersion": "1",
            "ExecutionId": "474925ef-1249-45a2-b93d-0123456789ab",
            "Status": "Success",
            "DetailedStatus": "Success",
            "CreatedTime": 1550505827.119,
            "ResourceCountByStatus": "{Success=1}"
        },
        {
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "AssociationVersion": "1",
            "ExecutionId": "7abb6378-a4a5-4f10-8312-0123456789ab",
            "Status": "Success",
            "DetailedStatus": "Success",
            "CreatedTime": 1550505536.843,
            "ResourceCountByStatus": "{Success=1}"
        },
        ...
    ]
}
```

Para obtener más información, consulte Visualización de los historiales de asociación en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeAssociationExecutions en la Referencia de comandos de la AWS CLI.

`describe-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-association`.

AWS CLI

Ejemplo 1: obtención de los detalles de una asociación

En el siguiente ejemplo de `describe-association` se describe la asociación del ID de asociación especificado.

```
aws ssm describe-association \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab"
```

Salida:

```
{
    "AssociationDescription": {
        "Name": "AWS-GatherSoftwareInventory",
        "AssociationVersion": "1",
        "Date": 1534864780.995,
        "LastUpdateAssociationDate": 1543235759.81,
        "Overview": {
            "Status": "Success",
            "AssociationStatusAggregatedCount": {
                "Success": 2
            }
        },
        "DocumentVersion": "$DEFAULT",
        "Parameters": {
            "applications": [
                "Enabled"
            ],
            "awsComponents": [
                "Enabled"
            ],
```

```
            "customInventory": [
                "Enabled"
            ],
            "files": [
                ""
            ],
            "instanceDetailedInformation": [
                "Enabled"
            ],
            "networkConfig": [
                "Enabled"
            ],
            "services": [
                "Enabled"
            ],
            "windowsRegistry": [
                ""
            ],
            "windowsRoles": [
                "Enabled"
            ],
            "windowsUpdates": [
                "Enabled"
            ]
        },
        "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
        "Targets": [
            {
                "Key": "InstanceIds",
                "Values": [
                    "*"
                ]
            }
        ],
        "ScheduleExpression": "rate(24 hours)",
        "LastExecutionDate": 1550501886.0,
        "LastSuccessfulExecutionDate": 1550501886.0,
        "AssociationName": "Inventory-Association"
    }
}
```

Para obtener más información, consulte Edición y creación de una nueva versión de una asociación en la Guía del usuario de AWS Systems Manager.

Ejemplo 2: obtención de los detalles de una asociación para una instancia y un documento específicos

En el siguiente ejemplo de `describe-association` se describe la asociación entre una instancia y un documento.

```
aws ssm describe-association \
    --instance-id "i-1234567890abcdef0" \
    --name "AWS-UpdateSSMAgent"
```

Salida:

```
{
    "AssociationDescription": {
        "Status": {
            "Date": 1487876122.564,
            "Message": "Associated with AWS-UpdateSSMAgent",
            "Name": "Associated"
        },
        "Name": "AWS-UpdateSSMAgent",
        "InstanceId": "i-1234567890abcdef0",
        "Overview": {
            "Status": "Pending",
            "DetailedStatus": "Associated",
            "AssociationStatusAggregatedCount": {
                "Pending": 1
            }
        },
        "AssociationId": "d8617c07-2079-4c18-9847-1234567890ab",
        "DocumentVersion": "$DEFAULT",
        "LastUpdateAssociationDate": 1487876122.564,
        "Date": 1487876122.564,
        "Targets": [
            {
                "Values": [
                    "i-1234567890abcdef0"
                ],
                "Key": "InstanceIds"
            }
        ]
    }
}
```

Para obtener más información, consulte Edición y creación de una nueva versión de una asociación en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeAssociation en la Referencia de comandos de la AWS CLI.

`describe-automation-executions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-automation-executions`.

AWS CLI

Descripción de una ejecución de automatización

En el siguiente ejemplo de `describe-automation-executions` se muestran detalles sobre una ejecución de Automatización.

```
aws ssm describe-automation-executions \
    --filters Key=ExecutionId,Values=73c8eef8-f4ee-4a05-820c-e354fEXAMPLE
```

Salida:

```
{
    "AutomationExecutionMetadataList": [
        {
            "AutomationExecutionId": "73c8eef8-f4ee-4a05-820c-e354fEXAMPLE",
            "DocumentName": "AWS-StartEC2Instance",
            "DocumentVersion": "1",
            "AutomationExecutionStatus": "Success",
            "ExecutionStartTime": 1583737233.748,
            "ExecutionEndTime": 1583737234.719,
            "ExecutedBy": "arn:aws:sts::29884EXAMPLE:assumed-role/mw_service_role/
OrchestrationService",
            "LogFile": "",
            "Outputs": {},
            "Mode": "Auto",
            "Targets": [],
            "ResolvedTargets": {
                "ParameterValues": [],
                "Truncated": false
            },
            "AutomationType": "Local"
        }
```

```
    ]
}
```

Para obtener más información, consulte Ejecución de una automatización sencilla en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeAutomationExecutions en la Referencia de comandos de la AWS CLI.

`describe-automation-step-executions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-automation-step-executions`.

AWS CLI

Ejemplo 1: descripción de todos los pasos de una ejecución de automatización

En el siguiente ejemplo de `describe-automation-step-executions` se muestran detalles sobre los pasos de una ejecución de Automatización.

```
aws ssm describe-automation-step-executions \
    --automation-execution-id 73c8eef8-f4ee-4a05-820c-e354fEXAMPLE
```

Salida:

```
{
    "StepExecutions": [
        {
            "StepName": "startInstances",
            "Action": "aws:changeInstanceState",
            "ExecutionStartTime": 1583737234.134,
            "ExecutionEndTime": 1583737234.672,
            "StepStatus": "Success",
            "Inputs": {
                "DesiredState": "\"running\"",
                "InstanceIds": "[\"i-0cb99161f6EXAMPLE\"]"
            },
            "Outputs": {
                "InstanceStates": [
                    "running"
                ]
```

```
            },
            "StepExecutionId": "95e70479-cf20-4d80-8018-7e4e2EXAMPLE",
            "OverriddenParameters": {}
        }
    ]
}
```

Ejemplo 2: descripción de un paso concreto de una ejecución de automatización

En el siguiente ejemplo de `describe-automation-step-executions` se muestran detalles sobre un paso específico de una ejecución de Automatización.

```
aws ssm describe-automation-step-executions \
    --automation-execution-id 73c8eef8-f4ee-4a05-820c-e354fEXAMPLE \
    --filters Key=StepExecutionId,Values=95e70479-cf20-4d80-8018-7e4e2EXAMPLE
```

Para obtener más información, consulte Running an Automation Workflow Step by Step (Command Line) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeAutomationStepExecutions en la Referencia de comandos de la AWS CLI.

`describe-available-patches`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-available-patches`.

AWS CLI

Obtención de las revisiones disponibles

En el siguiente ejemplo de `describe-available-patches` se obtienen detalles sobre todas las revisiones disponibles para Windows Server 2019 que tienen una gravedad de MSRC crítica.

```
aws ssm describe-available-patches \
    --
filters "Key=PRODUCT,Values=WindowsServer2019" "Key=MSRC_SEVERITY,Values=Critical"
```

Salida:

```
{
    "Patches": [
        {
```

```
            "Id": "fe6bd8c2-3752-4c8b-ab3e-1a7ed08767ba",
            "ReleaseDate": 1544047205.0,
            "Title": "2018-11 Update for Windows Server 2019 for x64-based Systems
 (KB4470788)",
            "Description": "Install this update to resolve issues in Windows. For a
 complete listing of the issues that are included in this update, see the associated
 Microsoft Knowledge Base article for more information. After you install this item,
 you may have to restart your computer.",
            "ContentUrl": "https://support.microsoft.com/en-us/kb/4470788",
            "Vendor": "Microsoft",
            "ProductFamily": "Windows",
            "Product": "WindowsServer2019",
            "Classification": "SecurityUpdates",
            "MsrcSeverity": "Critical",
            "KbNumber": "KB4470788",
            "MsrcNumber": "",
            "Language": "All"
        },
        {
            "Id": "c96115e1-5587-4115-b851-22baa46a3f11",
            "ReleaseDate": 1549994410.0,
            "Title": "2019-02 Security Update for Adobe Flash Player for Windows
 Server 2019 for x64-based Systems (KB4487038)",
            "Description": "A security issue has been identified in a Microsoft
 software product that could affect your system. You can help protect your system
 by installing this update from Microsoft. For a complete listing of the issues that
 are included in this update, see the associated Microsoft Knowledge Base article.
 After you install this update, you may have to restart your system.",
            "ContentUrl": "https://support.microsoft.com/en-us/kb/4487038",
            "Vendor": "Microsoft",
            "ProductFamily": "Windows",
            "Product": "WindowsServer2019",
            "Classification": "SecurityUpdates",
            "MsrcSeverity": "Critical",
            "KbNumber": "KB4487038",
            "MsrcNumber": "",
            "Language": "All"
        },
        ...
    ]
}
```

Obtención de detalles de una revisión específica

En el siguiente ejemplo de `describe-available-patches` se recuperan los detalles sobre la revisión especificada.

```
aws ssm describe-available-patches \
    --filters "Key=PATCH_ID,Values=KB4480979"
```

Salida:

```
{
    "Patches": [
        {
            "Id": "680861e3-fb75-432e-818e-d72e5f2be719",
            "ReleaseDate": 1546970408.0,
            "Title": "2019-01 Security Update for Adobe Flash Player for Windows
 Server 2016 for x64-based Systems (KB4480979)",
            "Description": "A security issue has been identified in a Microsoft
 software product that could affect your system. You can help protect your system
 by installing this update from Microsoft. For a complete listing of the issues that
 are included in this update, see the associated Microsoft Knowledge Base article.
 After you install this update, you may have to restart your system.",
            "ContentUrl": "https://support.microsoft.com/en-us/kb/4480979",
            "Vendor": "Microsoft",
            "ProductFamily": "Windows",
            "Product": "WindowsServer2016",
            "Classification": "SecurityUpdates",
            "MsrcSeverity": "Critical",
            "KbNumber": "KB4480979",
            "MsrcNumber": "",
            "Language": "All"
        }
    ]
}
```

Para obtener más información, consulte Cómo funcionan las operaciones de Patch Manager en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeAvailablePatches en la Referencia de comandos de la AWS CLI.

`describe-document-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-document-permission`.

AWS CLI

Descripción de los permisos de los documentos

En el siguiente ejemplo de `describe-document-permission` se muestran los detalles de los permisos sobre un documento de Systems Manager que se comparte públicamente.

```
aws ssm describe-document-permission \
    --name "Example" \
    --permission-type "Share"
```

Salida:

```
{
    "AccountIds": [
        "all"
    ],
    "AccountSharingInfoList": [
        {
            "AccountId": "all",
            "SharedDocumentVersion": "$DEFAULT"
        }
    ]
}
```

Para obtener más información, consulte Compartir un documento de Systems Manager en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeDocumentPermission en la Referencia de comandos de la AWS CLI.

`describe-document`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-document`.

AWS CLI

Visualización de los detalles de un documento

En el siguiente ejemplo de `describe-document` se muestran detalles sobre un documento de Systems Manager de su cuenta de AWS.

```
aws ssm describe-document \
    --name "Example"
```

Salida:

```
{
    "Document": {
        "Hash": "fc2410281f40779e694a8b95975d0f9f316da8a153daa94e3d9921102EXAMPLE",
        "HashType": "Sha256",
        "Name": "Example",
        "Owner": "29884EXAMPLE",
        "CreatedDate": 1583257938.266,
        "Status": "Active",
        "DocumentVersion": "1",
        "Description": "Document Example",
        "Parameters": [
            {
                "Name": "AutomationAssumeRole",
                "Type": "String",
                "Description": "(Required) The ARN of the role that allows
 Automation to perform the actions on your behalf. If no role is specified, Systems
 Manager Automation uses your IAM permissions to execute this document.",
                "DefaultValue": ""
            },
            {
                "Name": "InstanceId",
                "Type": "String",
                "Description": "(Required) The ID of the Amazon EC2 instance.",
                "DefaultValue": ""
            }
        ],
        "PlatformTypes": [
            "Windows",
            "Linux"
        ],
        "DocumentType": "Automation",
        "SchemaVersion": "0.3",
        "LatestVersion": "1",
        "DefaultVersion": "1",
        "DocumentFormat": "YAML",
        "Tags": []
    }
```

```
}
```

Para obtener más información, consulte Crear contenido en el documento de SSM en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeDocument en la Referencia de comandos de la AWS CLI.

`describe-effective-instance-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-effective-instance-associations`.

AWS CLI

Obtención de los detalles de las asociaciones efectivas de una instancia

En el siguiente ejemplo de `describe-effective-instance-associations` se recuperan los detalles sobre las asociaciones efectivas de una instancia.

Comando:

```
aws ssm describe-effective-instance-associations --instance-id "i-1234567890abcdef0"
```

Salida:

```
{
    "Associations": [
        {
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "InstanceId": "i-1234567890abcdef0",
            "Content": "{\n    \"schemaVersion\": \"1.2\",\n    \"description\":
 \"Update the Amazon SSM Agent to the latest version or specified version.\",\n
   \"parameters\": {\n        \"version\": {\n            \"default\": \"\",\n
         \"description\": \"(Optional) A specific version of the Amazon SSM Agent
 to install. If not specified, the agent will be updated to the latest version.\",
\n            \"type\": \"String\"\n        },\n        \"allowDowngrade\": {\n
            \"default\": \"false\",\n            \"description\": \"(Optional)
 Allow the Amazon SSM Agent service to be downgraded to an earlier version. If
 set to false, the service can be upgraded to newer versions only (default). If
 set to true, specify the earlier version.\",\n            \"type\": \"String\",
\n            \"allowedValues\": [\n                \"true\",\n
```

```
 \"false\"\n            ]\n        }\n    },\n    \"runtimeConfig\": {\n
 \"aws:updateSsmAgent\": {\n            \"properties\": [\n                {\n
              \"agentName\": \"amazon-ssm-agent\",\n                \"source\":
 \"https://s3.{Region}.amazonaws.com/amazon-ssm-{Region}/ssm-agent-manifest.json\",
\n                \"allowDowngrade\": \"{{ allowDowngrade }}\",\n
 \"targetVersion\": \"{{ version }}\"\n                }\n            ]\n        }\n
    }\n}\n",
            "AssociationVersion": "1"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeEffectiveInstanceAssociations en la Referencia de comandos de la AWS CLI.

`describe-effective-patches-for-patch-baseline`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-effective-patches-for-patch-baseline`.

AWS CLI

Ejemplo 1: obtención de todas las revisiones definidas por una línea de base de revisiones personalizada

En el siguiente ejemplo de `describe-effective-patches-for-patch-baseline` se devuelven las revisiones definidas por una línea de base de revisiones personalizada en la cuenta de AWS actual. Tenga en cuenta que, para una línea de base personalizada, solo se requiere el ID para `--baseline-id`.

```
aws ssm describe-effective-patches-for-patch-baseline \
    --baseline-id "pb-08b654cf9b9681f04"
```

Salida:

```
{
    "EffectivePatches": [
        {
            "Patch": {
                "Id": "fe6bd8c2-3752-4c8b-ab3e-1a7ed08767ba",
                "ReleaseDate": 1544047205.0,
```

```
                "Title": "2018-11 Update for Windows Server 2019 for x64-based
Systems (KB4470788)",
                "Description": "Install this update to resolve issues in Windows.
For a complete listing of the issues that are included in this update, see the
associated Microsoft Knowledge Base article for more information. After you install
this item, you may have to restart your computer.",
                "ContentUrl": "https://support.microsoft.com/en-us/kb/4470788",
                "Vendor": "Microsoft",
                "ProductFamily": "Windows",
                "Product": "WindowsServer2019",
                "Classification": "SecurityUpdates",
                "MsrcSeverity": "Critical",
                "KbNumber": "KB4470788",
                "MsrcNumber": "",
                "Language": "All"
            },
            "PatchStatus": {
                "DeploymentStatus": "APPROVED",
                "ComplianceLevel": "CRITICAL",
                "ApprovalDate": 1544047205.0
            }
        },
        {
            "Patch": {
                "Id": "915a6b1a-f556-4d83-8f50-b2e75a9a7e58",
                "ReleaseDate": 1549994400.0,
                "Title": "2019-02 Cumulative Update for .NET Framework 3.5 and 4.7.2
for Windows Server 2019 for x64 (KB4483452)",
                "Description": "A security issue has been identified in a Microsoft
software product that could affect your system. You can help protect your system by
installing this update from Microsoft. For a complete listing of the issues that
are included in this update, see the associated Microsoft Knowledge Base article.
After you install this update, you may have to restart your system.",
                "ContentUrl": "https://support.microsoft.com/en-us/kb/4483452",
                "Vendor": "Microsoft",
                "ProductFamily": "Windows",
                "Product": "WindowsServer2019",
                "Classification": "SecurityUpdates",
                "MsrcSeverity": "Important",
                "KbNumber": "KB4483452",
                "MsrcNumber": "",
                "Language": "All"
            },
            "PatchStatus": {
```

```
                "DeploymentStatus": "APPROVED",
                "ComplianceLevel": "CRITICAL",
                "ApprovalDate": 1549994400.0
            }
        },
        ...
    ],
    "NextToken": "--token string truncated--"
}
```

Ejemplo 2: obtención de todas las revisiones definidas por una línea de base de revisiones administrada de AWS

En el siguiente ejemplo de `describe-effective-patches-for-patch-baseline` se devuelven las revisiones definidas por una línea de base de revisiones administrada de AWS. Tenga en cuenta que, para una línea de base administrada de AWS, se requiere el ARN de la línea de base para `--baseline-id`.

```
aws ssm describe-effective-patches-for-patch-baseline \
    --baseline-id "arn:aws:ssm:us-east-2:733109147000:patchbaseline/
pb-020d361a05defe4ed"
```

Consulte el ejemplo 1 para ver una salida de muestra.

Para obtener más información, consulte Cómo se seleccionan las revisiones de seguridad en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeEffectivePatchesForPatchBaseline en la Referencia de comandos de la AWS CLI.

`describe-instance-associations-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-associations-status`.

AWS CLI

Descripción del estado de las asociaciones de una instancia

En este ejemplo se muestran los detalles de las asociaciones de una instancia.

Comando:

```
aws ssm describe-instance-associations-status --instance-id "i-1234567890abcdef0"
```

Salida:

```
{
  "InstanceAssociationStatusInfos": [
      {
          "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
          "Name": "AWS-GatherSoftwareInventory",
          "DocumentVersion": "1",
          "AssociationVersion": "1",
          "InstanceId": "i-1234567890abcdef0",
          "ExecutionDate": 1550501886.0,
          "Status": "Success",
          "ExecutionSummary": "1 out of 1 plugin processed, 1 success, 0 failed, 0
 timedout, 0 skipped. ",
          "AssociationName": "Inventory-Association"
      },
      {
          "AssociationId": "5c5a31f6-6dae-46f9-944c-0123456789ab",
          "Name": "AWS-UpdateSSMAgent",
          "DocumentVersion": "1",
          "AssociationVersion": "1",
          "InstanceId": "i-1234567890abcdef0",
          "ExecutionDate": 1550505828.548,
          "Status": "Success",
          "DetailedStatus": "Success",
          "AssociationName": "UpdateSSMAgent"
      }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeInstanceAssociationsStatus en la Referencia de comandos de la AWS CLI.

`describe-instance-information`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-information`.

AWS CLI

Ejemplo 1: descripción de la información de las instancias administradas

En el siguiente ejemplo de `describe-instance-information` se recuperan los detalles de cada una de las instancias administradas.

```
aws ssm describe-instance-information
```

Ejemplo 2: descripción de la información sobre una instancia administrada específica

En el siguiente ejemplo de `describe-instance-information` se muestran los detalles de la instancia administrada `i-028ea792daEXAMPLE`.

```
aws ssm describe-instance-information \
    --filters "Key=InstanceIds,Values=i-028ea792daEXAMPLE"
```

Ejemplo 3: descripción de la información sobre las instancias administradas con una clave de etiqueta específica

En el siguiente ejemplo de `describe-instance-information` se muestran los detalles de las instancias administradas que tienen la clave de etiqueta `DEV`.

```
aws ssm describe-instance-information \
    --filters "Key=tag-key,Values=DEV"
```

Salida:

```
{
    "InstanceInformationList": [
        {
            "InstanceId": "i-028ea792daEXAMPLE",
            "PingStatus": "Online",
            "LastPingDateTime": 1582221233.421,
            "AgentVersion": "2.3.842.0",
            "IsLatestVersion": true,
            "PlatformType": "Linux",
            "PlatformName": "SLES",
            "PlatformVersion": "15.1",
            "ResourceType": "EC2Instance",
            "IPAddress": "192.0.2.0",
            "ComputerName": "ip-198.51.100.0.us-east-2.compute.internal",
            "AssociationStatus": "Success",
            "LastAssociationExecutionDate": 1582220806.0,
            "LastSuccessfulAssociationExecutionDate": 1582220806.0,
```

```
            "AssociationOverview": {
                "DetailedStatus": "Success",
                "InstanceAssociationStatusAggregatedCount": {
                    "Success": 2
                }
            }
        }
    ]
}
```

Para obtener más información, consulte Managed Instances en la Guía del usuario de AWS.

- Para obtener información sobre la API, consulte DescribeInstanceInformation en la Referencia de comandos de la AWS CLI.

`describe-instance-patch-states-for-patch-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-patch-states-for-patch-group`.

AWS CLI

Ejemplo 1: obtención de los estados de las instancias de un grupo de revisiones

En el siguiente ejemplo de `describe-instance-patch-states-for-patch-group` se obtienen detalles sobre los estados resumidos de las revisiones por instancia en el grupo de revisiones especificado.

```
aws ssm describe-instance-patch-states-for-patch-group \
    --patch-group "Production"
```

Salida:

```
{
    "InstancePatchStates": [
        {
            "InstanceId": "i-02573cafcfEXAMPLE",
            "PatchGroup": "Production",
            "BaselineId": "pb-0c10e65780EXAMPLE",
            "SnapshotId": "a3f5ff34-9bc4-4d2c-a665-4d1c1EXAMPLE",
            "OwnerInformation": "",
```

```
            "InstalledCount": 32,
            "InstalledOtherCount": 1,
            "InstalledPendingRebootCount": 0,
            "InstalledRejectedCount": 0,
            "MissingCount": 2,
            "FailedCount": 0,
            "UnreportedNotApplicableCount": 2671,
            "NotApplicableCount": 400,
            "OperationStartTime": "2021-08-04T11:03:50.590000-07:00",
            "OperationEndTime": "2021-08-04T11:04:21.555000-07:00",
            "Operation": "Scan",
            "RebootOption": "NoReboot",
            "CriticalNonCompliantCount": 0,
            "SecurityNonCompliantCount": 1,
            "OtherNonCompliantCount": 0
        },
        {
            "InstanceId": "i-0471e04240EXAMPLE",
            "PatchGroup": "Production",
            "BaselineId": "pb-09ca3fb51fEXAMPLE",
            "SnapshotId": "05d8ffb0-1bbe-4812-ba2d-d9b7bEXAMPLE",
            "OwnerInformation": "",
            "InstalledCount": 32,
            "InstalledOtherCount": 1,
            "InstalledPendingRebootCount": 0,
            "InstalledRejectedCount": 0,
            "MissingCount": 2,
            "FailedCount": 0,
            "UnreportedNotApplicableCount": 2671,
            "NotApplicableCount": 400,
            "OperationStartTime": "2021-08-04T22:06:20.340000-07:00",
            "OperationEndTime": "2021-08-04T22:07:11.220000-07:00",
            "Operation": "Scan",
            "RebootOption": "NoReboot",
            "CriticalNonCompliantCount": 0,
            "SecurityNonCompliantCount": 1,
            "OtherNonCompliantCount": 0
        }
    ]
}
```

Ejemplo 2: obtención de los estados de las instancias de un grupo de revisiones al que le faltan más de cinco revisiones

En el siguiente ejemplo de `describe-instance-patch-states-for-patch-group` se obtienen detalles sobre los estados resumidos de las revisiones del grupo de revisiones especificado en las instancias a las que les faltan más de cinco revisiones.

```
aws ssm describe-instance-patch-states-for-patch-group \
    --filters Key=MissingCount,Type=GreaterThan,Values=5 \
    --patch-group "Production"
```

Salida:

```
{
    "InstancePatchStates": [
        {
            "InstanceId": "i-02573cafcfEXAMPLE",
            "PatchGroup": "Production",
            "BaselineId": "pb-0c10e65780EXAMPLE",
            "SnapshotId": "a3f5ff34-9bc4-4d2c-a665-4d1c1EXAMPLE",
            "OwnerInformation": "",
            "InstalledCount": 46,
            "InstalledOtherCount": 4,
            "InstalledPendingRebootCount": 1,
            "InstalledRejectedCount": 1,
            "MissingCount": 7,
            "FailedCount": 0,
            "UnreportedNotApplicableCount": 232,
            "NotApplicableCount": 654,
            "OperationStartTime": "2021-08-04T11:03:50.590000-07:00",
            "OperationEndTime": "2021-08-04T11:04:21.555000-07:00",
            "Operation": "Scan",
            "RebootOption": "NoReboot",
            "CriticalNonCompliantCount": 0,
            "SecurityNonCompliantCount": 1,
            "OtherNonCompliantCount": 1
        }
    ]
}
```

Ejemplo 3: obtención de los estados de las instancias de un grupo de revisiones con menos de diez instancias que requieren un reinicio

En el siguiente ejemplo de `describe-instance-patch-states-for-patch-group` se obtienen detalles sobre los estados resumidos de las revisiones del grupo de revisiones especificado en las instancias con menos de diez instancias que requieren un reinicio.

```
aws ssm describe-instance-patch-states-for-patch-group \
    --filters Key=InstalledPendingRebootCount,Type=LessThan,Values=10 \
    --patch-group "Production"
```

Salida:

```
{
    "InstancePatchStates": [
        {
            "InstanceId": "i-02573cafcfEXAMPLE",
            "BaselineId": "pb-0c10e65780EXAMPLE",
            "SnapshotId": "a3f5ff34-9bc4-4d2c-a665-4d1c1EXAMPLE",
            "PatchGroup": "Production",
            "OwnerInformation": "",
            "InstalledCount": 32,
            "InstalledOtherCount": 1,
            "InstalledPendingRebootCount": 4,
            "InstalledRejectedCount": 0,
            "MissingCount": 2,
            "FailedCount": 0,
            "UnreportedNotApplicableCount": 846,
            "NotApplicableCount": 212,
            "OperationStartTime": "2021-08-046T11:03:50.590000-07:00",
            "OperationEndTime": "2021-08-06T11:04:21.555000-07:00",
            "Operation": "Scan",
            "RebootOption": "NoReboot",
            "CriticalNonCompliantCount": 0,
            "SecurityNonCompliantCount": 1,
            "OtherNonCompliantCount": 0
        }
    ]
}
```

Para obtener más información, consulte Conocimiento de los valores del estado de conformidad de parches en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeInstancePatchStatesForPatchGroup en la Referencia de comandos de la AWS CLI.

describe-instance-patch-states

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-patch-states`.

AWS CLI

Obtención de los estados resumidos de las revisiones en instancias

En este ejemplo de `describe-instance-patch-states` se obtienen los estados resumidos de las revisiones en una instancia.

```
aws ssm describe-instance-patch-states \
    --instance-ids "i-1234567890abcdef0"
```

Salida:

```
{
    "InstancePatchStates": [
        {
            "InstanceId": "i-1234567890abcdef0",
            "PatchGroup": "my-patch-group",
            "BaselineId": "pb-0713accee01234567",
            "SnapshotId": "521c3536-930c-4aa9-950e-01234567abcd",
            "CriticalNonCompliantCount": 2,
            "SecurityNonCompliantCount": 2,
            "OtherNonCompliantCount": 1,
            "InstalledCount": 123,
            "InstalledOtherCount": 334,
            "InstalledPendingRebootCount": 0,
            "InstalledRejectedCount": 0,
            "MissingCount": 1,
            "FailedCount": 2,
            "UnreportedNotApplicableCount": 11,
            "NotApplicableCount": 2063,
            "OperationStartTime": "2021-05-03T11:00:56-07:00",
            "OperationEndTime": "2021-05-03T11:01:09-07:00",
            "Operation": "Scan",
            "LastNoRebootInstallOperationTime": "2020-06-14T12:17:41-07:00",
            "RebootOption": "RebootIfNeeded"
        }
    ]
}
```

Para obtener más información, consulte Conocimiento de los valores del estado de conformidad de parches en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeInstancePatchStates en la Referencia de comandos de la AWS CLI.

`describe-instance-patches`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-instance-patches`.

AWS CLI

Ejemplo 1: obtención de los detalles del estado de una revisión en una instancia

En el siguiente ejemplo de `describe-instance-patches` se recuperan los detalles sobre la instancia especificada.

```
aws ssm describe-instance-patches \
    --instance-id "i-1234567890abcdef0"
```

Salida:

```
{
    "Patches": [
        {
            "Title": "2019-01 Security Update for Adobe Flash Player for Windows
 Server 2016 for x64-based Systems (KB4480979)",
            "KBId": "KB4480979",
            "Classification": "SecurityUpdates",
            "Severity": "Critical",
            "State": "Installed",
            "InstalledTime": "2019-01-09T00:00:00+00:00"
        },
        {
            "Title": "",
            "KBId": "KB4481031",
            "Classification": "",
            "Severity": "",
            "State": "InstalledOther",
            "InstalledTime": "2019-02-08T00:00:00+00:00"
        },
        ...
```

```
    ],
    "NextToken": "--token string truncated--"
}
```

Ejemplo 2: obtención de una lista de las revisiones que se encuentran en el estado Faltante en una instancia

En el siguiente ejemplo de `describe-instance-patches` se recupera información sobre las revisiones que se encuentran en el estado Falta en la instancia especificada.

```
aws ssm describe-instance-patches \
    --instance-id "i-1234567890abcdef0" \
    --filters Key=State,Values=Missing
```

Salida:

```
{
    "Patches": [
        {
            "Title": "Windows Malicious Software Removal Tool x64 - February 2019
 (KB890830)",
            "KBId": "KB890830",
            "Classification": "UpdateRollups",
            "Severity": "Unspecified",
            "State": "Missing",
            "InstalledTime": "1970-01-01T00:00:00+00:00"
        },
        ...
    ],
    "NextToken": "--token string truncated--"
}
```

Para obtener más información, consulte Conocimiento de los valores del estado de conformidad de parches en la Guía del usuario de AWS Systems Manager.

Ejemplo 3: obtención de una lista de las revisiones instaladas desde un valor de InstalledTime específico en una instancia

En el siguiente ejemplo de `describe-instance-patches` se recupera información sobre las revisiones instaladas desde un tiempo específico en la instancia especificada combinando el uso de `--filters` y `--query`.

```
aws ssm describe-instance-patches \
    --instance-id "i-1234567890abcdef0" \
    --filters Key=State,Values=Installed \
    --query "Patches[?InstalledTime >= `2023-01-01T16:00:00`]"
```

Salida:

```
{
    "Patches": [
        {
            "Title": "2023-03 Cumulative Update for Windows Server 2019 (1809) for
 x64-based Systems (KB5023702)",
            "KBId": "KB5023702",
            "Classification": "SecurityUpdates",
            "Severity": "Critical",
            "State": "Installed",
            "InstalledTime": "2023-03-16T11:00:00+00:00"
        },
        ...
    ],
    "NextToken": "--token string truncated--"
}
```

- Para obtener información sobre la API, consulte DescribeInstancePatches en la Referencia de comandos de la AWS CLI.

`describe-inventory-deletions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-inventory-deletions`.

AWS CLI

Para obtener eliminaciones de inventario

En este ejemplo, se recuperan los detalles de las operaciones de eliminación de inventario.

Comando:

```
aws ssm describe-inventory-deletions
```

Salida:

```
{
  "InventoryDeletions": [
      {
          "DeletionId": "6961492a-8163-44ec-aa1e-01234567850",
          "TypeName": "Custom:RackInformation",
          "DeletionStartTime": 1550254911.0,
          "LastStatus": "InProgress",
          "LastStatusMessage": "The Delete is in progress",
          "DeletionSummary": {
              "TotalCount": 0,
              "RemainingCount": 0,
              "SummaryItems": []
          },
          "LastStatusUpdateTime": 1550254911.0
      },
      {
          "DeletionId": "d72ac9e8-1f60-4d40-b1c6-987654321c4d",
          "TypeName": "Custom:RackInfo",
          "DeletionStartTime": 1550254859.0,
          "LastStatus": "InProgress",
          "LastStatusMessage": "The Delete is in progress",
          "DeletionSummary": {
              "TotalCount": 1,
              "RemainingCount": 1,
              "SummaryItems": [
                  {
                      "Version": "1.0",
                      "Count": 1,
                      "RemainingCount": 1
                  }
              ]
          },
          "LastStatusUpdateTime": 1550254859.0
      }
  ]
}
```


Para obtener detalles de una eliminación de inventario específica

En este ejemplo, se obtienen los detalles de una operación de eliminación de inventario específica.

Comando:

```
aws ssm describe-inventory-deletions --deletion-id "d72ac9e8-1f60-4d40-
b1c6-987654321c4d"
```

Salida:

```
{
  "InventoryDeletions": [
      {
          "DeletionId": "d72ac9e8-1f60-4d40-b1c6-987654321c4d",
          "TypeName": "Custom:RackInfo",
          "DeletionStartTime": 1550254859.0,
          "LastStatus": "InProgress",
          "LastStatusMessage": "The Delete is in progress",
          "DeletionSummary": {
              "TotalCount": 1,
              "RemainingCount": 1,
              "SummaryItems": [
                  {
                      "Version": "1.0",
                      "Count": 1,
                      "RemainingCount": 1
                  }
              ]
          },
          "LastStatusUpdateTime": 1550254859.0
      }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeInventoryDeletions en la Referencia de comandos de la AWS CLI.

`describe-maintenance-window-execution-task-invocations`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-maintenance-window-execution-task-invocations`.

AWS CLI

Obtención de las invocaciones de tareas específicas hechas para la ejecución de una tarea en un periodo de mantenimiento

En el siguiente ejemplo de `describe-maintenance-window-execution-task-invocations` se muestran las invocaciones de la tarea especificada que se ejecutó como parte de la ejecución del periodo de mantenimiento especificado.

```
aws ssm describe-maintenance-window-execution-task-invocations \
    --window-execution-id "518d5565-5969-4cca-8f0e-da3b2a638355" \
    --task-id "ac0c6ae1-daa3-4a89-832e-d384503b6586"
```

Salida:

```
{
    "WindowExecutionTaskInvocationIdentities": [
        {
            "Status": "SUCCESS",
            "Parameters": "{\"documentName\":\"AWS-RunShellScript\",\"instanceIds\":
[\"i-0000293ffd8c57862\"],\"parameters\":{\"commands\":[\"df\"]},\"maxConcurrency\":
\"1\",\"maxErrors\":\"1\"}",
            "InvocationId": "e274b6e1-fe56-4e32-bd2a-8073c6381d8b",
            "StartTime": 1487692834.723,
            "EndTime": 1487692834.871,
            "WindowExecutionId": "518d5565-5969-4cca-8f0e-da3b2a638355",
            "TaskExecutionId": "ac0c6ae1-daa3-4a89-832e-d384503b6586"
        }
    ]
}
```

Para obtener más información, consulte Ver información sobre tareas y ejecuciones de tareas (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeMaintenanceWindowExecutionTaskInvocations en la Referencia de comandos de la AWS CLI.

`describe-maintenance-window-execution-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-maintenance-window-execution-tasks`.

AWS CLI

Enumeración de todas las tareas asociadas a la ejecución de un periodo de mantenimiento

En el siguiente ejemplo de `ssm describe-maintenance-window-execution-tasks` se enumeran todas las tareas asociadas a la ejecución del periodo de mantenimiento especificado.

```
aws ssm describe-maintenance-window-execution-tasks \
    --window-execution-id "518d5565-5969-4cca-8f0e-da3b2EXAMPLE"
```

Salida:

```
{
    "WindowExecutionTaskIdentities": [
        {
            "Status": "SUCCESS",
            "TaskArn": "AWS-RunShellScript",
            "StartTime": 1487692834.684,
            "TaskType": "RUN_COMMAND",
            "EndTime": 1487692835.005,
            "WindowExecutionId": "518d5565-5969-4cca-8f0e-da3b2EXAMPLE",
            "TaskExecutionId": "ac0c6ae1-daa3-4a89-832e-d3845EXAMPLE"
        }
    ]
}
```

Para obtener más información, consulte Ver información sobre tareas y ejecuciones de tareas (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeMaintenanceWindowExecutionTasks en la Referencia de comandos de la AWS CLI.

`describe-maintenance-window-executions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-maintenance-window-executions`.

AWS CLI

Ejemplo 1: enumeración de todas las ejecuciones de un periodo de mantenimiento

En el siguiente ejemplo de `describe-maintenance-window-executions` se enumeran todas las ejecuciones del periodo de mantenimiento especificado.

```
aws ssm describe-maintenance-window-executions \
```

```
    --window-id "mw-ab12cd34eEXAMPLE"
```

Salida:

```
{
    "WindowExecutions": [
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "WindowExecutionId": "6027b513-64fe-4cf0-be7d-1191aEXAMPLE",
            "Status": "IN_PROGRESS",
            "StartTime": "2021-08-04T11:00:00.000000-07:00"

        },
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "WindowExecutionId": "ff75b750-4834-4377-8f61-b3cadEXAMPLE",
            "Status": "SUCCESS",
            "StartTime": "2021-08-03T11:00:00.000000-07:00",
            "EndTime": "2021-08-03T11:37:21.450000-07:00"
        },
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "WindowExecutionId": "9fac7dd9-ff21-42a5-96ad-bbc4bEXAMPLE",
            "Status": "FAILED",
            "StatusDetails": "One or more tasks in the orchestration failed.",
            "StartTime": "2021-08-02T11:00:00.000000-07:00",
            "EndTime": "2021-08-02T11:22:36.190000-07:00"
        }
    ]
}
```

Ejemplo 2: enumeración de todas las ejecuciones de un periodo de mantenimiento antes de una fecha especificada

En el siguiente ejemplo de `describe-maintenance-window-executions` se enumeran todas las ejecuciones del periodo de mantenimiento especificado antes de la fecha especificada.

```
aws ssm describe-maintenance-window-executions \
    --window-id "mw-ab12cd34eEXAMPLE" \
    --filters "Key=ExecutedBefore,Values=2021-08-03T00:00:00Z"
```

Salida:

```
{
    "WindowExecutions": [
        {
        "WindowId": "mw-ab12cd34eEXAMPLE",
        "WindowExecutionId": "9fac7dd9-ff21-42a5-96ad-bbc4bEXAMPLE",
        "Status": "FAILED",
        "StatusDetails": "One or more tasks in the orchestration failed.",
        "StartTime": "2021-08-02T11:00:00.000000-07:00",
        "EndTime": "2021-08-02T11:22:36.190000-07:00"
    }
    ]
}
```

Ejemplo 3: enumeración de todas las ejecuciones de un periodo de mantenimiento después de una fecha especificada

En el siguiente ejemplo de `describe-maintenance-window-executions` se enumeran todas las ejecuciones del periodo de mantenimiento especificado después de la fecha especificada.

```
aws ssm describe-maintenance-window-executions \
    --window-id "mw-ab12cd34eEXAMPLE" \
    --filters "Key=ExecutedAfter,Values=2021-08-04T00:00:00Z"
```

Salida:

```
{
    "WindowExecutions": [
        {
        "WindowId": "mw-ab12cd34eEXAMPLE",
        "WindowExecutionId": "6027b513-64fe-4cf0-be7d-1191aEXAMPLE",
        "Status": "IN_PROGRESS",
        "StartTime": "2021-08-04T11:00:00.000000-07:00"
        }
    ]
}
```

Para obtener más información, consulte Ver información sobre tareas y ejecuciones de tareas (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeMaintenanceWindowExecutions en la Referencia de comandos de la AWS CLI.

describe-maintenance-window-schedule

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-maintenance-window-schedule`.

AWS CLI

Ejemplo 1: enumeración de todas las próximas ejecuciones de un período de mantenimiento

En el siguiente ejemplo de `describe-maintenance-window-schedule`, se enumeran las próximas ejecuciones del período de mantenimiento especificado.

```
aws ssm describe-maintenance-window-schedule \
    --window-id mw-ab12cd34eEXAMPLE
```

Salida:

```
{
    "ScheduledWindowExecutions": [
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "Name": "My-First-Maintenance-Window",
            "ExecutionTime": "2020-02-19T16:00Z"
        },
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "Name": "My-First-Maintenance-Window",
            "ExecutionTime": "2020-02-26T16:00Z"
        },
        ...
    ]
}
```

Ejemplo 2: enumeración de todas las próximas ejecuciones de un período de mantenimiento antes de una fecha determinada

En el siguiente ejemplo de `describe-maintenance-window-schedule`, se enumeran las próximas ejecuciones del período de mantenimiento especificado que se van a producir antes de la fecha especificada.

```
aws ssm describe-maintenance-window-schedule \
    --window-id mw-0ecb1226dd7b2e9a6 \
```

```
    --filters "Key=ScheduledBefore,Values=2020-02-15T06:00:00Z"
```

Ejemplo 3: enumeración de todas las próximas ejecuciones de un período de mantenimiento después de una fecha determinada

En el siguiente ejemplo de `describe-maintenance-window-schedule`, se enumeran las próximas ejecuciones del período de mantenimiento especificado que se van a producir después de la fecha especificada.

```
aws ssm describe-maintenance-window-schedule \
    --window-id mw-0ecb1226dd7b2e9a6 \
    --filters "Key=ScheduledAfter,Values=2020-02-15T06:00:00Z"
```

Para obtener más información, consulte Ver información sobre períodos de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeMaintenanceWindowSchedule en la Referencia de comandos de la AWS CLI.

`describe-maintenance-window-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-maintenance-window-targets`.

AWS CLI

Ejemplo 1: enumeración de todos los destinos de un periodo de mantenimiento

En el siguiente ejemplo de `describe-maintenance-window-targets` se enumeran todos los destinos de un periodo de mantenimiento.

```
aws ssm describe-maintenance-window-targets \
    --window-id "mw-06cf17cbefEXAMPLE"
```

Salida:

```
{
    "Targets": [
        {
            "ResourceType": "INSTANCE",
            "OwnerInformation": "Single instance",
```

```
            "WindowId": "mw-06cf17cbefEXAMPLE",
            "Targets": [
                {
                    "Values": [
                        "i-0000293ffdEXAMPLE"
                    ],
                    "Key": "InstanceIds"
                }
            ],
            "WindowTargetId": "350d44e6-28cc-44e2-951f-4b2c9EXAMPLE"
        },
        {
            "ResourceType": "INSTANCE",
            "OwnerInformation": "Two instances in a list",
            "WindowId": "mw-06cf17cbefEXAMPLE",
            "Targets": [
                {
                    "Values": [
                        "i-0000293ffdEXAMPLE",
                        "i-0cb2b964d3EXAMPLE"
                    ],
                    "Key": "InstanceIds"
                }
            ],
            "WindowTargetId": "e078a987-2866-47be-bedd-d9cf4EXAMPLE"
        }
    ]
}
```

Ejemplo 2: enumeración de todos los destinos de un periodo de mantenimiento que coincida con un valor específico de información del propietario

En este ejemplo de `describe-maintenance-window-targets` se enumeran todos los destinos de un periodo de mantenimiento con un valor específico.

```
aws ssm describe-maintenance-window-targets \
    --window-id "mw-0ecb1226ddEXAMPLE" \
    --filters "Key=OwnerInformation,Values=CostCenter1"
```

Salida:

```
{
    "Targets": [
```

```
        {
            "WindowId": "mw-0ecb1226ddEXAMPLE",
            "WindowTargetId": "da89dcc3-7f9c-481d-ba2b-edcb7d0057f9",
            "ResourceType": "INSTANCE",
            "Targets": [
                {
                    "Key": "tag:Environment",
                    "Values": [
                        "Prod"
                    ]
                }
            ],
            "OwnerInformation": "CostCenter1",
            "Name": "ProdTarget1"
        }
    ]
}
```

Para obtener más información, consulte Ver información sobre períodos de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeMaintenanceWindowTargets en la Referencia de comandos de la AWS CLI.

`describe-maintenance-window-tasks`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-maintenance-window-tasks`.

AWS CLI

Ejemplo 1: enumeración de todas las tareas de un periodo de mantenimiento

En el siguiente ejemplo de `describe-maintenance-window-tasks` se enumeran todas las tareas del periodo de mantenimiento especificado.

```
aws ssm describe-maintenance-window-tasks \
    --window-id "mw-06cf17cbefEXAMPLE"
```

Salida:

```
{
```

```
    "Tasks": [
        {
            "WindowId": "mw-06cf17cbefEXAMPLE",
            "WindowTaskId": "018b31c3-2d77-4b9e-bd48-c91edEXAMPLE",
            "TaskArn": "AWS-RestartEC2Instance",
            "TaskParameters": {},
            "Type": "AUTOMATION",
            "Description": "Restarting EC2 Instance for maintenance",
            "MaxConcurrency": "1",
            "MaxErrors": "1",
            "Name": "My-Automation-Example-Task",
            "Priority": 0,
            "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "Targets": [
                {
                    "Key": "WindowTargetIds",
                    "Values": [
                        "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
                    ]
                }
            ]
        },
        {
            "WindowId": "mw-06cf17cbefEXAMPLE",
            "WindowTaskId": "1943dee0-0a17-4978-9bf4-3cc2fEXAMPLE",
            "TaskArn": "AWS-DisableS3BucketPublicReadWrite",
            "TaskParameters": {},
            "Type": "AUTOMATION",
            "Description": "Automation task to disable read/write access on public
 S3 buckets",
            "MaxConcurrency": "10",
            "MaxErrors": "5",
            "Name": "My-Disable-S3-Public-Read-Write-Access-Automation-Task",
            "Priority": 0,
            "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "Targets": [
                {
                    "Key": "WindowTargetIds",
                    "Values": [
                        "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
                    ]
                }
```

```
            ]
        }
    ]
}
```

Ejemplo 2: enumeración de todas las tareas de un periodo de mantenimiento que invoca el documento de comandos AWS-RunPowerShellScript

En el siguiente ejemplo de `describe-maintenance-window-tasks` se enumeran todas las tareas del periodo de mantenimiento especificado que invoca el documento de comandos `AWS-RunPowerShellScript`.

```
aws ssm describe-maintenance-window-tasks \
    --window-id "mw-ab12cd34eEXAMPLE" \
    --filters "Key=TaskArn,Values=AWS-RunPowerShellScript"
```

Salida:

```
{
    "Tasks": [
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "WindowTaskId": "0d36e6b4-3a4f-411e-adcb-3558eEXAMPLE",
            "TaskArn": "AWS-RunPowerShellScript",
            "Type": "RUN_COMMAND",
            "Targets": [
                {
                    "Key": "WindowTargetIds",
                    "Values": [
                        "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
                    ]
                }
            ],
            "TaskParameters": {},
            "Priority": 1,
            "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "MaxConcurrency": "1",
            "MaxErrors": "1",
            "Name": "MyTask"
        }
    ]
```

```
}
```

Ejemplo 3: enumeración de todas las tareas de un periodo de mantenimiento que tienen una prioridad de 3

En el siguiente ejemplo de `describe-maintenance-window-tasks` se enumeran todas las tareas del periodo de mantenimiento especificado que tienen una `Priority` de 3.

```
aws ssm describe-maintenance-window-tasks \
    --window-id "mw-ab12cd34eEXAMPLE" \
    --filters "Key=Priority,Values=3"
```

Salida:

```
{
    "Tasks": [
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "WindowTaskId": "0d36e6b4-3a4f-411e-adcb-3558eEXAMPLE",
            "TaskArn": "AWS-RunPowerShellScript",
            "Type": "RUN_COMMAND",
            "Targets": [
                {
                    "Key": "WindowTargetIds",
                    "Values": [
                        "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
                    ]
                }
            ],
            "TaskParameters": {},
            "Priority": 3,
            "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "MaxConcurrency": "1",
            "MaxErrors": "1",
            "Name": "MyRunCommandTask"
        },
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "WindowTaskId": "ee45feff-ad65-4a6c-b478-5cab8EXAMPLE",
            "TaskArn": "AWS-RestartEC2Instance",
            "Type": "AUTOMATION",
```

```
            "Targets": [
                {
                    "Key": "WindowTargetIds",
                    "Values": [
                        "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
                    ]
                }
            ],
            "TaskParameters": {},
            "Priority": 3,
            "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "MaxConcurrency": "10",
            "MaxErrors": "5",
            "Name": "My-Automation-Task",
            "Description": "A description for my Automation task"
        }
    ]
}
```

Ejemplo 4: enumeración de todas las tareas de un periodo de mantenimiento que tienen una prioridad de 1 y uso del comando de ejecución

En este ejemplo de `describe-maintenance-window-tasks` se enumeran todas las tareas del periodo de mantenimiento especificado que tienen una `Priority` de 1 y el uso del `Run Command`.

```
aws ssm describe-maintenance-window-tasks \
    --window-id "mw-ab12cd34eEXAMPLE" \
    --filters "Key=Priority,Values=1" "Key=TaskType,Values=RUN_COMMAND"
```

Salida:

```
{
    "Tasks": [
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "WindowTaskId": "0d36e6b4-3a4f-411e-adcb-3558eEXAMPLE",
            "TaskArn": "AWS-RunPowerShellScript",
            "Type": "RUN_COMMAND",
            "Targets": [
                {
```

```
                    "Key": "WindowTargetIds",
                    "Values": [
                        "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
                    ]
                }
            ],
            "TaskParameters": {},
            "Priority": 1,
            "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "MaxConcurrency": "1",
            "MaxErrors": "1",
            "Name": "MyRunCommandTask"
        }
    ]
}
```

Para obtener más información, consulte Ver información sobre períodos de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeMaintenanceWindowTasks en la Referencia de comandos de la AWS CLI.

`describe-maintenance-windows-for-target`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-maintenance-windows-for-target`.

AWS CLI

Para enumerar todos los períodos de mantenimiento asociados a una instancia específica

En el siguiente ejemplo de `describe-maintenance-windows-for-target`, se enumeran los períodos de mantenimiento con destinos o tareas asociados a la instancia especificada.

```
aws ssm describe-maintenance-windows-for-target \
    --targets Key=InstanceIds,Values=i-1234567890EXAMPLE \
    --resource-type INSTANCE
```

Salida:

```
{
```

```
    "WindowIdentities": [
        {
            "WindowId": "mw-0c5ed765acEXAMPLE",
            "Name": "My-First-Maintenance-Window"
        }
    ]
}
```

Para obtener más información, consulte Ver información sobre períodos de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeMaintenanceWindowsForTarget en la Referencia de comandos de la AWS CLI.

`describe-maintenance-windows`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-maintenance-windows`.

AWS CLI

Ejemplo 1: enumeración de todos los periodos de mantenimiento

En el siguiente ejemplo de `describe-maintenance-windows` se enumeran todos los periodos de mantenimiento de su cuenta de AWS en la región actual.

```
aws ssm describe-maintenance-windows
```

Salida:

```
{
    "WindowIdentities": [
        {
            "WindowId": "mw-0ecb1226ddEXAMPLE",
            "Name": "MyMaintenanceWindow-1",
            "Enabled": true,
            "Duration": 2,
            "Cutoff": 1,
            "Schedule": "rate(180 minutes)",
            "NextExecutionTime": "2020-02-12T23:19:20.596Z"
        },
        {
            "WindowId": "mw-03eb9db428EXAMPLE",
```

```
            "Name": "MyMaintenanceWindow-2",
            "Enabled": true,
            "Duration": 3,
            "Cutoff": 1,
            "Schedule": "rate(7 days)",
            "NextExecutionTime": "2020-02-17T23:22:00.956Z"
        },
    ]
}
```

Ejemplo 2: enumeración de todos los periodos de mantenimiento habilitados

En el siguiente ejemplo de `describe-maintenance-windows` se enumeran todos los periodos de mantenimiento habilitados.

```
aws ssm describe-maintenance-windows \
    --filters "Key=Enabled,Values=true"
```

Ejemplo 3: enumeración de los periodos de mantenimiento que coincidan con un nombre específico

En este ejemplo de `describe-maintenance-windows` se enumeran todos los periodos de mantenimiento con el nombre especificado.

```
aws ssm describe-maintenance-windows \
    --filters "Key=Name,Values=MyMaintenanceWindow"
```

Para obtener más información, consulte Ver información sobre períodos de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeMaintenanceWindows en la Referencia de comandos de la AWS CLI.

`describe-ops-items`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-ops-items`.

AWS CLI

Visualización de un conjunto de OpsItems

En el siguiente ejemplo de `describe-ops-items` se muestra una lista de todos los OpsItems abiertos en su cuenta de AWS.

```
aws ssm describe-ops-items \
    --ops-item-filters "Key=Status,Values=Open,Operator=Equal"
```

Salida:

```
{
    "OpsItemSummaries": [
        {
            "CreatedBy": "arn:aws:sts::111222333444:assumed-role/OpsItem-CWE-Role/
fbf77cbe264a33509569f23e4EXAMPLE",
            "CreatedTime": "2020-03-14T17:02:46.375000-07:00",
            "LastModifiedBy": "arn:aws:sts::111222333444:assumed-role/OpsItem-CWE-
Role/fbf77cbe264a33509569f23e4EXAMPLE",
            "LastModifiedTime": "2020-03-14T17:02:46.375000-07:00",
            "Source": "SSM",
            "Status": "Open",
            "OpsItemId": "oi-7cfc5EXAMPLE",
            "Title": "SSM Maintenance Window execution failed",
            "OperationalData": {
                "/aws/dedup": {
                    "Value": "{\"dedupString\":\"SSMOpsItems-SSM-maintenance-window-
execution-failed\"}",
                    "Type": "SearchableString"
                },
                "/aws/resources": {
                    "Value": "[{\"arn\":\"arn:aws:ssm:us-
east-2:111222333444:maintenancewindow/mw-034093d322EXAMPLE\"}]",
                    "Type": "SearchableString"
                }
            },
            "Category": "Availability",
            "Severity": "3"
        },
        {
            "CreatedBy": "arn:aws:sts::1112223233444:assumed-role/OpsItem-CWE-Role/
fbf77cbe264a33509569f23e4EXAMPLE",
            "CreatedTime": "2020-02-26T11:43:15.426000-08:00",
            "LastModifiedBy": "arn:aws:sts::111222333444:assumed-role/OpsItem-CWE-
Role/fbf77cbe264a33509569f23e4EXAMPLE",
            "LastModifiedTime": "2020-02-26T11:43:15.426000-08:00",
```

```
            "Source": "EC2",
            "Status": "Open",
            "OpsItemId": "oi-6f966EXAMPLE",
            "Title": "EC2 instance stopped",
            "OperationalData": {
                "/aws/automations": {
                    "Value": "[ { \"automationType\": \"AWS:SSM:Automation\",
 \"automationId\": \"AWS-RestartEC2Instance\" } ]",
                    "Type": "SearchableString"
                },
                "/aws/dedup": {
                    "Value": "{\"dedupString\":\"SSMOpsItems-EC2-instance-stopped
\"}",
                    "Type": "SearchableString"
                },
                "/aws/resources": {
                    "Value": "[{\"arn\":\"arn:aws:ec2:us-
east-2:111222333444:instance/i-0beccfbc02EXAMPLE\"}]",
                    "Type": "SearchableString"
                }
            },
            "Category": "Availability",
            "Severity": "3"
        }
    ]
}
```

Para obtener más información, consulte Trabajo con OpsItems en la AWSGuía del usuario de Systems Manager.

- Para obtener información sobre la API, consulte DescribeOpsItems en la Referencia de comandos de la AWS CLI.

`describe-parameters`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-parameters`.

AWS CLI

Ejemplo 1: Creación de una lista de todos los parámetros

En el siguiente ejemplo de `describe-parameters` se enumeran todos los parámetros de la cuenta y la región de AWS actuales.

```
aws ssm describe-parameters
```

Salida:

```
{
    "Parameters": [
        {
            "Name": "MySecureStringParameter",
            "Type": "SecureString",
            "KeyId": "alias/aws/ssm",
            "LastModifiedDate": 1582155479.205,
            "LastModifiedUser": "arn:aws:sts::111222333444:assumed-role/Admin/
Richard-Roe-Managed",
            "Description": "This is a SecureString parameter",
            "Version": 2,
            "Tier": "Advanced",
            "Policies": [
                {
                    "PolicyText": "{\"Type\":\"Expiration\",\"Version\":\"1.0\",
\"Attributes\":{\"Timestamp\":\"2020-07-07T22:30:00Z\"}}",
                    "PolicyType": "Expiration",
                    "PolicyStatus": "Pending"
                },
                {
                    "PolicyText": "{\"Type\":\"ExpirationNotification\",\"Version\":
\"1.0\",\"Attributes\":{\"Before\":\"12\",\"Unit\":\"Hours\"}}",
                    "PolicyType": "ExpirationNotification",
                    "PolicyStatus": "Pending"
                }
            ]
        },
        {
            "Name": "MyStringListParameter",
            "Type": "StringList",
            "LastModifiedDate": 1582154764.222,
            "LastModifiedUser": "arn:aws:iam::111222333444:user/Mary-Major",
            "Description": "This is a StringList parameter",
            "Version": 1,
            "Tier": "Standard",
            "Policies": []
        },
        {
            "Name": "MyStringParameter",
```

```
            "Type": "String",
            "LastModifiedDate": 1582154711.976,
            "LastModifiedUser": "arn:aws:iam::111222333444:user/Alejandro-Rosalez",
            "Description": "This is a String parameter",
            "Version": 1,
            "Tier": "Standard",
            "Policies": []
        },
        {
            "Name": "latestAmi",
            "Type": "String",
            "LastModifiedDate": 1580862415.521,
            "LastModifiedUser": "arn:aws:sts::111222333444:assumed-role/lambda-ssm-
role/Automation-UpdateSSM-Param",
            "Version": 3,
            "Tier": "Standard",
            "Policies": []
        }
    ]
}
```

Ejemplo 2: Creación de una lista de todos los parámetros que coinciden con metadatos específicos

En este ejemplo de `describe-parameters` se enumeran todos los parámetros que coinciden con un filtro.

aws ssm describe-parameters --filters "Key=Type,Values=StringList"

Salida:

```
{
    "Parameters": [
        {
            "Name": "MyStringListParameter",
            "Type": "StringList",
            "LastModifiedDate": 1582154764.222,
            "LastModifiedUser": "arn:aws:iam::111222333444:user/Mary-Major",
            "Description": "This is a StringList parameter",
            "Version": 1,
            "Tier": "Standard",
            "Policies": []
        }
```

```
    ]
}
```

Para obtener más información, consulte Búsqueda de parámetros de Systems Manager en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeParameters en la Referencia de comandos de la AWS CLI.

`describe-patch-baselines`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-patch-baselines`.

AWS CLI

Ejemplo 1: enumeración de todas las líneas de base de revisiones

En el siguiente ejemplo de `describe-patch-baselines` se recuperan los detalles de todas las líneas de base de revisiones de su cuenta en la región actual.

```
aws ssm describe-patch-baselines
```

Salida:

```
{
    "BaselineIdentities": [
        {
            "BaselineName": "AWS-SuseDefaultPatchBaseline",
            "DefaultBaseline": true,
            "BaselineDescription": "Default Patch Baseline for Suse Provided by
 AWS.",
            "BaselineId": "arn:aws:ssm:us-east-2:733109147000:patchbaseline/
pb-0123fdb36e334a3b2",
            "OperatingSystem": "SUSE"
        },
        {
            "BaselineName": "AWS-DefaultPatchBaseline",
            "DefaultBaseline": false,
            "BaselineDescription": "Default Patch Baseline Provided by AWS.",
            "BaselineId": "arn:aws:ssm:us-east-2:733109147000:patchbaseline/
pb-020d361a05defe4ed",
            "OperatingSystem": "WINDOWS"
```

```
        },
        ...
        {
            "BaselineName": "MyWindowsPatchBaseline",
            "DefaultBaseline": true,
            "BaselineDescription": "My patch baseline for EC2 instances for Windows
 Server",
            "BaselineId": "pb-0ad00e0dd7EXAMPLE",
            "OperatingSystem": "WINDOWS"
        }
    ]
}
```

Ejemplo 2: enumeración de todas las líneas de base de revisiones proporcionadas por AWS

En el siguiente ejemplo de `describe-patch-baselines` se enumeran todas las líneas de base de revisiones proporcionadas por AWS.

```
aws ssm describe-patch-baselines \
    --filters "Key=OWNER,Values=[AWS]"
```

Ejemplo 3: enumeración de todas las líneas de base de revisiones de su propiedad

En el siguiente ejemplo de `describe-patch-baselines` se enumeran todas las líneas de base de revisiones personalizadas creadas en su cuenta en la región actual.

```
aws ssm describe-patch-baselines \
    --filters "Key=OWNER,Values=[Self]"
```

Para obtener más información, consulte Acerca de las líneas de base de revisiones personalizadas y predefinidas en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribePatchBaselines en la Referencia de comandos de la AWS CLI.

`describe-patch-group-state`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-patch-group-state`.

AWS CLI

Obtención del estado de un grupo de revisiones

En el siguiente ejemplo de `describe-patch-group-state` se recupera el resumen general de conformidad de las revisiones de un grupo de revisiones.

```
aws ssm describe-patch-group-state \
    --patch-group "Production"
```

Salida:

```
{
    "Instances": 21,
    "InstancesWithCriticalNonCompliantPatches": 1,
    "InstancesWithFailedPatches": 2,
    "InstancesWithInstalledOtherPatches": 3,
    "InstancesWithInstalledPatches": 21,
    "InstancesWithInstalledPendingRebootPatches": 2,
    "InstancesWithInstalledRejectedPatches": 1,
    "InstancesWithMissingPatches": 3,
    "InstancesWithNotApplicablePatches": 4,
    "InstancesWithOtherNonCompliantPatches": 1,
    "InstancesWithSecurityNonCompliantPatches": 1,
    "InstancesWithUnreportedNotApplicablePatches": 2
}
```

Para obtener más información, consulte Acerca de los grupos de revisiones <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-patchgroups.html>__ y Conocimiento de los valores del estado de conformidad de parches en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribePatchGroupState en la Referencia de comandos de la AWS CLI.

`describe-patch-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-patch-groups`.

AWS CLI

Visualización de los registros de grupos de revisiones

En el siguiente ejemplo de `describe-patch-groups` se enumeran los registros de los grupos de revisiones.

```
aws ssm describe-patch-groups
```

Salida:

```
{
    "Mappings": [
        {
            "PatchGroup": "Production",
            "BaselineIdentity": {
                "BaselineId": "pb-0123456789abcdef0",
                "BaselineName": "ProdPatching",
                "OperatingSystem": "WINDOWS",
                "BaselineDescription": "Patches for Production",
                "DefaultBaseline": false
            }
        },
        {
            "PatchGroup": "Development",
            "BaselineIdentity": {
                "BaselineId": "pb-0713accee01234567",
                "BaselineName": "DevPatching",
                "OperatingSystem": "WINDOWS",
                "BaselineDescription": "Patches for Development",
                "DefaultBaseline": true
            }
        },
        ...
    ]
}
```

Para obtener más información, consulte Creación de un grupo de revisiones <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-group-tagging.html>__ y Añadir un grupo de revisiones a una línea de base de revisiones en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribePatchGroups en la Referencia de comandos de la AWS CLI.

`describe-patch-properties`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-patch-properties`.

AWS CLI

Para enumerar la disponibilidad de parches de Amazon Linux

En el siguiente ejemplo de `describe-patch-properties`, se muestra una lista de los productos de Amazon Linux para los que hay parches disponibles en su cuenta de AWS.

```
aws ssm describe-patch-properties \
    --operating-system AMAZON_LINUX \
    --property PRODUCT
```

Salida:

```
{
    "Properties": [
        {
            "Name": "AmazonLinux2012.03"
        },
        {
            "Name": "AmazonLinux2012.09"
        },
        {
            "Name": "AmazonLinux2013.03"
        },
        {
            "Name": "AmazonLinux2013.09"
        },
        {
            "Name": "AmazonLinux2014.03"
        },
        {
            "Name": "AmazonLinux2014.09"
        },
        {
            "Name": "AmazonLinux2015.03"
        },
        {
            "Name": "AmazonLinux2015.09"
        },
        {
            "Name": "AmazonLinux2016.03"
        },
        {
```

```
            "Name": "AmazonLinux2016.09"
        },
        {
            "Name": "AmazonLinux2017.03"
        },
        {
            "Name": "AmazonLinux2017.09"
        },
        {
            "Name": "AmazonLinux2018.03"
        }
    ]
}
```

Para obtener más información, consulte Acerca de las líneas de base de revisiones en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribePatchProperties en la Referencia de comandos de la AWS CLI.

`describe-sessions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-sessions`.

AWS CLI

Ejemplo 1: enumeración de todas las sesiones de Session Manager activas

En este ejemplo de `describe-sessions`, se recupera una lista de las sesiones activas que se han creado recientemente (tanto las sesiones conectadas como las desconectadas) en los últimos 30 días y que ha iniciado el usuario especificado. Este comando solo devuelve los resultados de las conexiones a destinos iniciados mediante Session Manager. No enumera las conexiones realizadas a través de otros medios, como las conexiones de escritorio remoto o SSH.

```
aws ssm describe-sessions \
    --state "Active" \
    --filters "key=Owner,value=arn:aws:sts::123456789012:assumed-role/Administrator/
Shirley-Rodriguez"
```

Salida:

```
{
    "Sessions": [
        {
            "SessionId": "John-07a16060613c408b5",
            "Target": "i-1234567890abcdef0",
            "Status": "Connected",
            "StartDate": 1550676938.352,
            "Owner": "arn:aws:sts::123456789012:assumed-role/Administrator/Shirley-
Rodriguez",
            "OutputUrl": {}
        },
        {
            "SessionId": "John-01edf534b8b56e8eb",
            "Target": "i-9876543210abcdef0",
            "Status": "Connected",
            "StartDate": 1550676842.194,
            "Owner": "arn:aws:sts::123456789012:assumed-role/Administrator/Shirley-
Rodriguez",
            "OutputUrl": {}
        }
    ]
}
```

Ejemplo 2: enumeración de todas las sesiones de Session Manager finalizadas

En este ejemplo de `describe-sessions`, se recupera una lista de las sesiones finalizadas más recientemente en los últimos 30 días para todos los usuarios.

```
aws ssm describe-sessions \
    --state "History"
```

Salida:

```
{
    "Sessions": [
        {
            "SessionId": "Mary-Major-0022b1eb2b0d9e3bd",
            "Target": "i-1234567890abcdef0",
            "Status": "Terminated",
            "StartDate": 1550520701.256,
            "EndDate": 1550521931.563,
```

```
            "Owner": "arn:aws:sts::123456789012:assumed-role/Administrator/Mary-
Major"
        },
        {
            "SessionId": "Jane-Roe-0db53f487931ed9d4",
            "Target": "i-9876543210abcdef0",
            "Status": "Terminated",
            "StartDate": 1550161369.149,
            "EndDate": 1550162580.329,
            "Owner": "arn:aws:sts::123456789012:assumed-role/Administrator/Jane-Roe"
        },
        ...
    ],
    "NextToken": "--token string truncated--"
}
```

Para obtener más información, consulte Visualización del historial de sesiones en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DescribeSessions en la Referencia de comandos de la AWS CLI.

`disassociate-ops-item-related-item`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-ops-item-related-item`.

AWS CLI

Para eliminar una asociación de elementos relacionados

En el siguiente ejemplo de `disassociate-ops-item-related-item`, se elimina la asociación entre el OpsItem y un elemento relacionado.

```
aws ssm disassociate-ops-item-related-item \
    --ops-item-id "oi-f99f2EXAMPLE" \
    --association-id "e2036148-cccb-490e-ac2a-390e5EXAMPLE"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with Incident Manager incidents in OpsCenter en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte DisassociateOpsItemRelatedItem en la Referencia de comandos de la AWS CLI.

`get-automation-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-automation-execution`.

AWS CLI

Visualización de los detalles sobre una ejecución de automatización

En el siguiente ejemplo de `get-automation-execution` se muestra información detallada sobre una ejecución de Automatización.

```
aws ssm get-automation-execution \
    --automation-execution-id 73c8eef8-f4ee-4a05-820c-e354fEXAMPLE
```

Salida:

```
{
    "AutomationExecution": {
        "AutomationExecutionId": "73c8eef8-f4ee-4a05-820c-e354fEXAMPLE",
        "DocumentName": "AWS-StartEC2Instance",
        "DocumentVersion": "1",
        "ExecutionStartTime": 1583737233.748,
        "ExecutionEndTime": 1583737234.719,
        "AutomationExecutionStatus": "Success",
        "StepExecutions": [
            {
                "StepName": "startInstances",
                "Action": "aws:changeInstanceState",
                "ExecutionStartTime": 1583737234.134,
                "ExecutionEndTime": 1583737234.672,
                "StepStatus": "Success",
                "Inputs": {
                    "DesiredState": "\"running\"",
                    "InstanceIds": "[\"i-0cb99161f6EXAMPLE\"]"
                },
                "Outputs": {
                    "InstanceStates": [
                        "running"
                    ]
```

```
                },
                "StepExecutionId": "95e70479-cf20-4d80-8018-7e4e2EXAMPLE",
                "OverriddenParameters": {}
            }
        ],
        "StepExecutionsTruncated": false,
        "Parameters": {
            "AutomationAssumeRole": [
                ""
            ],
            "InstanceId": [
                "i-0cb99161f6EXAMPLE"
            ]
        },
        "Outputs": {},
        "Mode": "Auto",
        "ExecutedBy": "arn:aws:sts::29884EXAMPLE:assumed-role/mw_service_role/
OrchestrationService",
        "Targets": [],
        "ResolvedTargets": {
            "ParameterValues": [],
            "Truncated": false
        }
    }
}
```

Para obtener más información, consulte Tutorial: Actualizar una AMI de Linux (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetAutomationExecution en la Referencia de comandos de la AWS CLI.

`get-calendar-state`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-calendar-state`.

AWS CLI

Ejemplo 1: obtención del estado actual de un calendario de cambios

En este ejemplo de `get-calendar-state`, se devuelve el estado de un calendario en el momento actual. Debido a que el ejemplo no especifica una hora, se muestra el estado actual del calendario.

```
aws ssm get-calendar-state \
    --calendar-names "MyCalendar"
```

Salida:

```
{
    "State": "OPEN",
    "AtTime": "2020-02-19T22:28:51Z",
    "NextTransitionTime": "2020-02-24T21:15:19Z"
}
```

Ejemplo 2: obtención del estado de un calendario de cambios en una hora determinada

En este ejemplo de `get-calendar-state`, se devuelve el estado de un calendario en la hora especificada.

```
aws ssm get-calendar-state \
    --calendar-names "MyCalendar" \
    --at-time "2020-07-19T21:15:19Z"
```

Salida:

```
{
    "State": "CLOSED",
    "AtTime": "2020-07-19T21:15:19Z"
}
```

Para obtener más información, consulte Obtención del estado de un calendario de cambios en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetCalendarState en la Referencia de comandos de la AWS CLI.

`get-command-invocation`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-command-invocation`.

AWS CLI

Visualización de los detalles de la invocación de un comando

En el siguiente ejemplo de `get-command-invocation` se muestran todas las invocaciones del comando especificado en la instancia especificada.

```
aws ssm get-command-invocation \
    --command-id "ef7fdfd8-9b57-4151-a15c-db9a12345678" \
    --instance-id "i-1234567890abcdef0"
```

Salida:

```
{
    "CommandId": "ef7fdfd8-9b57-4151-a15c-db9a12345678",
    "InstanceId": "i-1234567890abcdef0",
    "Comment": "b48291dd-ba76-43e0-b9df-13e11ddaac26:6960febb-2907-4b59-8e1a-
d6ce8EXAMPLE",
    "DocumentName": "AWS-UpdateSSMAgent",
    "DocumentVersion": "",
    "PluginName": "aws:updateSsmAgent",
    "ResponseCode": 0,
    "ExecutionStartDateTime": "2020-02-19T18:18:03.419Z",
    "ExecutionElapsedTime": "PT0.091S",
    "ExecutionEndDateTime": "2020-02-19T18:18:03.419Z",
    "Status": "Success",
    "StatusDetails": "Success",
    "StandardOutputContent": "Updating amazon-ssm-agent from 2.3.842.0 to latest
\nSuccessfully downloaded https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/
ssm-agent-manifest.json\namazon-ssm-agent 2.3.842.0 has already been installed,
 update skipped\n",
    "StandardOutputUrl": "",
    "StandardErrorContent": "",
    "StandardErrorUrl": "",
    "CloudWatchOutputConfig": {
        "CloudWatchLogGroupName": "",
        "CloudWatchOutputEnabled": false
    }
}
```

Para obtener más información, consulte Descripción de los estados del comando en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetCommandInvocation en la Referencia de comandos de la AWS CLI.

`get-connection-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-connection-status`.

AWS CLI

Visualización del estado de conexión de una instancia administrada

En este ejemplo de `get-connection-status` se devuelve el estado de conexión de la instancia administrada especificada.

```
aws ssm get-connection-status \
    --target i-1234567890abcdef0
```

Salida:

```
{
    "Target": "i-1234567890abcdef0",
    "Status": "connected"
}
```

- Para obtener información sobre la API, consulte GetConnectionStatus en la Referencia de comandos de la AWS CLI.

`get-default-patch-baseline`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-default-patch-baseline`.

AWS CLI

Ejemplo 1: visualización de la línea de base de revisiones de Windows predeterminada

En el siguiente ejemplo de `get-default-patch-baseline` se recuperan los detalles de la línea de base de revisiones predeterminada para Windows Server.

```
aws ssm get-default-patch-baseline
```

Salida:

```
{
  "BaselineId": "pb-0713accee01612345",
  "OperatingSystem": "WINDOWS"
```

```
}
```

Ejemplo 2: visualización de la línea de base de revisiones predeterminada para Amazon Linux

En el siguiente ejemplo de `get-default-patch-baseline` se recuperan los detalles de la línea de base de revisiones predeterminada para Amazon Linux.

```
aws ssm get-default-patch-baseline \
    --operating-system AMAZON_LINUX
```

Salida:

```
{
    "BaselineId": "pb-047c6eb9c8fc12345",
    "OperatingSystem": "AMAZON_LINUX"
}
```

Para obtener más información, consulte Acerca de las líneas de base de revisiones personalizadas y predefinidas <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-baselines.html>__ y Configuración de una línea de base de revisiones existente como valor predeterminado en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetDefaultPatchBaseline en la Referencia de comandos de la AWS CLI.

`get-deployable-patch-snapshot-for-instance`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-deployable-patch-snapshot-for-instance`.

AWS CLI

Recuperación de la instantánea actual de la línea de base de revisiones que usa una instancia

En el siguiente ejemplo de `get-deployable-patch-snapshot-for-instance` se recuperan los detalles de la instantánea actual correspondiente a la línea de base de revisiones especificada que usa una instancia. Este comando debe ejecutarse desde la instancia con las credenciales de la instancia. Para asegurarse de que usa las credenciales de la instancia, ejecute `aws configure` y especifique solo la región de la instancia. Deje vacíos los campos `Access Key` y `Secret Key`.

Consejo: Use `uuidgen` para generar un `snapshot-id`.

```
aws ssm get-deployable-patch-snapshot-for-instance \
    --instance-id "i-1234567890abcdef0" \
    --snapshot-id "521c3536-930c-4aa9-950e-01234567abcd"
```

Salida:

```
{
    "InstanceId": "i-1234567890abcdef0",
    "SnapshotId": "521c3536-930c-4aa9-950e-01234567abcd",
    "Product": "AmazonLinux2018.03",
    "SnapshotDownloadUrl": "https://patch-baseline-snapshot-us-
east-1.s3.amazonaws.com/
ed85194ef27214f5984f28b4d664d14f7313568fea7d4b6ac6c10ad1f729d7e7-773304212436/
AMAZON_LINUX-521c3536-930c-4aa9-950e-01234567abcd?X-Amz-Algorithm=AWS4-HMAC-
SHA256&X-Amz-Date=20190215T164031Z&X-Amz-SignedHeaders=host&X-Amz-Expires=86400&X-
Amz-Credential=AKIAJ5C56P35AEBRX2QQ%2F20190215%2Fus-east-1%2Fs3%2Faws4_request&X-
Amz-Signature=efaaaf6e3878e77f48a6697e015efdbda9c426b09c5822055075c062f6ad2149"
}
```

Para obtener más información, consulte Nombre del parámetro: Snapshot ID en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetDeployablePatchSnapshotForInstance en la Referencia de comandos de la AWS CLI.

`get-document`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-document`.

AWS CLI

Obtención del contenido de un documento

En el siguiente ejemplo de `get-document` se muestra el contenido de un documento de Systems Manager.

```
aws ssm get-document \
    --name "AWS-RunShellScript"
```

Salida:


```
{
    "Name": "AWS-RunShellScript",
    "DocumentVersion": "1",
    "Status": "Active",
    "Content": "{\n    \"schemaVersion\":\"1.2\",\n    \"description\":\"Run a
 shell script or specify the commands to run.\",\n    \"parameters\":{\n
 \"commands\":{\n            \"type\":\"StringList\",\n            \"description
\":\"(Required) Specify a shell script or a command to run.\",\n
 \"minItems\":1,\n            \"displayType\":\"textarea\"\n        },\n
 \"workingDirectory\":{\n            \"type\":\"String\",\n            \"default
\":\"\",\n            \"description\":\"(Optional) The path to the working
 directory on your instance.\",\n            \"maxChars\":4096\n        },\n
   \"executionTimeout\":{\n            \"type\":\"String\",\n            \"default
\":\"3600\",\n            \"description\":\"(Optional) The time in seconds for a
 command to complete before it is considered to have failed. Default is 3600 (1
 hour). Maximum is 172800 (48 hours).\",\n            \"allowedPattern\":\"([1-9]
[0-9]{0,4})|(1[0-6][0-9]{4})|(17[0-1][0-9]{3})|(172[0-7][0-9]{2})|(172800)\"\n
        }\n    },\n    \"runtimeConfig\":{\n        \"aws:runShellScript\":{\n
            \"properties\":[\n                {\n                    \"id\":
\"0.aws:runShellScript\",\n                    \"runCommand\":\"{{ commands }}\",\n
                    \"workingDirectory\":\"{{ workingDirectory }}\",\n
       \"timeoutSeconds\":\"{{ executionTimeout }}\"\n                }\n
  ]\n        }\n    }\n}\n",
    "DocumentType": "Command",
    "DocumentFormat": "JSON"
}
```


Para obtener más información, consulte Documentos de AWS Systems Manager en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetDocument en la Referencia de comandos de la AWS CLI.

`get-inventory-schema`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-inventory-schema`.

AWS CLI

Visualización del esquema del inventario

En este ejemplo se obtiene una lista con los nombres de los tipos de inventario de la cuenta.

Comando:

```
aws ssm get-inventory-schema
```

Salida:

```
{
  "Schemas": [
      {
          "TypeName": "AWS:AWSComponent",
          "Version": "1.0",
          "Attributes": [
              {
                  "Name": "Name",
                  "DataType": "STRING"
              },
              {
                  "Name": "ApplicationType",
                  "DataType": "STRING"
              },
              {
                  "Name": "Publisher",
                  "DataType": "STRING"
              },
              {
                  "Name": "Version",
                  "DataType": "STRING"
              },
              {
                  "Name": "InstalledTime",
                  "DataType": "STRING"
              },
              {
                  "Name": "Architecture",
                  "DataType": "STRING"
              },
              {
                  "Name": "URL",
                  "DataType": "STRING"
              }
          ]
```

```
        },
        ...
    ],
    "NextToken": "--token string truncated--"
}
```

Visualización del esquema de inventario de un tipo de inventario específico

En este ejemplo se devuelve el esquema del inventario de un tipo de inventario AWS:AWSComponent.

Comando:

```
aws ssm get-inventory-schema --type-name "AWS:AWSComponent"
```

- Para obtener información sobre la API, consulte GetInventorySchema en la Referencia de comandos de la AWS CLI.

`get-inventory`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-inventory`.

AWS CLI

Visualización del inventario

En este ejemplo se obtienen los metadatos personalizados del inventario.

Comando:

```
aws ssm get-inventory
```

Salida:

```
{
    "Entities": [
        {
            "Data": {
                "AWS:InstanceInformation": {
                    "Content": [
                        {
```

```
                        "ComputerName": "ip-172-31-44-222.us-
west-2.compute.internal",
                        "InstanceId": "i-0cb2b964d3e14fd9f",
                        "IpAddress": "172.31.44.222",
                        "AgentType": "amazon-ssm-agent",
                        "ResourceType": "EC2Instance",
                        "AgentVersion": "2.0.672.0",
                        "PlatformVersion": "2016.09",
                        "PlatformName": "Amazon Linux AMI",
                        "PlatformType": "Linux"
                    }
                ],
                "TypeName": "AWS:InstanceInformation",
                "SchemaVersion": "1.0",
                "CaptureTime": "2017-02-20T18:03:58Z"
            }
        },
        "Id": "i-0cb2b964d3e14fd9f"
    }
  ]
}
```

- Para obtener información sobre la API, consulte GetInventory en la Referencia de comandos de la AWS CLI.

`get-maintenance-window-execution-task-invocation`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-maintenance-window-execution-task-invocation`.

AWS CLI

Para obtener información sobre una invocación de tareas de período de mantenimiento

En el siguiente ejemplo de `get-maintenance-window-execution-task-invocation`, se enumera información sobre una invocación de tareas específica que forma parte de la ejecución del período de mantenimiento indicado.

```
aws ssm get-maintenance-window-execution-task-invocation \
    --window-execution-id "bc494bfa-e63b-49f6-8ad1-aa9f2EXAMPLE" \
    --task-id "96f2ad59-97e3-461d-a63d-40c8aEXAMPLE" \
    --invocation-id "a5273e2c-d2c6-4880-b3e1-5e550EXAMPLE"
```

Salida:

```
{
    "Status": "SUCCESS",
    "Parameters": "{\"comment\":\"\",\"documentName\":\"AWS-RunPowerShellScript\",
\"instanceIds\":[\"i-1234567890EXAMPLE\"],\"maxConcurrency\":\"1\",\"maxErrors\":
\"1\",\"parameters\":{\"executionTimeout\":[\"3600\"],\"workingDirectory\":[\"\"],
\"commands\":[\"echo Hello\"]},\"timeoutSeconds\":600}",
    "ExecutionId": "03b6baa0-5460-4e15-83f2-ea685EXAMPLE",
    "InvocationId": "a5273e2c-d2c6-4880-b3e1-5e550EXAMPLE",
    "StartTime": 1549998326.421,
    "TaskType": "RUN_COMMAND",
    "EndTime": 1550001931.784,
    "WindowExecutionId": "bc494bfa-e63b-49f6-8ad1-aa9f2EXAMPLE",
    "StatusDetails": "Failed",
    "TaskExecutionId": "96f2ad59-97e3-461d-a63d-40c8aEXAMPLE"
}
```

Para obtener más información, consulte Ver información sobre tareas y ejecuciones de tareas (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetMaintenanceWindowExecutionTaskInvocation en la Referencia de comandos de la AWS CLI.

`get-maintenance-window-execution-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-maintenance-window-execution-task`.

AWS CLI

Obtención de información sobre la ejecución de una tarea del periodo de mantenimiento

En el siguiente ejemplo de `get-maintenance-window-execution-task` se muestra información sobre una tarea que forma parte de la ejecución del periodo de mantenimiento especificado.

```
aws ssm get-maintenance-window-execution-task \
    --window-execution-id "518d5565-5969-4cca-8f0e-da3b2EXAMPLE" \
    --task-id "ac0c6ae1-daa3-4a89-832e-d3845EXAMPLE"
```

Salida:

```
{
    "WindowExecutionId": "518d5565-5969-4cca-8f0e-da3b2EXAMPLE",
    "TaskExecutionId": "ac0c6ae1-daa3-4a89-832e-d3845EXAMPLE",
    "TaskArn": "AWS-RunPatchBaseline",
    "ServiceRole": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
    "Type": "RUN_COMMAND",
    "TaskParameters": [
        {
            "BaselineOverride": {
                "Values": [
                    ""
                ]
            },
            "InstallOverrideList": {
                "Values": [
                    ""
                ]
            },
            "Operation": {
                "Values": [
                    "Scan"
                ]
            },
            "RebootOption": {
                "Values": [
                    "RebootIfNeeded"
                ]
            },
            "SnapshotId": {
                "Values": [
                    "{{ aws:ORCHESTRATION_ID }}"
                ]
            },
            "aws:InstanceId": {
                "Values": [
                    "i-02573cafcfEXAMPLE",
                    "i-0471e04240EXAMPLE",
                    "i-07782c72faEXAMPLE"
                ]
            }
        }
```

```
    ],
    "Priority": 1,
    "MaxConcurrency": "1",
    "MaxErrors": "3",
    "Status": "SUCCESS",
    "StartTime": "2021-08-04T11:45:35.088000-07:00",
    "EndTime": "2021-08-04T11:53:09.079000-07:00"
}
```

Para obtener más información, consulte Ver información sobre tareas y ejecuciones de tareas (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetMaintenanceWindowExecutionTask en la Referencia de comandos de la AWS CLI.

`get-maintenance-window-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-maintenance-window-execution`.

AWS CLI

Obtención de información sobre la ejecución de una tarea del periodo de mantenimiento

En el siguiente ejemplo de `get-maintenance-window-execution` se muestra información sobre una tarea que se ejecutó como parte de la ejecución del periodo de mantenimiento especificado.

```
aws ssm get-maintenance-window-execution \
    --window-execution-id "518d5565-5969-4cca-8f0e-da3b2EXAMPLE"
```

Salida:

```
{
    "Status": "SUCCESS",
    "TaskIds": [
        "ac0c6ae1-daa3-4a89-832e-d3845EXAMPLE"
    ],
    "StartTime": 1487692834.595,
    "EndTime": 1487692835.051,
    "WindowExecutionId": "518d5565-5969-4cca-8f0e-da3b2EXAMPLE",
}
```

Para obtener más información, consulte Ver información sobre tareas y ejecuciones de tareas (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetMaintenanceWindowExecution en la Referencia de comandos de la AWS CLI.

`get-maintenance-window-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-maintenance-window-task`.

AWS CLI

Para obtener información sobre una tarea de período de mantenimiento

En el siguiente ejemplo de `get-maintenance-window-task`, se obtienen los detalles de la tarea del período de mantenimiento especificado.

```
aws ssm get-maintenance-window-task \
    --window-id mw-0c5ed765acEXAMPLE \
    --window-task-id 0e842a8d-2d44-4886-bb62-af8dcEXAMPLE
```

Salida:

```
{
    "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
    "MaxErrors": "1",
    "TaskArn": "AWS-RunPowerShellScript",
    "MaxConcurrency": "1",
    "WindowTaskId": "0e842a8d-2d44-4886-bb62-af8dcEXAMPLE",
    "TaskParameters": {},
    "Priority": 1,
    "TaskInvocationParameters": {
        "RunCommand": {
            "Comment": "",
            "TimeoutSeconds": 600,
            "Parameters": {
                "commands": [
                    "echo Hello"
                ],
                "executionTimeout": [
                    "3600"
                ],
```

```
                "workingDirectory": [
                    ""
                ]
            }
        }
    },
    "WindowId": "mw-0c5ed765acEXAMPLE",
    "TaskType": "RUN_COMMAND",
    "Targets": [
        {
            "Values": [
                "84c818da-b619-4d3d-9651-946f3EXAMPLE"
            ],
            "Key": "WindowTargetIds"
        }
    ],
    "Name": "ExampleTask"
}
```

Para obtener más información, consulte Ver información sobre períodos de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetMaintenanceWindowTask en la Referencia de comandos de la AWS CLI.

`get-maintenance-window`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-maintenance-window`.

AWS CLI

Obtención de información sobre un periodo de mantenimiento

En el siguiente ejemplo de `get-maintenance-window` se recuperan los detalles sobre el periodo de mantenimiento especificado.

```
aws ssm get-maintenance-window \
    --window-id "mw-03eb9db428EXAMPLE"
```

Salida:

```
{
```

```
    "AllowUnassociatedTargets": true,
    "CreatedDate": 1515006912.957,
    "Cutoff": 1,
    "Duration": 6,
    "Enabled": true,
    "ModifiedDate": 2020-01-01T10:04:04.099Z,
    "Name": "My-Maintenance-Window",
    "Schedule": "rate(3 days)",
    "WindowId": "mw-03eb9db428EXAMPLE",
    "NextExecutionTime": "2020-02-25T00:08:15.099Z"
}
```

Para obtener más información, consulte Ver información sobre períodos de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetMaintenanceWindow en la Referencia de comandos de la AWS CLI.

`get-ops-item`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ops-item`.

AWS CLI

Para ver información sobre un OpsItem

En el siguiente ejemplo de `get-ops-item`, se muestran los detalles del OpsItem especificado.

```
aws ssm get-ops-item \
    --ops-item-id oi-0b725EXAMPLE
```

Salida:

```
{
    "OpsItem": {
        "CreatedBy": "arn:aws:sts::111222333444:assumed-role/OpsItem-CWE-Role/
fbf77cbe264a33509569f23e4EXAMPLE",
        "CreatedTime": "2019-12-04T15:52:16.793000-08:00",
        "Description": "CloudWatch Event Rule SSMOpsItems-EC2-instance-terminated
 was triggered. Your EC2 instance has terminated. See below for more details.",
        "LastModifiedBy": "arn:aws:sts::111222333444:assumed-role/OpsItem-CWE-Role/
fbf77cbe264a33509569f23e4EXAMPLE",
```

```
        "LastModifiedTime": "2019-12-04T15:52:16.793000-08:00",
        "Notifications": [],
        "RelatedOpsItems": [],
        "Status": "Open",
        "OpsItemId": "oi-0b725EXAMPLE",
        "Title": "EC2 instance terminated",
        "Source": "EC2",
        "OperationalData": {
            "/aws/automations": {
                "Value": "[ { \"automationType\": \"AWS:SSM:Automation\",
 \"automationId\": \"AWS-CreateManagedWindowsInstance\" }, { \"automationType\":
 \"AWS:SSM:Automation\", \"automationId\": \"AWS-CreateManagedLinuxInstance\" } ]",
                "Type": "SearchableString"
            },
            "/aws/dedup": {
                "Value": "{\"dedupString\":\"SSMOpsItems-EC2-instance-terminated
\"}",
                "Type": "SearchableString"
            },
            "/aws/resources": {
                "Value": "[{\"arn\":\"arn:aws:ec2:us-east-2:111222333444:instance/
i-05adec7e97EXAMPLE\"}]",
                "Type": "SearchableString"
            },
            "event-time": {
                "Value": "2019-12-04T23:52:16Z",
                "Type": "String"
            },
            "instance-state": {
                "Value": "terminated",
                "Type": "String"
            }
        },
        "Category": "Availability",
        "Severity": "4"
    }
}
```

Para obtener más información, consulte Trabajo con OpsItems en la AWSGuía del usuario de Systems Manager.

- Para obtener información sobre la API, consulte GetOpsItem en la Referencia de comandos de la AWS CLI.

get-ops-summary

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ops-summary`.

AWS CLI

Para ver un resumen de todos los OpsItems

En el siguiente ejemplo de `get-ops-summary`, se muestra un resumen de todos los OpsItems de su cuenta de AWS.

```
aws ssm get-ops-summary
```

Salida:

```
{
    "Entities": [
        {
            "Id": "oi-4309fEXAMPLE",
            "Data": {
                "AWS:OpsItem": {
                    "CaptureTime": "2020-02-26T18:58:32.918Z",
                    "Content": [
                        {
                            "AccountId": "111222333444",
                            "Category": "Availability",
                            "CreatedBy": "arn:aws:sts::111222333444:assumed-role/
OpsItem-CWE-Role/fbf77cbe264a33509569f23e4EXAMPLE",
                            "CreatedTime": "2020-02-26T19:10:44.149Z",
                            "Description": "CloudWatch Event Rule SSMOpsItems-EC2-
instance-terminated was triggered. Your EC2 instance has terminated. See below for
 more details.",
                            "LastModifiedBy": "arn:aws:sts::111222333444:assumed-
role/OpsItem-CWE-Role/fbf77cbe264a33509569f23e4EXAMPLE",
                            "LastModifiedTime": "2020-02-26T19:10:44.149Z",
                            "Notifications": "",
                            "OperationalData": "{\"/aws/automations\":
{\"type\":\"SearchableString\",\"value\":\"[ { \\\"automationType\\\": \\
\"AWS:SSM:Automation\\\", \\\"automationId\\\": \\\"AWS-CreateManagedWindowsInstance
\\\" }, { \\\"automationType\\\": \\\"AWS:SSM:Automation\\\", \\\"automationId
\\\": \\\"AWS-CreateManagedLinuxInstance\\\" } ]\"},\"/aws/resources\":
{\"type\":\"SearchableString\",\"value\":\"[{\\\"arn\\\":\\\"arn:aws:ec2:us-
east-2:111222333444:instance/i-0acbd0800fEXAMPLE\\\"}]\"},\"/aws/dedup\":{\"type\":
```

```
\"SearchableString\",\"value\":\"{\\\"dedupString\\\":\\\"SSMOpsItems-EC2-instance-
terminated\\\"}\"}}",
                            "OpsItemId": "oi-4309fEXAMPLE",
                            "RelatedItems": "",
                            "Severity": "3",
                            "Source": "EC2",
                            "Status": "Open",
                            "Title": "EC2 instance terminated"
                        }
                    ]
                }
            }
        },
        {
            "Id": "oi-bb2a0e6a4541",
            "Data": {
                "AWS:OpsItem": {
                    "CaptureTime": "2019-11-26T19:20:06.161Z",
                    "Content": [
                        {
                            "AccountId": "111222333444",
                            "Category": "Availability",
                            "CreatedBy": "arn:aws:sts::111222333444:assumed-role/
OpsItem-CWE-Role/fbf77cbe264a33509569f23e4EXAMPLE",
                            "CreatedTime": "2019-11-26T20:00:07.237Z",
                            "Description": "CloudWatch Event Rule SSMOpsItems-SSM-
maintenance-window-execution-failed was triggered. Your SSM Maintenance Window
 execution has failed. See below for more details.",
                            "LastModifiedBy": "arn:aws:sts::111222333444:assumed-
role/OpsItem-CWE-Role/fbf77cbe264a33509569f23e4EXAMPLE",
                            "LastModifiedTime": "2019-11-26T20:00:07.237Z",
                            "Notifications": "",
                            "OperationalData": "{\"/aws/resources\":{\"type
\":\"SearchableString\",\"value\":\"[{\\\"arn\\\":\\\"arn:aws:ssm:us-
east-2:111222333444:maintenancewindow/mw-0e83ba440dEXAMPLE\\\"}]\"},\"/aws/dedup\":
{\"type\":\"SearchableString\",\"value\":\"{\\\"dedupString\\\":\\\"SSMOpsItems-SSM-
maintenance-window-execution-failed\\\"}\"}}",
                            "OpsItemId": "oi-bb2a0EXAMPLE",
                            "RelatedItems": "",
                            "Severity": "3",
                            "Source": "SSM",
                            "Status": "Open",
                            "Title": "SSM Maintenance Window execution failed"
                        }
```

```
                    ]
                }
            }
        }
    ]
}
```

Para obtener más información, consulte Trabajo con OpsItems en la AWSGuía del usuario de Systems Manager.

- Para obtener información sobre la API, consulte GetOpsSummary en la Referencia de comandos de la AWS CLI.

`get-parameter-history`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-parameter-history`.

AWS CLI

Obtención del historial de valores de un parámetro

En el siguiente ejemplo de `get-parameter-history` se enumera el historial de cambios del parámetro especificado, incluido su valor.

```
aws ssm get-parameter-history \
    --name "MyStringParameter"
```

Salida:

```
{
    "Parameters": [
        {
            "Name": "MyStringParameter",
            "Type": "String",
            "LastModifiedDate": 1582154711.976,
            "LastModifiedUser": "arn:aws:iam::111222333444:user/Mary-Major",
            "Description": "This is the first version of my String parameter",
            "Value": "Veni",
            "Version": 1,
            "Labels": [],
            "Tier": "Standard",
            "Policies": []
        },
```

```
        {
            "Name": "MyStringParameter",
            "Type": "String",
            "LastModifiedDate": 1582156093.471,
            "LastModifiedUser": "arn:aws:iam::111222333444:user/Mary-Major",
            "Description": "This is the second version of my String parameter",
            "Value": "Vidi",
            "Version": 2,
            "Labels": [],
            "Tier": "Standard",
            "Policies": []
        },
        {
            "Name": "MyStringParameter",
            "Type": "String",
            "LastModifiedDate": 1582156117.545,
            "LastModifiedUser": "arn:aws:iam::111222333444:user/Mary-Major",
            "Description": "This is the third version of my String parameter",
            "Value": "Vici",
            "Version": 3,
            "Labels": [],
            "Tier": "Standard",
            "Policies": []
        }
    ]
}
```

Para obtener más información, consulte Trabajo con versiones de parámetros en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetParameterHistory en la Referencia de comandos de la AWS CLI.

`get-parameter`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-parameter`.

AWS CLI

Ejemplo 1: visualización del valor de un parámetro

En el siguiente ejemplo de `get-parameter` se enumera el valor del parámetro único especificado.

```
aws ssm get-parameter \
    --name "MyStringParameter"
```

Salida:

```
{
    "Parameter": {
        "Name": "MyStringParameter",
        "Type": "String",
        "Value": "Veni",
        "Version": 1,
        "LastModifiedDate": 1530018761.888,
        "ARN": "arn:aws:ssm:us-east-2:111222333444:parameter/MyStringParameter"
        "DataType": "text"
    }
}
```

Para obtener más información, consulte Uso de Parameter Store en la Guía del usuario de AWS Systems Manager.

Ejemplo 2: descifrar el valor de un parámetro SecureString

En el siguiente ejemplo de `get-parameter` se cambia el valor del parámetro `SecureString` especificado.

```
aws ssm get-parameter \
    --name "MySecureStringParameter" \
    --with-decryption
```

Salida:

```
{
    "Parameter": {
        "Name": "MySecureStringParameter",
        "Type": "SecureString",
        "Value": "16679b88-310b-4895-a943-e0764EXAMPLE",
        "Version": 2,
        "LastModifiedDate": 1582155479.205,
        "ARN": "arn:aws:ssm:us-east-2:111222333444:parameter/
MySecureStringParameter"
        "DataType": "text"
```

```
    }
}
```

Para obtener más información, consulte Uso de Parameter Store en la Guía del usuario de AWS Systems Manager.

Ejemplo 3: visualización del valor de un parámetro mediante etiquetas

En el siguiente ejemplo de `get-parameter` se enumera el valor del parámetro único especificado con una etiqueta especificada.

```
aws ssm get-parameter \
    --name "MyParameter:label"
```

Salida:

```
{
    "Parameter": {
        "Name": "MyParameter",
        "Type": "String",
        "Value": "parameter version 2",
        "Version": 2,
        "Selector": ":label",
        "LastModifiedDate": "2021-07-12T09:49:15.865000-07:00",
        "ARN": "arn:aws:ssm:us-west-2:786973925828:parameter/MyParameter",
        "DataType": "text"
    }
}
```

Para obtener más información, consulte Trabajo con etiquetas de parámetros en la Guía del usuario de AWS Systems Manager.

Ejemplo 4: visualización del valor de un parámetro mediante etiquetas

En el siguiente ejemplo de `get-parameter` se enumera el valor de la versión de parámetro único especificado.

```
aws ssm get-parameter \
    --name "MyParameter:2"
```

Salida:

```
{
    "Parameter": {
        "Name": "MyParameter",
        "Type": "String",
        "Value": "parameter version 2",
        "Version": 2,
        "Selector": ":2",
        "LastModifiedDate": "2021-07-12T09:49:15.865000-07:00",
        "ARN": "arn:aws:ssm:us-west-2:786973925828:parameter/MyParameter",
        "DataType": "text"
    }
}
```

Para obtener más información, consulte Trabajo con etiquetas de parámetros en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetParameter en la Referencia de comandos de la AWS CLI.

`get-parameters-by-path`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-parameters-by-path`.

AWS CLI

Para enumerar los parámetros de una ruta específica

En el siguiente ejemplo de `get-parameters-by-path`, se enumeran los parámetros de la jerarquía especificada.

```
aws ssm get-parameters-by-path \
    --path "/site/newyork/department/"
```

Salida:

```
{
    "Parameters": [
        {
            "Name": "/site/newyork/department/marketing",
            "Type": "String",
            "Value": "Floor 2",
            "Version": 1,
```

```
            "LastModifiedDate": 1530018761.888,
            "ARN": "arn:aws:ssm:us-east-1:111222333444:parameter/site/newyork/
department/marketing"
        },
        {
            "Name": "/site/newyork/department/infotech",
            "Type": "String",
            "Value": "Floor 3",
            "Version": 1,
            "LastModifiedDate": 1530018823.429,
            "ARN": "arn:aws:ssm:us-east-1:111222333444:parameter/site/newyork/
department/infotech"
        },
        ...
    ]
}
```

Para obtener más información, consulte Trabajo con jerarquías de parámetros en Parameter Store en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetParametersByPath en la Referencia de comandos de la AWS CLI.

`get-parameters`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-parameters`.

AWS CLI

Ejemplo 1: enumeración de los valores de un parámetro

En el siguiente ejemplo de `get-parameters` se enumeran los valores de los tres parámetros especificados.

```
aws ssm get-parameters \
    --names "MyStringParameter" "MyStringListParameter" "MyInvalidParameterName"
```

Salida:

```
{
    "Parameters": [
        {
```

```
            "Name": "MyStringListParameter",
            "Type": "StringList",
            "Value": "alpha,beta,gamma",
            "Version": 1,
            "LastModifiedDate": 1582154764.222,
            "ARN": "arn:aws:ssm:us-east-2:111222333444:parameter/
MyStringListParameter"
            "DataType": "text"
        },
        {
            "Name": "MyStringParameter",
            "Type": "String",
            "Value": "Vici",
            "Version": 3,
            "LastModifiedDate": 1582156117.545,
            "ARN": "arn:aws:ssm:us-east-2:111222333444:parameter/MyStringParameter"
            "DataType": "text"
        }
    ],
    "InvalidParameters": [
        "MyInvalidParameterName"
    ]
}
```

Para obtener más información, consulte Uso de Parameter Store en la Guía del usuario de AWS Systems Manager.

Ejemplo 2: enumeración de los nombres y valores de varios parámetros mediante la opción “--query

En el siguiente ejemplo de `get-parameters` se enumeran los nombres y valores de los parámetros especificados.

```
aws ssm get-parameters \
    --names MyStringParameter MyStringListParameter \
    --query "Parameters[*].{Name:Name,Value:Value}"
```

Salida:

```
[
    {
        "Name": "MyStringListParameter",
```

```
        "Value": "alpha,beta,gamma"
    },
    {
        "Name": "MyStringParameter",
        "Value": "Vidi"
    }
]
```

Para obtener más información, consulte Uso de Parameter Store en la Guía del usuario de AWS Systems Manager.

Ejemplo 3: visualización del valor de un parámetro mediante etiquetas

En el siguiente ejemplo de `get-parameter` se enumera el valor del parámetro único especificado con una etiqueta especificada.

```
aws ssm get-parameter \
    --name "MyParameter:label"
```

Salida:

```
{
    "Parameters": [
        {
            "Name": "MyLabelParameter",
            "Type": "String",
            "Value": "parameter by label",
            "Version": 1,
            "Selector": ":label",
            "LastModifiedDate": "2021-07-12T09:49:15.865000-07:00",
            "ARN": "arn:aws:ssm:us-west-2:786973925828:parameter/MyParameter",
            "DataType": "text"
        },
        {
            "Name": "MyVersionParameter",
            "Type": "String",
            "Value": "parameter by version",
            "Version": 2,
            "Selector": ":2",
            "LastModifiedDate": "2021-03-24T16:20:28.236000-07:00",
            "ARN": "arn:aws:ssm:us-west-2:786973925828:parameter/unlabel-param",
            "DataType": "text"
```

```
        }
    ],
    "InvalidParameters": []
}
```

Para obtener más información, consulte Trabajo con etiquetas de parámetros en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetParameters en la Referencia de comandos de la AWS CLI.

`get-patch-baseline-for-patch-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-patch-baseline-for-patch-group`.

AWS CLI

Visualización de la línea de base de revisiones de un grupo de revisiones

En el siguiente ejemplo de `get-patch-baseline-for-patch-group` se recuperan los detalles sobre la línea de base de revisiones del grupo de revisiones especificado.

```
aws ssm get-patch-baseline-for-patch-group \
    --patch-group "DEV"
```

Salida:

```
{
    "PatchGroup": "DEV",
    "BaselineId": "pb-0123456789abcdef0",
    "OperatingSystem": "WINDOWS"
}
```

Para obtener más información, consulte Creación de un grupo de revisiones <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-group-tagging.html>__ y Añadir un grupo de revisiones a una línea de base de revisiones en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetPatchBaselineForPatchGroup en la Referencia de comandos de la AWS CLI.

get-patch-baseline

En el siguiente ejemplo de código, se muestra cómo utilizar `get-patch-baseline`.

AWS CLI

Visualización de una línea de base de revisiones

En el siguiente ejemplo de `get-patch-baseline` se recuperan los detalles de la línea de base de revisiones especificada.

```
aws ssm get-patch-baseline \
    --baseline-id "pb-0123456789abcdef0"
```

Salida:

```
{
    "BaselineId": "pb-0123456789abcdef0",
    "Name": "WindowsPatching",
    "OperatingSystem": "WINDOWS",
    "GlobalFilters": {
        "PatchFilters": []
    },
    "ApprovalRules": {
        "PatchRules": [
            {
                "PatchFilterGroup": {
                    "PatchFilters": [
                        {
                            "Key": "PRODUCT",
                            "Values": [
                                "WindowsServer2016"
                            ]
                        }
                    ]
                },
                "ComplianceLevel": "CRITICAL",
                "ApproveAfterDays": 0,
                "EnableNonSecurity": false
            }
        ]
    },
    "ApprovedPatches": [],
```

```
    "ApprovedPatchesComplianceLevel": "UNSPECIFIED",
    "ApprovedPatchesEnableNonSecurity": false,
    "RejectedPatches": [],
    "RejectedPatchesAction": "ALLOW_AS_DEPENDENCY",
    "PatchGroups": [
        "QA",
        "DEV"
    ],
    "CreatedDate": 1550244180.465,
    "ModifiedDate": 1550244180.465,
    "Description": "Patches for Windows Servers",
    "Sources": []
}
```

Para obtener más información, consulte Acerca de las líneas de base de revisiones en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetPatchBaseline en la Referencia de comandos de la AWS CLI.

`get-service-setting`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-setting`.

AWS CLI

Para recuperar la configuración del servicio para el rendimiento del almacén de parámetros

En el siguiente ejemplo de `get-service-setting`, se recupera la configuración de servicio actual del rendimiento del almacén de parámetros de la región especificada.

```
aws ssm get-service-setting \
    --setting-id arn:aws:ssm:us-east-1:123456789012:servicesetting/ssm/parameter-store/high-throughput-enabled
```

Salida:

```
{
    "ServiceSetting": {
        "SettingId": "/ssm/parameter-store/high-throughput-enabled",
        "SettingValue": "false",
        "LastModifiedDate": 1555532818.578,
```

```
        "LastModifiedUser": "System",
        "ARN": "arn:aws:ssm:us-east-1:123456789012:servicesetting/ssm/parameter-
store/high-throughput-enabled",
        "Status": "Default"
    }
}
```

Para obtener más información, consulte Aumentar o disminuir el rendimiento de Parameter Store en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte GetServiceSetting en la Referencia de comandos de la AWS CLI.

`label-parameter-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `label-parameter-version`.

AWS CLI

Ejemplo 1: adición de una etiqueta a la versión más reciente de un parámetro

En el siguiente ejemplo de `label-parameter-version`, se agrega una etiqueta a la versión más reciente del parámetro especificado.

```
aws ssm label-parameter-version \
    --name "MyStringParameter" \
    --labels "ProductionReady"
```

Salida:

```
{
    "InvalidLabels": [],
    "ParameterVersion": 3
}
```

Para obtener más información, consulte Trabajo con etiquetas de parámetros en la Guía del usuario de AWS Systems Manager.

Ejemplo 2: adición de una etiqueta a una versión específica de un parámetro

En el siguiente ejemplo de `label-parameter-version`, se agrega una etiqueta a la versión especificada de un parámetro.

```
aws ssm label-parameter-version \
    --name "MyStringParameter" \
    --labels "ProductionReady" \
    --parameter-version "2" --labels "DevelopmentReady"
```

Para obtener más información, consulte Trabajo con etiquetas de parámetros en la Guía del usuario de AWS Systems Manager.

- Para obtener detalles sobre la API, consulte LabelParameterVersion en la Referencia de comandos de la AWS CLI.

`list-association-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-association-versions`.

AWS CLI

Enumeración de todas las versiones de una asociación para un ID de asociación específico

En el siguiente ejemplo de `list-association-versions` se enumeran todas las versiones de las asociaciones especificadas.

```
aws ssm list-association-versions \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab"
```

Salida:

```
{
"AssociationVersions": [
        {
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "AssociationVersion": "1",
            "CreatedDate": 1550505536.726,
            "Name": "AWS-UpdateSSMAgent",
            "Parameters": {
                "allowDowngrade": [
                    "false"
                ],
                "version": [
                    ""
                ]
            },
```

```
            "Targets": [
                {
                    "Key": "InstanceIds",
                    "Values": [
                        "i-1234567890abcdef0"
                    ]
                }
            ],
            "ScheduleExpression": "cron(0 00 12 ? * SUN *)",
            "AssociationName": "UpdateSSMAgent"
        }
    ]
}
```

Para obtener más información, consulte Trabajo con asociaciones en Systems Manager en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte ListAssociationVersions en la Referencia de comandos de la AWS CLI.

`list-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-associations`.

AWS CLI

Ejemplo 1: enumeración de las asociaciones de una instancia específica

En el siguiente ejemplo de list-associations se enumeran todas las asociaciones con el valor UpdateSSMAgent para AssociationName.

```
aws ssm list-associations /
    --association-filter-list "key=AssociationName,value=UpdateSSMAgent"
```

Salida:

```
{
    "Associations": [
        {
            "Name": "AWS-UpdateSSMAgent",
            "InstanceId": "i-1234567890abcdef0",
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "AssociationVersion": "1",
```

```
            "Targets": [
                {
                    "Key": "InstanceIds",
                    "Values": [
                        "i-016648b75dd622dab"
                    ]
                }
            ],
            "Overview": {
                "Status": "Pending",
                "DetailedStatus": "Associated",
                "AssociationStatusAggregatedCount": {
                    "Pending": 1
                }
            },
            "ScheduleExpression": "cron(0 00 12 ? * SUN *)",
            "AssociationName": "UpdateSSMAgent"
        }
    ]
}
```

Para obtener más información, consulte Trabajo con asociaciones en Systems Manager en la Guía del usuario de Systems Manager.

Ejemplo 2: enumeración de las asociaciones de un documento específico

En el siguiente ejemplo de list-associations se enumeran todas las asociaciones del documento especificado.

```
aws ssm list-associations /
    --association-filter-list "key=Name,value=AWS-UpdateSSMAgent"
```

Salida:

```
{
    "Associations": [
        {
            "Name": "AWS-UpdateSSMAgent",
            "InstanceId": "i-1234567890abcdef0",
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "AssociationVersion": "1",
            "Targets": [
                {
```

```
                    "Key": "InstanceIds",
                    "Values": [
                        "i-1234567890abcdef0"
                    ]
                }
            ],
            "LastExecutionDate": 1550505828.548,
            "Overview": {
                "Status": "Success",
                "DetailedStatus": "Success",
                "AssociationStatusAggregatedCount": {
                    "Success": 1
                }
            },
            "ScheduleExpression": "cron(0 00 12 ? * SUN *)",
            "AssociationName": "UpdateSSMAgent"
        },
    {
            "Name": "AWS-UpdateSSMAgent",
            "InstanceId": "i-9876543210abcdef0",
            "AssociationId": "fbc07ef7-b985-4684-b82b-0123456789ab",
            "AssociationVersion": "1",
            "Targets": [
                {
                    "Key": "InstanceIds",
                    "Values": [
                        "i-9876543210abcdef0"
                    ]
                }
            ],
            "LastExecutionDate": 1550507531.0,
            "Overview": {
                "Status": "Success",
                "AssociationStatusAggregatedCount": {
                    "Success": 1
                }
            }
        }
    ]
}
```

Para obtener más información, consulte Trabajo con asociaciones en Systems Manager en la Guía del usuario de Systems Manager.

- Para obtener información sobre la API, consulte ListAssociations en la Referencia de comandos de la AWS CLI.

`list-command-invocations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-command-invocations`.

AWS CLI

Enumeración de las invocaciones de un comando específico

En el siguiente ejemplo de `list-command-invocations` se enumeran todas las invocaciones de un comando.

```
aws ssm list-command-invocations \
    --command-id "ef7fdfd8-9b57-4151-a15c-db9a12345678" \
    --details
```

Salida:

```
{
    "CommandInvocations": [
        {
            "CommandId": "ef7fdfd8-9b57-4151-a15c-db9a12345678",
            "InstanceId": "i-02573cafcfEXAMPLE",
            "InstanceName": "",
            "Comment": "b48291dd-ba76-43e0-
b9df-13e11ddaac26:6960febb-2907-4b59-8e1a-d6ce8EXAMPLE",
            "DocumentName": "AWS-UpdateSSMAgent",
            "DocumentVersion": "",
            "RequestedDateTime": 1582136283.089,
            "Status": "Success",
            "StatusDetails": "Success",
            "StandardOutputUrl": "",
            "StandardErrorUrl": "",
            "CommandPlugins": [
                {
                    "Name": "aws:updateSsmAgent",
                    "Status": "Success",
                    "StatusDetails": "Success",
                    "ResponseCode": 0,
                    "ResponseStartDateTime": 1582136283.419,
```

```
                    "ResponseFinishDateTime": 1582136283.51,
                    "Output": "Updating amazon-ssm-agent from 2.3.842.0 to latest
\nSuccessfully downloaded https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/
ssm-agent-manifest.json\namazon-ssm-agent 2.3.842.0 has already been installed,
 update skipped\n",
                    "StandardOutputUrl": "",
                    "StandardErrorUrl": "",
                    "OutputS3Region": "us-east-2",
                    "OutputS3BucketName": "",
                    "OutputS3KeyPrefix": ""
                }
            ],
            "ServiceRole": "",
            "NotificationConfig": {
                "NotificationArn": "",
                "NotificationEvents": [],
                "NotificationType": ""
            },
            "CloudWatchOutputConfig": {
                "CloudWatchLogGroupName": "",
                "CloudWatchOutputEnabled": false
            }
        },
        {
            "CommandId": "ef7fdfd8-9b57-4151-a15c-db9a12345678",
            "InstanceId": "i-0471e04240EXAMPLE",
            "InstanceName": "",
            "Comment": "b48291dd-ba76-43e0-
b9df-13e11ddaac26:6960febb-2907-4b59-8e1a-d6ce8EXAMPLE",
            "DocumentName": "AWS-UpdateSSMAgent",
            "DocumentVersion": "",
            "RequestedDateTime": 1582136283.02,
            "Status": "Success",
            "StatusDetails": "Success",
            "StandardOutputUrl": "",
            "StandardErrorUrl": "",
            "CommandPlugins": [
                {
                    "Name": "aws:updateSsmAgent",
                    "Status": "Success",
                    "StatusDetails": "Success",
                    "ResponseCode": 0,
                    "ResponseStartDateTime": 1582136283.812,
                    "ResponseFinishDateTime": 1582136295.031,
```

```
                    "Output": "Updating amazon-ssm-agent from 2.3.672.0 to latest
\nSuccessfully downloaded https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/
ssm-agent-manifest.json\nSuccessfully downloaded https://s3.us-east-2.amazonaws.com/
amazon-ssm-us-east-2/amazon-ssm-agent-updater/2.3.842.0/amazon-ssm-agent-updater-
snap-amd64.tar.gz\nSuccessfully downloaded https://s3.us-east-2.amazonaws.com/
amazon-ssm-us-east-2/amazon-ssm-agent/2.3.672.0/amazon-ssm-agent-snap-amd64.tar.gz
\nSuccessfully downloaded https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/
amazon-ssm-agent/2.3.842.0/amazon-ssm-agent-snap-amd64.tar.gz\nInitiating amazon-
ssm-agent update to 2.3.842.0\namazon-ssm-agent updated successfully to 2.3.842.0",
                    "StandardOutputUrl": "",
                    "StandardErrorUrl": "",
                    "OutputS3Region": "us-east-2",
                    "OutputS3BucketName": "",
                    "OutputS3KeyPrefix": "8bee3135-398c-4d31-99b6-e42d2EXAMPLE/
i-0471e04240EXAMPLE/awsupdateSsmAgent"
                }
            ],
            "ServiceRole": "",
            "NotificationConfig": {
                "NotificationArn": "",
                "NotificationEvents": [],
                "NotificationType": ""
            },
            "CloudWatchOutputConfig": {
                "CloudWatchLogGroupName": "",
                "CloudWatchOutputEnabled": false
            }
        }
    ]
}
```

Para obtener más información, consulte Descripción de los estados del comando en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte ListCommandInvocations en la Referencia de comandos de la AWS CLI.

`list-commands`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-commands`.

AWS CLI

Ejemplo 1: obtención del estado de un comando específico

En el siguiente ejemplo de `list-commands` se recupera y muestra el estado del comando especificado.

```
aws ssm list-commands \
    --command-id "0831e1a8-a1ac-4257-a1fd-c831bEXAMPLE"
```

Ejemplo 2: obtención del estado de los comandos solicitados después de una fecha específica

En el siguiente ejemplo de `list-commands` se recuperan los detalles de los comandos solicitados después de la fecha especificada.

```
aws ssm list-commands \
    --filter "key=InvokedAfter,value=2020-02-01T00:00:00Z"
```

Ejemplo 3: enumeración de todos los comandos solicitados en una cuenta de AWS

En el siguiente ejemplo de `list-commands` se enumeran todos los comandos que han solicitado los usuarios de la cuenta y la región de AWS actuales.

```
aws ssm list-commands
```

Salida:

```
{
    "Commands": [
        {
            "CommandId": "8bee3135-398c-4d31-99b6-e42d2EXAMPLE",
            "DocumentName": "AWS-UpdateSSMAgent",
            "DocumentVersion": "",
            "Comment": "b48291dd-ba76-43e0-
b9df-13e11ddaac26:6960febb-2907-4b59-8e1a-d6ce8EXAMPLE",
            "ExpiresAfter": "2020-02-19T11:28:02.500000-08:00",
            "Parameters": {},
            "InstanceIds": [
                "i-028ea792daEXAMPLE",
                "i-02feef8c46EXAMPLE",
                "i-038613f3f0EXAMPLE",
                "i-03a530a2d4EXAMPLE",
```

```
                "i-083b678d37EXAMPLE",
                "i-0dee81debaEXAMPLE"
            ],
            "Targets": [],
            "RequestedDateTime": "2020-02-19T10:18:02.500000-08:00",
            "Status": "Success",
            "StatusDetails": "Success",
            "OutputS3BucketName": "",
            "OutputS3KeyPrefix": "",
            "MaxConcurrency": "50",
            "MaxErrors": "100%",
            "TargetCount": 6,
            "CompletedCount": 6,
            "ErrorCount": 0,
            "DeliveryTimedOutCount": 0,
            "ServiceRole": "",
            "NotificationConfig": {
                "NotificationArn": "",
                "NotificationEvents": [],
                "NotificationType": ""
            },
            "CloudWatchOutputConfig": {
                "CloudWatchLogGroupName": "",
                "CloudWatchOutputEnabled": false
            }
        }
        {
            "CommandId": "e9ade581-c03d-476b-9b07-26667EXAMPLE",
            "DocumentName": "AWS-FindWindowsUpdates",
            "DocumentVersion": "1",
            "Comment": "",
            "ExpiresAfter": "2020-01-24T12:37:31.874000-08:00",
            "Parameters": {
                "KbArticleIds": [
                    ""
                ],
                "UpdateLevel": [
                    "All"
                ]
            },
            "InstanceIds": [],
            "Targets": [
                {
                    "Key": "InstanceIds",
```

```
                    "Values": [
                        "i-00ec29b21eEXAMPLE",
                        "i-09911ddd90EXAMPLE"
                    ]
                }
            ],
            "RequestedDateTime": "2020-01-24T11:27:31.874000-08:00",
            "Status": "Success",
            "StatusDetails": "Success",
            "OutputS3BucketName": "my-us-east-2-bucket",
            "OutputS3KeyPrefix": "my-rc-output",
            "MaxConcurrency": "50",
            "MaxErrors": "0",
            "TargetCount": 2,
            "CompletedCount": 2,
            "ErrorCount": 0,
            "DeliveryTimedOutCount": 0,
            "ServiceRole": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "NotificationConfig": {
                "NotificationArn": "arn:aws:sns:us-east-2:111222333444:my-us-east-2-
notification-arn",
                "NotificationEvents": [
                    "All"
                ],
                "NotificationType": "Invocation"
            },
            "CloudWatchOutputConfig": {
                "CloudWatchLogGroupName": "",
                "CloudWatchOutputEnabled": false
            }
        }
        {
            "CommandId": "d539b6c3-70e8-4853-80e5-0ce4fEXAMPLE",
            "DocumentName": "AWS-RunPatchBaseline",
            "DocumentVersion": "1",
            "Comment": "",
            "ExpiresAfter": "2020-01-24T12:21:04.350000-08:00",
            "Parameters": {
                "InstallOverrideList": [
                    ""
                ],
                "Operation": [
                    "Install"
```

```
                ],
                "RebootOption": [
                    "RebootIfNeeded"
                ],
                "SnapshotId": [
                    ""
                ]
            },
            "InstanceIds": [],
            "Targets": [
                {
                    "Key": "InstanceIds",
                    "Values": [
                        "i-00ec29b21eEXAMPLE",
                        "i-09911ddd90EXAMPLE"
                    ]
                }
            ],
            "RequestedDateTime": "2020-01-24T11:11:04.350000-08:00",
            "Status": "Success",
            "StatusDetails": "Success",
            "OutputS3BucketName": "my-us-east-2-bucket",
            "OutputS3KeyPrefix": "my-rc-output",
            "MaxConcurrency": "50",
            "MaxErrors": "0",
            "TargetCount": 2,
            "CompletedCount": 2,
            "ErrorCount": 0,
            "DeliveryTimedOutCount": 0,
            "ServiceRole": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "NotificationConfig": {
                "NotificationArn": "arn:aws:sns:us-east-2:111222333444:my-us-east-2-
notification-arn",
                "NotificationEvents": [
                    "All"
                ],
                "NotificationType": "Invocation"
            },
            "CloudWatchOutputConfig": {
                "CloudWatchLogGroupName": "",
                "CloudWatchOutputEnabled": false
            }
        }
```

```
    ]
}
```

Para obtener más información, consulte Running Commands Using Systems Manager Run Command en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte ListCommands en la Referencia de comandos de la AWS CLI.

`list-compliance-items`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-compliance-items`.

AWS CLI

Enumeración de los elementos de conformidad de una instancia específica

En este ejemplo se enumeran todos los elementos de conformidad de la instancia especificada.

Comando:

```
aws ssm list-compliance-items --resource-ids "i-1234567890abcdef0" --resource-
types "ManagedInstance"
```

Salida:

```
{
  "ComplianceItems": [
      {
          "ComplianceType": "Association",
          "ResourceType": "ManagedInstance",
          "ResourceId": "i-1234567890abcdef0",
          "Id": "8dfe3659-4309-493a-8755-0123456789ab",
          "Title": "",
          "Status": "COMPLIANT",
          "Severity": "UNSPECIFIED",
          "ExecutionSummary": {
              "ExecutionTime": 1550408470.0
          },
          "Details": {
              "DocumentName": "AWS-GatherSoftwareInventory",
              "DocumentVersion": "1"
          }
```

```
        },
        {
            "ComplianceType": "Association",
            "ResourceType": "ManagedInstance",
            "ResourceId": "i-1234567890abcdef0",
            "Id": "e4c2ed6d-516f-41aa-aa2a-0123456789ab",
            "Title": "",
            "Status": "COMPLIANT",
            "Severity": "UNSPECIFIED",
            "ExecutionSummary": {
                "ExecutionTime": 1550508475.0
            },
            "Details": {
                "DocumentName": "AWS-UpdateSSMAgent",
                "DocumentVersion": "1"
            }
        },
                ...
    ],
    "NextToken": "--token string truncated--"
}
```

Enumeración de los elementos de conformidad de una instancia y un ID de asociación específicos

En este ejemplo se enumeran todos los elementos de conformidad de la instancia y el ID de asociación especificados.

Comando:

```
aws ssm list-compliance-items --resource-ids "i-1234567890abcdef0" --resource-
types "ManagedInstance" --
filters "Key=ComplianceType,Values=Association,Type=EQUAL" "Key=Id,Values=e4c2ed6d-516f-41aa
aa2a-0123456789ab,Type=EQUAL"
```

Enumeración de los elementos de conformidad de una instancia después de una fecha y hora específicas

En este ejemplo se enumeran todos los elementos de conformidad de una instancia después de la fecha y hora especificada.

Comando:

```
aws ssm list-compliance-items --resource-ids "i-1234567890abcdef0" --resource-
types "ManagedInstance" --
filters "Key=ExecutionTime,Values=2019-02-18T16:00:00Z,Type=GREATER_THAN"
```

- Para obtener información sobre la API, consulte ListComplianceItems en la Referencia de comandos de la AWS CLI.

`list-compliance-summaries`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-compliance-summaries`.

AWS CLI

Enumeración de los resúmenes de conformidad de todos los tipos de conformidad

En este ejemplo se enumeran los resúmenes de conformidad de todos los tipos de conformidad de su cuenta.

Comando:

```
aws ssm list-compliance-summaries
```

Salida:

```
{
  "ComplianceSummaryItems": [
      {
          "ComplianceType": "Association",
          "CompliantSummary": {
              "CompliantCount": 2,
              "SeveritySummary": {
                  "CriticalCount": 0,
                  "HighCount": 0,
                  "MediumCount": 0,
                  "LowCount": 0,
                  "InformationalCount": 0,
                  "UnspecifiedCount": 2
              }
          },
          "NonCompliantSummary": {
              "NonCompliantCount": 0,
              "SeveritySummary": {
```

```
                    "CriticalCount": 0,
                    "HighCount": 0,
                    "MediumCount": 0,
                    "LowCount": 0,
                    "InformationalCount": 0,
                    "UnspecifiedCount": 0
                }
            }
        },
        {
            "ComplianceType": "Patch",
            "CompliantSummary": {
                "CompliantCount": 1,
                "SeveritySummary": {
                    "CriticalCount": 0,
                    "HighCount": 0,
                    "MediumCount": 0,
                    "LowCount": 0,
                    "InformationalCount": 0,
                    "UnspecifiedCount": 1
                }
            },
            "NonCompliantSummary": {
                "NonCompliantCount": 1,
                "SeveritySummary": {
                    "CriticalCount": 1,
                    "HighCount": 0,
                    "MediumCount": 0,
                    "LowCount": 0,
                    "InformationalCount": 0,
                    "UnspecifiedCount": 0
                }
            }
        },
                ...
    ],
    "NextToken": "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAyfQ=="
}
```

Enumeración de los resúmenes de conformidad de un tipo de conformidad específico

En este ejemplo se muestra el resumen de conformidad del tipo de conformidad de la revisión.

Comando:

```
aws ssm list-compliance-summaries --
filters "Key=ComplianceType,Values=Patch,Type=EQUAL"
```

- Para obtener información sobre la API, consulte ListComplianceSummaries en la Referencia de comandos de la AWS CLI.

`list-document-metadata-history`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-document-metadata-history`.

AWS CLI

Ejemplo: Visualización del historial y el estado de aprobación de una plantilla de cambios

En el siguiente ejemplo de `list-document-metadata-history`, se devuelve el historial de aprobaciones de la plantilla de cambios del administrador de cambios especificada.

```
aws ssm list-document-metadata-history \
    --name MyChangeManageTemplate \
    --metadata DocumentReviews
```

Salida:

```
{
    "Name": "MyChangeManagerTemplate",
    "DocumentVersion": "1",
    "Author": "arn:aws:iam::111222333444;:user/JohnDoe",
    "Metadata": {
        "ReviewerResponse": [
            {
                "CreateTime": "2021-07-30T11:58:28.025000-07:00",
                "UpdatedTime": "2021-07-30T12:01:19.274000-07:00",
                "ReviewStatus": "APPROVED",
                "Comment": [
                    {
                        "Type": "COMMENT",
                        "Content": "I approve this template version"
                    }
                ],
                "Reviewer": "arn:aws:iam::111222333444;:user/ShirleyRodriguez"
            },
            {
```

```
                "CreateTime": "2021-07-30T11:58:28.025000-07:00",
                "UpdatedTime": "2021-07-30T11:58:28.025000-07:00",
                "ReviewStatus": "PENDING"
            }
        ]
    }
}
```

Para obtener más información, consulte Revisión y aprobación o rechazo de las plantillas de cambios en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte ListDocumentMetadataHistory en la Referencia de comandos de la AWS CLI.

`list-document-versions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-document-versions`.

AWS CLI

Enumeración de las versiones de los documentos

En el siguiente ejemplo de `list-document-versions` se enumeran todas las versiones de un documento de Systems Manager.

```
aws ssm list-document-versions \
    --name "Example"
```

Salida:

```
{
    "DocumentVersions": [
        {
            "Name": "Example",
            "DocumentVersion": "1",
            "CreatedDate": 1583257938.266,
            "IsDefaultVersion": true,
            "DocumentFormat": "YAML",
            "Status": "Active"
        }
    ]
}
```

Para obtener más información, consulte Ejecución de comandos mediante una versión de documento específica en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte ListDocumentVersions en la Referencia de comandos de la AWS CLI.

`list-documents`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-documents`.

AWS CLI

Ejemplo 1: enumeración de documentos

En el siguiente ejemplo de `list-documents` se enumeran los documentos propiedad de la cuenta solicitante etiquetados con la etiqueta personalizada.

```
aws ssm list-documents \
    --filters Key=Owner,Values=Self Key=tag:DocUse,Values=Testing
```

Salida:

```
{
    "DocumentIdentifiers": [
        {
            "Name": "Example",
            "Owner": "29884EXAMPLE",
            "PlatformTypes": [
                "Windows",
                "Linux"
            ],
            "DocumentVersion": "1",
            "DocumentType": "Automation",
            "SchemaVersion": "0.3",
            "DocumentFormat": "YAML",
            "Tags": [
                {
                    "Key": "DocUse",
                    "Value": "Testing"
                }
            ]
        }
    ]
```

```
}
```

Para obtener más información, consulte Documentos de AWS Systems Manager en la Guía del usuario de AWS Systems Manager.

Ejemplo 2: enumeración de los documentos compartidos

En el siguiente ejemplo de `list-documents` se enumeran los documentos compartidos, incluidos los documentos compartidos privados que no son propiedad de AWS.

```
aws ssm list-documents \
    --filters Key=Name,Values=sharedDocNamePrefix  Key=Owner,Values=Private
```

Salida:

```
{
    "DocumentIdentifiers": [
        {
            "Name": "Example",
            "Owner": "12345EXAMPLE",
            "PlatformTypes": [
                "Windows",
                "Linux"
            ],
            "DocumentVersion": "1",
            "DocumentType": "Command",
            "SchemaVersion": "0.3",
            "DocumentFormat": "YAML",
            "Tags": []
        }
    ]
}
```

Para obtener más información, consulte Documentos de AWS Systems Manager en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte ListDocuments en la Referencia de comandos de la AWS CLI.

`list-inventory-entries`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-inventory-entries`.

AWS CLI

Ejemplo 1: visualización de las entradas de tipos de inventario específicos de una instancia

En el siguiente ejemplo de `list-inventory-entries` se enumeran las entradas de inventario del tipo de inventario AWS:Application en una instancia específica.

```
aws ssm list-inventory-entries \
    --instance-id "i-1234567890abcdef0" \
    --type-name "AWS:Application"
```

Salida:

```
{
  "TypeName": "AWS:Application",
  "InstanceId": "i-1234567890abcdef0",
  "SchemaVersion": "1.1",
  "CaptureTime": "2019-02-15T12:17:55Z",
  "Entries": [
    {
      "Architecture": "i386",
      "Name": "Amazon SSM Agent",
      "PackageId": "{88a60be2-89a1-4df8-812a-80863c2a2b68}",
      "Publisher": "Amazon Web Services",
      "Version": "2.3.274.0"
    },
    {
      "Architecture": "x86_64",
      "InstalledTime": "2018-05-03T13:42:34Z",
      "Name": "AmazonCloudWatchAgent",
      "Publisher": "",
      "Version": "1.200442.0"
    }
  ]
}
```

Ejemplo 2: visualización de las entradas de inventario personalizadas asignadas a una instancia

En el siguiente ejemplo de `list-inventory-entries` se muestra una entrada de inventario personalizada asignada a una instancia.

```
aws ssm list-inventory-entries \
    --instance-id "i-1234567890abcdef0" \
```

```
    --type-name "Custom:RackInfo"
```

Salida:

```
{
  "TypeName": "Custom:RackInfo",
  "InstanceId": "i-1234567890abcdef0",
  "SchemaVersion": "1.0",
  "CaptureTime": "2021-05-22T10:01:01Z",
  "Entries": [
    {
      "RackLocation": "Bay B/Row C/Rack D/Shelf E"
    }
  ]
}
```

- Para obtener información sobre la API, consulte ListInventoryEntries en la Referencia de comandos de la AWS CLI.

`list-ops-item-related-items`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-ops-item-related-items`.

AWS CLI

Para enumerar los recursos de elementos relacionados de un OpsItem

En el siguiente ejemplo de `list-ops-item-related-items`, se enumeran los recursos de elementos relacionados de un OpsItem.

```
aws ssm list-ops-item-related-items \
    --ops-item-id "oi-f99f2EXAMPLE"
```

Salida:

```
{
    "Summaries": [
        {
            "OpsItemId": "oi-f99f2EXAMPLE",
            "AssociationId": "e2036148-cccb-490e-ac2a-390e5EXAMPLE",
            "ResourceType": "AWS::SSMIncidents::IncidentRecord",
            "AssociationType": "IsParentOf",
```

```
            "ResourceUri": "arn:aws:ssm-incidents::111122223333:incident-record/
example-response/64bd9b45-1d0e-2622-840d-03a87a1451fa",
            "CreatedBy": {
                "Arn": "arn:aws:sts::111122223333:assumed-role/
AWSServiceRoleForIncidentManager/IncidentResponse"
            },
            "CreatedTime": "2021-08-11T18:47:14.994000+00:00",
            "LastModifiedBy": {
                "Arn": "arn:aws:sts::111122223333:assumed-role/
AWSServiceRoleForIncidentManager/IncidentResponse"
            },
            "LastModifiedTime": "2021-08-11T18:47:14.994000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Working with Incident Manager incidents in OpsCenter en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte ListOpsItemRelatedItems en la Referencia de comandos de la AWS CLI.

`list-resource-compliance-summaries`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-compliance-summaries`.

AWS CLI

Cómo enumerar los recuentos resumidos de conformidad para cada recurso

En este ejemplo se enumeran los recuentos resumidos de conformidad para cada recurso.

Comando:

```
aws ssm list-resource-compliance-summaries
```

Salida:

```
{
  "ResourceComplianceSummaryItems": [
      {
          "ComplianceType": "Association",
```

```
            "ResourceType": "ManagedInstance",
            "ResourceId": "i-1234567890abcdef0",
            "Status": "COMPLIANT",
            "OverallSeverity": "UNSPECIFIED",
            "ExecutionSummary": {
                "ExecutionTime": 1550509273.0
            },
            "CompliantSummary": {
                "CompliantCount": 2,
                "SeveritySummary": {
                    "CriticalCount": 0,
                    "HighCount": 0,
                    "MediumCount": 0,
                    "LowCount": 0,
                    "InformationalCount": 0,
                    "UnspecifiedCount": 2
                }
            },
            "NonCompliantSummary": {
                "NonCompliantCount": 0,
                "SeveritySummary": {
                    "CriticalCount": 0,
                    "HighCount": 0,
                    "MediumCount": 0,
                    "LowCount": 0,
                    "InformationalCount": 0,
                    "UnspecifiedCount": 0
                }
            }
        },
        {
            "ComplianceType": "Patch",
            "ResourceType": "ManagedInstance",
            "ResourceId": "i-9876543210abcdef0",
            "Status": "COMPLIANT",
            "OverallSeverity": "UNSPECIFIED",
            "ExecutionSummary": {
                "ExecutionTime": 1550248550.0,
                "ExecutionId": "7abb6378-a4a5-4f10-8312-0123456789ab",
                "ExecutionType": "Command"
            },
            "CompliantSummary": {
                "CompliantCount": 397,
                "SeveritySummary": {
```

```
                "CriticalCount": 0,
                "HighCount": 0,
                "MediumCount": 0,
                "LowCount": 0,
                "InformationalCount": 0,
                "UnspecifiedCount": 397
            }
        },
        "NonCompliantSummary": {
            "NonCompliantCount": 0,
            "SeveritySummary": {
                "CriticalCount": 0,
                "HighCount": 0,
                "MediumCount": 0,
                "LowCount": 0,
                "InformationalCount": 0,
                "UnspecifiedCount": 0
            }
        }
    }
  ],
  "NextToken": "--token string truncated--"
}
```

Cómo enumerar los resúmenes de conformidad de un tipo de conformidad específico para cada recurso

En este ejemplo se enumeran los resúmenes de conformidad de cada recurso del tipo de conformidad de la revisión.

Comando:

```
aws ssm list-resource-compliance-summaries --
filters "Key=ComplianceType,Values=Patch,Type=EQUAL"
```

- Para obtener información sobre la API, consulte ListResourceComplianceSummaries en la Referencia del comando de la AWS CLI.

`list-resource-data-sync`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-data-sync`.

AWS CLI

Para enumerar las configuraciones de sincronización de datos de recursos

En este ejemplo, se recupera información sobre las configuraciones de sincronización de los datos de los recursos.

```
aws ssm list-resource-data-sync
```

Salida:

```
{
    "ResourceDataSyncItems": [
        {
            "SyncName": "MyResourceDataSync",
            "S3Destination": {
                "BucketName": "ssm-resource-data-sync",
                "SyncFormat": "JsonSerDe",
                "Region": "us-east-1"
            },
            "LastSyncTime": 1550261472.003,
            "LastSuccessfulSyncTime": 1550261472.003,
            "LastStatus": "Successful",
            "SyncCreatedTime": 1543235736.72,
            "LastSyncStatusMessage": "The sync was successfully completed"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListResourceDataSync en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Cómo enumerar las etiquetas aplicadas a una línea de base de revisiones

En el siguiente ejemplo de `list-tags-for-resource` se muestran las etiquetas de una línea de base de revisiones.

```
aws ssm list-tags-for-resource \
    --resource-type "PatchBaseline" \
    --resource-id "pb-0123456789abcdef0"
```

Salida:

```
{
    "TagList": [
        {
            "Key": "Environment",
            "Value": "Production"
        },
        {
            "Key": "Region",
            "Value": "EMEA"
        }
    ]
}
```

Para obtener más información, consulte Tagging AWS Resources en la Referencia general de AWS.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`modify-document-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-document-permission`.

AWS CLI

Modificación de los permisos de los documentos

En el siguiente ejemplo de `modify-document-permission` se comparte un documento de Systems Manager públicamente.

```
aws ssm modify-document-permission \
    --name "Example" \
    --permission-type "Share" \
    --account-ids-to-add "All"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Compartir un documento de Systems Manager en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte ModifyDocumentPermission en la Referencia de comandos de la AWS CLI.

`put-compliance-items`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-compliance-items`.

AWS CLI

Registro de un tipo de conformidad y de los detalles de conformidad en una instancia designada

En este ejemplo se registra el tipo de conformidad `Custom:AVCheck` en la instancia administrada especificada. No se obtienen resultados si el comando se ejecuta satisfactoriamente.

Comando:

```
aws ssm put-compliance-items --resource-id "i-1234567890abcdef0" --
resource-type "ManagedInstance" --compliance-type "Custom:AVCheck"
 --execution-summary "ExecutionTime=2019-02-18T16:00:00Z" --
items "Id=Version2.0,Title=ScanHost,Severity=CRITICAL,Status=COMPLIANT"
```

- Para obtener información sobre la API, consulte PutComplianceItems en la Referencia de comandos de la AWS CLI.

`put-inventory`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-inventory`.

AWS CLI

Cómo asignar metadatos de cliente a una instancia

En este ejemplo se asigna información de ubicación de bastidores a una instancia. No se obtienen resultados si el comando se ejecuta satisfactoriamente.

Comando (Linux):

```
aws ssm put-inventory --instance-id "i-016648b75dd622dab" --items
 '[{"TypeName": "Custom:RackInfo","SchemaVersion": "1.0","CaptureTime":
 "2019-01-22T10:01:01Z","Content":[{"RackLocation": "Bay B/Row C/Rack D/Shelf
 E"}]}]'
```

Comando (Windows):

```
aws ssm put-inventory --instance-id "i-016648b75dd622dab" --
items "TypeName=Custom:RackInfo,SchemaVersion=1.0,CaptureTime=2019-01-22T10:01:01Z,Content=[
 B/Row C/Rack D/Shelf F'}]"
```

- Para obtener información sobre la API, consulte PutInventory en la Referencia de comandos de la AWS CLI.

`put-parameter`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-parameter`.

AWS CLI

Ejemplo 1: Cambio del valor de un parámetro

En el siguiente ejemplo de `put-parameter` se cambia el valor del parámetro especificado.

```
aws ssm put-parameter \
    --name "MyStringParameter" \
    --type "String" \
    --value "Vici" \
    --overwrite
```

Salida:

```
{
    "Version": 2,
    "Tier": "Standard"
}
```

Para obtener más información, consulte Crear un parámetro de Systems Manager (CLI de AWS), Administración de niveles de parámetros y Trabajo con políticas de parámetros en la Guía del usuario de AWS Systems Manager.

Ejemplo 2: Creación de un parámetro avanzado

En el siguiente ejemplo de `put-parameter` se crea un parámetro avanzado.

```
aws ssm put-parameter \
    --name "MyAdvancedParameter" \
    --description "This is an advanced parameter" \
    --value "Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod
 tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam,
 quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat
 [truncated]" \
    --type "String" \
    --tier Advanced
```

Salida:

```
{
    "Version": 1,
    "Tier": "Advanced"
}
```

Para obtener más información, consulte Crear un parámetro de Systems Manager (CLI de AWS), Administración de niveles de parámetros y Trabajo con políticas de parámetros en la Guía del usuario de AWS Systems Manager.

Ejemplo 3: cambio de un parámetro estándar a un parámetro avanzado

En el siguiente ejemplo de `put-parameter`, se convierte un parámetro estándar existente en un parámetro avanzado.

```
aws ssm put-parameter \
    --name "MyConvertedParameter" \
    --value "abc123" \
    --type "String" \
    --tier Advanced \
    --overwrite
```

Salida:

```
{
    "Version": 2,
```

```
    "Tier": "Advanced"
}
```

Para obtener más información, consulte Crear un parámetro de Systems Manager (CLI de AWS), Administración de niveles de parámetros y Trabajo con políticas de parámetros en la Guía del usuario de AWS Systems Manager.

Ejemplo 4: creación de un parámetro con una política adjunta

En el siguiente ejemplo de `put-parameter` se crea un parámetro avanzado con una política de parámetros adjunta.

```
aws ssm put-parameter \
    --name "/Finance/Payroll/q2accesskey" \
    --value "P@sSwW)rd" \
    --type "SecureString" \
    --tier Advanced \
    --policies "[{\"Type\":\"Expiration\",\"Version\":\"1.0\",\"Attributes\":
{\"Timestamp\":\"2020-06-30T00:00:00.000Z\"}},{\"Type\":\"ExpirationNotification\",
\"Version\":\"1.0\",\"Attributes\":{\"Before\":\"5\",\"Unit\":\"Days\"}},{\"Type\":
\"NoChangeNotification\",\"Version\":\"1.0\",\"Attributes\":{\"After\":\"60\",\"Unit
\":\"Days\"}}]"
```

Salida:

```
{
    "Version": 1,
    "Tier": "Advanced"
}
```

Para obtener más información, consulte Crear un parámetro de Systems Manager (CLI de AWS), Administración de niveles de parámetros y Trabajo con políticas de parámetros en la Guía del usuario de AWS Systems Manager.

Ejemplo 5: adición de una política a un parámetro existente

En el siguiente ejemplo de `put-parameter` se asocia una política a un parámetro avanzado existente.

```
aws ssm put-parameter \
    --name "/Finance/Payroll/q2accesskey" \
```

```
    --value "N3wP@sSwW)rd" \
    --type "SecureString" \
    --tier Advanced \
    --policies "[{\"Type\":\"Expiration\",\"Version\":\"1.0\",\"Attributes\":
{\"Timestamp\":\"2020-06-30T00:00:00.000Z\"}},{\"Type\":\"ExpirationNotification\",
\"Version\":\"1.0\",\"Attributes\":{\"Before\":\"5\",\"Unit\":\"Days\"}},{\"Type\":
\"NoChangeNotification\",\"Version\":\"1.0\",\"Attributes\":{\"After\":\"60\",\"Unit
\":\"Days\"}}]"
    --overwrite
```

Salida:

```
{
    "Version": 2,
    "Tier": "Advanced"
}
```

Para obtener más información, consulte Crear un parámetro de Systems Manager (CLI de AWS), Administración de niveles de parámetros y Trabajo con políticas de parámetros en la Guía del usuario de AWS Systems Manager.

- Para obtener información acerca de la API, consulte PutParameter en la Referencia de comandos de la AWS CLI.

`register-default-patch-baseline`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-default-patch-baseline`.

AWS CLI

Configuración de la línea de base de revisiones predeterminada

En el siguiente ejemplo de `register-default-patch-baseline` se registra la línea de base de revisiones personalizada especificada como la línea de base de revisiones predeterminada para el tipo de sistema operativo que admite.

```
aws ssm register-default-patch-baseline \
    --baseline-id "pb-abc123cf9bEXAMPLE"
```

Salida:

```
{
    "BaselineId":"pb-abc123cf9bEXAMPLE"
}
```

En el siguiente ejemplo de `register-default-patch-baseline` se registra la línea de base de revisiones predeterminada que ha proporcionado AWS para CentOS como la línea de base de revisiones predeterminada.

```
aws ssm register-default-patch-baseline \
    --baseline-id "arn:aws:ssm:us-east-2:733109147000:patchbaseline/
pb-0574b43a65ea646ed"
```

Salida:

```
{
    "BaselineId":"pb-abc123cf9bEXAMPLE"
}
```

Para obtener más información, consulte Acerca de las líneas de base de revisiones personalizadas y predefinidas en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte RegisterDefaultPatchBaseline en la Referencia de comandos de la AWS CLI.

`register-patch-baseline-for-patch-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-patch-baseline-for-patch-group`.

AWS CLI

Registro de una línea de base de revisiones de un grupo de revisiones

En el siguiente ejemplo de `register-patch-baseline-for-patch-group` se registra una línea de base de revisiones para un grupo de revisiones.

```
aws ssm register-patch-baseline-for-patch-group \
    --baseline-id "pb-045f10b4f382baeda" \
    --patch-group "Production"
```

Salida:

```
{
    "BaselineId": "pb-045f10b4f382baeda",
    "PatchGroup": "Production"
}
```

Para obtener más información, consulte Creación de un grupo de revisiones <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-group-tagging.html>__ y Añadir un grupo de revisiones a una línea de base de revisiones en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte RegisterPatchBaselineForPatchGroup en la Referencia de comandos de la AWS CLI.

`register-target-with-maintenance-window`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-target-with-maintenance-window`.

AWS CLI

Ejemplo 1: registro de un único destino con un periodo de mantenimiento

En el siguiente ejemplo de `register-target-with-maintenance-window` se registra una instancia con un periodo de mantenimiento.

```
aws ssm register-target-with-maintenance-window \
    --window-id "mw-ab12cd34ef56gh78" \
    --target "Key=InstanceIds,Values=i-0000293ffd8c57862" \
    --owner-information "Single instance" \
    --resource-type "INSTANCE"
```

Salida:

```
{
    "WindowTargetId":"1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

Ejemplo 2: registro de varios destinos con un periodo de mantenimiento mediante los ID de instancia

En el siguiente ejemplo de `register-target-with-maintenance-window` se registran dos instancias con un periodo de mantenimiento especificando sus ID de instancia.

```
aws ssm register-target-with-maintenance-window \
    --window-id "mw-ab12cd34ef56gh78" \
    --target "Key=InstanceIds,Values=i-0000293ffd8c57862,i-0cb2b964d3e14fd9f" \
    --owner-information "Two instances in a list" \
    --resource-type "INSTANCE"
```

Salida:

```
{
    "WindowTargetId":"1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

Ejemplo 3: registro de destinos con un periodo de mantenimiento mediante etiquetas de recursos

En el siguiente ejemplo de `register-target-with-maintenance-window` se registran las instancias con un periodo de mantenimiento especificando las etiquetas de recursos que se han aplicado a las instancias.

```
aws ssm register-target-with-maintenance-window \
    --window-id "mw-06cf17cbefcb4bf4f" \
    --targets "Key=tag:Environment,Values=Prod" "Key=Role,Values=Web" \
    --owner-information "Production Web Servers" \
    --resource-type "INSTANCE"
```

Salida:

```
{
    "WindowTargetId":"1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

Ejemplo 4: registro de destinos mediante un grupo de claves de etiquetas

En el siguiente ejemplo de `register-target-with-maintenance-window` se registran instancias que tienen una o más claves asignadas, independientemente de los valores de la clave.

```
aws ssm register-target-with-maintenance-window \
```

```
    --window-id "mw-0c50858d01EXAMPLE" \
    --resource-type "INSTANCE" \
    --target "Key=tag-key,Values=Name,Instance-Type,CostCenter"
```

Salida:

```
{
    "WindowTargetId":"1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

Ejemplo 5: registro de destinos con un nombre de grupo de recursos

En el siguiente ejemplo de `register-target-with-maintenance-window` se registra un grupo de recursos especificado, independientemente del tipo de recursos que contiene.

```
aws ssm register-target-with-maintenance-window \
    --window-id "mw-0c50858d01EXAMPLE" \
    --resource-type "RESOURCE_GROUP" \
    --target "Key=resource-groups:Name,Values=MyResourceGroup"
```

Salida:

```
{
    "WindowTargetId":"1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

Para obtener más información, consulte Registrar una instancia de destino con el periodo de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte RegisterTargetWithMaintenanceWindow en la Referencia de comandos de la AWS CLI.

`register-task-with-maintenance-window`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-task-with-maintenance-window`.

AWS CLI

Ejemplo 1: registro de una tarea de Automatización con un periodo de mantenimiento

En el siguiente ejemplo de `register-task-with-maintenance-window` se registra una tarea de Automatización con un periodo de mantenimiento destinado a una instancia.

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-082dcd7649EXAMPLE" \
    --targets Key=InstanceIds,Values=i-1234520122EXAMPLE \
    --task-arn AWS-RestartEC2Instance \
    --service-role-arn arn:aws:iam::111222333444:role/SSM --task-type AUTOMATION \
    --task-invocation-parameters "{\"Automation\":{\"DocumentVersion\":\"\$LATEST\",
\"Parameters\":{\"InstanceId\":[\"{{RESOURCE_ID}}\"]}}}" \
    --priority 0 \
    --max-concurrency 1 \
    --max-errors 1 \
    --name "AutomationExample" \
    --description "Restarting EC2 Instance for maintenance"
```

Salida:

```
{
    "WindowTaskId":"11144444-5555-6666-7777-88888888"
}
```

Para obtener más información, consulte Registrar una tarea con el periodo de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

Ejemplo 2: registro de una tarea de Lambda con un periodo de mantenimiento

En el siguiente ejemplo de `register-task-with-maintenance-window` se registra una tarea de Lambda con un periodo de mantenimiento destinado a una instancia.

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-082dcd7649dee04e4" \
    --targets Key=InstanceIds,Values=i-12344d305eEXAMPLE \
    --task-arn arn:aws:lambda:us-east-1:111222333444:function:SSMTestLAMBDA \
    --service-role-arn arn:aws:iam::111222333444:role/SSM \
    --task-type LAMBDA \
    --task-invocation-parameters '{"Lambda":{"Payload":"{\"InstanceId\":
\"{{RESOURCE_ID}}\",\"targetType\":\"{{TARGET_TYPE}}\"}","Qualifier":"$LATEST"}}' \
    --priority 0 \
    --max-concurrency 10 \
    --max-errors 5 \
    --name "Lambda_Example" \
```

```
    --description "My Lambda Example"
```

Salida:

```
{
    "WindowTaskId":"22244444-5555-6666-7777-88888888"
}
```

Para obtener más información, consulte Registrar una tarea con el periodo de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

Ejemplo 3: registro de una tarea de ejecución de un comando con un periodo de mantenimiento

En el siguiente ejemplo de `register-task-with-maintenance-window` se registra una tarea de ejecución de un comando con un periodo de mantenimiento destinado a una instancia.

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-082dcd7649dee04e4" \
    --targets "Key=InstanceIds,Values=i-12344d305eEXAMPLE" \
    --service-role-arn "arn:aws:iam::111222333444:role/SSM" \
    --task-type "RUN_COMMAND" \
    --name "SSMInstallPowerShellModule" \
    --task-arn "AWS-InstallPowerShellModule" \
    --task-invocation-parameters "{\"RunCommand\":{\"Comment\":\"\",
\"OutputS3BucketName\":\"runcommandlogs\",\"Parameters\":{\"commands\":[\"Get-
Module -ListAvailable\"],\"executionTimeout\":[\"3600\"],\"source\":[\"https:\/
\/gallery.technet.microsoft.com\/EZOut-33ae0fb7\/file\/110351\/1\/EZOut.zip\"],
\"workingDirectory\":[\"\\\\\"]},\"TimeoutSeconds\":600}}" \
    --max-concurrency 1 \
    --max-errors 1 \
    --priority 10
```

Salida:

```
{
    "WindowTaskId":"33344444-5555-6666-7777-88888888"
}
```

Para obtener más información, consulte Registrar una tarea con el periodo de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

Ejemplo 4: registro de una tarea de Step Functions con un periodo de mantenimiento

En el siguiente ejemplo de `register-task-with-maintenance-window` se registra una tarea de Step Functions con un periodo de mantenimiento destinado a una instancia.

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-1234d787d6EXAMPLE" \
    --targets Key=WindowTargetIds,Values=12347414-69c3-49f8-95b8-ed2dcEXAMPLE \
    --task-arn arn:aws:states:us-
east-1:111222333444:stateMachine:SSMTestStateMachine \
    --service-role-arn arn:aws:iam::111222333444:role/MaintenanceWindows \
    --task-type STEP_FUNCTIONS \
    --task-invocation-parameters '{"StepFunctions":{"Input":"{\"InstanceId\":
\"{{RESOURCE_ID}}\"}"}}' \
    --priority 0 \
    --max-concurrency 10 \
    --max-errors 5 \
    --name "Step_Functions_Example" \
    --description "My Step Functions Example"
```

Salida:

```
{
    "WindowTaskId":"44444444-5555-6666-7777-88888888"
}
```

Para obtener más información, consulte Registrar una tarea con el periodo de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

Ejemplo 5: registro de una tarea mediante un ID de destino de un periodo de mantenimiento

En el siguiente ejemplo de `register-task-with-maintenance-window` se registra una tarea mediante un ID de destino de un periodo de mantenimiento. El ID de destino del periodo de mantenimiento estaba en el resultado del comando `aws ssm register-target-with-maintenance-window`. También puede recuperarlo del resultado del comando `aws ssm describe-maintenance-window-targets`.

```
aws ssm register-task-with-maintenance-window \
    --targets "Key=WindowTargetIds,Values=350d44e6-28cc-44e2-951f-4b2c9EXAMPLE" \
    --task-arn "AWS-RunShellScript" \
    --service-role-arn "arn:aws:iam::111222333444:role/MaintenanceWindowsRole" \
    --window-id "mw-ab12cd34eEXAMPLE" \
    --task-type "RUN_COMMAND" \
    --task-parameters  "{\"commands\":{\"Values\":[\"df\"]}}" \
```

```
    --max-concurrency 1 \
    --max-errors 1 \
    --priority 10
```

Salida:

```
{
    "WindowTaskId":"33344444-5555-6666-7777-88888888"
}
```

Para obtener más información, consulte Registrar una tarea con el periodo de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte RegisterTaskWithMaintenanceWindow en la Referencia de comandos de la AWS CLI.

`remove-tags-from-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-tags-from-resource`.

AWS CLI

Cómo eliminar una etiqueta de una línea de base de revisiones

En el siguiente ejemplo de `remove-tags-from-resource` se eliminan las etiquetas de una línea de base de revisiones.

```
aws ssm remove-tags-from-resource \
    --resource-type "PatchBaseline" \
    --resource-id "pb-0123456789abcdef0" \
    --tag-keys "Region"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging AWS Resources en la Referencia general de AWS.

- Para obtener información sobre la API, consulte RemoveTagsFromResource en la Referencia de comandos de la AWS CLI.

`reset-service-setting`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-service-setting`.

AWS CLI

Para restablecer la configuración del servicio para el rendimiento del almacén de parámetros

En el siguiente ejemplo de `reset-service-setting`, se restablece la configuración del servicio para el rendimiento del almacén de parámetros en la región especificada para que deje de utilizar el rendimiento incrementado.

```
aws ssm reset-service-setting \
    --setting-id arn:aws:ssm:us-east-1:123456789012:servicesetting/ssm/parameter-store/high-throughput-enabled
```

Salida:

```
{
    "ServiceSetting": {
        "SettingId": "/ssm/parameter-store/high-throughput-enabled",
        "SettingValue": "false",
        "LastModifiedDate": 1555532818.578,
        "LastModifiedUser": "System",
        "ARN": "arn:aws:ssm:us-east-1:123456789012:servicesetting/ssm/parameter-store/high-throughput-enabled",
        "Status": "Default"
    }
}
```

Para obtener más información, consulte Aumentar o disminuir el rendimiento de Parameter Store en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte ResetServiceSetting en la Referencia de comandos de la AWS CLI.

`resume-session`

En el siguiente ejemplo de código, se muestra cómo utilizar `resume-session`.

AWS CLI

Para reanudar una sesión de Session Manager

En este ejemplo de `resume-session`, se reanuda una sesión de Session Manager con una instancia después de haberla desconectado. Tenga en cuenta que este comando interactivo requiere que el complemento Session Manager esté instalado en la máquina cliente que realiza la llamada.

```
aws ssm resume-session \
    --session-id Mary-Major-07a16060613c408b5
```

Salida:

```
{
    "SessionId": "Mary-Major-07a16060613c408b5",
    "TokenValue":
 "AAEAAVbTGsaOnyvcUoNGqifbv5r/8lgxuQljCuY8qVcvOnoBAAAAAFxtd3jIXAFUUXGTJ7zF/
AWJPwDviOlF5p3dlAgrqVIVO6IEXhkHLz0/1gXKRKEME71E6TLOplLDJAMZ
+kREejkZu4c5AxMkrQjMF+gtHP1bYJKTwtHQd1wjulPLexO8SHl7g5R/
wekrj6WsDUpnEegFBfGftpAIz2GXQVfTJXKfkc5qepQ11C11DOIT2dozOqXgHwfQHfAKLErM5dWDZqKwyT1Z3iw7unQd
+ihfGa6MEJJ97Jmat/a2TspEnOjNn9Mvu5iwXIW2yCvWZrGUj+/
QI5Xr7s1XJBEnSKR54o4fN0GV9RWl0RZsZm1m1ki0JJtiwwgZ",
    "StreamUrl": "wss://ssmmessages.us-east-2.amazonaws.com/v1/data-channel/Mary-
Major-07a16060613c408b5?role=publish_subscribe"
}
```

Para obtener más información, consulte Instalación del complemento de Session Manager para la AWS CLI en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte ResumeSession en la Referencia de comandos de la AWS CLI.

`send-automation-signal`

En el siguiente ejemplo de código, se muestra cómo utilizar `send-automation-signal`.

AWS CLI

Para enviar una señal a una ejecución de automatización

En el siguiente ejemplo de `send-automation-signal`, se envía una señal de aprobación a una ejecución de automatización.

```
aws ssm send-automation-signal \
    --automation-execution-id 73c8eef8-f4ee-4a05-820c-e354fEXAMPLE \
    --signal-type "Approve"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Ejecución de una automatización que requiere aprobaciones en la Guía del usuario de AWS Systems Manager.

- Para obtener detalles sobre la API, consulte SendAutomationSignal en la Referencia de comandos de la AWS CLI.

`send-command`

En el siguiente ejemplo de código, se muestra cómo utilizar `send-command`.

AWS CLI

Ejemplo 1: ejecución de un comando en una o más instancias remotas

En el siguiente ejemplo de `send-command` se ejecuta un comando `echo` en una instancia de destino.

```
aws ssm send-command \
    --document-name "AWS-RunShellScript" \
    --parameters 'commands=["echo HelloWorld"]' \
    --targets "Key=instanceids,Values=i-1234567890abcdef0" \
    --comment "echo HelloWorld"
```

Salida:

```
{
    "Command": {
        "CommandId": "92853adf-ba41-4cd6-9a88-142d1EXAMPLE",
        "DocumentName": "AWS-RunShellScript",
        "DocumentVersion": "",
        "Comment": "echo HelloWorld",
        "ExpiresAfter": 1550181014.717,
        "Parameters": {
```

```
            "commands": [
                "echo HelloWorld"
            ]
        },
        "InstanceIds": [
            "i-0f00f008a2dcbefe2"
        ],
        "Targets": [],
        "RequestedDateTime": 1550173814.717,
        "Status": "Pending",
        "StatusDetails": "Pending",
        "OutputS3BucketName": "",
        "OutputS3KeyPrefix": "",
        "MaxConcurrency": "50",
        "MaxErrors": "0",
        "TargetCount": 1,
        "CompletedCount": 0,
        "ErrorCount": 0,
        "DeliveryTimedOutCount": 0,
        "ServiceRole": "",
        "NotificationConfig": {
            "NotificationArn": "",
            "NotificationEvents": [],
            "NotificationType": ""
        },
        "CloudWatchOutputConfig": {
            "CloudWatchLogGroupName": "",
            "CloudWatchOutputEnabled": false
        }
    }
}
```

Para obtener más información, consulte Running Commands Using Systems Manager Run Command en la Guía del usuario de AWS Systems Manager.

Ejemplo 2: obtención de información sobre la IP de una instancia

En el siguiente ejemplo de `send-command` se obtiene información sobre la IP de una instancia.

```
aws ssm send-command \
    --instance-ids "i-1234567890abcdef0" \
    --document-name "AWS-RunShellScript" \
    --comment "IP config" \
```

```
    --parameters "commands=ifconfig"
```

Consulte el ejemplo 1 para ver una salida de muestra.

Para obtener más información, consulte Running Commands Using Systems Manager Run Command en la Guía del usuario de AWS Systems Manager.

Ejemplo 3: ejecución de un comando en instancias con etiquetas específicas

En el siguiente ejemplo de `send-command` se ejecuta un comando en instancias que tienen la clave de etiqueta “ENV” y el valor “Dev”.

```
aws ssm send-command \
    --targets "Key=tag:ENV,Values=Dev" \
    --document-name "AWS-RunShellScript" \
    --parameters "commands=ifconfig"
```

Consulte el ejemplo 1 para ver una salida de muestra.

Para obtener más información, consulte Running Commands Using Systems Manager Run Command en la Guía del usuario de AWS Systems Manager.

Ejemplo 4: ejecución de un comando que envía notificaciones de SNS

En el siguiente ejemplo de `send-command` se ejecuta un comando que envía notificaciones de SNS para todos los eventos de notificación y el tipo de notificación `Command`.

```
aws ssm send-command \
    --instance-ids "i-1234567890abcdef0" \
    --document-name "AWS-RunShellScript" \
    --comment "IP config" \
    --parameters "commands=ifconfig" \
    --service-role-arn "arn:aws:iam::123456789012:role/SNS_Role" \
    --notification-config "NotificationArn=arn:aws:sns:us-
east-1:123456789012:SNSTopicName,NotificationEvents=All,NotificationType=Command"
```

Consulte el ejemplo 1 para ver una salida de muestra.

Para obtener más información, consulte Running Commands Using Systems Manager Run Command en la Guía del usuario de AWS Systems Manager.

Ejemplo 5: ejecución de un comando que genera un resultado en S3 y CloudWatch

En el siguiente ejemplo de `send-command` se ejecuta un comando que envía los detalles del comando a un bucket de S3 y a un grupo de registro de Registros de CloudWatch.

```
aws ssm send-command \
    --instance-ids "i-1234567890abcdef0" \
    --document-name "AWS-RunShellScript" \
    --comment "IP config" \
    --parameters "commands=ifconfig" \
    --output-s3-bucket-name "s3-bucket-name" \
    --output-s3-key-prefix "runcommand" \
    --cloud-watch-output-
config "CloudWatchOutputEnabled=true,CloudWatchLogGroupName=CWLGroupName"
```

Consulte el ejemplo 1 para ver una salida de muestra.

Para obtener más información, consulte Running Commands Using Systems Manager Run Command en la Guía del usuario de AWS Systems Manager.

Ejemplo 6: ejecución de comandos en varias instancias con etiquetas diferentes

En el siguiente ejemplo de `send-command` se ejecuta un comando en instancias con dos claves y valores de etiqueta diferentes.

```
aws ssm send-command \
    --document-name "AWS-RunPowerShellScript" \
    --parameters commands=["echo helloWorld"] \
    --targets Key=tag:Env,Values=Dev Key=tag:Role,Values=WebServers
```

Consulte el ejemplo 1 para ver una salida de muestra.

Para obtener más información, consulte Running Commands Using Systems Manager Run Command en la Guía del usuario de AWS Systems Manager.

Ejemplo 7: definición de varias instancias como destino con la misma clave de etiqueta

En el siguiente ejemplo de `send-command` se ejecuta un comando en instancias que tienen la misma clave de etiqueta, pero con valores diferentes.

```
aws ssm send-command \
    --document-name "AWS-RunPowerShellScript" \
    --parameters commands=["echo helloWorld"] \
    --targets Key=tag:Env,Values=Dev,Test
```

Consulte el ejemplo 1 para ver una salida de muestra.

Para obtener más información, consulte Running Commands Using Systems Manager Run Command en la Guía del usuario de AWS Systems Manager.

Ejemplo 8: ejecución de un comando que usa un documento compartido

En el siguiente ejemplo de `send-command` se ejecuta un documento compartido en una instancia de destino.

```
aws ssm send-command \
    --document-name "arn:aws:ssm:us-east-1:123456789012:document/ExampleDocument" \
    --targets "Key=instanceids,Values=i-1234567890abcdef0"
```

Consulte el ejemplo 1 para ver una salida de muestra.

Para obtener más información, consulte Uso compartido de documentos de SSM en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte SendCommand en la Referencia de comandos de la AWS CLI.

`start-associations-once`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-associations-once`.

AWS CLI

Para ejecutar una asociación de forma inmediata y solo una vez

En el siguiente ejemplo de `start-associations-once`, se ejecuta la asociación especificada inmediatamente y solo una vez. No se obtienen resultados si el comando se ejecuta satisfactoriamente.

```
aws ssm start-associations-once \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Visualización de los historiales de asociación en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte StartAssociationsOnce en la Referencia de comandos de la AWS CLI.

`start-automation-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-automation-execution`.

AWS CLI

Ejemplo 1: ejecución de un documento de automatización

En el siguiente ejemplo de `start-automation-execution` se ejecuta un documento de Automatización.

```
aws ssm start-automation-execution \
    --document-name "AWS-UpdateLinuxAmi" \
    --parameters "AutomationAssumeRole=arn:aws:iam::123456789012:role/
SSMAutomationRole,SourceAmiId=ami-EXAMPLE,IamInstanceProfileName=EC2InstanceRole"
```

Salida:

```
{
  "AutomationExecutionId": "4105a4fc-f944-11e6-9d32-0a1b2EXAMPLE"
}
```

Para obtener más información, consulte Ejecución manual de un flujo de trabajo de Automatización en la Guía del usuario de AWS Systems Manager.

Ejemplo 2: ejecución de un documento de automatización compartido

En el siguiente ejemplo de `start-automation-execution` se ejecuta un documento de Automatización compartido.

```
aws ssm start-automation-execution \
    --document-name "arn:aws:ssm:us-east-1:123456789012:document/ExampleDocument"
```

Salida:

```
{
  "AutomationExecutionId": "4105a4fc-f944-11e6-9d32-0a1b2EXAMPLE"
}
```

Para obtener más información, consulte Uso compartido de documentos de SSM en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte StartAutomationExecution en la Referencia de comandos de la AWS CLI.

`start-change-request-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-change-request-execution`.

AWS CLI

Ejemplo 1: inicio de una solicitud de cambio

En el siguiente ejemplo de `start-change-request-execution`, se inicia una solicitud de cambio con un mínimo de opciones especificadas.

```
aws ssm start-change-request-execution \
    --change-request-name MyChangeRequest \
    --document-name AWS-HelloWorldChangeTemplate \
    --runbooks '[{"DocumentName": "AWS-HelloWorld","Parameters":
 {"AutomationAssumeRole": ["arn:aws:iam:us-east-2:1112223233444:role/
MyChangeManagerAssumeRole"]}}]' \
    --parameters
 Approver="JohnDoe",ApproverType="IamUser",ApproverSnsTopicArn="arn:aws:sns:us-
east-2:1112223233444:MyNotificationTopic"
```

Salida:

```
{
  "AutomationExecutionId": "9d32a4fc-f944-11e6-4105-0a1b2EXAMPLE"
}
```

Ejemplo 2: inicio de una solicitud de cambio con un archivo JSON externo

En el siguiente ejemplo de `start-automation-execution`, se inicia una solicitud de cambio con un mínimo de opciones especificadas en un archivo JSON.

```
aws ssm start-change-request-execution \
    --cli-input-json file://MyChangeRequest.json
```

Contenido de `MyChangeRequest.json`:

```
{
    "ChangeRequestName": "MyChangeRequest",
    "DocumentName": "AWS-HelloWorldChangeTemplate",
    "DocumentVersion": "$DEFAULT",
    "ScheduledTime": "2021-12-30T03:00:00",
    "ScheduledEndTime": "2021-12-30T03:05:00",
    "Tags": [
        {
            "Key": "Purpose",
            "Value": "Testing"
        }
    ],
    "Parameters": {
        "Approver": [
            "JohnDoe"
        ],
        "ApproverType": [
            "IamUser"
        ],
        "ApproverSnsTopicArn": [
            "arn:aws:sns:us-east-2:111222333444;:MyNotificationTopic
        ]
    },
    "Runbooks": [
        {
            "DocumentName": "AWS-HelloWorld",
            "DocumentVersion": "1",
            "MaxConcurrency": "1",
            "MaxErrors": "1",
            "Parameters": {
                "AutomationAssumeRole": [
                    "arn:aws:iam::111222333444:role/MyChangeManagerAssumeRole"
                ]
            }
        }
    ],
    "ChangeDetails": "### Document Name: HelloWorldChangeTemplate\n\n## What does
 this document do?\nThis change template demonstrates the feature set available
 for creating change templates for Change Manager. This template starts a Runbook
 workflow for the Automation document called AWS-HelloWorld.\n\n## Input Parameters
\n* ApproverSnsTopicArn: (Required) Amazon Simple Notification Service ARN for
 approvers.\n* Approver: (Required) The name of the approver to send this request
```

```
 to.\n* ApproverType: (Required) The type of reviewer.\n  * Allowed Values: IamUser,
 IamGroup, IamRole, SSOGroup, SSOUser\n\n## Output Parameters\nThis document has no
 outputs \n"
}
```

Salida:

```
{
  "AutomationExecutionId": "9d32a4fc-f944-11e6-4105-0a1b2EXAMPLE"
}
```

Para obtener más información, consulte Creación de solicitudes de cambio en la Guía del usuario AWS Systems Manager.

- Para obtener información sobre la API, consulte StartChangeRequestExecution en la Referencia de comandos de la AWS CLI.

`start-session`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-session`.

AWS CLI

Ejemplo 1: iniciar una sesión de Session Manager

Este ejemplo de `start-session` establece una conexión a una instancia para una sesión de Session Manager. Tenga en cuenta que este comando interactivo requiere que el complemento Session Manager esté instalado en la máquina cliente que realiza la llamada.

```
aws ssm start-session \
    --target "i-1234567890abcdef0"
```

Salida:

```
Starting session with SessionId: Jane-Roe-07a16060613c408b5
```

Ejemplo 2: iniciar una sesión de Session Manager mediante SSH

Este ejemplo de `start-session` establece una conexión a una instancia para una sesión de Session Manager mediante SSH. Tenga en cuenta que este comando interactivo requiere que el complemento Session Manager esté instalado en la máquina cliente que realiza la llamada y

que el comando use el usuario predeterminado de la instancia, como `ec2-user` en el caso de las instancias EC2 para Linux.

```
ssh -i /path/my-key-pair.pem ec2-user@i-02573cafcfEXAMPLE
```

Salida:

```
Starting session with SessionId: ec2-user-07a16060613c408b5
```

Para obtener más información, consulte Iniciar una sesión e Instalar el complemento Session Manager para la CLI de AWS en la Guía del usuario de AWS.

- Para obtener más información sobre la API, consulte StartSession en la Referencia de comandos de la AWS CLI.

`stop-automation-execution`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-automation-execution`.

AWS CLI

Detención de una ejecución de automatización

En el siguiente ejemplo de `stop-automation-execution` se detiene un documento de Automatización.

```
aws ssm stop-automation-execution
    --automation-execution-id "4105a4fc-f944-11e6-9d32-0a1b2EXAMPLE"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Ejecución manual de un flujo de trabajo de Automatización en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte StopAutomationExecution en la Referencia de comandos de la AWS CLI.

`terminate-session`

En el siguiente ejemplo de código, se muestra cómo utilizar `terminate-session`.

AWS CLI

Para finalizar una sesión de Session Manager

En este ejemplo de `terminate-session`, se finaliza permanentemente una sesión creada por el usuario Shirley-Rodriguez y se cierra la conexión de datos entre el cliente de Session Manager y SSM Agente de la instancia.

```
aws ssm terminate-session \
    --session-id "Shirley-Rodriguez-07a16060613c408b5"
```

Salida:

```
{
    "SessionId": "Shirley-Rodriguez-07a16060613c408b5"
}
```

Para obtener más información, consulte Finalización de una sesión en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte TerminateSession en la Referencia de comandos de la AWS CLI.

`unlabel-parameter-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `unlabel-parameter-version`.

AWS CLI

Para eliminar etiquetas de parámetros

En el siguiente ejemplo de `unlabel-parameter-version`, se eliminan las etiquetas especificadas de la versión del parámetro especificada.

```
aws ssm unlabel-parameter-version \
    --name "parameterName" \
    --parameter-version "version" \
    --labels "label_1" "label_2" "label_3"
```

Salida:

```
{
    "RemovedLabels": [
        "label_1"
        "label_2"
        "label_3"
    ],
    "InvalidLabels": []
}
```

Para obtener más información, consulte Utilizar la AWS CLI para eliminar etiquetas de parámetros en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte UnlabelParameterVersion en la Referencia de comandos de la AWS CLI.

`update-association-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-association-status`.

AWS CLI

Actualización del estado de la asociación

En el siguiente ejemplo de `update-association-status` se actualiza el estado de la asociación entre una instancia y un documento.

```
aws ssm update-association-status \
    --name "AWS-UpdateSSMAgent" \
    --instance-id "i-1234567890abcdef0" \
    --association-
status "Date=1424421071.939,Name=Pending,Message=temp_status_change,AdditionalInfo=Additiona
Config-Needed"
```

Salida:

```
{
    "AssociationDescription": {
        "Name": "AWS-UpdateSSMAgent",
        "InstanceId": "i-1234567890abcdef0",
        "AssociationVersion": "1",
        "Date": 1550507529.604,
        "LastUpdateAssociationDate": 1550507806.974,
```

```
        "Status": {
            "Date": 1424421071.0,
            "Name": "Pending",
            "Message": "temp_status_change",
            "AdditionalInfo": "Additional-Config-Needed"
        },
        "Overview": {
            "Status": "Success",
            "AssociationStatusAggregatedCount": {
                "Success": 1
            }
        },
        "DocumentVersion": "$DEFAULT",
        "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
        "Targets": [
            {
                "Key": "InstanceIds",
                "Values": [
                    "i-1234567890abcdef0"
                ]
            }
        ],
        "LastExecutionDate": 1550507808.0,
        "LastSuccessfulExecutionDate": 1550507808.0
    }
}
```

Para obtener más información, consulte Trabajo con asociaciones en Systems Manager en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte UpdateAssociationStatus en la Referencia de comandos de la AWS CLI.

`update-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-association`.

AWS CLI

Ejemplo 1: actualización de una asociación de documentos

En el siguiente ejemplo de `update-association` se actualiza una asociación con una nueva versión del documento.

```
aws ssm update-association \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab" \
    --document-version "\$LATEST"
```

Salida:

```
{
    "AssociationDescription": {
        "Name": "AWS-UpdateSSMAgent",
        "AssociationVersion": "2",
        "Date": 1550508093.293,
        "LastUpdateAssociationDate": 1550508106.596,
        "Overview": {
            "Status": "Pending",
            "DetailedStatus": "Creating"
        },
        "DocumentVersion": "$LATEST",
        "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
        "Targets": [
            {
                "Key": "tag:Name",
                "Values": [
                    "Linux"
                ]
            }
        ],
        "LastExecutionDate": 1550508094.879,
        "LastSuccessfulExecutionDate": 1550508094.879
    }
}
```

Para obtener más información, consulte Edición y creación de una nueva versión de una asociación en la Guía del usuario de AWS Systems Manager.

Ejemplo 2: actualización de la expresión de programación de una asociación

En el siguiente ejemplo de `update-association` se actualiza la expresión de programación de la asociación especificada.

```
aws ssm update-association \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab" \
    --schedule-expression "cron(0 0 0/4 1/1 * ? *)"
```

Salida:

```
{
    "AssociationDescription": {
        "Name": "AWS-HelloWorld",
        "AssociationVersion": "2",
        "Date": "2021-02-08T13:54:19.203000-08:00",
        "LastUpdateAssociationDate": "2021-06-29T11:51:07.933000-07:00",
        "Overview": {
            "Status": "Pending",
            "DetailedStatus": "Creating"
        },
        "DocumentVersion": "$DEFAULT",
        "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
        "Targets": [
            {
                "Key": "aws:NoOpAutomationTag",
                "Values": [
                    "AWS-NoOpAutomationTarget-Value"
                ]
            }
        ],
        "ScheduleExpression": "cron(0 0 0/4 1/1 * ? *)",
        "LastExecutionDate": "2021-06-26T19:00:48.110000-07:00",
        "ApplyOnlyAtCronInterval": false
    }
}
```

Para obtener más información, consulte Edición y creación de una nueva versión de una asociación en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte UpdateAssociation en la Referencia de comandos de la AWS CLI.

`update-document-default-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-document-default-version`.

AWS CLI

Actualización de la versión predeterminada de un documento

En el siguiente ejemplo de `update-document-default-version` se actualiza la versión predeterminada de un documento de Systems Manager.

```
aws ssm update-document-default-version \
    --name "Example" \
    --document-version "2"
```

Salida:

```
{
    "Description": {
        "Name": "Example",
        "DefaultVersion": "2"
    }
}
```

Para obtener más información, consulte Escribir contenido en el documento de SSM en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte UpdateDocumentDefaultVersion en la Referencia de comandos de la AWS CLI.

`update-document-metadata`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-document-metadata`.

AWS CLI

Ejemplo: aprobación de la versión más reciente de la plantilla de cambios

En el siguiente ejemplo de `update-document-metadata`, se proporciona una aprobación de la última versión de una plantilla de cambios que se ha enviado para revisión.

```
aws ssm update-document-metadata \
    --name MyChangeManagerTemplate \
    --document-reviews 'Action=Approve,Comment=[{Type=Comment,Content=Approved!}]'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Revisión y aprobación o rechazo de las plantillas de cambios en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte UpdateDocumentMetadata en la Referencia de comandos de la AWS CLI.

`update-document`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-document`.

AWS CLI

Creación de una nueva versión de un documento

En el siguiente ejemplo de `update-document` se crea una nueva versión de un documento cuando se ejecuta en una computador con Windows. El documento especificado por `--document` debe estar en formato JSON. Tenga en cuenta que se debe hacer referencia a `file://` seguido de la ruta del archivo de contenido. Debido a que $ está al principio del parámetro `--document-version`, en Windows debe escribir el valor entre comillas dobles. En Linux, MacOS o en una línea de comandos de PowerShell, debe escribir el valor entre comillas simples.

Versión de Windows:

```
aws ssm update-document \
    --name "RunShellScript" \
    --content "file://RunShellScript.json" \
    --document-version "$LATEST"
```

Versión de Linux o Mac:

```
aws ssm update-document \
    --name "RunShellScript" \
    --content "file://RunShellScript.json" \
    --document-version '$LATEST'
```

Salida:

```
{
  "DocumentDescription": {
      "Status": "Updating",
      "Hash": "f775e5df4904c6fa46686c4722fae9de1950dace25cd9608ff8d622046b68d9b",
      "Name": "RunShellScript",
```

```
      "Parameters": [
          {
              "Type": "StringList",
              "Name": "commands",
              "Description": "(Required) Specify a shell script or a command to
 run."
          }
      ],
      "DocumentType": "Command",
      "PlatformTypes": [
          "Linux"
      ],
      "DocumentVersion": "2",
      "HashType": "Sha256",
      "CreatedDate": 1487899655.152,
      "Owner": "809632081692",
      "SchemaVersion": "2.0",
      "DefaultVersion": "1",
      "LatestVersion": "2",
      "Description": "Run an updated script"
  }
}
```

- Para obtener información sobre la API, consulte UpdateDocument en la Referencia de la API de la AWS CLI.

update-maintenance-window-target

En el siguiente ejemplo de código, se muestra cómo utilizar `update-maintenance-window-target`.

AWS CLI

Para actualizar un destino del período de mantenimiento

En el siguiente ejemplo de `update-maintenance-window-target`, se actualiza únicamente el nombre de un destino del período de mantenimiento.

```
aws ssm update-maintenance-window-target \
    --window-id "mw-0c5ed765acEXAMPLE" \
    --window-target-id "57e8344e-fe64-4023-8191-6bf05EXAMPLE" \
    --name "NewName" \
```

```
    --no-replace
```

Salida:

```
{
    "Description": "",
    "OwnerInformation": "",
    "WindowTargetId": "57e8344e-fe64-4023-8191-6bf05EXAMPLE",
    "WindowId": "mw-0c5ed765acEXAMPLE",
    "Targets": [
        {
            "Values": [
                "i-1234567890EXAMPLE"
            ],
            "Key": "InstanceIds"
        }
    ],
    "Name": "NewName"
}
```

Para obtener más información, consulte Actualizar un período de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte UpdateMaintenanceWindowTarget en la Referencia de comandos de la AWS CLI.

`update-maintenance-window-task`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-maintenance-window-task`.

AWS CLI

Para actualizar una tarea del período de mantenimiento

En el siguiente ejemplo de `update-maintenance-window-task`, se actualiza el rol de servicio para una tarea del período de mantenimiento.

```
aws ssm update-maintenance-window-task \
    --window-id "mw-0c5ed765acEXAMPLE" \
    --window-task-id "23d3809e-9fbe-4ddf-b41a-b49d7EXAMPLE" \
    --service-role-arn "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM"
```

Salida:

```
{
    "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
    "MaxErrors": "1",
    "TaskArn": "AWS-UpdateEC2Config",
    "MaxConcurrency": "1",
    "WindowTaskId": "23d3809e-9fbe-4ddf-b41a-b49d7EXAMPLE",
    "TaskParameters": {},
    "Priority": 1,
    "TaskInvocationParameters": {
        "RunCommand": {
            "TimeoutSeconds": 600,
            "Parameters": {
                "allowDowngrade": [
                    "false"
                ]
            }
        }
    },
    "WindowId": "mw-0c5ed765acEXAMPLE",
    "Description": "UpdateEC2Config",
    "Targets": [
        {
            "Values": [
                "57e8344e-fe64-4023-8191-6bf05EXAMPLE"
            ],
            "Key": "WindowTargetIds"
        }
    ],
    "Name": "UpdateEC2Config"
}
```

Para obtener más información, consulte Actualizar un período de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte UpdateMaintenanceWindowTask en la Referencia de comandos de la AWS CLI.

`update-maintenance-window`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-maintenance-window`.

AWS CLI

Ejemplo 1: actualización de un periodo de mantenimiento

En el siguiente ejemplo de `update-maintenance-window` se actualiza el nombre de un periodo de mantenimiento.

```
aws ssm update-maintenance-window \
    --window-id "mw-1a2b3c4d5e6f7g8h9" \
    --name "My-Renamed-MW"
```

Salida:

```
{
    "Cutoff": 1,
    "Name": "My-Renamed-MW",
    "Schedule": "cron(0 16 ? * TUE *)",
    "Enabled": true,
    "AllowUnassociatedTargets": true,
    "WindowId": "mw-1a2b3c4d5e6f7g8h9",
    "Duration": 4
}
```

Ejemplo 2: desactivación de un periodo de mantenimiento

En el siguiente ejemplo de `update-maintenance-window` se desactiva un periodo de mantenimiento.

```
aws ssm update-maintenance-window \
    --window-id "mw-1a2b3c4d5e6f7g8h9" \
    --no-enabled
```

Ejemplo 3: activación de un periodo de mantenimiento

En el siguiente ejemplo de `update-maintenance-window` se activa un periodo de mantenimiento.

```
aws ssm update-maintenance-window \
    --window-id "mw-1a2b3c4d5e6f7g8h9" \
    --enabled
```

Para obtener más información, consulte Actualizar un período de mantenimiento (AWS CLI) en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte UpdateMaintenanceWindow en la Referencia de comandos de la AWS CLI.

`update-managed-instance-role`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-managed-instance-role`.

AWS CLI

Actualización del rol de IAM de una instancia administrada

En el siguiente ejemplo de `update-managed-instance-role` se actualiza el perfil de instancia de IAM de una instancia gestionada.

```
aws ssm update-managed-instance-role \
    --instance-id "mi-08ab247cdfEXAMPLE" \
    --iam-role "ExampleRole"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Step 4: Create an IAM Instance Profile for Systems Manager en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte UpdateManagedInstanceRole en la Referencia de comandos de la AWS CLI.

`update-ops-item`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-ops-item`.

AWS CLI

Cómo actualizar un OpsItem

En el siguiente ejemplo de `update-ops-item` se actualizan la descripción, la prioridad y la categoría de un OpsItem. Además, el comando especifica un tema de SNS al que se envían las notificaciones cuando se edita o cambia este OpsItem.

```
aws ssm update-ops-item \
```

```
    --ops-item-id "oi-287b5EXAMPLE" \
    --description "Primary OpsItem for failover event 2020-01-01-fh398yf" \
    --priority 2 \
    --category "Security" \
    --notifications "Arn=arn:aws:sns:us-east-2:111222333444:my-us-east-2-topic"
```

Salida:

```
This command produces no output.
```

Para obtener más información, consulte Trabajo con OpsItems en la AWSGuía del usuario de Systems Manager.

- Para obtener información sobre la API, consulte UpdateOpsItem en la Referencia de comandos de la AWS CLI.

update-patch-baseline

En el siguiente ejemplo de código, se muestra cómo utilizar `update-patch-baseline`.

AWS CLI

Ejemplo 1: actualización de una línea de base de revisiones

En el siguiente ejemplo de `update-patch-baseline` se agregan dos revisiones especificadas como rechazadas y una revisión como aprobada a la línea de base de revisiones especificada.

```
aws ssm update-patch-baseline \
        --baseline-id "pb-0123456789abcdef0" \
        --rejected-patches "KB2032276" "MS10-048" \
        --approved-patches "KB2124261"
```

Salida:

```
{
    "BaselineId": "pb-0123456789abcdef0",
    "Name": "WindowsPatching",
    "OperatingSystem": "WINDOWS",
    "GlobalFilters": {
        "PatchFilters": []
```

```
    },
    "ApprovalRules": {
        "PatchRules": [
            {
                "PatchFilterGroup": {
                    "PatchFilters": [
                        {
                            "Key": "PRODUCT",
                            "Values": [
                                "WindowsServer2016"
                            ]
                        }
                    ]
                },
                "ComplianceLevel": "CRITICAL",
                "ApproveAfterDays": 0,
                "EnableNonSecurity": false
            }
        ]
    },
    "ApprovedPatches": [
        "KB2124261"
    ],
    "ApprovedPatchesComplianceLevel": "UNSPECIFIED",
    "ApprovedPatchesEnableNonSecurity": false,
    "RejectedPatches": [
        "KB2032276",
        "MS10-048"
    ],
    "RejectedPatchesAction": "ALLOW_AS_DEPENDENCY",
    "CreatedDate": 1550244180.465,
    "ModifiedDate": 1550244180.465,
    "Description": "Patches for Windows Servers",
    "Sources": []
}
```

Ejemplo 2: cambio del nombre de una línea de base de revisiones

En el siguiente ejemplo de `update-patch-baseline` se cambia el nombre de la línea de base de revisiones especificada.

```
aws ssm update-patch-baseline \
    --baseline-id "pb-0713accee01234567" \
```

```
    --name "Windows-Server-2012-R2-Important-and-Critical-Security-Updates"
```

Para obtener más información, consulte Actualización o eliminación de una línea de base de revisiones <https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-baseline-update-or-delete.html>`__ en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte UpdatePatchBaseline en la Referencia de comandos de la AWS CLI.

`update-resource-data-sync`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-resource-data-sync`.

AWS CLI

Para actualizar una sincronización de datos de recursos

En el siguiente ejemplo de `update-resource-data-sync`, se actualiza una sincronización de datos de recursos SyncFromSource.

```
aws ssm update-resource-data-sync \
    --sync-name exampleSync \
    --sync-type SyncFromSource \
    --sync-source '{"SourceType":"SingleAccountMultiRegions", "SourceRegions":["us-east-1", "us-west-2"]}'
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de Systems Manager Explorer para mostrar datos de varias cuentas y regiones en la Guía del usuario AWS Systems Manager.

- Para obtener información sobre la API, consulte UpdateResourceDataSync en la Referencia de comandos de la AWS CLI.

`update-service-setting`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-service-setting`.

AWS CLI

Para actualizar la configuración del servicio para el rendimiento del almacén de parámetros

En el siguiente ejemplo de `update-service-setting`, se actualiza la configuración actual del servicio para el rendimiento del almacén de parámetros en la región especificada para que utilice el rendimiento incrementado.

```
aws ssm update-service-setting \
    --setting-id arn:aws:ssm:us-east-1:123456789012:servicesetting/ssm/parameter-store/high-throughput-enabled \
    --setting-value true
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Aumentar o disminuir el rendimiento de Parameter Store en la Guía del usuario de AWS Systems Manager.

- Para obtener información sobre la API, consulte UpdateServiceSetting en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon Textract que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon Textract.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`analyze-document`

En el siguiente ejemplo de código, se muestra cómo utilizar `analyze-document`.

AWS CLI

Análisis del texto de un documento

En el siguiente ejemplo de `analyze-document` se muestra cómo analizar el texto de un documento.

Linux/macOS:

```
aws textract analyze-document \
    --document '{"S3Object":{"Bucket":"bucket","Name":"document"}}' \
    --feature-types '["TABLES","FORMS"]'
```

Windows:

```
aws textract analyze-document \
    --document "{\"S3Object\":{\"Bucket\":\"bucket\",\"Name\":\"document\"}}" \
    --feature-types "[\"TABLES\",\"FORMS\"]" \
    --region region-name
```

Salida:

```
{
    "Blocks": [
        {
            "Geometry": {
                "BoundingBox": {
                    "Width": 1.0,
                    "Top": 0.0,
                    "Left": 0.0,
                    "Height": 1.0
                },
                "Polygon": [
                    {
                        "Y": 0.0,
                        "X": 0.0
                    },
                    {
                        "Y": 0.0,
                        "X": 1.0
                    },
                    {
                        "Y": 1.0,
                        "X": 1.0
                    },
                    {
                        "Y": 1.0,
```

```
                        "X": 0.0
                    }
                ]
            },
            "Relationships": [
                {
                    "Type": "CHILD",
                    "Ids": [
                        "87586964-d50d-43e2-ace5-8a890657b9a0",
                        "a1e72126-21d9-44f4-a8d6-5c385f9002ba",
                        "e889d012-8a6b-4d2e-b7cd-7a8b327d876a"
                    ]
                }
            ],
            "BlockType": "PAGE",
            "Id": "c2227f12-b25d-4e1f-baea-1ee180d926b2"
        }
    ],
    "DocumentMetadata": {
        "Pages": 1
    }
}
```

Para obtener más información, consulte Análisis del texto de un documento con Amazon Textract en la Guía para desarrolladores de Amazon Textract

- Para obtener información acerca de la API, consulte AnalyzeDocument en la Referencia de comandos de la AWS CLI.

`detect-document-text`

En el siguiente ejemplo de código, se muestra cómo utilizar `detect-document-text`.

AWS CLI

Detección de texto en un documento

En el siguiente ejemplo de `detect-document-text` se muestra cómo detectar texto en un documento.

Linux/macOS:

```
aws textract detect-document-text \
```

```
    --document '{"S3Object":{"Bucket":"bucket","Name":"document"}}'
```

Windows:

```
aws textract detect-document-text \
    --document "{\"S3Object\":{\"Bucket\":\"bucket\",\"Name\":\"document\"}}" \
    --region region-name
```

Salida:

```
{
    "Blocks": [
        {
            "Geometry": {
                "BoundingBox": {
                    "Width": 1.0,
                    "Top": 0.0,
                    "Left": 0.0,
                    "Height": 1.0
                },
                "Polygon": [
                    {
                        "Y": 0.0,
                        "X": 0.0
                    },
                    {
                        "Y": 0.0,
                        "X": 1.0
                    },
                    {
                        "Y": 1.0,
                        "X": 1.0
                    },
                    {
                        "Y": 1.0,
                        "X": 0.0
                    }
                ]
            },
            "Relationships": [
                {
                    "Type": "CHILD",
                    "Ids": [
```

```
                    "896a9f10-9e70-4412-81ce-49ead73ed881",
                    "0da18623-dc4c-463d-a3d1-9ac050e9e720",
                    "167338d7-d38c-4760-91f1-79a8ec457bb2"
                ]
            }
        ],
        "BlockType": "PAGE",
        "Id": "21f0535e-60d5-4bc7-adf2-c05dd851fa25"
    },
    {
        "Relationships": [
            {
                "Type": "CHILD",
                "Ids": [
                    "62490c26-37ea-49fa-8034-7a9ff9369c9c",
                    "1e4f3f21-05bd-4da9-ba10-15d01e66604c"
                ]
            }
        ],
        "Confidence": 89.11581420898438,
        "Geometry": {
            "BoundingBox": {
                "Width": 0.33642634749412537,
                "Top": 0.17169663310050964,
                "Left": 0.13885067403316498,
                "Height": 0.49159330129623413
            },
            "Polygon": [
                {
                    "Y": 0.17169663310050964,
                    "X": 0.13885067403316498
                },
                {
                    "Y": 0.17169663310050964,
                    "X": 0.47527703642845154
                },
                {
                    "Y": 0.6632899641990662,
                    "X": 0.47527703642845154
                },
                {
                    "Y": 0.6632899641990662,
                    "X": 0.13885067403316498
                }
```

```
                ]
            },
            "Text": "He llo,",
            "BlockType": "LINE",
            "Id": "896a9f10-9e70-4412-81ce-49ead73ed881"
        },
        {
            "Relationships": [
                {
                    "Type": "CHILD",
                    "Ids": [
                        "19b28058-9516-4352-b929-64d7cef29daf"
                    ]
                }
            ],
            "Confidence": 85.5694351196289,
            "Geometry": {
                "BoundingBox": {
                    "Width": 0.33182239532470703,
                    "Top": 0.23131252825260162,
                    "Left": 0.5091826915740967,
                    "Height": 0.3766750991344452
                },
                "Polygon": [
                    {
                        "Y": 0.23131252825260162,
                        "X": 0.5091826915740967
                    },
                    {
                        "Y": 0.23131252825260162,
                        "X": 0.8410050868988037
                    },
                    {
                        "Y": 0.607987642288208,
                        "X": 0.8410050868988037
                    },
                    {
                        "Y": 0.607987642288208,
                        "X": 0.5091826915740967
                    }
                ]
            },
            "Text": "worlc",
            "BlockType": "LINE",
```

```
            "Id": "0da18623-dc4c-463d-a3d1-9ac050e9e720"
        }
    ],
    "DocumentMetadata": {
        "Pages": 1
    }
}
```

Para obtener más información, consulte Detección del texto de un documento con Amazon Textract en la Guía para desarrolladores de Amazon Textract

- Para obtener información sobre la API, consulte DetectDocumentText en la Referencia de comandos de la AWS CLI.

`get-document-analysis`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-document-analysis`.

AWS CLI

Obtención de los resultados del análisis de texto asíncrono de un documento de varias páginas

En el siguiente ejemplo de `get-document-analysis` se muestra cómo obtener los resultados del análisis de texto asíncrono de un documento de varias páginas.

```
aws textract get-document-analysis \
    --job-id df7cf32ebbd2a5de113535fcf4d921926a701b09b4e7d089f3aebadb41e0712b \
    --max-results 1000
```

Salida:

```
{
    "Blocks": [
        {
            "Geometry": {
                "BoundingBox": {
                    "Width": 1.0,
                    "Top": 0.0,
                    "Left": 0.0,
                    "Height": 1.0
                },
                "Polygon": [
```

```
                    {
                        "Y": 0.0,
                        "X": 0.0
                    },
                    {
                        "Y": 0.0,
                        "X": 1.0
                    },
                    {
                        "Y": 1.0,
                        "X": 1.0
                    },
                    {
                        "Y": 1.0,
                        "X": 0.0
                    }
                ]
            },
            "Relationships": [
                {
                    "Type": "CHILD",
                    "Ids": [
                        "75966e64-81c2-4540-9649-d66ec341cd8f",
                        "bb099c24-8282-464c-a179-8a9fa0a057f0",
                        "5ebf522d-f9e4-4dc7-bfae-a288dc094595"
                    ]
                }
            ],
            "BlockType": "PAGE",
            "Id": "247c28ee-b63d-4aeb-9af0-5f7ea8ba109e",
            "Page": 1
        }
    ],
    "NextToken": "cY1W3eTFvoB0cH7YrKVudI4Gb0H8J0xAYLo8xI/JunCIPWCthaKQ+07n/
ElyutsSy0+1VOImoTRmP1zw4P0RFtaeV9Bzhnfedpx1YqwB4xaGDA==",
    "DocumentMetadata": {
        "Pages": 1
    },
    "JobStatus": "SUCCEEDED"
}
```


Para obtener más información, consulte Detección y análisis de texto en documentos de varias páginas en la Guía para desarrolladores de Amazon Textract

- Para obtener información sobre la API, consulte GetDocumentAnalysis en la Referencia de comandos de la AWS CLI.

`get-document-text-detection`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-document-text-detection`.

AWS CLI

Para obtener los resultados de la detección de texto asíncrono de un documento de varias páginas

En el siguiente ejemplo de `get-document-text-detection`, se muestra cómo obtener los resultados de la detección de texto asíncrono en un documento de varias páginas.

```
aws textract get-document-text-detection \
    --job-id 57849a3dc627d4df74123dca269d69f7b89329c870c65bb16c9fd63409d200b9 \
    --max-results 1000
```

Output

```
{
    "Blocks": [
        {
            "Geometry": {
                "BoundingBox": {
                    "Width": 1.0,
                    "Top": 0.0,
                    "Left": 0.0,
                    "Height": 1.0
                },
                "Polygon": [
                    {
                        "Y": 0.0,
                        "X": 0.0
                    },
                    {
                        "Y": 0.0,
                        "X": 1.0
                    },
                    {
```

```
                        "Y": 1.0,
                        "X": 1.0
                    },
                    {
                        "Y": 1.0,
                        "X": 0.0
                    }
                ]
            },
            "Relationships": [
                {
                    "Type": "CHILD",
                    "Ids": [
                        "1b926a34-0357-407b-ac8f-ec473160c6a9",
                        "0c35dc17-3605-4c9d-af1a-d9451059df51",
                        "dea3db8a-52c2-41c0-b50c-81f66f4aa758"
                    ]
                }
            ],
            "BlockType": "PAGE",
            "Id": "84671a5e-8c99-43be-a9d1-6838965da33e",
            "Page": 1
        }
    ],
    "NextToken": "GcqyoAJuZwujOT35EN4LCI3EUzMtiLq3nKyFFHvU5q1SaIdEBcSty+njNgoWwuMP/
muqc96S4o5NzDqehhXvhkodMyVO5OJGyms5lsrCxibWJw==",
    "DocumentMetadata": {
        "Pages": 1
    },
    "JobStatus": "SUCCEEDED"
}
```

Para obtener más información, consulte Detección y análisis de texto en documentos de varias páginas en la Guía para desarrolladores de Amazon Textract

- Para obtener información sobre la API, consulte GetDocumentTextDetection en la Referencia de comandos de la AWS CLI.

`start-document-analysis`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-document-analysis`.

AWS CLI

Cómo empezar a analizar el texto de un documento de varias páginas

En el siguiente ejemplo de `start-document-analysis` se muestra cómo iniciar el análisis asíncrono de texto de un documento de varias páginas.

Linux/macOS:

```
aws textract start-document-analysis \
    --document-location '{"S3Object":{"Bucket":"bucket","Name":"document"}}' \
    --feature-types '["TABLES","FORMS"]' \
    --notification-channel "SNSTopicArn=arn:snsTopic,RoleArn=roleArn"
```

Windows:

```
aws textract start-document-analysis \
    --document-location "{\"S3Object\":{\"Bucket\":\"bucket\",\"Name\":\"document
\"}}" \
    --feature-types "[\"TABLES\", \"FORMS\"]" \
    --region region-name \
    --notification-channel "SNSTopicArn=arn:snsTopic,RoleArn=roleArn"
```

Salida:

```
{
    "JobId": "df7cf32ebbd2a5de113535fcf4d921926a701b09b4e7d089f3aebadb41e0712b"
}
```

Para obtener más información, consulte Detección y análisis de texto en documentos de varias páginas en la Guía para desarrolladores de Amazon Textract

- Para obtener información sobre la API, consulte StartDocumentAnalysis en la Referencia de comandos de la AWS CLI.

`start-document-text-detection`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-document-text-detection`.

AWS CLI

Cómo empezar a detectar texto en un documento de varias páginas

En el siguiente ejemplo de `start-document-text-detection` se muestra cómo iniciar la detección asíncrona de texto de un documento de varias páginas.

Linux/macOS:

```
aws textract start-document-text-detection \
        --document-location '{"S3Object":{"Bucket":"bucket","Name":"document"}}' \
        --notification-channel "SNSTopicArn=arn:snsTopic,RoleArn=roleARN"
```

Windows:

```
aws textract start-document-text-detection \
    --document-location "{\"S3Object\":{\"Bucket\":\"bucket\",\"Name\":\"document
\"}}" \
    --region region-name \
    --notification-channel "SNSTopicArn=arn:snsTopic,RoleArn=roleArn"
```

Salida:

```
{
    "JobId": "57849a3dc627d4df74123dca269d69f7b89329c870c65bb16c9fd63409d200b9"
}
```

Para obtener más información, consulte Detección y análisis de texto en documentos de varias páginas en la Guía para desarrolladores de Amazon Textract

- Para obtener información sobre la API, consulte StartDocumentTextDetection en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon Transcribe que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon Transcribe.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-language-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-language-model`.

AWS CLI

Ejemplo 1: creación de un modelo de lenguaje personalizado con datos de entrenamiento y afinación

En el siguiente ejemplo de `create-language-model`, se crea un modelo de lenguaje personalizado. Puede utilizar un modelo de lenguaje personalizado para mejorar el rendimiento de la transcripción en ámbitos como el jurídico, la hostelería, las finanzas y los seguros. En language-code, introduzca un código de idioma válido. En base-model-name, especifique el modelo base que mejor se adapte a la frecuencia de muestreo del audio que desea transcribir con su modelo de lenguaje personalizado. En model-name, especifique el nombre con el que quiere llamar al modelo de lenguaje personalizado.

```
aws transcribe create-language-model \
    --language-code language-code \
    --base-model-name base-model-name \
    --model-name cli-clm-example \
    --input-data-config S3Uri="s3://amzn-s3-demo-bucket/Amazon-S3-Prefix-for-
training-data",TuningDataS3Uri="s3://amzn-s3-demo-bucket/Amazon-S3-Prefix-for-
tuning-data",DataAccessRoleArn="arn:aws:iam::AWS-account-number:role/IAM-role-with-
permissions-to-create-a-custom-language-model"
```

Salida:

```
{
    "LanguageCode": "language-code",
    "BaseModelName": "base-model-name",
    "ModelName": "cli-clm-example",
    "InputDataConfig": {
        "S3Uri": "s3://amzn-s3-demo-bucket/Amazon-S3-Prefix/",
        "TuningDataS3Uri": "s3://amzn-s3-demo-bucket/Amazon-S3-Prefix/",
```

```
        "DataAccessRoleArn": "arn:aws:iam::AWS-account-number:role/IAM-role-with-
permissions-create-a-custom-language-model"
    },
    "ModelStatus": "IN_PROGRESS"
}
```

Para obtener más información, consulte Mejora de la precisión de la transcripción específica de dominios con modelos de idiomas personalizados en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 2: creación de un modelo de lenguaje personalizado solo con datos de entrenamiento

En el siguiente ejemplo de `create-language-model` se transcribe un archivo de audio. Puede utilizar un modelo de lenguaje personalizado para mejorar el rendimiento de la transcripción en ámbitos como el jurídico, la hostelería, las finanzas y los seguros. En language-code, introduzca un código de idioma válido. En base-model-name, especifique el modelo base que mejor se adapte a la frecuencia de muestreo del audio que desea transcribir con su modelo de lenguaje personalizado. En model-name, especifique el nombre con el que quiere llamar al modelo de lenguaje personalizado.

```
aws transcribe create-language-model \
    --language-code en-US \
    --base-model-name base-model-name \
    --model-name cli-clm-example \
    --input-data-config S3Uri="s3://amzn-s3-demo-bucket/Amazon-S3-Prefix-For-
Training-Data",DataAccessRoleArn="arn:aws:iam::AWS-account-number:role/IAM-role-
with-permissions-to-create-a-custom-language-model"
```

Salida:

```
{
    "LanguageCode": "en-US",
    "BaseModelName": "base-model-name",
    "ModelName": "cli-clm-example",
    "InputDataConfig": {
        "S3Uri": "s3://amzn-s3-demo-bucket/Amazon-S3-Prefix-For-Training-Data/",
        "DataAccessRoleArn": "arn:aws:iam::your-AWS-account-number:role/IAM-role-
with-permissions-to-create-a-custom-language-model"
    },
    "ModelStatus": "IN_PROGRESS"
}
```

Para obtener más información, consulte Mejora de la precisión de la transcripción específica de dominios con modelos de idiomas personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte CreateLanguageModel en la Referencia de comandos de la AWS CLI.

`create-medical-vocabulary`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-medical-vocabulary`.

AWS CLI

Para crear un vocabulario médico personalizado

En el siguiente ejemplo de `create-medical-vocabulary` se crea un vocabulario personalizado. Para crear un vocabulario personalizado, debe haber creado un archivo de texto con todos los términos que desee transcribir con mayor precisión. En vocabulary-file-uri, especifique el URI de Amazon Simple Storage Service (Amazon S3) de este archivo de texto. En language-code, especifique un código de idioma correspondiente al idioma del vocabulario personalizado. En vocabulary-name, especifique cómo desea llamar al vocabulario personalizado.

```
aws transcribe create-medical-vocabulary \
    --vocabulary-name cli-medical-vocab-example \
    --language-code language-code \
    --vocabulary-file-uri https://amzn-s3-demo-bucket.AWS-Region.amazonaws.com/the-text-file-for-the-medical-custom-vocabulary.txt
```

Salida:

```
{
    "VocabularyName": "cli-medical-vocab-example",
    "LanguageCode": "language-code",
    "VocabularyState": "PENDING"
}
```

Para obtener más información, consulte Vocabularios médicos personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte CreateMedicalVocabulary en la Referencia de comandos de la AWS CLI.

`create-vocabulary-filter`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-vocabulary-filter`.

AWS CLI

Para crear un filtro de vocabulario

En el siguiente ejemplo de `create-vocabulary-filter`, se crea un filtro de vocabulario que utiliza un archivo de texto que contiene una lista de palabras que no desea que aparezcan en una transcripción. En language-code, especifique un código de idioma correspondiente al idioma del filtro de vocabulario. En vocabulary-filter-file-uri, especifique el URI de Amazon Simple Storage Service (Amazon S3) de este archivo de texto. En vocabulary-filter-name, especifique el nombre del filtro de vocabulario.

```
aws transcribe create-vocabulary-filter \
    --language-code language-code \
    --vocabulary-filter-file-uri s3://amzn-s3-demo-bucket/vocabulary-filter.txt \
    --vocabulary-filter-name cli-vocabulary-filter-example
```

Salida:

```
{
    "VocabularyFilterName": "cli-vocabulary-filter-example",
    "LanguageCode": "language-code"
}
```

Para obtener más información, consulte Filtering Unwanted Words en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener más información sobre la API, consulte CreateVocabularyFilter en la Referencia de comandos de la AWS CLI.

`create-vocabulary`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-vocabulary`.

AWS CLI

Para crear un vocabulario personalizado

En el siguiente ejemplo de `create-vocabulary` se crea un vocabulario personalizado. Para crear un vocabulario personalizado, debe haber creado un archivo de texto con todos los términos que desee transcribir con mayor precisión. En vocabulary-file-uri, especifique el URI de Amazon Simple Storage Service (Amazon S3) de este archivo de texto. En language-code, especifique un código de idioma correspondiente al idioma del vocabulario personalizado. En vocabulary-name, especifique cómo desea llamar al vocabulario personalizado.

```
aws transcribe create-vocabulary \
    --language-code language-code \
    --vocabulary-name cli-vocab-example \
    --vocabulary-file-uri s3://amzn-s3-demo-bucket/Amazon-S3-prefix/the-text-file-for-the-custom-vocabulary.txt
```

Salida:

```
{
    "VocabularyName": "cli-vocab-example",
    "LanguageCode": "language-code",
    "VocabularyState": "PENDING"
}
```

Para obtener más información, consulte Vocabularios personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte CreateVocabulary en la Referencia de comandos de la AWS CLI.

`delete-language-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-language-model`.

AWS CLI

Para eliminar un modelo de lenguaje personalizado

En el siguiente ejemplo de `delete-language-model`, se elimina un modelo de lenguaje personalizado.

```
aws transcribe delete-language-model \
    --model-name model-name
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Mejora de la precisión de la transcripción específica de dominios con modelos de idiomas personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte DeleteLanguageModel en la Referencia de comandos de la AWS CLI.

`delete-medical-transcription-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-medical-transcription-job`.

AWS CLI

Para eliminar un trabajo de transcripción médica

En el siguiente ejemplo de `delete-medical-transcription-job` se elimina un trabajo de transcripción médica.

```
aws transcribe delete-medical-transcription-job \
    --medical-transcription-job-name medical-transcription-job-name
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteMedicalTranscriptionJob en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte DeleteMedicalTranscriptionJob en la Referencia de comandos de la AWS CLI.

`delete-medical-vocabulary`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-medical-vocabulary`.

AWS CLI

Para eliminar un vocabulario médico personalizado

En el siguiente ejemplo de `delete-medical-vocabulary`, se elimina un vocabulario médico personalizado. En vocabulary-name, especifique el nombre del vocabulario médico personalizado.

```
aws transcribe delete-vocabulary \
    --vocabulary-name medical-custom-vocabulary-name
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Vocabularios médicos personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte DeleteMedicalVocabulary en la Referencia de comandos de la AWS CLI.

`delete-transcription-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-transcription-job`.

AWS CLI

Para eliminar uno de los trabajos de transcripción

En el siguiente ejemplo de `delete-transcription-job` se elimina uno de los trabajos de transcripción.

```
aws transcribe delete-transcription-job \
    --transcription-job-name your-transcription-job
```

Este comando no genera ninguna salida.

Para obtener más información, consulte DeleteTranscriptionJob en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte DeleteTranscriptionJob en la Referencia de comandos de la AWS CLI.

`delete-vocabulary-filter`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-vocabulary-filter`.

AWS CLI

Para eliminar un filtro de vocabulario

En el siguiente ejemplo de `delete-vocabulary-filter`, se elimina un filtro de vocabulario.

```
aws transcribe delete-vocabulary-filter \
    --vocabulary-filter-name vocabulary-filter-name
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Filtering Unwanted Words en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener detalles sobre la API, consulte DeleteVocabularyFilter en la Referencia de comandos de la AWS CLI.

`delete-vocabulary`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-vocabulary`.

AWS CLI

Para eliminar un vocabulario personalizado

En el siguiente ejemplo de `delete-vocabulary` se elimina un vocabulario personalizado.

```
aws transcribe delete-vocabulary \
    --vocabulary-name vocabulary-name
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Vocabularios personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte DeleteVocabulary en la Referencia de comandos de la AWS CLI.

`describe-language-model`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-language-model`.

AWS CLI

Para obtener información sobre un modelo de lenguaje personalizado específico

En el siguiente ejemplo de `describe-language-model`, se obtiene información sobre un modelo de lenguaje personalizado específico. Por ejemplo, en BaseModelName puede ver si su modelo se ha entrenado con un modelo NarrowBand o WideBand. Los modelos de lenguaje personalizados con un modelo base NarrowBand pueden transcribir audio con una velocidad de muestreo inferior a 16 kHz. Los modelos de lenguaje que utilizan un modelo base WideBand pueden transcribir audio con una frecuencia de muestreo superior a 16 kHz. El parámetro S3Uri indica el prefijo Amazon S3 que ha utilizado para acceder a los datos de entrenamiento para crear el modelo de lenguaje personalizado.

```
aws transcribe describe-language-model \
    --model-name cli-clm-example
```

Salida:

```
{
    "LanguageModel": {
        "ModelName": "cli-clm-example",
        "CreateTime": "2020-09-25T17:57:38.504000+00:00",
        "LastModifiedTime": "2020-09-25T17:57:48.585000+00:00",
        "LanguageCode": "language-code",
        "BaseModelName": "base-model-name",
        "ModelStatus": "IN_PROGRESS",
        "UpgradeAvailability": false,
        "InputDataConfig": {
            "S3Uri": "s3://amzn-s3-demo-bucket/Amazon-S3-Prefix/",
            "TuningDataS3Uri": "s3://amzn-s3-demo-bucket/Amazon-S3-Prefix/",
            "DataAccessRoleArn": "arn:aws:iam::AWS-account-number:role/IAM-role-
with-permissions-to-create-a-custom-language-model"
        }
    }
}
```

Para obtener más información, consulte Mejora de la precisión de la transcripción específica de dominios con modelos de idiomas personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte DescribeLanguageModel en la Referencia de comandos de la AWS CLI.

get-medical-transcription-job

En el siguiente ejemplo de código, se muestra cómo utilizar `get-medical-transcription-job`.

AWS CLI

Para obtener información acerca de un trabajo de transcripción médica determinado

En el siguiente ejemplo de `get-medical-transcription-job`, se obtiene información sobre un determinado trabajo de transcripción médica. Para acceder a los resultados de la transcripción, utilice el parámetro TranscriptFileUri. Si ha habilitado características adicionales para el trabajo de transcripción, puede consultarlas en el objeto Settings. El parámetro Specialty muestra la especialidad médica del proveedor. El parámetro Type indica si el discurso del trabajo de transcripción corresponde a una conversación o un dictado de temática médica.

```
aws transcribe get-medical-transcription-job \
    --medical-transcription-job-name vocabulary-dictation-medical-transcription-job
```

Salida:

```
{
    "MedicalTranscriptionJob": {
        "MedicalTranscriptionJobName": "vocabulary-dictation-medical-transcription-
job",
        "TranscriptionJobStatus": "COMPLETED",
        "LanguageCode": "en-US",
        "MediaSampleRateHertz": 48000,
        "MediaFormat": "mp4",
        "Media": {
            "MediaFileUri": "s3://Amazon-S3-Prefix/your-audio-file.file-extension"
        },
        "Transcript": {
            "TranscriptFileUri": "https://s3.Region.amazonaws.com/Amazon-S3-Prefix/
vocabulary-dictation-medical-transcription-job.json"
        },
        "StartTime": "2020-09-21T21:17:27.045000+00:00",
        "CreationTime": "2020-09-21T21:17:27.016000+00:00",
        "CompletionTime": "2020-09-21T21:17:59.561000+00:00",
        "Settings": {
            "ChannelIdentification": false,
            "ShowAlternatives": false,
            "VocabularyName": "cli-medical-vocab-example"
```

```
        },
        "Specialty": "PRIMARYCARE",
        "Type": "DICTATION"
    }
}
```

Para obtener más información, consulte Batch Transcription en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte GetMedicalTranscriptionJob en la Referencia de comandos de la AWS CLI.

`get-medical-vocabulary`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-medical-vocabulary`.

AWS CLI

Para obtener información sobre un vocabulario médico personalizado

En el siguiente ejemplo de `get-medical-vocabulary`, se obtiene información sobre un vocabulario médico personalizado. Puede usar el parámetro VocabularyState para ver el estado de procesamiento del vocabulario. Si es READY, puede usarlo en la operación StartMedicalTranscriptionJob.

```
aws transcribe get-medical-vocabulary \
    --vocabulary-name medical-vocab-example
```

Salida:

```
{
    "VocabularyName": "medical-vocab-example",
    "LanguageCode": "en-US",
    "VocabularyState": "READY",
    "LastModifiedTime": "2020-09-19T23:59:04.349000+00:00",
    "DownloadUri": "https://link-to-download-the-text-file-used-to-create-your-
medical-custom-vocabulary"
}
```

Para obtener más información, consulte Vocabularios médicos personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte GetMedicalVocabulary en la Referencia de comandos de la AWS CLI.

`get-transcription-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-transcription-job`.

AWS CLI

Para obtener información acerca de un determinado trabajo de transcripción

En el siguiente ejemplo de `get-transcription-job` se obtiene información sobre un determinado trabajo de transcripción. Para acceder a los resultados de la transcripción, utilice el parámetro TranscriptFileUri. Utilice el parámetro MediaFileUri para ver qué archivo de audio ha transcrito con este trabajo. Puede usar el objeto Settings para ver las características opcionales que ha habilitado en el trabajo de transcripción.

```
aws transcribe get-transcription-job \
    --transcription-job-name your-transcription-job
```

Salida:

```
{
    "TranscriptionJob": {
        "TranscriptionJobName": "your-transcription-job",
        "TranscriptionJobStatus": "COMPLETED",
        "LanguageCode": "language-code",
        "MediaSampleRateHertz": 48000,
        "MediaFormat": "mp4",
        "Media": {
            "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.file-
extension"
        },
        "Transcript": {
            "TranscriptFileUri": "https://Amazon-S3-file-location-of-transcription-
output"
        },
        "StartTime": "2020-09-18T22:27:23.970000+00:00",
        "CreationTime": "2020-09-18T22:27:23.948000+00:00",
        "CompletionTime": "2020-09-18T22:28:21.197000+00:00",
        "Settings": {
            "ChannelIdentification": false,
```

```
            "ShowAlternatives": false
        },
        "IdentifyLanguage": true,
        "IdentifiedLanguageScore": 0.8672199249267578
    }
}
```

Para obtener más información, consulte Introducción (interfaz de línea de comandos de AWS) en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte GetTranscriptionJob en la Referencia de comandos de la AWS CLI.

`get-vocabulary-filter`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-vocabulary-filter`.

AWS CLI

Para obtener información sobre un filtro de vocabulario

En el siguiente ejemplo de `get-vocabulary-filter`, se obtiene información sobre un filtro de vocabulario. Puede usar el parámetro DownloadUri para obtener la lista de palabras que ha utilizado para crear el filtro de vocabulario.

```
aws transcribe get-vocabulary-filter \
    --vocabulary-filter-name testFilter
```

Salida:

```
{
    "VocabularyFilterName": "testFilter",
    "LanguageCode": "language-code",
    "LastModifiedTime": "2020-05-07T22:39:32.147000+00:00",
    "DownloadUri": "https://Amazon-S3-location-to-download-your-vocabulary-filter"
}
```

Para obtener más información, consulte Filtering Unwanted Words en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte GetVocabularyFilter en la Referencia de comandos de la AWS CLI.

`get-vocabulary`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-vocabulary`.

AWS CLI

Para obtener información sobre un vocabulario personalizado

En el siguiente ejemplo de `get-vocabulary` se obtiene información sobre un vocabulario personalizado creado anteriormente.

```
aws transcribe get-vocabulary \
    --vocabulary-name cli-vocab-1
```

Salida:

```
{
    "VocabularyName": "cli-vocab-1",
    "LanguageCode": "language-code",
    "VocabularyState": "READY",
    "LastModifiedTime": "2020-09-19T23:22:32.836000+00:00",
    "DownloadUri": "https://link-to-download-the-text-file-used-to-create-your-
custom-vocabulary"
}
```

Para obtener más información, consulte Vocabularios personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte GetVocabulary en la Referencia de comandos de la AWS CLI.

`list-language-models`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-language-models`.

AWS CLI

Para enumerar sus modelos de lenguaje personalizados

En el siguiente ejemplo de `list-language-models`, se enumeran los modelos de lenguaje personalizados asociados a su cuenta y región de AWS. Puede utilizar los parámetros `S3Uri`

y `TuningDataS3Uri` para buscar los prefijos de Amazon S3 que ha utilizado como datos de entrenamiento o de afinación. El BaseModelName le indica si ha utilizado un modelo NarrowBand o WideBand para crear un modelo de lenguaje personalizado. Puede transcribir audio con una frecuencia de muestreo inferior a 16 kHz con un modelo de lenguaje personalizado mediante un modelo base NarrowBand. Puede transcribir audio a 16 kHz o más con un modelo de lenguaje personalizado utilizando un modelo base WideBand. El parámetro `ModelStatus` muestra si puede utilizar el modelo de lenguaje personalizado en un trabajo de transcripción. Si el valor es COMPLETED, puede usarlo en un trabajo de transcripción.

```
aws transcribe list-language-models
```

Salida:

```
{
    "Models": [
        {
            "ModelName": "cli-clm-2",
            "CreateTime": "2020-09-25T17:57:38.504000+00:00",
            "LastModifiedTime": "2020-09-25T17:57:48.585000+00:00",
            "LanguageCode": "language-code",
            "BaseModelName": "WideBand",
            "ModelStatus": "IN_PROGRESS",
            "UpgradeAvailability": false,
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket/clm-training-data/",
                "TuningDataS3Uri": "s3://amzn-s3-demo-bucket/clm-tuning-data/",
                "DataAccessRoleArn": "arn:aws:iam::AWS-account-number:role/IAM-role-
used-to-create-the-custom-language-model"
            }
        },
        {
            "ModelName": "cli-clm-1",
            "CreateTime": "2020-09-25T17:16:01.835000+00:00",
            "LastModifiedTime": "2020-09-25T17:16:15.555000+00:00",
            "LanguageCode": "language-code",
            "BaseModelName": "WideBand",
            "ModelStatus": "IN_PROGRESS",
            "UpgradeAvailability": false,
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket/clm-training-data/",
                "DataAccessRoleArn": "arn:aws:iam::AWS-account-number:role/IAM-role-
used-to-create-the-custom-language-model"
```

```
            }
        },
        {
            "ModelName": "clm-console-1",
            "CreateTime": "2020-09-24T19:26:28.076000+00:00",
            "LastModifiedTime": "2020-09-25T04:25:22.271000+00:00",
            "LanguageCode": "language-code",
            "BaseModelName": "NarrowBand",
            "ModelStatus": "COMPLETED",
            "UpgradeAvailability": false,
            "InputDataConfig": {
                "S3Uri": "s3://amzn-s3-demo-bucket/clm-training-data/",
                "DataAccessRoleArn": "arn:aws:iam::AWS-account-number:role/IAM-role-
used-to-create-the-custom-language-model"
            }
        }
    ]
}
```

Para obtener más información, consulte Mejora de la precisión de la transcripción específica de dominios con modelos de idiomas personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte ListLanguageModels en la Referencia de comandos de la AWS CLI.

`list-medical-transcription-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-medical-transcription-jobs`.

AWS CLI

Para enumerar los trabajos de transcripción médica

En el siguiente ejemplo de `list-medical-transcription-jobs` se enumeran los trabajos de transcripción médica asociados a su y región de AWS. Para obtener más información sobre un determinado trabajo de transcripción, copie el valor de un parámetro MedicalTranscriptionJobName en el resultado de la transcripción y especifique ese valor en la opción `MedicalTranscriptionJobName` del comando `get-medical-transcription-job`. Para ver más trabajos de transcripción, copie el valor del parámetro NextToken, vuelva a ejecutar

el comando `list-medical-transcription-jobs` y especifique ese valor en la opción `--next-token`.

```
aws transcribe list-medical-transcription-jobs
```

Salida:

```
{
    "NextToken": "3/PblzkiGhzjER3KHuQt2fmbPLF7cDYafjFMEoGn44ON/
gsuUSTIkGyanvRE6WMXFd/ZTEc2EZj+P9eii/
z1O2FDYli6RLI0WoRX4RwMisVrh9G0Kie0Y8ikBCdtqlZB10Wa9McC+ebOl
+LaDtZPC4u6ttoHLRlEfzqstHXSgapXg3tEBtm9piIaPB6MOM5BB6t86+qtmocTR/
qrteHZBBudhTfbCwhsxaqujHiiUvFdm3BQbKKWIW06yV9b+4f38oD2lVIan
+vfUs3gBYAl5VTDmXXzQPBQOHPjtwmFI+IWX15nSUjWuN3TUylHgPWzDaYT8qBtu0Z+3UG4V6b
+K2CC0XszXg5rBq9hYgNzy4XoFh/6s5DoSnzq49Q9xHgHdT2yBADFmvFK7myZBsj75+2vQZOSVpWUPy3WT/32zFAcoEL
+mFYfUjtTZ8n/jq7aQEjQ42A
+X/7K6JgOcdVPtEg8PlDr5kgYYG3q3OmYXX37U3FZuJmnTI63VtIXsNnOU5eGoYObtpk00Nq9UkzgSJxqj84ZD5n
+S0EGy9ZUYBJRRcGeYUM3Q4DbSJfUwSAqcFdLIWZdp8qIREMQIBWy7BLwSdyqsQo2vRrd53hm5aWM7SVf6pPq6X/
IXR5+1eUOOD8/coaTT4ES2DerbV6RkV4o0VT1d0SdVX/
MmtkNG8nYj8PqU07w7988quh1ZP6D80veJS1q73tUUR9MjnGernW2tAnvnLNhdefBcD
+sZVfYq3iBMFY7wTy1P1G6NqW9GrYDYoX3tTPWlD7phpbVSyKrh/
PdYrps5UxnsGoA1b7L/FfAXDfUoGrGUB4N3JsPYXX9D++g+6gV1qBBs/
WfF934aKqfD6UTggm/zV3GAOWiBpfvAZRvEb924i6yGHyMC7y54O1ZAwSBupmI
+FFd13CaPO4kN1vJlth6aM5vUPXg4BpyUhtbRhwD/KxCvf9K0tLJGyL1A==",
    "MedicalTranscriptionJobSummaries": [
        {
            "MedicalTranscriptionJobName": "vocabulary-dictation-medical-
transcription-job",
            "CreationTime": "2020-09-21T21:17:27.016000+00:00",
            "StartTime": "2020-09-21T21:17:27.045000+00:00",
            "CompletionTime": "2020-09-21T21:17:59.561000+00:00",
            "LanguageCode": "en-US",
            "TranscriptionJobStatus": "COMPLETED",
            "OutputLocationType": "CUSTOMER_BUCKET",
            "Specialty": "PRIMARYCARE",
            "Type": "DICTATION"
        },
        {
            "MedicalTranscriptionJobName": "alternatives-dictation-medical-
transcription-job",
            "CreationTime": "2020-09-21T21:01:14.569000+00:00",
            "StartTime": "2020-09-21T21:01:14.592000+00:00",
            "CompletionTime": "2020-09-21T21:01:43.606000+00:00",
```

```
            "LanguageCode": "en-US",
            "TranscriptionJobStatus": "COMPLETED",
            "OutputLocationType": "CUSTOMER_BUCKET",
            "Specialty": "PRIMARYCARE",
            "Type": "DICTATION"
        },
        {
            "MedicalTranscriptionJobName": "alternatives-conversation-medical-
transcription-job",
            "CreationTime": "2020-09-21T19:09:18.171000+00:00",
            "StartTime": "2020-09-21T19:09:18.199000+00:00",
            "CompletionTime": "2020-09-21T19:10:22.516000+00:00",
            "LanguageCode": "en-US",
            "TranscriptionJobStatus": "COMPLETED",
            "OutputLocationType": "CUSTOMER_BUCKET",
            "Specialty": "PRIMARYCARE",
            "Type": "CONVERSATION"
        },
        {
            "MedicalTranscriptionJobName": "speaker-id-conversation-medical-
transcription-job",
            "CreationTime": "2020-09-21T18:43:37.157000+00:00",
            "StartTime": "2020-09-21T18:43:37.265000+00:00",
            "CompletionTime": "2020-09-21T18:44:21.192000+00:00",
            "LanguageCode": "en-US",
            "TranscriptionJobStatus": "COMPLETED",
            "OutputLocationType": "CUSTOMER_BUCKET",
            "Specialty": "PRIMARYCARE",
            "Type": "CONVERSATION"
        },
        {
            "MedicalTranscriptionJobName": "multichannel-conversation-medical-
transcription-job",
            "CreationTime": "2020-09-20T23:46:44.053000+00:00",
            "StartTime": "2020-09-20T23:46:44.081000+00:00",
            "CompletionTime": "2020-09-20T23:47:35.851000+00:00",
            "LanguageCode": "en-US",
            "TranscriptionJobStatus": "COMPLETED",
            "OutputLocationType": "CUSTOMER_BUCKET",
            "Specialty": "PRIMARYCARE",
            "Type": "CONVERSATION"
        }
    ]
```

```
}
```

Para obtener más información, consulte https://docs.aws.amazon.com/transcribe/latest/dg/batch-med-transcription.html> en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte ListMedicalTranscriptionJobs en la Referencia del comando de la AWS CLI.

`list-medical-vocabularies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-medical-vocabularies`.

AWS CLI

Para enumerar los vocabularios médicos personalizados

En el siguiente ejemplo de `list-medical-vocabularies`, se enumeran los vocabularios médicos personalizados asociados a su cuenta y región de AWS. Para obtener más información sobre un trabajo de transcripción determinado, copie el valor de un parámetro `MedicalTranscriptionJobName` en el resultado de la transcripción y especifique ese valor en la opción `MedicalTranscriptionJobName` del comando `get-medical-transcription-job`. Para ver más trabajos de transcripción, copie el valor del parámetro `NextToken`, vuelva a ejecutar el comando `list-medical-transcription-jobs` y especifique ese valor en la opción `--next-token`.

```
aws transcribe list-medical-vocabularies
```

Salida:

```
{
    "Vocabularies": [
        {
            "VocabularyName": "cli-medical-vocab-2",
            "LanguageCode": "en-US",
            "LastModifiedTime": "2020-09-21T21:44:59.521000+00:00",
            "VocabularyState": "READY"
        },
        {
            "VocabularyName": "cli-medical-vocab-1",
            "LanguageCode": "en-US",
            "LastModifiedTime": "2020-09-19T23:59:04.349000+00:00",
```

```
            "VocabularyState": "READY"
        }
    ]
}
```

Para obtener más información, consulte Vocabularios médicos personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte ListMedicalVocabularies en la Referencia de comandos de la AWS CLI.

`list-transcription-jobs`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-transcription-jobs`.

AWS CLI

Para enumerar los trabajos de transcripción

En el siguiente ejemplo de `list-transcription-jobs` se enumeran los trabajos de transcripción asociados a su cuenta y región de AWS.

```
aws transcribe list-transcription-jobs
```

Salida:

```
{
    "NextToken": "NextToken",
    "TranscriptionJobSummaries": [
        {
            "TranscriptionJobName": "speak-id-job-1",
            "CreationTime": "2020-08-17T21:06:15.391000+00:00",
            "StartTime": "2020-08-17T21:06:15.416000+00:00",
            "CompletionTime": "2020-08-17T21:07:05.098000+00:00",
            "LanguageCode": "language-code",
            "TranscriptionJobStatus": "COMPLETED",
            "OutputLocationType": "SERVICE_BUCKET"
        },
        {
            "TranscriptionJobName": "job-1",
            "CreationTime": "2020-08-17T20:50:24.207000+00:00",
            "StartTime": "2020-08-17T20:50:24.230000+00:00",
            "CompletionTime": "2020-08-17T20:52:18.737000+00:00",
```

```
            "LanguageCode": "language-code",
            "TranscriptionJobStatus": "COMPLETED",
            "OutputLocationType": "SERVICE_BUCKET"
        },
        {
            "TranscriptionJobName": "sdk-test-job-4",
            "CreationTime": "2020-08-17T20:32:27.917000+00:00",
            "StartTime": "2020-08-17T20:32:27.956000+00:00",
            "CompletionTime": "2020-08-17T20:33:15.126000+00:00",
            "LanguageCode": "language-code",
            "TranscriptionJobStatus": "COMPLETED",
            "OutputLocationType": "SERVICE_BUCKET"
        },
        {
            "TranscriptionJobName": "Diarization-speak-id",
            "CreationTime": "2020-08-10T22:10:09.066000+00:00",
            "StartTime": "2020-08-10T22:10:09.116000+00:00",
            "CompletionTime": "2020-08-10T22:26:48.172000+00:00",
            "LanguageCode": "language-code",
            "TranscriptionJobStatus": "COMPLETED",
            "OutputLocationType": "SERVICE_BUCKET"
        },
        {
            "TranscriptionJobName": "your-transcription-job-name",
            "CreationTime": "2020-07-29T17:45:09.791000+00:00",
            "StartTime": "2020-07-29T17:45:09.826000+00:00",
            "CompletionTime": "2020-07-29T17:46:20.831000+00:00",
            "LanguageCode": "language-code",
            "TranscriptionJobStatus": "COMPLETED",
            "OutputLocationType": "SERVICE_BUCKET"
        }
    ]
}
```

Para obtener más información, consulte Introducción (interfaz de línea de comandos de AWS) en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte ListTranscriptionJobs en la Referencia de comandos de la AWS CLI.

`list-vocabularies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-vocabularies`.

AWS CLI

Para enumerar los vocabularios personalizados

En el siguiente ejemplo de `list-vocabularies` se enumeran los vocabularios personalizados asociados a su cuenta y región de AWS.

```
aws transcribe list-vocabularies
```

Salida:

```
{
    "NextToken": "NextToken",
    "Vocabularies": [
        {
            "VocabularyName": "ards-test-1",
            "LanguageCode": "language-code",
            "LastModifiedTime": "2020-04-27T22:00:27.330000+00:00",
            "VocabularyState": "READY"
        },
        {
            "VocabularyName": "sample-test",
            "LanguageCode": "language-code",
            "LastModifiedTime": "2020-04-24T23:04:11.044000+00:00",
            "VocabularyState": "READY"
        },
        {
            "VocabularyName": "CRLF-to-LF-test-3-1",
            "LanguageCode": "language-code",
            "LastModifiedTime": "2020-04-24T22:12:22.277000+00:00",
            "VocabularyState": "READY"
        },
        {
            "VocabularyName": "CRLF-to-LF-test-2",
            "LanguageCode": "language-code",
            "LastModifiedTime": "2020-04-24T21:53:50.455000+00:00",
            "VocabularyState": "READY"
        },
        {
            "VocabularyName": "CRLF-to-LF-1-1",
            "LanguageCode": "language-code",
            "LastModifiedTime": "2020-04-24T21:39:33.356000+00:00",
            "VocabularyState": "READY"
```

```
        }
    ]
}
```

Para obtener más información, consulte Vocabularios personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte ListVocabularies en la Referencia de comandos de la AWS CLI.

`list-vocabulary-filters`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-vocabulary-filters`.

AWS CLI

Para enumerar sus filtros de vocabulario

En el siguiente ejemplo de `list-vocabulary-filters`, se enumeran los filtros de vocabulario asociados a su cuenta y región de AWS.

```
aws transcribe list-vocabulary-filters
```

Salida:

```
{
    "NextToken": "NextToken": [
        {
            "VocabularyFilterName": "testFilter",
            "LanguageCode": "language-code",
            "LastModifiedTime": "2020-05-07T22:39:32.147000+00:00"
        },
        {
            "VocabularyFilterName": "testFilter2",
            "LanguageCode": "language-code",
            "LastModifiedTime": "2020-05-21T23:29:35.174000+00:00"
        },
        {
            "VocabularyFilterName": "filter2",
            "LanguageCode": "language-code",
            "LastModifiedTime": "2020-05-08T20:18:26.426000+00:00"
        },
        {
```

```
            "VocabularyFilterName": "filter-review",
            "LanguageCode": "language-code",
            "LastModifiedTime": "2020-06-03T18:52:30.448000+00:00"
        },
        {
            "VocabularyFilterName": "crlf-filt",
            "LanguageCode": "language-code",
            "LastModifiedTime": "2020-05-22T19:42:42.737000+00:00"
        }
    ]
}
```

Para obtener más información, consulte Filtering Unwanted Words en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte ListVocabularyFilters en la Referencia de comandos de la AWS CLI.

`start-medical-transcription-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-medical-transcription-job`.

AWS CLI

Ejemplo 1: transcribir un dictado médico almacenado como un archivo de audio

En el siguiente ejemplo de `start-medical-transcription-job` se transcribe un archivo de audio. Especifique la ubicación del resultado de la transcripción en el parámetro `OutputBucketName`.

```
aws transcribe start-medical-transcription-job \
    --cli-input-json file://myfile.json
```

Contenidos de `myfile.json`:

```
{
    "MedicalTranscriptionJobName": "simple-dictation-medical-transcription-job",
    "LanguageCode": "language-code",
    "Specialty": "PRIMARYCARE",
    "Type": "DICTATION",
    "OutputBucketName":"amzn-s3-demo-bucket",
```

```
    "Media": {
        "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.extension"
    }
}
```

Salida:

```
{
    "MedicalTranscriptionJob": {
        "MedicalTranscriptionJobName": "simple-dictation-medical-transcription-job",
        "TranscriptionJobStatus": "IN_PROGRESS",
        "LanguageCode": "language-code",
        "Media": {
            "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.extension"
        },
        "StartTime": "2020-09-20T00:35:22.256000+00:00",
        "CreationTime": "2020-09-20T00:35:22.218000+00:00",
        "Specialty": "PRIMARYCARE",
        "Type": "DICTATION"
    }
}
```

Para obtener más información, consulte Información general de la transcripción por lotes en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 2: transcribir un diálogo entre el médico y el paciente almacenado como un archivo de audio

En el siguiente ejemplo de `start-medical-transcription-job` se transcribe un archivo de audio que contiene un diálogo entre el médico y el paciente. Especifique la ubicación del resultado de la transcripción en el parámetro OutputBucketName.

```
aws transcribe start-medical-transcription-job \
    --cli-input-json file://mysecondfile.json
```

Contenido de `mysecondfile.json`:

```
{
    "MedicalTranscriptionJobName": "simple-dictation-medical-transcription-job",
    "LanguageCode": "language-code",
    "Specialty": "PRIMARYCARE",
    "Type": "CONVERSATION",
```

```
    "OutputBucketName":"amzn-s3-demo-bucket",
    "Media": {
        "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.extension"
    }
}
```

Salida:

```
{
    "MedicalTranscriptionJob": {
        "MedicalTranscriptionJobName": "simple-conversation-medical-transcription-
job",
        "TranscriptionJobStatus": "IN_PROGRESS",
        "LanguageCode": "language-code",
        "Media": {
            "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.extension"
        },
        "StartTime": "2020-09-20T23:19:49.965000+00:00",
        "CreationTime": "2020-09-20T23:19:49.941000+00:00",
        "Specialty": "PRIMARYCARE",
        "Type": "CONVERSATION"
    }
}
```

Para obtener más información, consulte Información general de la transcripción por lotes en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 3: transcribir un archivo de audio multicanal de un diálogo entre el médico y el paciente

En el siguiente ejemplo de `start-medical-transcription-job` se transcribe el audio de cada canal del archivo de audio y se combinan las transcripciones independientes de cada canal en un único resultado de transcripción. Especifique la ubicación del resultado de la transcripción en el parámetro `OutputBucketName`.

```
aws transcribe start-medical-transcription-job \
    --cli-input-json file://mythirdfile.json
```

Contenido de `mythirdfile.json`:

```
{
    "MedicalTranscriptionJobName": "multichannel-conversation-medical-transcription-
job",
```

```
    "LanguageCode": "language-code",
    "Specialty": "PRIMARYCARE",
    "Type": "CONVERSATION",
    "OutputBucketName":"amzn-s3-demo-bucket",
        "Media": {
          "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.extension"
        },
        "Settings":{
          "ChannelIdentification": true
        }
}
```

Salida:

```
{
    "MedicalTranscriptionJob": {
        "MedicalTranscriptionJobName": "multichannel-conversation-medical-
transcription-job",
        "TranscriptionJobStatus": "IN_PROGRESS",
        "LanguageCode": "language-code",
        "Media": {
            "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.extension"
        },
        "StartTime": "2020-09-20T23:46:44.081000+00:00",
        "CreationTime": "2020-09-20T23:46:44.053000+00:00",
        "Settings": {
            "ChannelIdentification": true
        },
        "Specialty": "PRIMARYCARE",
        "Type": "CONVERSATION"
    }
}
```

Para obtener más información, consulte Identificación de canales en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 4: transcribir un archivo de audio de un diálogo entre el médico y el paciente e identificar a los interlocutores en el resultado de la transcripción

En el siguiente ejemplo de `start-medical-transcription-job` se transcribe un archivo de audio y se etiqueta la voz de cada interlocutor en el resultado de la transcripción. Especifique la ubicación del resultado de la transcripción en el parámetro `OutputBucketName`.

```
aws transcribe start-medical-transcription-job \
    --cli-input-json file://myfourthfile.json
```

Contenido de `myfourthfile.json`:

```
{
    "MedicalTranscriptionJobName": "speaker-id-conversation-medical-transcription-
job",
    "LanguageCode": "language-code",
    "Specialty": "PRIMARYCARE",
    "Type": "CONVERSATION",
    "OutputBucketName":"amzn-s3-demo-bucket",
    "Media": {
        "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.extension"
        },
    "Settings":{
        "ShowSpeakerLabels": true,
        "MaxSpeakerLabels": 2
        }
}
```

Salida:

```
{
    "MedicalTranscriptionJob": {
        "MedicalTranscriptionJobName": "speaker-id-conversation-medical-
transcription-job",
        "TranscriptionJobStatus": "IN_PROGRESS",
        "LanguageCode": "language-code",
        "Media": {
            "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.extension"
        },
        "StartTime": "2020-09-21T18:43:37.265000+00:00",
        "CreationTime": "2020-09-21T18:43:37.157000+00:00",
        "Settings": {
            "ShowSpeakerLabels": true,
            "MaxSpeakerLabels": 2
        },
        "Specialty": "PRIMARYCARE",
        "Type": "CONVERSATION"
    }
}
```

Para obtener más información, consulte Identificación de interlocutores en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 5: transcribir una conversación médica almacenada como un archivo de audio con hasta dos alternativas de transcripción

En el siguiente ejemplo de `start-medical-transcription-job` crea hasta dos transcripciones alternativas a partir de un único archivo de audio. Cada transcripción tiene un nivel de confianza asociado. De forma predeterminada, Amazon Transcribe devuelve la transcripción con el nivel de confianza más alto. Puede especificar que Amazon Transcribe devuelva otras transcripciones con niveles de confianza más bajos. Especifique la ubicación del resultado de la transcripción en el parámetro `OutputBucketName`.

```
aws transcribe start-medical-transcription-job \
    --cli-input-json file://myfifthfile.json
```

Contenido de `myfifthfile.json`:

```
{
    "MedicalTranscriptionJobName": "alternatives-conversation-medical-transcription-
job",
    "LanguageCode": "language-code",
    "Specialty": "PRIMARYCARE",
    "Type": "CONVERSATION",
    "OutputBucketName":"amzn-s3-demo-bucket",
    "Media": {
        "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.extension"
    },
    "Settings":{
        "ShowAlternatives": true,
        "MaxAlternatives": 2
    }
}
```

Salida:

```
{
    "MedicalTranscriptionJob": {
        "MedicalTranscriptionJobName": "alternatives-conversation-medical-
transcription-job",
        "TranscriptionJobStatus": "IN_PROGRESS",
```

```
        "LanguageCode": "language-code",
        "Media": {
            "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.extension"
        },
        "StartTime": "2020-09-21T19:09:18.199000+00:00",
        "CreationTime": "2020-09-21T19:09:18.171000+00:00",
        "Settings": {
            "ShowAlternatives": true,
            "MaxAlternatives": 2
        },
        "Specialty": "PRIMARYCARE",
        "Type": "CONVERSATION"
    }
}
```

Para obtener más información, consulte Transcripciones alternativas en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 6: transcribir un archivo de audio de un dictado médico con hasta dos transcripciones alternativas

En el siguiente ejemplo de `start-medical-transcription-job` se transcribe un archivo de audio y se utiliza un filtro de vocabulario para ocultar las palabras no deseadas. Especifique la ubicación del resultado de la transcripción en el parámetro OutputBucketName.

```
aws transcribe start-medical-transcription-job \
    --cli-input-json file://mysixthfile.json
```

Contenido de `mysixthfile.json`:

```
{
    "MedicalTranscriptionJobName": "alternatives-conversation-medical-transcription-
job",
    "LanguageCode": "language-code",
    "Specialty": "PRIMARYCARE",
    "Type": "DICTATION",
    "OutputBucketName":"amzn-s3-demo-bucket",
    "Media": {
        "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.extension"
    },
    "Settings":{
          "ShowAlternatives": true,
```

```
            "MaxAlternatives": 2
    }
}
```

Salida:

```
{
    "MedicalTranscriptionJob": {
        "MedicalTranscriptionJobName": "alternatives-dictation-medical-
transcription-job",
        "TranscriptionJobStatus": "IN_PROGRESS",
        "LanguageCode": "language-code",
        "Media": {
            "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.extension"
        },
        "StartTime": "2020-09-21T21:01:14.592000+00:00",
        "CreationTime": "2020-09-21T21:01:14.569000+00:00",
        "Settings": {
            "ShowAlternatives": true,
            "MaxAlternatives": 2
        },
        "Specialty": "PRIMARYCARE",
        "Type": "DICTATION"
    }
}
```

Para obtener más información, consulte Transcripciones alternativas en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 7: transcribir un archivo de audio de un dictado médico con mayor precisión mediante un vocabulario personalizado

En el siguiente ejemplo de `start-medical-transcription-job` se transcribe un archivo de audio y se utiliza un vocabulario médico personalizado que haya creado anteriormente para aumentar la precisión de la transcripción. Especifique la ubicación del resultado de la transcripción en el parámetro `OutputBucketName`.

```
aws transcribe start-transcription-job \
    --cli-input-json file://myseventhfile.json
```

Contenido de `mysixthfile.json`:

```
{
    "MedicalTranscriptionJobName": "vocabulary-dictation-medical-transcription-job",
    "LanguageCode": "language-code",
    "Specialty": "PRIMARYCARE",
    "Type": "DICTATION",
    "OutputBucketName":"amzn-s3-demo-bucket",
    "Media": {
        "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.extension"
    },
    "Settings":{
        "VocabularyName": "cli-medical-vocab-1"
    }
}
```

Salida:

```
{
    "MedicalTranscriptionJob": {
        "MedicalTranscriptionJobName": "vocabulary-dictation-medical-transcription-
job",
        "TranscriptionJobStatus": "IN_PROGRESS",
        "LanguageCode": "language-code",
        "Media": {
            "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.extension"
        },
        "StartTime": "2020-09-21T21:17:27.045000+00:00",
        "CreationTime": "2020-09-21T21:17:27.016000+00:00",
        "Settings": {
            "VocabularyName": "cli-medical-vocab-1"
        },
        "Specialty": "PRIMARYCARE",
        "Type": "DICTATION"
    }
}
```

Para obtener más información, consulte Vocabularios médicos personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte StartMedicalTranscriptionJob en la Referencia de comandos de la AWS CLI.

`start-transcription-job`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-transcription-job`.

AWS CLI

Ejemplo 1: transcribir un archivo de audio

En el siguiente ejemplo de `start-transcription-job` se transcribe un archivo de audio.

```
aws transcribe start-transcription-job \
    --cli-input-json file://myfile.json
```

Contenidos de `myfile.json`:

```
{
    "TranscriptionJobName": "cli-simple-transcription-job",
    "LanguageCode": "the-language-of-your-transcription-job",
    "Media": {
        "MediaFileUri": "s3://amzn-s3-demo-bucket/Amazon-S3-prefix/your-media-file-
name.file-extension"
    }
}
```

Para obtener más información, consulte Introducción (interfaz de línea de comandos de AWS) en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 2: transcribir un archivo de audio multicanal

En el siguiente ejemplo de `start-transcription-job` se transcribe un archivo de audio multicanal.

```
aws transcribe start-transcription-job \
    --cli-input-json file://mysecondfile.json
```

Contenido de `mysecondfile.json`:

```
{
    "TranscriptionJobName": "cli-channelid-job",
    "LanguageCode": "the-language-of-your-transcription-job",
    "Media": {
```

```
        "MediaFileUri": "s3://amzn-s3-demo-bucket/Amazon-S3-prefix/your-media-file-
name.file-extension"
    },
    "Settings":{
        "ChannelIdentification":true
    }
}
```

Salida:

```
{
    "TranscriptionJob": {
        "TranscriptionJobName": "cli-channelid-job",
        "TranscriptionJobStatus": "IN_PROGRESS",
        "LanguageCode": "the-language-of-your-transcription-job",
        "Media": {
            "MediaFileUri": "s3://amzn-s3-demo-bucket/Amazon-S3-prefix/your-media-
file-name.file-extension"
        },
        "StartTime": "2020-09-17T16:07:56.817000+00:00",
        "CreationTime": "2020-09-17T16:07:56.784000+00:00",
        "Settings": {
            "ChannelIdentification": true
        }
    }
}
```

Para obtener más información, consulte Transcripción de audio multicanal en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 3: transcribir un archivo de audio e identificar a los distintos interlocutores

En el siguiente ejemplo de `start-transcription-job` se transcribe un archivo de audio y se identifica la voz de los interlocutores en el resultado de la transcripción.

```
aws transcribe start-transcription-job \
    --cli-input-json file://mythirdfile.json
```

Contenido de `mythirdfile.json`:

```
{
    "TranscriptionJobName": "cli-speakerid-job",
```

```
    "LanguageCode": "the-language-of-your-transcription-job",
    "Media": {
        "MediaFileUri": "s3://amzn-s3-demo-bucket/Amazon-S3-prefix/your-media-file-
name.file-extension"
    },
    "Settings":{
    "ShowSpeakerLabels": true,
    "MaxSpeakerLabels": 2
    }
}
```

Salida:

```
{
    "TranscriptionJob": {
        "TranscriptionJobName": "cli-speakerid-job",
        "TranscriptionJobStatus": "IN_PROGRESS",
        "LanguageCode": "the-language-of-your-transcription-job",
        "Media": {
            "MediaFileUri": "s3://amzn-s3-demo-bucket/Amazon-S3-prefix/your-media-
file-name.file-extension"
        },
        "StartTime": "2020-09-17T16:22:59.696000+00:00",
        "CreationTime": "2020-09-17T16:22:59.676000+00:00",
        "Settings": {
            "ShowSpeakerLabels": true,
            "MaxSpeakerLabels": 2
        }
    }
}
```

Para obtener más información, consulte Identificación de interlocutores en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 4: transcribir un archivo de audio y ocultar las palabras no deseadas en el resultado de la transcripción

En el siguiente ejemplo de `start-transcription-job` se transcribe un archivo de audio y se utiliza un filtro de vocabulario que ha creado anteriormente para ocultar las palabras no deseadas.

```
aws transcribe start-transcription-job \
    --cli-input-json file://myfourthfile.json
```

Contenido de `myfourthfile.json`:

```
{
    "TranscriptionJobName": "cli-filter-mask-job",
    "LanguageCode": "the-language-of-your-transcription-job",
    "Media": {
          "MediaFileUri": "s3://amzn-s3-demo-bucket/Amazon-S3-prefix/your-media-
file-name.file-extension"
    },
    "Settings":{
        "VocabularyFilterName": "your-vocabulary-filter",
        "VocabularyFilterMethod": "mask"
    }
}
```

Salida:

```
{
    "TranscriptionJob": {
        "TranscriptionJobName": "cli-filter-mask-job",
        "TranscriptionJobStatus": "IN_PROGRESS",
        "LanguageCode": "the-language-of-your-transcription-job",
        "Media": {
            "MediaFileUri": "s3://Amazon-S3-Prefix/your-media-file.file-extension"
        },
        "StartTime": "2020-09-18T16:36:18.568000+00:00",
        "CreationTime": "2020-09-18T16:36:18.547000+00:00",
        "Settings": {
            "VocabularyFilterName": "your-vocabulary-filter",
            "VocabularyFilterMethod": "mask"
        }
    }
}
```

Para obtener más información, consulte Filtrado de transcripciones en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 5: transcribir un archivo de audio y eliminar las palabras no deseadas en el resultado de la transcripción

En el siguiente ejemplo de `start-transcription-job` se transcribe un archivo de audio y se utiliza un filtro de vocabulario que ha creado anteriormente para ocultar las palabras no deseadas.

```
aws transcribe start-transcription-job \
    --cli-input-json file://myfifthfile.json
```

Contenido de `myfifthfile.json`:

```
{
    "TranscriptionJobName": "cli-filter-remove-job",
    "LanguageCode": "the-language-of-your-transcription-job",
    "Media": {
        "MediaFileUri": "s3://amzn-s3-demo-bucket/Amazon-S3-prefix/your-media-file-
name.file-extension"
    },
    "Settings":{
        "VocabularyFilterName": "your-vocabulary-filter",
        "VocabularyFilterMethod": "remove"
    }
}
```

Salida:

```
{
    "TranscriptionJob": {
        "TranscriptionJobName": "cli-filter-remove-job",
        "TranscriptionJobStatus": "IN_PROGRESS",
        "LanguageCode": "the-language-of-your-transcription-job",
        "Media": {
            "MediaFileUri": "s3://amzn-s3-demo-bucket/Amazon-S3-prefix/your-media-
file-name.file-extension"
        },
        "StartTime": "2020-09-18T16:36:18.568000+00:00",
        "CreationTime": "2020-09-18T16:36:18.547000+00:00",
        "Settings": {
            "VocabularyFilterName": "your-vocabulary-filter",
            "VocabularyFilterMethod": "remove"
        }
    }
}
```

Para obtener más información, consulte Filtrado de transcripciones en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 6: transcribir un archivo de audio con mayor precisión mediante un vocabulario personalizado

En el siguiente ejemplo de `start-transcription-job` se transcribe un archivo de audio y se utiliza un filtro de vocabulario que ha creado anteriormente para ocultar las palabras no deseadas.

```
aws transcribe start-transcription-job \
    --cli-input-json file://mysixthfile.json
```

Contenido de `mysixthfile.json`:

```
{
    "TranscriptionJobName": "cli-vocab-job",
    "LanguageCode": "the-language-of-your-transcription-job",
    "Media": {
        "MediaFileUri": "s3://amzn-s3-demo-bucket/Amazon-S3-prefix/your-media-file-
name.file-extension"
    },
    "Settings":{
        "VocabularyName": "your-vocabulary"
    }
}
```

Salida:

```
{
    "TranscriptionJob": {
        "TranscriptionJobName": "cli-vocab-job",
        "TranscriptionJobStatus": "IN_PROGRESS",
        "LanguageCode": "the-language-of-your-transcription-job",
        "Media": {
            "MediaFileUri": "s3://amzn-s3-demo-bucket/Amazon-S3-prefix/your-media-
file-name.file-extension"
        },
        "StartTime": "2020-09-18T16:36:18.568000+00:00",
        "CreationTime": "2020-09-18T16:36:18.547000+00:00",
        "Settings": {
            "VocabularyName": "your-vocabulary"
        }
    }
}
```

Para obtener más información, consulte Filtrado de transcripciones en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 7: identificar el idioma de un archivo de audio y transcribirlo

En el siguiente ejemplo de `start-transcription-job` se transcribe un archivo de audio y se utiliza un filtro de vocabulario que ha creado anteriormente para ocultar las palabras no deseadas.

```
aws transcribe start-transcription-job \
    --cli-input-json file://myseventhfile.json
```

Contenido de `myseventhfile.json`:

```
{
    "TranscriptionJobName": "cli-identify-language-transcription-job",
    "IdentifyLanguage": true,
    "Media": {
        "MediaFileUri": "s3://amzn-s3-demo-bucket/Amazon-S3-prefix/your-media-file-
name.file-extension"
    }
}
```

Salida:

```
{
    "TranscriptionJob": {
        "TranscriptionJobName": "cli-identify-language-transcription-job",
        "TranscriptionJobStatus": "IN_PROGRESS",
        "Media": {
            "MediaFileUri": "s3://amzn-s3-demo-bucket/Amazon-S3-prefix/your-media-
file-name.file-extension"
        },
        "StartTime": "2020-09-18T22:27:23.970000+00:00",
        "CreationTime": "2020-09-18T22:27:23.948000+00:00",
        "IdentifyLanguage": true
    }
}
```

Para obtener más información, consulte Identificación del idioma en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 8: transcribir un archivo de audio con información de identificación personal redactada

En el siguiente ejemplo de `start-transcription-job` se transcribe un archivo de audio y se redacta la información de identificación personal en el resultado de la transcripción.

```
aws transcribe start-transcription-job \
    --cli-input-json file://myeighthfile.json
```

Contenido de `myeigthfile.json`:

```
{
    "TranscriptionJobName": "cli-redaction-job",
    "LanguageCode": "language-code",
    "Media": {
        "MediaFileUri": "s3://Amazon-S3-Prefix/your-media-file.file-extension"
    },
    "ContentRedaction": {
        "RedactionOutput":"redacted",
        "RedactionType":"PII"
    }
}
```

Salida:

```
{
    "TranscriptionJob": {
        "TranscriptionJobName": "cli-redaction-job",
        "TranscriptionJobStatus": "IN_PROGRESS",
        "LanguageCode": "language-code",
        "Media": {
            "MediaFileUri": "s3://Amazon-S3-Prefix/your-media-file.file-extension"
        },
        "StartTime": "2020-09-25T23:49:13.195000+00:00",
        "CreationTime": "2020-09-25T23:49:13.176000+00:00",
        "ContentRedaction": {
            "RedactionType": "PII",
            "RedactionOutput": "redacted"
        }
    }
}
```

Para obtener más información, consulte Redacción automática de contenido en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 9: generar una transcripción con información de identificación personal (PII) redactada y una transcripción sin redactar

En el siguiente ejemplo de `start-transcription-job` se generan dos transcripciones del archivo de audio, una con la información de identificación personal redactada y la otra sin ninguna redacción.

```
aws transcribe start-transcription-job \
    --cli-input-json file://myninthfile.json
```

Contenido de `myninthfile.json`:

```
{
    "TranscriptionJobName": "cli-redaction-job-with-unredacted-transcript",
    "LanguageCode": "language-code",
    "Media": {
          "MediaFileUri": "s3://Amazon-S3-Prefix/your-media-file.file-extension"
        },
    "ContentRedaction": {
        "RedactionOutput":"redacted_and_unredacted",
        "RedactionType":"PII"
    }
}
```

Salida:

```
{
    "TranscriptionJob": {
        "TranscriptionJobName": "cli-redaction-job-with-unredacted-transcript",
        "TranscriptionJobStatus": "IN_PROGRESS",
        "LanguageCode": "language-code",
        "Media": {
            "MediaFileUri": "s3://Amazon-S3-Prefix/your-media-file.file-extension"
        },
        "StartTime": "2020-09-25T23:59:47.677000+00:00",
        "CreationTime": "2020-09-25T23:59:47.653000+00:00",
        "ContentRedaction": {
            "RedactionType": "PII",
            "RedactionOutput": "redacted_and_unredacted"
        }
    }
}
```

Para obtener más información, consulte Redacción automática de contenido en la Guía para desarrolladores de Amazon Transcribe.

Ejemplo 10: usar un modelo de idioma personalizado que haya creado previamente para transcribir un archivo de audio

En el siguiente ejemplo de `start-transcription-job` se transcribe un archivo de audio con un modelo de idioma personalizado que haya creado anteriormente.

```
aws transcribe start-transcription-job \
    --cli-input-json file://mytenthfile.json
```

Contenido de `mytenthfile.json`:

```
{
    "TranscriptionJobName": "cli-clm-2-job-1",
    "LanguageCode": "language-code",
    "Media": {
        "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.file-extension"
    },
    "ModelSettings": {
        "LanguageModelName":"cli-clm-2"
    }
}
```

Salida:

```
{
    "TranscriptionJob": {
        "TranscriptionJobName": "cli-clm-2-job-1",
        "TranscriptionJobStatus": "IN_PROGRESS",
        "LanguageCode": "language-code",
        "Media": {
            "MediaFileUri": "s3://amzn-s3-demo-bucket/your-audio-file.file-
extension"
        },
        "StartTime": "2020-09-28T17:56:01.835000+00:00",
        "CreationTime": "2020-09-28T17:56:01.801000+00:00",
        "ModelSettings": {
            "LanguageModelName": "cli-clm-2"
        }
    }
```

```
}
```

Para obtener más información, consulte Mejora de la precisión de la transcripción específica de dominios con modelos de idiomas personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte StartTranscriptionJob en la Referencia de comandos de la AWS CLI.

`update-medical-vocabulary`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-medical-vocabulary`.

AWS CLI

Para actualizar un vocabulario médico personalizado con términos nuevos

En el siguiente ejemplo de `update-medical-vocabulary`, se sustituyen los términos utilizados en un vocabulario médico personalizado por otros nuevos. Requisito previo: sustituir los términos de un vocabulario médico personalizado, necesita un archivo con términos nuevos.

```
aws transcribe update-medical-vocabulary \
    --vocabulary-file-uri s3://amzn-s3-demo-bucket/Amazon-S3-Prefix/medical-custom-vocabulary.txt \
    --vocabulary-name medical-custom-vocabulary \
    --language-code language
```

Salida:

```
{
    "VocabularyName": "medical-custom-vocabulary",
    "LanguageCode": "en-US",
    "VocabularyState": "PENDING"
}
```

Para obtener más información, consulte Vocabularios médicos personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte UpdateMedicalVocabulary en la Referencia de comandos de la AWS CLI.

`update-vocabulary-filter`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-vocabulary-filter`.

AWS CLI

Para reemplazar las palabras de un filtro de vocabulario

En el siguiente ejemplo de `update-vocabulary-filter`, se sustituyen las palabras de un filtro de vocabulario por otras nuevas. Requisito previo: actualizar un filtro de vocabulario con palabras nuevas, debe guardarlas como archivo de texto.

```
aws transcribe update-vocabulary-filter \
    --vocabulary-filter-file-uri s3://amzn-s3-demo-bucket/Amazon-S3-Prefix/your-text-file-to-update-your-vocabulary-filter.txt \
    --vocabulary-filter-name vocabulary-filter-name
```

Salida:

```
{
    "VocabularyFilterName": "vocabulary-filter-name",
    "LanguageCode": "language-code",
    "LastModifiedTime": "2020-09-23T18:40:35.139000+00:00"
}
```

Para obtener más información, consulte Filtering Unwanted Words en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte UpdateVocabularyFilter en la Referencia de comandos de la AWS CLI.

`update-vocabulary`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-vocabulary`.

AWS CLI

Para actualizar un vocabulario personalizado con términos nuevos.

En el siguiente ejemplo de `update-vocabulary` se sobrescriben los términos utilizados para crear un vocabulario personalizado con los nuevos que proporcione. Requisito previo: sustituir los términos de un vocabulario personalizado, necesita un archivo con términos nuevos.

```
aws transcribe update-vocabulary \
    --vocabulary-file-uri s3://amzn-s3-demo-bucket/Amazon-S3-Prefix/custom-vocabulary.txt \
    --vocabulary-name custom-vocabulary \
    --language-code language-code
```

Salida:

```
{
    "VocabularyName": "custom-vocabulary",
    "LanguageCode": "language",
    "VocabularyState": "PENDING"
}
```

Para obtener más información, consulte Vocabularios personalizados en la Guía para desarrolladores de Amazon Transcribe.

- Para obtener información sobre la API, consulte UpdateVocabulary en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon Translate que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon Translate.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`import-terminology`

En el siguiente ejemplo de código, se muestra cómo utilizar `import-terminology`.

AWS CLI

Para importar una terminología personalizada de un archivo

En el siguiente ejemplo de `import-terminology`, se crea una terminología llamada `MyTestTerminology` desde el archivo `test-terminology.csv`:

```
aws translate import-terminology \
    --name MyTestTerminology \
    --description "Creating a test terminology in AWS Translate" \
    --merge-strategy OVERWRITE \
    --data-file fileb://test-terminology.csv \
    --terminology-data Format=CSV
```

Contenido de `test-terminology.csv`:

en,fr,es,zh Hello world!,Bonjour tout le monde!,Hola Mundo!,????
Amazon,Amazon,Amazon,Amazon

Salida:

```
{
    "TerminologyProperties": {
        "SourceLanguageCode": "en",
        "Name": "MyTestTerminology",
        "TargetLanguageCodes": [
            "fr",
            "es",
            "zh"
        ],
        "SizeBytes": 97,
        "LastUpdatedAt": 1571089500.851,
        "CreatedAt": 1571089500.851,
        "TermCount": 6,
        "Arn": "arn:aws:translate:us-west-2:123456789012:terminology/
MyTestTerminology/LATEST",
        "Description": "Creating a test terminology in AWS Translate"
    }
}
```

- Para obtener información sobre la API, consulte ImportTerminology en la Referencia de comandos de la AWS CLI.

Trusted Advisor Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Trusted Advisor.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`get-organization-recommendation`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-organization-recommendation`.

AWS CLI

Para obtener una recomendación de una organización

En el siguiente ejemplo de `get-organization-recommendation`, se obtiene una recomendación de una organización por su identificador.

```
aws trustedadvisor get-organization-recommendation \
    --organization-recommendation-identifier arn:aws:trustedadvisor:::organization-recommendation/9534ec9b-bf3a-44e8-8213-2ed68b39d9d5
```

Salida:

```
{
    "organizationRecommendation": {
        "arn": "arn:aws:trustedadvisor:::organization-recommendation/9534ec9b-bf3a-44e8-8213-2ed68b39d9d5",
        "name": "Lambda Runtime Deprecation Warning",
```

```
        "description": "One or more lambdas are using a deprecated runtime",
        "awsServices": [
            "lambda"
        ],
        "checkArn": "arn:aws:trustedadvisor:::check/L4dfs2Q4C5",
        "id": "9534ec9b-bf3a-44e8-8213-2ed68b39d9d5",
        "lifecycleStage": "resolved",
        "pillars": [
            "security"
        ],
        "resourcesAggregates": {
            "errorCount": 0,
            "okCount": 0,
            "warningCount": 0
        },
        "source": "ta_check",
        "status": "warning",
        "type": "priority"
    }
}
```

Para obtener más información, consulte Get started with the Trusted Advisor API en la Guía del usuario de AWS Trusted Advisor.

- Para obtener información sobre la API, consulte GetOrganizationRecommendation en la Referencia de comandos de la AWS CLI.

`get-recommendation`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-recommendation`.

AWS CLI

Para obtener una recomendación

En el siguiente ejemplo de `get-recommendation`, se obtiene una recomendación por su identificador.

```
aws trustedadvisor get-recommendation \
    --recommendation-
identifier arn:aws:trustedadvisor::000000000000:recommendation/55fa4d2e-
bbb7-491a-833b-5773e9589578
```

Salida:

```
{
    "recommendation": {
        "arn": "arn:aws:trustedadvisor::000000000000:recommendation/55fa4d2e-
bbb7-491a-833b-5773e9589578",
        "name": "MFA Recommendation",
        "description": "Enable multi-factor authentication",
        "awsServices": [
            "iam"
        ],
        "checkArn": "arn:aws:trustedadvisor:::check/7DAFEmoDos",
        "id": "55fa4d2e-bbb7-491a-833b-5773e9589578",
        "lastUpdatedAt": "2023-11-01T15:57:58.673Z",
        "pillarSpecificAggregates": {
            "costOptimizing": {
                "estimatedMonthlySavings": 0.0,
                "estimatedPercentMonthlySavings": 0.0
            }
        },
        "pillars": [
            "security"
        ],
        "resourcesAggregates": {
            "errorCount": 1,
            "okCount": 0,
            "warningCount": 0
        },
        "source": "ta_check",
        "status": "error",
        "type": "standard"
    }
}
```

Para obtener más información, consulte Get started with the Trusted Advisor API en la Guía del usuario de AWS Trusted Advisor.

- Para obtener información sobre la API, consulte GetRecommendation en la Referencia de comandos de la AWS CLI.

`list-checks`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-checks`.

AWS CLI

Para enumerar las comprobaciones de Trusted Advisor

En el siguiente ejemplo de `list-checks`, se enumeran todas las comprobaciones de Trusted Advisor.

```
aws trustedadvisor list-checks
```

Salida:

```
{
    "checkSummaries": [
        {
            "arn": "arn:aws:trustedadvisor:::check/1iG5NDGVre",
            "awsServices": [
                "EC2"
            ],
            "description": "Checks security groups for rules that allow unrestricted
 access to a resource. Unrestricted access increases opportunities for malicious
 activity (hacking, denial-of-service attacks, loss of data)",
            "id": "1iG5NDGVre",
            "metadata": {
                "0": "Region",
                "1": "Security Group Name",
                "2": "Security Group ID",
                "3": "Protocol",
                "4": "Port",
                "5": "Status",
                "6": "IP Range"
            },
            "name": "Security Groups - Unrestricted Access",
            "pillars": [
                "security"
            ],
            "source": "ta_check"
        },
        {
            "arn": "arn:aws:trustedadvisor:::check/1qazXsw23e",
            "awsServices": [
                "RDS"
            ],
```

```
            "description": "Checks your usage of RDS and provides recommendations
on purchase of Reserved Instances to help reduce costs incurred from using RDS
On-Demand. AWS generates these recommendations by analyzing your On-Demand usage
for the past 30 days. We then simulate every combination of reservations in the
generated category of usage in order to identify the best number of each type
of Reserved Instance to purchase to maximize your savings. This check covers
recommendations based on partial upfront payment option with 1-year or 3-year
commitment. This check is not available to accounts linked in Consolidated Billing.
Recommendations are only available for the Paying Account.",
            "id": "1qazXsw23e",
            "metadata": {
                "0": "Region",
                "1": "Family",
                "2": "Instance Type",
                "3": "License Model",
                "4": "Database Edition",
                "5": "Database Engine",
                "6": "Deployment Option",
                "7": "Recommended number of Reserved Instances to purchase",
                "8": "Expected Average Reserved Instance Utilization",
                "9": "Estimated Savings with Recommendation (monthly)"
                "10": "Upfront Cost of Reserved Instances",
                "11": "Estimated cost of Reserved Instances (monthly)",
                "12": "Estimated On-Demand Cost Post Recommended Reserved Instance
Purchase (monthly)",
                "13": "Estimated Break Even (months)",
                "14": "Lookback Period (days)",
                "15": "Term (years)"
            },
            "name": "Amazon Relational Database Service (RDS) Reserved Instance
Optimization",
            "pillars": [
                "cost_optimizing"
            ],
            "source": "ta_check"
        },
        {
            "arn": "arn:aws:trustedadvisor:::check/1qw23er45t",
            "awsServices": [
                "Redshift"
            ],
            "description": "Checks your usage of Redshift and provides
recommendations on purchase of Reserved Nodes to help reduce costs incurred from
using Redshift On-Demand. AWS generates these recommendations by analyzing your
```

```
 On-Demand usage for the past 30 days. We then simulate every combination of
 reservations in the generated category of usage in order to identify the best
 number of each type of Reserved Nodes to purchase to maximize your savings. This
 check covers recommendations based on partial upfront payment option with 1-year or
 3-year commitment. This check is not available to accounts linked in Consolidated
 Billing. Recommendations are only available for the Paying Account.",
            "id": "1qw23er45t",
            "metadata": {
                "0": "Region",
                "1": "Family",
                "2": "Node Type",
                "3": "Recommended number of Reserved Nodes to purchase",
                "4": "Expected Average Reserved Node Utilization",
                "5": "Estimated Savings with Recommendation (monthly)",
                "6": "Upfront Cost of Reserved Nodes",
                "7": "Estimated cost of Reserved Nodes (monthly)",
                "8": "Estimated On-Demand Cost Post Recommended Reserved Nodes
 Purchase (monthly)",
                "9": "Estimated Break Even (months)",
                "10": "Lookback Period (days)",
                "11": "Term (years)",
            },
            "name": "Amazon Redshift Reserved Node Optimization",
            "pillars": [
                "cost_optimizing"
            ],
            "source": "ta_check"
        },
    ],
    "nextToken": "REDACTED"
}
```

Para obtener más información, consulte Get started with the Trusted Advisor API en la Guía del usuario de AWS Trusted Advisor.

- Para obtener información sobre la API, consulte ListChecks en la Referencia de comandos de la AWS CLI.

`list-organization-recommendation-accounts`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-organization-recommendation-accounts`.

AWS CLI

Para ver una lista de las cuentas recomendadas de la organización

En el siguiente ejemplo de `list-organization-recommendation-accounts`, se enumeran todos los resúmenes de recomendaciones de cuentas de una recomendación de la organización por su identificador.

```
aws trustedadvisor list-organization-recommendation-accounts \
    --organization-recommendation-identifier arn:aws:trustedadvisor:::organization-recommendation/9534ec9b-bf3a-44e8-8213-2ed68b39d9d5
```

Salida:

```
{
    "accountRecommendationLifecycleSummaries": [{
        "accountId": "000000000000",
        "accountRecommendationArn":
 "arn:aws:trustedadvisor::000000000000:recommendation/9534ec9b-
bf3a-44e8-8213-2ed68b39d9d5",
        "lifecycleStage": "resolved",
        "updateReason": "Resolved issue",
        "updateReasonCode": "valid_business_case",
        "lastUpdatedAt": "2023-01-17T18:25:44.552Z"
    }],
    "nextToken": "REDACTED"
}
```

Para obtener más información, consulte Get started with the Trusted Advisor API en la Guía del usuario de AWS Trusted Advisor.

- Para obtener información sobre la API, consulte ListOrganizationRecommendationAccounts en la Referencia de comandos de la AWS CLI.

`list-organization-recommendation-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-organization-recommendation-resources`.

AWS CLI

Para enumerar los recursos de recomendación de la organización

En el siguiente ejemplo de `list-organization-recommendation-resources`, se enumeran todos los recursos de una recomendación de la organización por su identificador.

```
aws trustedadvisor list-organization-recommendation-resources \
    --organization-recommendation-identifier arn:aws:trustedadvisor:::organization-recommendation/5a694939-2e54-45a2-ae72-730598fa89d0
```

Salida:

```
{
    "organizationRecommendationResourceSummaries": [
        {
            "arn": "arn:aws:trustedadvisor::000000000000:recommendation-resource/5a694939-2e54-45a2-ae72-730598fa89d0/bb38affc0ce0681d9a6cd13f30238ba03a8f63dfe7a379dc403c619119d86af",
            "awsResourceId": "database-1-instance-1",
            "id": "bb38affc0ce0681d9a6cd13f302383ba03a8f63dfe7a379dc403c619119d86af",
            "lastUpdatedAt": "2023-11-01T15:09:51.891Z",
            "metadata": {
                "0": "14",
                "1": "208.79999999999998",
                "2": "database-1-instance-1",
                "3": "db.r5.large",
                "4": "false",
                "5": "us-west-2",
                "6": "arn:aws:rds:us-west-2:000000000000:db:database-1-instance-1",
                "7": "1"
            },
            "recommendationArn": "arn:aws:trustedadvisor:::organization-recommendation/5a694939-2e54-45a2-ae72-730598fa89d0",
            "regionCode": "us-west-2",
            "status": "warning"
        },
        {
            "arn": "arn:aws:trustedadvisor::000000000000:recommendation-resource/5a694939-2e54-45a2-ae72-730598fa89d0/51fded4d7a3278818df9cfe344ff5762cec46c095a6763d1ba1ba53bd0e1b0e6",
            "awsResourceId": "database-1",
            "id": "51fded4d7a3278818df9cfe344ff5762cec46c095a6763d1ba1ba53bd0e1b0e6",
            "lastUpdatedAt": "2023-11-01T15:09:51.891Z",
            "metadata": {
```

```
                "0": "14",
                "1": "31.679999999999996",
                "2": "database-1",
                "3": "db.t3.small",
                "4": "false",
                "5": "us-west-2",
                "6": "arn:aws:rds:us-west-2:000000000000:db:database-1",
                "7": "20"
            },
            "recommendationArn": "arn:aws:trustedadvisor:::organization-
recommendation/5a694939-2e54-45a2-ae72-730598fa89d0",
            "regionCode": "us-west-2",
            "status": "warning"
        },
        {
            "arn": "arn:aws:trustedadvisor::000000000000:recommendation-
resource/5a694939-2e54-45a2-ae72-730598fa89d0/
f4d01bd20f4cd5372062aafc8786c489e48f0ead7cdab121463bf9f89e40a36b",
            "awsResourceId": "database-2-instance-1-us-west-2a",
            "id":
 "f4d01bd20f4cd5372062aafc8786c489e48f0ead7cdab121463bf9f89e40a36b",
            "lastUpdatedAt": "2023-11-01T15:09:51.891Z",
            "metadata": {
                "0": "14",
                "1": "187.20000000000002",
                "2": "database-2-instance-1-us-west-2a",
                "3": "db.r6g.large",
                "4": "true",
                "5": "us-west-2",
                "6": "arn:aws:rds:us-west-2:000000000000:db:database-2-instance-1-
us-west-2a",
                "7": "1"
            },
            "recommendationArn": "arn:aws:trustedadvisor:::organization-
recommendation/5a694939-2e54-45a2-ae72-730598fa89d0",
            "regionCode": "us-west-2",
            "status": "warning"
        },
    ],
    "nextToken": "REDACTED"
}
```

Para obtener más información, consulte Get started with the Trusted Advisor API en la Guía del usuario de AWS Trusted Advisor.

- Para obtener información sobre la API, consulte ListOrganizationRecommendationResources en la Referencia de comandos de la AWS CLI.

`list-organization-recommendations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-organization-recommendations`.

AWS CLI

Ejemplo 1: enumeración de las recomendaciones de la organización

En el siguiente ejemplo de `list-organization-recommendations`, se muestran todas las recomendaciones de la organización y no se incluye ningún filtro.

```
aws trustedadvisor list-organization-recommendations
```

Salida:

```
{
    "organizationRecommendationSummaries": [
        {
            "arn": "arn:aws:trustedadvisor:::organization-recommendation/9534ec9b-
bf3a-44e8-8213-2ed68b39d9d5",
            "name": "Lambda Runtime Deprecation Warning",
            "awsServices": [
                "lambda"
            ],
            "checkArn": "arn:aws:trustedadvisor:::check/L4dfs2Q4C5",
            "id": "9534ec9b-bf3a-44e8-8213-2ed68b39d9d5",
            "lifecycleStage": "resolved",
            "pillars": [
                "security"
            ],
            "resourcesAggregates": {
                "errorCount": 0,
                "okCount": 0,
                "warningCount": 0
            },
```

```
            "source": "ta_check",
            "status": "warning",
            "type": "priority"
        },
        {
            "arn": "arn:aws:trustedadvisor:::organization-
recommendation/4ecff4d4-1bc1-4c99-a5b8-0fff9ee500d6",
            "name": "Lambda Runtime Deprecation Warning",
            "awsServices": [
                "lambda"
            ],
            "checkArn": "arn:aws:trustedadvisor:::check/L4dfs2Q4C5",
            "id": "4ecff4d4-1bc1-4c99-a5b8-0fff9ee500d6",
            "lifecycleStage": "resolved",
            "pillars": [
                "security"
            ],
            "resourcesAggregates": {
                "errorCount": 0,
                "okCount": 0,
                "warningCount": 0
            },
            "source": "ta_check",
            "status": "warning",
            "type": "priority"
        },
    ],
    "nextToken": "REDACTED"
}
```

Para obtener más información, consulte Get started with the Trusted Advisor API en la Guía del usuario de AWS Trusted Advisor.

Ejemplo 2: enumeración de las recomendaciones de la organización con un filtro

En el siguiente ejemplo de `list-organization-recommendations`, se filtra y devuelve como máximo una recomendación de la organización que forma parte del pilar de seguridad.

```
aws trustedadvisor list-organization-recommendations \
    --pillar security \
    --max-items 100
```

Salida:

```
{
    "organizationRecommendationSummaries": [{
        "arn": "arn:aws:trustedadvisor:::organization-recommendation/9534ec9b-
bf3a-44e8-8213-2ed68b39d9d5",
        "name": "Lambda Runtime Deprecation Warning",
        "awsServices": [
            "lambda"
        ],
        "checkArn": "arn:aws:trustedadvisor:::check/L4dfs2Q4C5",
        "id": "9534ec9b-bf3a-44e8-8213-2ed68b39d9d5",
        "lifecycleStage": "resolved",
        "pillars": [
            "security"
        ],
        "resourcesAggregates": {
            "errorCount": 0,
            "okCount": 0,
            "warningCount": 0
        },
        "source": "ta_check",
        "status": "warning",
        "type": "priority"
    }],
    "nextToken": "REDACTED"
}
```

Para obtener más información, consulte Get started with the Trusted Advisor API en la Guía del usuario de AWS Trusted Advisor.

Ejemplo 3: enumeración de las recomendaciones de la organización con un token de paginación

En el siguiente ejemplo de `list-organization-recommendations`, se utiliza el nextToken devuelto de una solicitud anterior para buscar la siguiente página de recomendaciones de la organización.

```
aws trustedadvisor list-organization-recommendations \
    --pillar security \
    --max-items 100 \
    --starting-token <next-token>
```

Salida:

```
{
    "organizationRecommendationSummaries": [{
        "arn": "arn:aws:trustedadvisor:::organization-
recommendation/4ecff4d4-1bc1-4c99-a5b8-0fff9ee500d6",
        "name": "Lambda Runtime Deprecation Warning",
        "awsServices": [
            "lambda"
        ],
        "checkArn": "arn:aws:trustedadvisor:::check/L4dfs2Q4C5",
        "id": "4ecff4d4-1bc1-4c99-a5b8-0fff9ee500d6",
        "lifecycleStage": "resolved",
        "pillars": [
            "security"
        ],
        "resourcesAggregates": {
            "errorCount": 0,
            "okCount": 0,
            "warningCount": 0
        },
        "source": "ta_check",
        "status": "warning",
        "type": "priority"
    }]
}
```


Para obtener más información, consulte Get started with the Trusted Advisor API en la Guía del usuario de AWS Trusted Advisor.

- Para obtener información sobre la API, consulte ListOrganizationRecommendations en la Referencia de comandos de la AWS CLI.

`list-recommendation-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-recommendation-resources`.

AWS CLI

Para enumerar los recursos de una recomendación

En el siguiente ejemplo de `list-recommendation-resources`, se enumeran todos los recursos de una recomendación por su identificador.

```
aws trustedadvisor list-recommendation-resources \
    --recommendation-
identifier arn:aws:trustedadvisor::000000000000:recommendation/55fa4d2e-
bbb7-491a-833b-5773e9589578
```

Salida:

```
{
    "recommendationResourceSummaries": [
        {
            "arn": "arn:aws:trustedadvisor::000000000000:recommendation-
resource/55fa4d2e-
bbb7-491a-833b-5773e9589578/18959a1f1973cff8e706e9d9bde28bba36cd602a6b2cb86c8b6125283523601
            "id":
 "18959a1f1973cff8e706e9d9bde28bba36cd602a6b2cb86c8b61252835236010",
            "awsResourceId": "webcms-dev-01",
            "lastUpdatedAt": "2023-11-01T15:09:51.891Z",
            "metadata": {
                "0": "14",
                "1": "123.12000000000002",
                "2": "webcms-dev-01",
                "3": "db.m6i.large",
                "4": "false",
                "5": "us-east-1",
                "6": "arn:aws:rds:us-east-1:000000000000:db:webcms-dev-01",
                "7": "20"
            },
            "recommendationArn":
 "arn:aws:trustedadvisor::000000000000:recommendation/55fa4d2e-
bbb7-491a-833b-5773e9589578",
            "regionCode": "us-east-1",
            "status": "warning"
        },
        {
            "arn": "arn:aws:trustedadvisor::000000000000:recommendation-
resource/55fa4d2e-bbb7-491a-833b-5773e9589578/
e6367ff500ac90db8e4adeb4892e39ee9c36bbf812dcbce4b9e4fefcec9eb63e",
            "id":
 "e6367ff500ac90db8e4adeb4892e39ee9c36bbf812dcbce4b9e4fefcec9eb63e",
            "awsResourceId": "aws-dev-db-stack-instance-1",
            "lastUpdatedAt": "2023-11-01T15:09:51.891Z",
            "metadata": {
                "0": "14",
```

```
                "1": "29.52",
                "2": "aws-dev-db-stack-instance-1",
                "3": "db.t2.small",
                "4": "false",
                "5": "us-east-1",
                "6": "arn:aws:rds:us-east-1:000000000000:db:aws-dev-db-stack-
instance-1",
                "7": "1"
            },
            "recommendationArn":
 "arn:aws:trustedadvisor::000000000000:recommendation/55fa4d2e-
bbb7-491a-833b-5773e9589578",
            "regionCode": "us-east-1",
            "status": "warning"
        },
        {
            "arn": "arn:aws:trustedadvisor::000000000000:recommendation-
resource/55fa4d2e-
bbb7-491a-833b-5773e9589578/31aa78ba050a5015d2d38cca7f5f1ce88f70857c4e1c3ad03f8f9fd95dad7459
            "id":
 "31aa78ba050a5015d2d38cca7f5f1ce88f70857c4e1c3ad03f8f9fd95dad7459",
            "awsResourceId": "aws-awesome-apps-stack-db",
            "lastUpdatedAt": "2023-11-01T15:09:51.891Z",
            "metadata": {
                "0": "14",
                "1": "114.48000000000002",
                "2": "aws-awesome-apps-stack-db",
                "3": "db.m6g.large",
                "4": "false",
                "5": "us-east-1",
                "6": "arn:aws:rds:us-east-1:000000000000:db:aws-awesome-apps-stack-
db",
                "7": "100"
            },
            "recommendationArn":
 "arn:aws:trustedadvisor::000000000000:recommendation/55fa4d2e-
bbb7-491a-833b-5773e9589578",
            "regionCode": "us-east-1",
            "status": "warning"
        }
    ],
    "nextToken": "REDACTED"
}
```

Para obtener más información, consulte Get started with the Trusted Advisor API en la Guía del usuario de AWS Trusted Advisor.

- Para obtener información sobre la API, consulte ListRecommendationResources en la Referencia de comandos de la AWS CLI.

`list-recommendations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-recommendations`.

AWS CLI

Ejemplo 1: enumeración de las recomendaciones

En el siguiente ejemplo de `list-recommendations`, se enumeran todas las recomendaciones y no se incluye ningún filtro.

```
aws trustedadvisor list-recommendations
```

Salida:

```
{
    "recommendationSummaries": [
        {
            "arn": "arn:aws:trustedadvisor::000000000000:recommendation/55fa4d2e-
bbb7-491a-833b-5773e9589578",
            "name": "MFA Recommendation",
            "awsServices": [
                "iam"
            ],
            "checkArn": "arn:aws:trustedadvisor:::check/7DAFEmoDos",
            "id": "55fa4d2e-bbb7-491a-833b-5773e9589578",
            "lastUpdatedAt": "2023-11-01T15:57:58.673Z",
            "pillarSpecificAggregates": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            },
            "pillars": [
                "security"
            ],
            "resourcesAggregates": {
```

```
                "errorCount": 1,
                "okCount": 0,
                "warningCount": 0
            },
            "source": "ta_check",
            "status": "error",
            "type": "standard"
        },
        {
            "arn":
 "arn:aws:trustedadvisor::000000000000:recommendation/8b602b6f-452d-4cb2-8a9e-
c7650955d9cd",
            "name": "RDS clusters quota warning",
            "awsServices": [
                "rds"
            ],
            "checkArn": "arn:aws:trustedadvisor:::check/gjqMBn6pjz",
            "id": "8b602b6f-452d-4cb2-8a9e-c7650955d9cd",
            "lastUpdatedAt": "2023-11-01T15:58:17.397Z",
            "pillarSpecificAggregates": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            },
            "pillars": [
                "service_limits"
            ],
            "resourcesAggregates": {
                "errorCount": 0,
                "okCount": 3,
                "warningCount": 6
            },
            "source": "ta_check",
            "status": "warning",
            "type": "standard"
        }
    ],
    "nextToken": "REDACTED"
}
```


Para obtener más información, consulte Get started with the Trusted Advisor API en la Guía del usuario de AWS Trusted Advisor.

Ejemplo 2: enumeración de las recomendaciones con un filtro

En el siguiente ejemplo de `list-recommendations`, se enumeran todas las recomendaciones y se incluye un filtro.

```
aws trustedadvisor list-recommendations \
    --aws-service iam \
    --max-items 100
```

Salida:

```
{
    "recommendationSummaries": [{
        "arn": "arn:aws:trustedadvisor::000000000000:recommendation/55fa4d2e-
bbb7-491a-833b-5773e9589578",
        "name": "MFA Recommendation",
        "awsServices": [
            "iam"
        ],
        "checkArn": "arn:aws:trustedadvisor:::check/7DAFEmoDos",
        "id": "55fa4d2e-bbb7-491a-833b-5773e9589578",
        "lastUpdatedAt": "2023-11-01T15:57:58.673Z",
        "pillarSpecificAggregates": {
            "costOptimizing": {
                "estimatedMonthlySavings": 0.0,
                "estimatedPercentMonthlySavings": 0.0
            }
        },
        "pillars": [
            "security"
        ],
        "resourcesAggregates": {
            "errorCount": 1,
            "okCount": 0,
            "warningCount": 0
        },
        "source": "ta_check",
        "status": "error",
        "type": "standard"
    }],
    "nextToken": "REDACTED"
}
```

Para obtener más información, consulte Get started with the Trusted Advisor API en la Guía del usuario de AWS Trusted Advisor.

Ejemplo 3: enumeración de las recomendaciones con un token de paginación

En el siguiente ejemplo de `list-recommendations`, se utiliza el nextToken devuelto de una solicitud anterior para buscar la siguiente página de recomendaciones filtrada.

```
aws trustedadvisor list-recommendations \
    --aws-service rds \
    --max-items 100 \
    --starting-token <next-token>
```

Salida:

```
{
    "recommendationSummaries": [{
        "arn":
 "arn:aws:trustedadvisor::000000000000:recommendation/8b602b6f-452d-4cb2-8a9e-
c7650955d9cd",
        "name": "RDS clusters quota warning",
        "awsServices": [
            "rds"
        ],
        "checkArn": "arn:aws:trustedadvisor:::check/gjqMBn6pjz",
        "id": "8b602b6f-452d-4cb2-8a9e-c7650955d9cd",
        "lastUpdatedAt": "2023-11-01T15:58:17.397Z",
        "pillarSpecificAggregates": {
            "costOptimizing": {
                "estimatedMonthlySavings": 0.0,
                "estimatedPercentMonthlySavings": 0.0
            }
        },
        "pillars": [
            "service_limits"
        ],
        "resourcesAggregates": {
            "errorCount": 0,
            "okCount": 3,
            "warningCount": 6
        },
        "source": "ta_check",
        "status": "warning",
```

```
        "type": "standard"
    }]
}
```

Para obtener más información, consulte Get started with the Trusted Advisor API en la Guía del usuario de AWS Trusted Advisor.

- Para obtener información sobre la API, consulte ListRecommendations en la Referencia de comandos de la AWS CLI.

`update-organization-recommendation-lifecycle`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-organization-recommendation-lifecycle`.

AWS CLI

Para actualizar el ciclo de vida de las recomendaciones de una organización

En el siguiente ejemplo de `update-organization-recommendation-lifecycle`, se actualiza el ciclo de vida una recomendación de la organización por su identificador.

```
aws trustedadvisor update-organization-recommendation-lifecycle \
    --organization-recommendation-identifier arn:aws:trustedadvisor:::organization-recommendation/96b5e5ca-7930-444c-90c6-06d386128100 \
    --lifecycle-stage dismissed \
    --update-reason-code not_applicable
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Get started with the Trusted Advisor API en la Guía del usuario de AWS Trusted Advisor.

- Para obtener información acerca de la API, consulte UpdateOrganizationRecommendationLifecycle en la Referencia de comandos de la AWS CLI.

`update-recommendation-lifecycle`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-recommendation-lifecycle`.

AWS CLI

Para actualizar el ciclo de vida de una recomendación

En el siguiente ejemplo de `update-recommendation-lifecycle`, se actualiza el ciclo de vida una recomendación por su identificador.

```
aws trustedadvisor update-recommendation-lifecycle \
    --recommendation-
identifier arn:aws:trustedadvisor::000000000000:recommendation/861c9c6e-
f169-405a-8b59-537a8caccd7a \
    --lifecycle-stage resolved \
    --update-reason-code valid_business_case
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Get started with the Trusted Advisor API en la Guía del usuario de AWS Trusted Advisor.

- Para obtener información sobre la API, consulte UpdateRecommendationLifecycle en la Referencia de comandos de la AWS CLI.

Ejemplos de Verified Permissions que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Verified Permissions.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-identity-source`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-identity-source`.

AWS CLI

Para crear un origen de identidad

En el siguiente ejemplo de `create-identity-source`, se crea un origen de identidad que permite hacer referencia a las identidades almacenadas en el grupo de usuarios de Amazon Cognito especificado. Esas identidades están disponibles en Verified Permissions como entidades de tipo `User`.

```
aws verifiedpermissions create-identity-source \
    --configuration file://config.txt \
    --principal-entity-type "User" \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Contenido de `config.txt`:

```
{
    "cognitoUserPoolConfiguration": {
        "userPoolArn": "arn:aws:cognito-idp:us-west-2:123456789012:userpool/us-
west-2_1a2b3c4d5",
        "clientIds":["a1b2c3d4e5f6g7h8i9j0kalbmc"]
    }
}
```

Salida:

```
{
    "createdDate": "2023-05-19T20:30:28.214829+00:00",
    "identitySourceId": "ISEXAMPLEabcdefg111111",
    "lastUpdatedDate": "2023-05-19T20:30:28.214829+00:00",
    "policyStoreId": "PSEXAMPLEabcdefg111111"
}
```

Para obtener más información los orígenes de las identidades, consulte Using Amazon Verified Permissions with identity providers en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte CreateIdentitySource en la Referencia de comandos de la AWS CLI.

`create-policy-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-policy-store`.

AWS CLI

Para crear un almacén de políticas

En el siguiente ejemplo de `create-policy-store`, se crea un almacén de políticas en la región de AWS actual.

```
aws verifiedpermissions create-policy-store \
    --validation-settings "mode=STRICT"
```

Salida:

```
{
    "arn": "arn:aws:verifiedpermissions::123456789012:policy-store/
PSEXAMPLEabcdefg111111",
    "createdDate": "2023-05-16T17:41:29.103459+00:00",
    "lastUpdatedDate": "2023-05-16T17:41:29.103459+00:00",
    "policyStoreId": "PSEXAMPLEabcdefg111111"
}
```

Para obtener más información, consulte Amazon Verified Permissions policy stores en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte CreatePolicyStore en la Referencia de comandos de la AWS CLI.

`create-policy-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-policy-template`.

AWS CLI

Creación de una plantilla de política

En el siguiente ejemplo de `create-policy-template`, se crea una plantilla de política con una instrucción que contiene un marcador de posición para la entidad principal.

```
aws verifiedpermissions create-policy-template \
    --statement file://template1.txt \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Contenido de `template1.txt`:

```
permit(
    principal in ?principal,
    action == Action::"view",
    resource == Photo::"VacationPhoto94.jpg"
);
```

Salida:

```
{
    "createdDate": "2023-06-12T20:47:42.804511+00:00",
    "lastUpdatedDate": "2023-06-12T20:47:42.804511+00:00",
    "policyStoreId": "PSEXAMPLEabcdefg111111",
    "policyTemplateId": "PTEXAMPLEabcdefg111111"
}
```

Para obtener más información acerca de las plantillas de políticas, consulte Amazon Verified Permissions policy templates en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte CreatePolicyTemplate en la Referencia de comandos de la AWS CLI.

`create-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-policy`.

AWS CLI

Ejemplo 1: creación de una política estática

En el siguiente ejemplo de `create-policy`, se crea una política estática con un ámbito de la política que especifica tanto una entidad principal como un recurso.

```
aws verifiedpermissions create-policy \
```

```
    --definition file://definition1.txt \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Contenido del archivo `definition1.txt`:

```
{
    "static": {
        "description":  "Grant everyone of janeFriends UserGroup access to the
 vacationFolder Album",
        "statement": "permit(principal in UserGroup::\"janeFriends\", action,
 resource in Album::\"vacationFolder\" );"
    }
}
```

Salida:

```
{
    "createdDate": "2023-06-12T20:33:37.382907+00:00",
    "lastUpdatedDate": "2023-06-12T20:33:37.382907+00:00",
    "policyId": "SPEXAMPLEabcdefg111111",
    "policyStoreId": "PSEXAMPLEabcdefg111111",
    "policyType": "STATIC",
    "principal": {
        "entityId": "janeFriends",
        "entityType": "UserGroup"
    },
    "resource": {
        "entityId": "vacationFolder",
        "entityType": "Album"
    }
}
```

Ejemplo 2: creación de una política estática que conceda acceso general a un recurso

En el siguiente ejemplo de `create-policy`, se crea una política estática con un ámbito de la política que especifica únicamente un recurso.

```
aws verifiedpermissions create-policy \
    --definition file://definition2.txt \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Contenido del archivo `definition2.txt`:

```
{
    "static": {
        "description":  "Grant everyone access to the publicFolder Album",
        "statement": "permit(principal, action, resource in Album::\"publicFolder
\");"
    }
}
```

Salida:

```
{
    "createdDate": "2023-06-12T20:39:44.975897+00:00",
    "lastUpdatedDate": "2023-06-12T20:39:44.975897+00:00",
    "policyId": "PbfR73F8oh5MMfr9uRtFDB",
    "policyStoreId": "PSEXAMPLEabcdefg222222",
    "policyType": "STATIC",
    "resource": {
        "entityId": "publicFolder",
        "entityType": "Album"
    }
}
```

Ejemplo 3: creación de una política vinculada a una plantilla que esté asociada a la plantilla especificada

En el siguiente ejemplo de `create-policy`, se crea una política vinculada a una plantilla mediante la plantilla de política especificada y se asocia la entidad principal especificada a utilizar con la nueva política vinculada a la plantilla.

```
aws verifiedpermissions create-policy \
    --definition file://definition.txt \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Contenido de `definition.txt`:

```
{
    "templateLinked": {
        "policyTemplateId": "PTEXAMPLEabcdefg111111",
        "principal": {
            "entityType": "User",
            "entityId": "alice"
```

```
        }
    }
}
```

Salida:

```
{
    "createdDate": "2023-06-12T20:49:51.490211+00:00",
    "lastUpdatedDate": "2023-06-12T20:49:51.490211+00:00",
    "policyId": "TPEXAMPLEabcdefg111111",
    "policyStoreId": "PSEXAMPLEabcdefg111111",
    "policyType": "TEMPLATE_LINKED",
    "principal": {
        "entityId": "alice",
        "entityType": "User"
    },
    "resource": {
        "entityId": "VacationPhoto94.jpg",
        "entityType": "Photo"
    }
}
```

Para obtener más información sobre las políticas, consulte Amazon Verified Permissions policies en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte CreatePolicy en la Referencia de comandos de la AWS CLI.

`delete-identity-source`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-identity-source`.

AWS CLI

Para eliminar un origen de identidad

En el siguiente ejemplo de `delete-identity-source`, se elimina el origen de la identidad que tiene el ID especificado.

```
aws verifiedpermissions delete-identity-source \
    --identity-source-id ISEXAMPLEabcdefg111111 \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Este comando no genera ninguna salida.

Para obtener más información los orígenes de las identidades, consulte Using Amazon Verified Permissions with identity providers en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte DeleteIdentitySource en la Referencia de comandos de la AWS CLI.

`delete-policy-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-policy-store`.

AWS CLI

Para eliminar un almacén de políticas

En el siguiente ejemplo de `delete-policy-store`, se elimina el almacén de políticas que tiene el ID especificado.

```
aws verifiedpermissions delete-policy-store \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Amazon Verified Permissions policy stores en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte DeletePolicyStore en la Referencia de comandos de la AWS CLI.

`delete-policy-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-policy-template`.

AWS CLI

Para eliminar una plantilla de políticas

En el siguiente ejemplo de `delete-policy-template`, se elimina la plantilla de políticas que tiene el ID especificado.

```
aws verifiedpermissions delete-policy \
```

```
    --policy-template-id PTEXAMPLEabcdefg111111 \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Este comando no genera ninguna salida.

Para obtener más información acerca de las plantillas de políticas, consulte Amazon Verified Permissions policy templates en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte DeletePolicyTemplate en la Referencia de comandos de la AWS CLI.

`delete-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-policy`.

AWS CLI

Para eliminar una política estática o vinculada a una plantilla

En el siguiente ejemplo de `delete-policy`, se elimina la política que tiene el ID especificado.

```
aws verifiedpermissions delete-policy \
    --policy-id SPEXAMPLEabcdefg111111 \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Este comando no genera ninguna salida.

Para obtener más información sobre las políticas, consulte Amazon Verified Permissions policies en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte DeletePolicy en la Referencia de comandos de la AWS CLI.

`get-identity-source`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-identity-source`.

AWS CLI

Para recuperar detalles sobre un origen de identidad

En el siguiente ejemplo de `get-identity-source`, se muestran los detalles del origen de la identidad con el ID especificado.

```
aws verifiedpermissions get-identity-source \
    --identity-source  ISEXAMPLEabcdefg111111 \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Salida:

```
{
    "createdDate": "2023-06-12T22:27:49.150035+00:00",
    "details": {
        "clientIds": [ "a1b2c3d4e5f6g7h8i9j0kalbmc" ],
        "discoveryUrl": "https://cognito-idp.us-west-2.amazonaws.com/us-
west-2_1a2b3c4d5",
        "openIdIssuer": "COGNITO",
        "userPoolArn": "arn:aws:cognito-idp:us-west-2:123456789012:userpool/us-
west-2_1a2b3c4d5"
    },
    "identitySourceId": "ISEXAMPLEabcdefg111111",
    "lastUpdatedDate": "2023-06-12T22:27:49.150035+00:00",
    "policyStoreId": "PSEXAMPLEabcdefg111111",
    "principalEntityType": "User"
}
```

Para obtener más información los orígenes de las identidades, consulte Using Amazon Verified Permissions with identity providers en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte GetIdentitySource en la Referencia de comandos de la AWS CLI.

`get-policy-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-policy-store`.

AWS CLI

Para recuperar detalles sobre un almacén de políticas

En el siguiente ejemplo de `get-policy-store`, se muestran los detalles del almacén de políticas con el ID especificado.

```
aws verifiedpermissions get-policy-store \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Salida:

```
{
    "arn": "arn:aws:verifiedpermissions::123456789012:policy-store/
PSEXAMPLEabcdefg111111",
    "createdDate": "2023-06-05T20:16:46.225598+00:00",
    "lastUpdatedDate": "2023-06-08T20:40:23.173691+00:00",
    "policyStoreId": "PSEXAMPLEabcdefg111111",
    "validationSettings": { "mode": "OFF" }
}
```

Para obtener más información, consulte Amazon Verified Permissions policy stores en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte GetPolicyStore en la Referencia de comandos de la AWS CLI.

`get-policy-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-policy-template`.

AWS CLI

Para recuperar detalles sobre una plantilla de políticas

En el siguiente ejemplo de `get-policy-template`, se muestran los detalles de la plantilla de políticas con el ID especificado.

```
aws verifiedpermissions get-policy-template \
    --policy-template-id  PTEXAMPLEabcdefg111111 \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Salida:

```
{
    "createdDate": "2023-06-12T20:47:42.804511+00:00",
    "lastUpdatedDate": "2023-06-12T20:47:42.804511+00:00",
    "policyStoreId": "PSEXAMPLEabcdefg111111",
    "policyTemplateId": "PTEXAMPLEabcdefg111111",
    "statement": "permit(\n    principal in ?principal,\n    action == Action::
\"view\",\n    resource == Photo::\"VacationPhoto94.jpg\"\n);"
```

```
}
```

Para obtener más información acerca de las plantillas de políticas, consulte Amazon Verified Permissions policy templates en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte GetPolicyTemplate en la Referencia de comandos de la AWS CLI.

`get-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-policy`.

AWS CLI

Para recuperar información sobre una política

En el siguiente ejemplo de `get-policy`, se muestran los detalles de la política con el ID especificado.

```
aws verifiedpermissions get-policy \
    --policy-id PSEXAMPLEabcdefg111111 \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Salida:

```
{
    "createdDate": "2023-06-12T20:33:37.382907+00:00",
    "definition": {
        "static": {
            "description": "Grant everyone of janeFriends UserGroup access to the
 vacationFolder Album",
            "statement": "permit(principal in UserGroup::\"janeFriends\", action,
 resource in Album::\"vacationFolder\" );"
        }
    },
    "lastUpdatedDate": "2023-06-12T20:33:37.382907+00:00",
    "policyId": "SPEXAMPLEabcdefg111111",
    "policyStoreId": "PSEXAMPLEabcdefg111111",
    "policyType": "STATIC",
    "principal": {
        "entityId": "janeFriends",
        "entityType": "UserGroup"
```

```
    },
    "resource": {
        "entityId": "vacationFolder",
        "entityType": "Album"
    }
}
```

Para obtener más información sobre las políticas, consulte Amazon Verified Permissions policies en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte GetPolicy en la Referencia de comandos de la AWS CLI.

`get-schema`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-schema`.

AWS CLI

Para recuperar el esquema en un almacén de políticas

En el siguiente ejemplo de `get-schema`, se muestran los detalles del esquema en el almacén de políticas especificado.

```
aws verifiedpermissions get-schema \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Salida:

```
{
    "policyStoreId": "PSEXAMPLEabcdefg111111",
    "schema": "{\"MySampleNamespace\":{\"entityTypes\":{\"Employee\":{\"shape
\":{\"attributes\":{\"jobLevel\":{\"type\":\"Long\"},\"name\":{\"type\":\"String
\"}},\"type\":\"Record\"}}},\"actions\":{\"remoteAccess\":{\"appliesTo\":
{\"principalTypes\":[\"Employee\"]}}}}}",
    "createdDate": "2023-06-14T17:47:13.999885+00:00",
    "lastUpdatedDate": "2023-06-14T17:47:13.999885+00:00"
}
```

Para obtener más información sobre el esquema, consulte Policy store schema en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte GetSchema en la Referencia de comandos de la AWS CLI.

`is-authorized-with-token`

En el siguiente ejemplo de código, se muestra cómo utilizar `is-authorized-with-token`.

AWS CLI

Ejemplo 1: solicitud de una decisión de autorización para una solicitud de usuario (permitir)

En el siguiente ejemplo de `is-authorized-with-token`, se solicita una decisión de autorización para un usuario autenticado por Amazon Cognito. La solicitud utiliza el token de identidad proporcionado por Cognito en lugar del token de acceso. En este ejemplo, el almacén de información especificado está configurado para devolver las entidades principales como entidades de tipo `CognitoUser`.

```
aws verifiedpermissions is-authorized-with-token \
    --action actionId="View",actionType="Action" \
    --resource entityId="vacationPhoto94.jpg",entityType="Photo" \
    --policy-store-id PSEXAMPLEabcdefg111111 \
    --identity-token "AbCdE12345...long.string...54321EdCbA"
```

El almacén de políticas contiene una política con la siguiente instrucción que acepta identidades del grupo de usuarios y del ID de aplicación de Cognito especificados.

```
permit(
    principal == CognitoUser::"us-east-1_1a2b3c4d5|a1b2c3d4e5f6g7h8i9j0kalbmc",
    action,
    resource == Photo::"VacationPhoto94.jpg"
);
```

Salida:

```
{
    "decision":"Allow",
    "determiningPolicies":[
        {
        "determiningPolicyId":"SPEXAMPLEabcdefg111111"
        }
```

```
    ],
    "errors":[]
}
```

Para obtener más información las identidades de un grupo de usuarios de Cognito, consulte Using Amazon Verified Permissions with identity providers en la Guía del usuario de Amazon Verified Permissions.

- Para obtener más información sobre la API, consulte IsAuthorizedWithToken en la Referencia de comandos de la AWS CLI.

`is-authorized`

En el siguiente ejemplo de código, se muestra cómo utilizar `is-authorized`.

AWS CLI

Ejemplo 1: solicitud de una decisión de autorización para una solicitud de usuario (permitir)

En el siguiente ejemplo de `is-authorized`, se solicita una decisión de autorización para una entidad principal del tipo `User` denominada `Alice` que desea realizar la operación `updatePhoto` en un recurso del tipo `Photo` denominado `VacationPhoto94.jpg`.

La respuesta muestra que una política permite la solicitud.

```
aws verifiedpermissions is-authorized \
    --principal entityType=User,entityId=alice \
    --action actionType=Action,actionId=view \
    --resource entityType=Photo,entityId=VactionPhoto94.jpg \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Salida:

```
{
    "decision": "ALLOW",
    "determiningPolicies": [
        {
            "policyId": "SPEXAMPLEabcdefg111111"
        }
    ],
    "errors": []
```

```
}
```

Ejemplo 2: solicitud de una decisión de autorización para una solicitud de usuario (denegar)

El ejemplo siguiente es igual al ejemplo anterior, con la salvedad de que la entidad principal es `User::"Bob"`. El almacén de políticas no contiene ninguna política que permita a ese usuario acceder a`Album::"alice_folder"`.

El resultado indica que `Deny` estaba implícito porque la lista de `DeterminingPolicies` está vacía.

```
aws verifiedpermissions create-policy \
    --definition file://definition2.txt \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Salida:

```
{
    "decision": "DENY",
    "determiningPolicies": [],
    "errors": []
}
```

Para obtener más información, consulte la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte IsAuthorized en la Referencia de comandos de la AWS CLI.

`list-identity-sources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-identity-sources`.

AWS CLI

Para enumerar los orígenes de la identidad disponibles

En el siguiente ejemplo de `list-identity-sources`, se enumeran todos los orígenes de la identidad del almacén de políticas especificado.

```
aws verifiedpermissions list-identity-sources \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Salida:

```
{
    "identitySources": [
        {
            "createdDate": "2023-06-12T22:27:49.150035+00:00",
            "details": {
                "clientIds": [ "a1b2c3d4e5f6g7h8i9j0kalbmc" ],
                "discoveryUrl": "https://cognito-idp.us-west-2.amazonaws.com/us-
west-2_1a2b3c4d5",
                "openIdIssuer": "COGNITO",
                "userPoolArn": "arn:aws:cognito-idp:us-west-2:123456789012:userpool/
us-west-2_1a2b3c4d5"
            },
            "identitySourceId": "ISEXAMPLEabcdefg111111",
            "lastUpdatedDate": "2023-06-12T22:27:49.150035+00:00",
            "policyStoreId": "PSEXAMPLEabcdefg111111",
            "principalEntityType": "User"
        }
    ]
}
```

Para obtener más información los orígenes de las identidades, consulte Using Amazon Verified Permissions with identity providers en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte ListIdentitySources en la Referencia de comandos de la AWS CLI.

`list-policies`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-policies`.

AWS CLI

Para enumerar las políticas disponibles

En el siguiente ejemplo de `list-policies`, se enumeran todas las políticas del almacén de políticas especificado.

```
aws verifiedpermissions list-policies \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Salida:

```
{
    "policies": [
        {
            "createdDate": "2023-06-12T20:33:37.382907+00:00",
            "definition": {
                "static": {
                    "description": "Grant everyone of janeFriends UserGroup access
 to the vacationFolder Album"
                }
            },
            "lastUpdatedDate": "2023-06-12T20:33:37.382907+00:00",
            "policyId": "SPEXAMPLEabcdefg111111",
            "policyStoreId": "PSEXAMPLEabcdefg111111",
            "policyType": "STATIC",
            "principal": {
                "entityId": "janeFriends",
                "entityType": "UserGroup"
            },
            "resource": {
                "entityId": "vacationFolder",
                "entityType": "Album"
            }
        },
        {
            "createdDate": "2023-06-12T20:39:44.975897+00:00",
            "definition": {
                "static": {
                    "description": "Grant everyone access to the publicFolder Album"
                }
            },
            "lastUpdatedDate": "2023-06-12T20:39:44.975897+00:00",
            "policyId": "SPEXAMPLEabcdefg222222",
            "policyStoreId": "PSEXAMPLEabcdefg111111",
            "policyType": "STATIC",
            "resource": {
                "entityId": "publicFolder",
                "entityType": "Album"
            }
        },
        {
            "createdDate": "2023-06-12T20:49:51.490211+00:00",
            "definition": {
```

```
                "templateLinked": {
                    "policyTemplateId": "PTEXAMPLEabcdefg111111"
                }
            },
            "lastUpdatedDate": "2023-06-12T20:49:51.490211+00:00",
            "policyId": "SPEXAMPLEabcdefg333333",
            "policyStoreId": "PSEXAMPLEabcdefg111111",
            "policyType": "TEMPLATE_LINKED",
            "principal": {
                "entityId": "alice",
                "entityType": "User"
            },
            "resource": {
                "entityId": "VacationPhoto94.jpg",
                "entityType": "Photo"
            }
        }
    ]
}
```

Para obtener más información sobre las políticas, consulte Amazon Verified Permissions policies en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte ListPolicies en la Referencia de comandos de la AWS CLI.

`list-policy-stores`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-policy-stores`.

AWS CLI

Para enumerar los almacenes de políticas disponibles

En el siguiente ejemplo de `list-policy-stores`, se enumeran todos los almacenes de políticas de la región de AWS. Todos los comandos de Verified Permissions, excepto `create-policy-store` y `list-policy-stores` requieren que especifique el ID del almacén de políticas con el que desea trabajar.

```
aws verifiedpermissions list-policy-stores
```

Salida:

```
{
    "policyStores": [
        {
            "arn": "arn:aws:verifiedpermissions::123456789012:policy-store/
PSEXAMPLEabcdefg111111",
            "createdDate": "2023-06-05T20:16:46.225598+00:00",
            "policyStoreId": "PSEXAMPLEabcdefg111111"
        },
        {
            "arn": "arn:aws:verifiedpermissions::123456789012:policy-store/
PSEXAMPLEabcdefg222222",
            "createdDate": "2023-06-08T18:09:37.364356+00:00",
            "policyStoreId": "PSEXAMPLEabcdefg222222"
        },
        {
            "arn": "arn:aws:verifiedpermissions::123456789012:policy-store/
PSEXAMPLEabcdefg333333",
            "createdDate": "2023-06-08T18:09:46.920600+00:00",
            "policyStoreId": "PSEXAMPLEabcdefg333333"
        }
    ]
}
```

Para obtener más información, consulte Amazon Verified Permissions policy stores en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte ListPolicyStores en la Referencia de comandos de la AWS CLI.

`list-policy-templates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-policy-templates`.

AWS CLI

Para enumerar las plantillas de políticas disponibles

En el siguiente ejemplo de `list-policy-templates`, se enumeran todas las plantilla de políticas del almacén de políticas especificado.

```
aws verifiedpermissions list-policy-templates \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Salida:

```
{
    "policyTemplates": [
        {
            "createdDate": "2023-06-12T20:47:42.804511+00:00",
            "lastUpdatedDate": "2023-06-12T20:47:42.804511+00:00",
            "policyStoreId": "PSEXAMPLEabcdefg111111",
            "policyTemplateId": "PTEXAMPLEabcdefg111111"
        }
    ]
}
```

Para obtener más información acerca de las plantillas de políticas, consulte Amazon Verified Permissions policy templates en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte ListPolicyTemplates en la Referencia de comandos de la AWS CLI.

`put-schema`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-schema`.

AWS CLI

Para guardar un esquema en un almacén de políticas

En el siguiente ejemplo de `put-schema`, se crea o reemplaza el esquema del almacén de políticas especificado.

El parámetro `cedarJson` del archivo de entrada toma una representación de cadena de un objeto JSON. Contiene comillas incrustadas (") dentro del par de comillas más externas. Para ello, debe convertir el JSON en una cadena y poner una barra invertida (\) delante de todas las comillas incrustadas y combinar todas las líneas en una sola línea de texto sin saltos de línea.

Las cadenas de ejemplo se pueden mostrar agrupadas entre varias líneas para facilitar la lectura, pero la operación requiere que los parámetros se envíen como cadenas de una sola línea.

aws verifiedpermissions put-schema --definition file://schema.txt --policy-store-id PSEXAMPLEabcdefg111111

Contenido de `schema.txt`:

```
{
    "cedarJson": "{\"MySampleNamespace\": {\"actions\": {\"remoteAccess\": {
            \"appliesTo\": {\"principalTypes\": [\"Employee\"]}},\"entityTypes\": {
            \"Employee\": {\"shape\": {\"attributes\": {\"jobLevel\": {\"type\":
            \"Long\"},\"name\": {\"type\": \"String\"}},\"type\": \"Record\"}}}}}"
}
```

Salida:

```
{
    "policyStoreId": "PSEXAMPLEabcdefg111111",
    "namespaces": [
        "MySampleNamespace"
    ],
    "createdDate": "2023-06-14T17:47:13.999885+00:00",
    "lastUpdatedDate": "2023-06-14T17:47:13.999885+00:00"
}
```

Para obtener más información sobre el esquema, consulte Policy store schema en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte PutSchema en la Referencia de comandos de la AWS CLI.

`update-identity-source`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-identity-source`.

AWS CLI

Para actualizar un origen de identidad

En el siguiente ejemplo de `update-identity-source`, se modifica el origen de la identidad especificada al proporcionar una nueva configuración de grupo de usuarios de Cognito y cambiar el tipo de entidad devuelto por el origen de la identidad.

```
aws verifiedpermissions update-identity-source
    --identity-source-id ISEXAMPLEabcdefg111111 \
    --update-configuration file://config.txt \
    --principal-entity-type "Employee" \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Contenido de `config.txt`:

```
{
        "cognitoUserPoolConfiguration": {
                "userPoolArn": "arn:aws:cognito-idp:us-west-2:123456789012:userpool/
us-west-2_1a2b3c4d5",
                "clientIds":["a1b2c3d4e5f6g7h8i9j0kalbmc"]
        }
}
```

Salida:

```
{
    "createdDate": "2023-05-19T20:30:28.214829+00:00",
    "identitySourceId": "ISEXAMPLEabcdefg111111",
    "lastUpdatedDate": "2023-05-19T20:30:28.214829+00:00",
    "policyStoreId": "PSEXAMPLEabcdefg111111"
}
```

Para obtener más información los orígenes de las identidades, consulte Using Amazon Verified Permissions with identity providers en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte UpdateIdentitySource en la Referencia de comandos de la AWS CLI.

`update-policy-store`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-policy-store`.

AWS CLI

Para actualizar un almacén de políticas

En el siguiente ejemplo de `update-policy-store`, se modifica un almacén de políticas al cambiar su configuración de validación.

```
aws verifiedpermissions update-policy-store \
    --validation-settings "mode=STRICT" \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Salida:

```
{
    "arn": "arn:aws:verifiedpermissions::123456789012:policy-store/
PSEXAMPLEabcdefg111111",
    "createdDate": "2023-05-16T17:41:29.103459+00:00",
    "lastUpdatedDate": "2023-05-16T17:41:29.103459+00:00",
    "policyStoreId": "PSEXAMPLEabcdefg111111"
}
```

Para obtener más información, consulte Amazon Verified Permissions policy stores en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte UpdatePolicyStore en la Referencia de comandos de la AWS CLI.

`update-policy-template`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-policy-template`.

AWS CLI

Ejemplo 1: actualización de una plantilla de políticas

En el siguiente ejemplo de `update-policy-template`, se modifica la política vinculada a la plantilla especificada para reemplazar su instrucción de política.

```
aws verifiedpermissions update-policy-template \
    --policy-template-id PTEXAMPLEabcdefg111111 \
    --statement file://template1.txt \
    --policy-store-id PSEXAMPLEabcdefg111111
```

Contenido del archivo `template1.txt`:

```
permit(
    principal in ?principal,
    action == Action::"view",
    resource == Photo::"VacationPhoto94.jpg"
);
```

Salida:

```
{
```

```
    "createdDate": "2023-06-12T20:47:42.804511+00:00",
    "lastUpdatedDate": "2023-06-12T20:47:42.804511+00:00",
    "policyStoreId": "PSEXAMPLEabcdefg111111",
    "policyTemplateId": "PTEXAMPLEabcdefg111111"
}
```

Para obtener más información acerca de las plantillas de políticas, consulte Amazon Verified Permissions policy templates en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte UpdatePolicyTemplate en la Referencia de comandos de AWS CLI.

`update-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-policy`.

AWS CLI

Actualización de una política estática

En el siguiente ejemplo de `update-policy`, se modifica una política estática existente actualizando su descripción y su instrucción.

```
aws verifiedpermissions update-policy \
    --policy-id SPEXAMPLEabcdefg111111 \
    --definition file://updated-definition.txt \
    --policy-store-id PSEXAMPLEabcdefg111111
```

El parámetro `statement` toma una representación de cadena de un objeto JSON. Contiene comillas incrustadas (") dentro del par de comillas más externas. Para ello, debe convertir el JSON en una cadena y poner una barra invertida (\) delante de todas las comillas incrustadas y combinar todas las líneas en una sola línea de texto sin saltos de línea.

Puede mostrar cadenas de ejemplo agrupadas entre varias líneas para facilitar la lectura, pero la operación requiere que los parámetros se envíen como cadenas de una sola línea.

Contenido del archivo `updated-definition.txt`:

```
{
    "static": {
        "description": "Updated policy to grant janeFriends UserGroup access to the
 vacationFolder Album with view action only",
```

```
        "statement": "permit(principal in UserGroup::\"janeFriends\", action ==
 Action::\"view\", resource in Album::\"vacationFolder\" );"
    }
}
```

Salida:

```
{
    "createdDate": "2023-06-12T20:33:37.382907+00:00",
    "lastUpdatedDate": "2023-06-12T20:33:37.382907+00:00",
    "policyId": "SPEXAMPLEabcdefg111111",
    "policyStoreId": "PSEXAMPLEabcdefg111111",
    "policyType": "STATIC",
    "principal": {
        "entityId": "janeFriends",
        "entityType": "UserGroup"
    },
    "resource": {
        "entityId": "vacationFolder",
        "entityType": "Album"
    }
}
```

Para obtener más información sobre las políticas, consulte Amazon Verified Permissions policies en la Guía del usuario de Amazon Verified Permissions.

- Para obtener información sobre la API, consulte UpdatePolicy en la Referencia de comandos de la AWS CLI.

Ejemplos de VPC Lattice que utilizan la AWS CLI

En el siguiente ejemplo de código se muestra cómo realizar acciones e implementar escenarios comunes usando la AWS Command Line Interface con VPC Lattice.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-listener`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-listener`.

AWS CLI

Para crear un oyente

En el siguiente ejemplo de `create-listener`, se crea un oyente de HTTPS con una regla predeterminada que reenvíe el tráfico al grupo de destino de VPC Lattice especificado.

```
aws vpc-lattice create-listener \
    --name my-service-listener \
    --protocol HTTPS \
    --port 443 \
    --service-identifier svc-0285b53b2eEXAMPLE \
    --default-action file://listener-config.json
```

Contenido de `listener-config.json`:

```
{
    "forward": {
        "targetGroups": [
            {
                "targetGroupIdentifier": "tg-0eaa4b9ab4EXAMPLE"
            }
        ]
    }
}
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:service/
svc-0285b53b2eEXAMPLE/listener/listener-07cc7fb0abEXAMPLE",
    "defaultAction": {
        "forward": {
```

```
            "targetGroups": [
                {
                    "targetGroupIdentifier": "tg-0eaa4b9ab4EXAMPLE",
                    "weight": 100
                }
            ]
        }
    },
    "id": "listener-07cc7fb0abEXAMPLE",
    "name": "my-service-listener",
    "port": 443,
    "protocol": "HTTPS",
    "serviceArn": "arn:aws:vpc-lattice:us-east-2:123456789012:service/
svc-0285b53b2eEXAMPLE",
    "serviceId": "svc-0285b53b2eEXAMPLE"
}
```

Para obtener más información, consulte Listeners en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte CreateListener en la Referencia de comandos de la AWS CLI.

`create-resource-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-resource-configuration`.

AWS CLI

Creación de una configuración de recursos

En el siguiente ejemplo de `create-resource-configuration`, se crea una configuración de recursos que especifica una única dirección IPv4.

```
aws vpc-lattice create-resource-configuration \
    --name my-resource-config \
    --type SINGLE \
    --resource-gateway-identifier rgw-0bba03f3d56060135 \
    --resource-configuration-definition 'ipResource={ipAddress=10.0.14.85}'
```

Salida:

```
{
```

```
    "allowAssociationToShareableServiceNetwork": true,
    "arn": "arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/
rcfg-07129f3acded87625",
    "id": "rcfg-07129f3acded87625",
    "name": "my-resource-config",
    "portRanges": [
        "1-65535"
    ],
    "protocol": "TCP",
    "resourceConfigurationDefinition": {
        "ipResource": {
            "ipAddress": "10.0.14.85"
        }
    },
    "resourceGatewayId": "rgw-0bba03f3d56060135",
    "status": "ACTIVE",
    "type": "SINGLE"
}
```

Para obtener más información, consulte Configuraciones de recursos para recursos de VPC en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte CreateResourceConfiguration en la Referencia de comandos de la AWS CLI.

`create-resource-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-resource-gateway`.

AWS CLI

Creación de una puerta de enlace de recursos

En el siguiente ejemplo de `create-resource-gateway`, se crea una puerta de enlace de un recurso para la subred especificada.

```
aws vpc-lattice create-resource-gateway \
    --name my-resource-gateway \
    --vpc-identifier vpc-0bf4c2739bc05a69 \
    --subnet-ids subnet-08e8943905b63a683
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-1:123456789012:resourcegateway/
rgw-0bba03f3d56060135",
    "id": "rgw-0bba03f3d56060135",
    "ipAddressType": "IPV4",
    "name": "my-resource-gateway",
    "securityGroupIds": [
        "sg-087ffd596c5fe962c"
    ],
    "status": "ACTIVE",
    "subnetIds": [
        "subnet-08e8943905b63a683"
    ],
    "vpcIdentifier": "vpc-0bf4c2739bc05a694"
}
```

Para obtener más información, consulte Puertas de enlace de recursos en VPC Lattice en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte CreateResourceGateway en la Referencia de comandos de la AWS CLI.

`create-service-network-service-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-service-network-service-association`.

AWS CLI

Para crear una asociación de servicios

En el siguiente ejemplo de `create-service-network-service-association`, se asocia el servicio especificado a la red de servicios especificada.

```
aws vpc-lattice create-service-network-service-association \
    --service-identifier svc-0285b53b2eEXAMPLE \
    --service-network-identifier sn-080ec7dc93EXAMPLE
```

Salida:

```
{
```

```
    "arn": "arn:aws:vpc-lattice:us-
east-2:123456789012:servicenetworkserviceassociation/snsa-0e16955a8cEXAMPLE",
    "createdBy": "123456789012",
    "dnsEntry": {
        "domainName": "my-lattice-service-0285b53b2eEXAMPLE.7d67968.vpc-lattice-
svcs.us-east-2.on.aws",
        "hostedZoneId": "Z09127221KTH2CEXAMPLE"
    },
    "id": "snsa-0e16955a8cEXAMPLE",
    "status": "CREATE_IN_PROGRESS"
}
```

Para obtener más información, consulte Manage service associations en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte CreateServiceNetworkServiceAssociation en la Referencia de comandos de la AWS CLI.

`create-service-network-vpc-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-service-network-vpc-association`.

AWS CLI

Para crear una asociación de VPC

En el siguiente ejemplo de `create-service-network-vpc-association`, se asocia la vpc especificada a la red de servicio indicada. El grupo de seguridad especificado controla qué recursos de la VPC pueden acceder a la red de servicios y a sus servicios.

```
aws vpc-lattice create-service-network-vpc-association \
    --vpc-identifier vpc-0a1b2c3d4eEXAMPLE \
    --service-network-identifier sn-080ec7dc93EXAMPLE \
    --security-group-ids sg-0aee16bc6cEXAMPLE
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:servicenetworkvpcassociation/
snva-0821fc8631EXAMPLE",
```

```
    "createdBy": "123456789012",
    "id": "snva-0821fc8631EXAMPLE",
    "securityGroupIds": [
        "sg-0aee16bc6cEXAMPLE"
    ],
    "status": "CREATE_IN_PROGRESS"
}
```

Para obtener más información, consulte Manage VPC associations en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte CreateServiceNetworkVpcAssociation en la Referencia de comandos de la AWS CLI.

`create-service-network`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-service-network`.

AWS CLI

Para crear una red de servicios

En el siguiente ejemplo de `create-service-network`, se crea una red de servicios con el nombre especificado.

```
aws vpc-lattice create-service-network \
    --name my-service-network
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:servicenetwork/
sn-080ec7dc93EXAMPLE",
    "authType": "NONE",
    "id": "sn-080ec7dc93EXAMPLE",
    "name": "my-service-network"
}
```

Para obtener más información, consulte Service networks en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte CreateServiceNetwork en la Referencia de comandos de la AWS CLI.

`create-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-service`.

AWS CLI

Para crear un servicio

En el siguiente ejemplo de `create-service`, se crea un servicio con el nombre especificado.

```
aws vpc-lattice create-service \
    --name my-lattice-service
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:service/
svc-0285b53b2eEXAMPLE",
    "authType": "NONE",
    "dnsEntry": {
        "domainName": "my-lattice-service-0285b53b2eEXAMPLE.1a2b3c4.vpc-lattice-
svcs.us-east-2.on.aws",
        "hostedZoneId": "Z09127221KTH2CEXAMPLE"
    },
    "id": "svc-0285b53b2eEXAMPLE",
    "name": "my-lattice-service",
    "status": "CREATE_IN_PROGRESS"
}
```

Para obtener más información, consulte Services in VPC Lattice en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte CreateService en la Referencia de comandos de la AWS CLI.

`create-target-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-target-group`.

AWS CLI

Ejemplo 1: creación de un grupo de destino de tipo INSTANCE

En el siguiente ejemplo de `create-target-group`, se crea un grupo de destino con el nombre, el tipo y la configuración especificados.

```
aws vpc-lattice create-target-group \
    --name my-lattice-target-group-instance \
    --type INSTANCE \
    --config file://tg-config.json
```

Contenido de `tg-config.json`:

```
{
    "port": 443,
    "protocol": "HTTPS",
    "protocolVersion": "HTTP1",
    "vpcIdentifier": "vpc-f1663d9868EXAMPLE"
}
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:targetgroup/
tg-0eaa4b9ab4EXAMPLE",
    "config": {
        "healthCheck": {
            "enabled": true,
            "healthCheckIntervalSeconds": 30,
            "healthCheckTimeoutSeconds": 5,
            "healthyThresholdCount": 5,
            "matcher": {
                "httpCode": "200"
            },
            "path": "/",
            "protocol": "HTTPS",
            "protocolVersion": "HTTP1",
            "unhealthyThresholdCount": 2
        },
        "port": 443,
        "protocol": "HTTPS",
```

```
        "protocolVersion": "HTTP1",
        "vpcIdentifier": "vpc-f1663d9868EXAMPLE"
    },
    "id": "tg-0eaa4b9ab4EXAMPLE",
    "name": "my-lattice-target-group-instance",
    "status": "CREATE_IN_PROGRESS",
    "type": "INSTANCE"
}
```

Ejemplo 2: creación de un grupo de destino de tipo IP

En el siguiente ejemplo de `create-target-group`, se crea un grupo de destino con el nombre, el tipo y la configuración especificados.

```
aws vpc-lattice create-target-group \
    --name my-lattice-target-group-ip \
    --type IP \
    --config file://tg-config.json
```

Contenido de `tg-config.json`:

```
{
    "ipAddressType": "IPV4",
    "port": 443,
    "protocol": "HTTPS",
    "protocolVersion": "HTTP1",
    "vpcIdentifier": "vpc-f1663d9868EXAMPLE"
}
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:targetgroup/
tg-0eaa4b9ab4EXAMPLE",
    "config": {
        "healthCheck": {
            "enabled": true,
            "healthCheckIntervalSeconds": 30,
            "healthCheckTimeoutSeconds": 5,
            "healthyThresholdCount": 5,
            "matcher": {
                "httpCode": "200"
```

```
            },
            "path": "/",
            "protocol": "HTTPS",
            "protocolVersion": "HTTP1",
            "unhealthyThresholdCount": 2
        },
        "ipAddressType": "IPV4",
        "port": 443,
        "protocol": "HTTPS",
        "protocolVersion": "HTTP1",
        "vpcIdentifier": "vpc-f1663d9868EXAMPLE"
    },
    "id": "tg-0eaa4b9ab4EXAMPLE",
    "name": "my-lattice-target-group-ip",
    "status": "CREATE_IN_PROGRESS",
    "type": "IP"
}
```

Ejemplo 3: creación de un grupo de destino de tipo LAMBDA

En el siguiente ejemplo de `create-target-group`, se crea un grupo de destino con el nombre, el tipo y la configuración especificados.

```
aws vpc-lattice create-target-group \
    --name my-lattice-target-group-lambda \
    --type LAMBDA
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:targetgroup/
tg-0eaa4b9ab4EXAMPLE",
    "id": "tg-0eaa4b9ab4EXAMPLE",
    "name": "my-lattice-target-group-lambda",
    "status": "CREATE_IN_PROGRESS",
    "type": "LAMBDA"
}
```

Ejemplo 4: creación de un grupo de destino de tipo ALB

En el siguiente ejemplo de `create-target-group`, se crea un grupo de destino con el nombre, el tipo y la configuración especificados.

```
aws vpc-lattice create-target-group \
    --name my-lattice-target-group-alb \
    --type ALB \
    --config file://tg-config.json
```

Contenido de `tg-config.json`:

```
{
    "port": 443,
    "protocol": "HTTPS",
    "protocolVersion": "HTTP1",
    "vpcIdentifier": "vpc-f1663d9868EXAMPLE"
}
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:targetgroup/
tg-0eaa4b9ab4EXAMPLE",
    "config": {
        "port": 443,
        "protocol": "HTTPS",
        "protocolVersion": "HTTP1",
        "vpcIdentifier": "vpc-f1663d9868EXAMPLE"
    },
    "id": "tg-0eaa4b9ab4EXAMPLE",
    "name": "my-lattice-target-group-alb",
    "status": "CREATE_IN_PROGRESS",
    "type": "ALB"
}
```

Para obtener más información, consulte Target groups en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte CreateTargetGroup en la Referencia de comandos de la AWS CLI.

`delete-auth-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-auth-policy`.

AWS CLI

Para eliminar una política de autorización

En el siguiente ejemplo de `delete-auth-policy`, se elimina la política de autorización del servicio especificado.

```
aws vpc-lattice delete-auth-policy \
    --resource-identifier svc-0285b53b2eEXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Auth policies en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte DeleteAuthPolicy en la Referencia de comandos de la AWS CLI.

`delete-listener`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-listener`.

AWS CLI

Para eliminar un oyente

En el siguiente ejemplo de `delete-listener`, se elimina el oyente especificado.

```
aws vpc-lattice delete-listener \
    --listener-identifier listener-07cc7fb0abEXAMPLE \
    --service-identifier svc-0285b53b2eEXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Listeners en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte DeleteListener en la Referencia de comandos de la AWS CLI.

`delete-resource-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-resource-configuration`.

AWS CLI

Eliminación de una configuración de recursos

En el siguiente ejemplo de `delete-resource-configuration`, se elimina la configuración de recursos especificada.

```
aws vpc-lattice delete-resource-configuration \
    --resource-configuration-identifier rcfg-07129f3acded87625
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Puertas de enlace de recursos en VPC Lattice en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte DeleteResourceConfiguration en la Referencia de comandos de la AWS CLI.

`delete-resource-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-resource-gateway`.

AWS CLI

Eliminación de una puerta de enlace de recursos

En el siguiente ejemplo de `delete-resource-gateway`, se elimina la puerta de enlace de recursos especificada.

```
aws vpc-lattice delete-resource-gateway \
    --resource-gateway-identifier rgw-0bba03f3d56060135
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-1:123456789012:resourcegateway/
rgw-0bba03f3d56060135",
    "id": "rgw-0bba03f3d56060135",
    "name": "my-resource-gateway",
    "status": "DELETE_IN_PROGRESS"
}
```

Para obtener más información, consulte Puertas de enlace de recursos en VPC Lattice en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte DeleteResourceGateway en la Referencia de comandos de la AWS CLI.

`delete-service-network-service-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-service-network-service-association`.

AWS CLI

Para eliminar una asociación de servicios

En el siguiente ejemplo de `delete-service-network-service-association`, se desvincula la asociación de servicios especificada.

```
aws vpc-lattice delete-service-network-service-association \
    --service-network-service-association-identifier snsa-031fabb4d8EXAMPLE
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-
east-2:123456789012:servicenetworkserviceassociation/snsa-031fabb4d8EXAMPLE",
    "id": "snsa-031fabb4d8EXAMPLE",
    "status": "DELETE_IN_PROGRESS"
}
```

Para obtener más información, consulte Manage service associations en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte DeleteServiceNetworkServiceAssociation en la Referencia de comandos de la AWS CLI.

`delete-service-network-vpc-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-service-network-vpc-association`.

AWS CLI

Para eliminar una asociación de VPC

En el siguiente ejemplo de `delete-service-network-vpc-association`, se desvincula la asociación de VPC especificada.

```
aws vpc-lattice delete-service-network-vpc-association \
    --service-network-vpc-association-identifier snva-0821fc8631EXAMPLE
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:servicenetworkvpcassociation/
snva-0821fc8631EXAMPLE",
    "id": "snva-0821fc8631EXAMPLE",
    "status": "DELETE_IN_PROGRESS"
}
```

Para obtener más información, consulte Manage VPC associations en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte DeleteServiceNetworkVpcAssociation en la Referencia de comandos de la AWS CLI.

`delete-service-network`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-service-network`.

AWS CLI

Para eliminar una red de servicios

En el siguiente ejemplo de `delete-service-network`, se elimina la red de servicios especificada.

```
aws vpc-lattice delete-service-network \
    --service-network-identifier sn-080ec7dc93EXAMPLE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Service networks en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte DeleteServiceNetwork en la Referencia de comandos de la AWS CLI.

`delete-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-service`.

AWS CLI

Para eliminar un servicio

En el siguiente ejemplo de `delete-service`, se elimina el servicio especificado.

```
aws vpc-lattice delete-service \
    --service-identifier svc-0285b53b2eEXAMPLE
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-west-2:123456789012:service/
svc-0285b53b2eEXAMPLE",
    "id": "svc-0285b53b2eEXAMPLE",
    "name": "my-lattice-service",
    "status": "DELETE_IN_PROGRESS"
}
```

Para obtener más información, consulte Services in VPC Lattice en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte DeleteService en la Referencia de comandos de la AWS CLI.

`delete-target-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-target-group`.

AWS CLI

Para eliminar un grupo de destino

En el siguiente ejemplo de `delete-target-group` se elimina el grupo de destino especificado.

```
aws vpc-lattice delete-target-group \
    --target-group-identifier tg-0eaa4b9ab4EXAMPLE
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:targetgroup/
tg-0eaa4b9ab4EXAMPLE",
    "id": "tg-0eaa4b9ab4EXAMPLE",
    "status": "DELETE_IN_PROGRESS"
}
```

Para obtener más información, consulte Target groups en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte DeleteTargetGroup en la Referencia de comandos de la AWS CLI.

`deregister-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-targets`.

AWS CLI

Para anular el registro de un destino

En el siguiente ejemplo de `deregister-targets`, se retira el registro del destino especificado del grupo de destino indicado.

```
aws vpc-lattice deregister-targets \
    --targets i-07dd579bc5EXAMPLE \
    --target-group-identifier tg-0eaa4b9ab4EXAMPLE
```

Salida:

```
{
    "successful": [
        {
```

```
            "id": "i-07dd579bc5EXAMPLE",
            "port": 443
        }
    ],
    "unsuccessful": []
}
```

Para obtener más información, consulte Register targets en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte DeregisterTargets en la Referencia de comandos de la AWS CLI.

`get-auth-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-auth-policy`.

AWS CLI

Para obtener información acerca de una política de autorización

En el siguiente ejemplo de `get-auth-policy`, se obtiene información sobre la política de autenticación del servicio especificado.

```
aws vpc-lattice get-auth-policy \
    --resource-identifier svc-0285b53b2eEXAMPLE
```

Salida:

```
{
    "createdAt": "2023-06-07T03:51:20.266Z",
    "lastUpdatedAt": "2023-06-07T04:39:27.082Z",
    "policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":\"arn:aws:iam::123456789012:role/my-clients\"},
\"Action\":\"vpc-lattice-svcs:Invoke\",\"Resource\":\"arn:aws:vpc-lattice:us-
east-2:123456789012:service/svc-0285b53b2eEXAMPLE\"}]}",
    "state": "Active"
}
```

Para obtener más información, consulte Auth policies en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte GetAuthPolicy en la Referencia de comandos de la AWS CLI.

`get-listener`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-listener`.

AWS CLI

Para obtener información sobre un oyente del servicio

En el siguiente ejemplo de `get-listener`, se obtiene información sobre el oyente indicado del servicio especificado.

```
aws vpc-lattice get-listener \
    --listener-identifier listener-0ccf55918cEXAMPLE \
    --service-identifier svc-0285b53b2eEXAMPLE
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:service/
svc-0285b53b2eEXAMPLE/listener/listener-0ccf55918cEXAMPLE",
    "createdAt": "2023-05-07T05:08:45.192Z",
    "defaultAction": {
        "forward": {
            "targetGroups": [
                {
                    "targetGroupIdentifier": "tg-0ff213abb6EXAMPLE",
                    "weight": 1
                }
            ]
        }
    },
    "id": "listener-0ccf55918cEXAMPLE",
    "lastUpdatedAt": "2023-05-07T05:08:45.192Z",
    "name": "http-80",
    "port": 80,
    "protocol": "HTTP",
    "serviceArn": "arn:aws:vpc-lattice:us-east-2:123456789012:service/
svc-0285b53b2eEXAMPLE",
    "serviceId": "svc-0285b53b2eEXAMPLE"
```

```
}
```

Para obtener más información, consulte Define routing en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte GetListener en la Referencia de comandos de la AWS CLI.

`get-resource-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource-configuration`.

AWS CLI

Obtención de información sobre una configuración de recursos

En el siguiente ejemplo de `get-resource-configuration`, se obtiene información sobre la configuración de recursos especificada.

```
aws vpc-lattice get-resource-configuration \
    --resource-configuration-identifier rcfg-07129f3acded87625
```

Salida:

```
{
    "allowAssociationToShareableServiceNetwork": true,
    "amazonManaged": false,
    "arn": "arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/
rcfg-07129f3acded87625",
    "createdAt": "2025-02-01T00:57:35.871000+00:00",
    "id": "rcfg-07129f3acded87625",
    "lastUpdatedAt": "2025-02-01T00:57:46.874000+00:00",
    "name": "my-resource-config",
    "portRanges": [
        "1-65535"
    ],
    "protocol": "TCP",
    "resourceConfigurationDefinition": {
        "ipResource": {
            "ipAddress": "10.0.14.85"
        }
```

```
    },
    "resourceGatewayId": "rgw-0bba03f3d56060135",
    "status": "ACTIVE",
    "type": "SINGLE"
}
```

Para obtener más información, consulte Puertas de enlace de recursos en VPC Lattice en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte GetResourceConfiguration en la Referencia de comandos de la AWS CLI.

`get-resource-gateway`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resource-gateway`.

AWS CLI

Obtención de información sobre una puerta de enlace de recursos

En el siguiente ejemplo de `get-resource-gateway`, se obtiene información sobre la puerta de enlace de recursos especificada.

```
aws vpc-lattice get-resource-gateway \
    --resource-gateway-identifier rgw-0bba03f3d56060135
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-1:123456789012:resourcegateway/
rgw-0bba03f3d56060135",
    "createdAt": "2025-02-01T00:57:33.241000+00:00",
    "id": "rgw-0bba03f3d56060135",
    "ipAddressType": "IPV4",
    "lastUpdatedAt": "2025-02-01T00:57:44.351000+00:00",
    "name": "my-resource-gateway",
    "securityGroupIds": [
        "sg-087ffd596c5fe962c"
    ],
    "status": "ACTIVE",
    "subnetIds": [
        "subnet-08e8943905b63a683"
```

```
    ],
    "vpcId": "vpc-0bf4c2739bc05a694"
}
```

Para obtener más información, consulte Puertas de enlace de recursos en VPC Lattice en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte GetResourceGateway en la Referencia de comandos de la AWS CLI.

`get-service-network-service-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-network-service-association`.

AWS CLI

Para obtener información sobre una asociación de servicios

En el siguiente ejemplo de `get-service-network-service-association`, se obtiene información sobre la asociación de servicios especificada.

```
aws vpc-lattice get-service-network-service-association \
    --service-network-service-association-identifier snsa-031fabb4d8EXAMPLE
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-
east-2:123456789012:servicenetworkserviceassociation/snsa-031fabb4d8EXAMPLE",
    "createdAt": "2023-05-05T21:48:16.076Z",
    "createdBy": "123456789012",
    "dnsEntry": {
        "domainName": "my-lattice-service-0285b53b2eEXAMPLE.7d67968.vpc-lattice-
svcs.us-east-2.on.aws",
        "hostedZoneId": "Z09127221KTH2CEXAMPLE"
    },
    "id": "snsa-031fabb4d8EXAMPLE",
    "serviceArn": "arn:aws:vpc-lattice:us-east-2:123456789012:service/
svc-0285b53b2eEXAMPLE",
    "serviceId": "svc-0285b53b2eEXAMPLE",
```

```
    "serviceName": "my-lattice-service",
    "serviceNetworkArn": "arn:aws:vpc-lattice:us-east-2:123456789012:servicenetwork/
sn-080ec7dc93EXAMPLE",
    "serviceNetworkId": "sn-080ec7dc93EXAMPLE",
    "serviceNetworkName": "my-service-network",
    "status": "ACTIVE"
}
```

Para obtener más información, consulte Manage service associations en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte GetServiceNetworkServiceAssociation en la Referencia de comandos de la AWS CLI.

`get-service-network-vpc-association`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-network-vpc-association`.

AWS CLI

Para obtener información sobre una asociación de VPC

En el siguiente ejemplo de `get-service-network-vpc-association`, se obtiene información sobre la asociación de VPC especificada.

```
aws vpc-lattice get-service-network-vpc-association \
    --service-network-vpc-association-identifier snva-0821fc8631EXAMPLE
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:servicenetworkvpcassociation/
snva-0821fc8631EXAMPLE",
    "createdAt": "2023-06-06T23:41:08.421Z",
    "createdBy": "123456789012",
    "id": "snva-0c5dcb60d6EXAMPLE",
    "lastUpdatedAt": "2023-06-06T23:41:08.421Z",
    "securityGroupIds": [
        "sg-0aee16bc6cEXAMPLE"
    ],
```

```
    "serviceNetworkArn": "arn:aws:vpc-lattice:us-east-2:123456789012:servicenetwork/
sn-080ec7dc93EXAMPLE",
    "serviceNetworkId": "sn-080ec7dc93EXAMPLE",
    "serviceNetworkName": "my-service-network",
    "status": "ACTIVE",
    "vpcId": "vpc-0a1b2c3d4eEXAMPLE"
}
```

Para obtener más información, consulte Manage VPC associations en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte GetServiceNetworkVpcAssociation en la Referencia de comandos de la AWS CLI.

`get-service-network`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-network`.

AWS CLI

Para obtener información sobre una red de servicios

En el siguiente ejemplo `get-service-network`, se obtiene información sobre la red de servicios especificada.

```
aws vpc-lattice get-service-network \
    --service-network-identifier sn-080ec7dc93EXAMPLE
```

Salida:

```
{
   "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:servicenetwork/
sn-080ec7dc93EXAMPLE",
   "authType": "AWS_IAM",
   "createdAt": "2023-05-05T15:26:08.417Z",
   "id": "sn-080ec7dc93EXAMPLE",
   "lastUpdatedAt": "2023-05-05T15:26:08.417Z",
   "name": "my-service-network",
   "numberOfAssociatedServices": 2,
   "numberOfAssociatedVPCs": 3
}
```

Para obtener más información, consulte Service networks en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte GetServiceNetwork en la Referencia de comandos de la AWS CLI.

`get-service`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service`.

AWS CLI

Para obtener información sobre un servicio

En el siguiente ejemplo de `get-service`, se obtiene información sobre el servicio especificado.

```
aws vpc-lattice get-service \
    --service-identifier svc-0285b53b2eEXAMPLE
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:service/
svc-0285b53b2eEXAMPLE",
    "authType": "AWS_IAM",
    "createdAt": "2023-05-05T21:35:29.339Z",
    "dnsEntry": {
        "domainName": "my-lattice-service-0285b53b2eEXAMPLE.7d67968.vpc-lattice-
svcs.us-east-2.on.aws",
        "hostedZoneId": "Z09127221KTH2CFUOHIZH"
    },
    "id": "svc-0285b53b2eEXAMPLE",
    "lastUpdatedAt": "2023-05-05T21:35:29.339Z",
    "name": "my-lattice-service",
    "status": "ACTIVE"
}
```

Para obtener más información, consulte Services en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte GetService en la Referencia de comandos de la AWS CLI.

`get-target-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-target-group`.

AWS CLI

Para obtener información acerca de un grupo de destino

En el siguiente ejemplo de `get-target-group`, se obtiene información sobre el grupo de destino especificado, que tiene un tipo de destino `INSTANCE`.

```
aws vpc-lattice get-target-group \
    --target-group-identifier tg-0eaa4b9ab4EXAMPLE
```

Salida:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:targetgroup/
tg-0eaa4b9ab4EXAMPLE",
    "config": {
        "healthCheck": {
            "enabled": true,
            "healthCheckIntervalSeconds": 30,
            "healthCheckTimeoutSeconds": 5,
            "healthyThresholdCount": 5,
            "matcher": {
                "httpCode": "200"
            },
            "path": "/",
            "protocol": "HTTPS",
            "protocolVersion": "HTTP1",
            "unhealthyThresholdCount": 2
        },
        "port": 443,
        "protocol": "HTTPS",
        "protocolVersion": "HTTP1",
        "vpcIdentifier": "vpc-f1663d9868EXAMPLE"
    },
    "createdAt": "2023-05-06T04:41:04.122Z",
    "id": "tg-0eaa4b9ab4EXAMPLE",
    "lastUpdatedAt": "2023-05-06T04:41:04.122Z",
    "name": "my-target-group",
    "serviceArns": [
```

```
        "arn:aws:vpc-lattice:us-east-2:123456789012:service/svc-0285b53b2eEXAMPLE"
    ],
    "status": "ACTIVE",
    "type": "INSTANCE"
}
```

Para obtener más información, consulte Target groups en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte GetTargetGroup en la Referencia de comandos de la AWS CLI.

`list-listeners`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-listeners`.

AWS CLI

Para enumerar los oyentes del servicio

En el siguiente ejemplo de `list-listeners`, se enumeran los oyentes del servicio especificado.

```
aws vpc-lattice list-listeners \
    --service-identifier svc-0285b53b2eEXAMPLE
```

Salida:

```
{
    "items": [
        {
            "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:service/
svc-0285b53b2eEXAMPLE/listener/listener-0ccf55918cEXAMPLE",
            "createdAt": "2023-05-07T05:08:45.192Z",
            "id": "listener-0ccf55918cEXAMPLE",
            "lastUpdatedAt": "2023-05-07T05:08:45.192Z",
            "name": "http-80",
            "port": 80,
            "protocol": "HTTP"
        }
    ]
```

```
}
```

Para obtener más información, consulte Define routing en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte ListListeners en la Referencia de comandos de la AWS CLI.

`list-resource-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-configurations`.

AWS CLI

Muestra de las configuraciones de recursos

En el siguiente ejemplo de `list-resource-configurations`, se muestran las configuraciones de recursos.

```
aws vpc-lattice list-resource-configurations
```

Salida:

```
{
    "items": [
        {
            "amazonManaged": false,
            "arn": "arn:aws:vpc-lattice:us-
east-1:123456789012:resourceconfiguration/rcfg-07129f3acded87625",
            "createdAt": "2025-02-01T00:57:35.871000+00:00",
            "id": "rcfg-07129f3acded87625",
            "lastUpdatedAt": "2025-02-01T00:57:46.874000+00:00",
            "name": "my-resource-config",
            "resourceGatewayId": "rgw-0bba03f3d56060135",
            "status": "ACTIVE",
            "type": "SINGLE"
        }
    ]
}
```

Para obtener más información, consulte Configuraciones de recursos en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte ListResourceConfigurations en la Referencia de comandos de la AWS CLI.

`list-resource-endpoint-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-endpoint-associations`.

AWS CLI

Muestra de las asociaciones de puntos de conexión de VPC

En el siguiente ejemplo de `list-resource-endpoint-associations`, se muestran los puntos de conexión de VPC asociados a la configuración de recursos especificada.

```
aws vpc-lattice list-resource-endpoint-associations \
    --resource-configuration-identifier rcfg-07129f3acded87625
```

Salida:

```
{
    "items": [
        {
            "arn": "arn:aws:vpc-lattice:us-
east-1:123456789012:resourceendpointassociation/rea-0956a7435baf89326",
            "createdAt": "2025-02-01T00:57:38.998000+00:00",
            "id": "rea-0956a7435baf89326",
            "resourceConfigurationArn": "arn:aws:vpc-lattice:us-
east-1:123456789012:resourceconfiguration/rcfg-07129f3acded87625",
            "resourceConfigurationId": "rcfg-07129f3acded87625",
            "vpcEndpointId": "vpce-019b90d6f16d4f958",
            "vpcEndpointOwner": "123456789012"
        }
    ]
}
```

Para obtener más información, consulte Administrar asociaciones de una configuración de recursos de VPC Lattice en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte ListResourceEndpointAssociations en la Referencia de comandos de la AWS CLI.

`list-resource-gateways`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-gateways`.

AWS CLI

Muestra de las puertas de enlace de recursos

En el siguiente ejemplo de `list-resource-gateways`, se muestran todas las puertas de enlace de recursos.

```
aws vpc-lattice list-resource-gateways
```

Salida:

```
{
    "items": [
        {
            "arn": "arn:aws:vpc-lattice:us-east-1:123456789012:resourcegateway/
rgw-0bba03f3d56060135",
            "createdAt": "2025-02-01T00:57:33.241000+00:00",
            "id": "rgw-0bba03f3d56060135",
            "ipAddressType": "IPV4",
            "lastUpdatedAt": "2025-02-01T00:57:44.351000+00:00",
            "name": "my-resource-gateway",
            "seurityGroupIds": [
                "sg-087ffd596c5fe962c"
            ],
            "status": "ACTIVE",
            "subnetIds": [
                "subnet-08e8943905b63a683"
            ],
            "vpcIdentifier": "vpc-0bf4c2739bc05a694"
        }
    ]
}
```

Para obtener más información, consulte Puertas de enlace de recursos en VPC Lattice en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte ListResourceGateways en la Referencia de comandos de la AWS CLI.

`list-service-network-service-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-service-network-service-associations`.

AWS CLI

Para enumerar las asociaciones de servicios

En el siguiente ejemplo de `list-service-network-service-associations`, se enumeran las asociaciones de servicios para la red de servicios especificada. La opción `--query` limita el resultado a los ID de las asociaciones de servicios.

```
aws vpc-lattice list-service-network-service-associations \
    --service-network-identifier sn-080ec7dc93EXAMPLE \
    --query items[*].id
```

Salida:

```
[
    "snsa-031fabb4d8EXAMPLE",
    "snsa-0e16955a8cEXAMPLE"
]
```

Para obtener más información, consulte Manage service associations en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte ListServiceNetworkServiceAssociations en la Referencia de comandos de la AWS CLI.

`list-service-network-vpc-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-service-network-vpc-associations`.

AWS CLI

Para enumerar las asociaciones de VPC

En el siguiente ejemplo de `list-service-network-vpc-associations`, se enumeran las asociaciones de VPC para la red de servicios especificada. La opción `--query` limita el resultado a los ID de las asociaciones de VPC.

```
aws vpc-lattice list-service-network-vpc-associations \
    --service-network-identifier sn-080ec7dc93EXAMPLE \
    --query items[*].id
```

Salida:

```
[
    "snva-0821fc8631EXAMPLE",
    "snva-0c5dcb60d6EXAMPLE"
]
```

Para obtener más información, consulte Manage VPC associations en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte ListServiceNetworkVpcAssociations en la Referencia de comandos de la AWS CLI.

`list-service-network-vpc-endpoint-associations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-service-network-vpc-endpoint-associations`.

AWS CLI

Muestra de las asociaciones de puntos de conexión de VPC

En el siguiente ejemplo de `list-service-network-vpc-endpoint-associations`, se muestran los puntos de conexión de VPC asociados a la red de servicios especificada.

```
aws vpc-lattice list-service-network-vpc-endpoint-associations \
    --service-network-identifier sn-0808d1748faee0c1e
```

Salida:

```
{
    "items": [
        {
            "createdAt": "2025-02-01T01:21:36.667000+00:00",
            "serviceNetworkArn": "arn:aws:vpc-lattice:us-
east-1:123456789012:servicenetwork/sn-0808d1748faee0c1e",
            "state": "ACTIVE",
```

```
            "vpcEndpointId": "vpce-0cc199f605eaeace7",
            "vpcEndpointOwnerId": "123456789012"
        }
    ]
}
```

Para obtener más información, consulte Administrar las asociaciones para una red de servicios de VPC Lattice en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte ListServiceNetworkVpcEndpointAssociations en la Referencia de comandos de la AWS CLI.

`list-service-networks`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-service-networks`.

AWS CLI

Para enumerar sus redes de servicio

En el siguiente ejemplo de `list-service-networks`, se enumeran las redes de servicio que son propiedad de la cuenta que realiza la llamada o que se comparten con ella. La opción `--query` limita los resultados a los nombres de recursos de Amazon (ARN) de las redes de servicio.

```
aws vpc-lattice list-service-networks \
    --query items[*].arn
```

Salida:

```
[
    "arn:aws:vpc-lattice:us-east-2:123456789012:servicenetwork/
sn-080ec7dc93EXAMPLE",
    "arn:aws:vpc-lattice:us-east-2:111122223333:servicenetwork/sn-0ec4d436cfEXAMPLE"
]
```

Para obtener más información, consulte Service networks en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte ListServiceNetworks en la Referencia de comandos de la AWS CLI.

`list-services`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-services`.

AWS CLI

Para enumerar sus servicios

En el siguiente ejemplo de `list-services`, se enumeran los servicios que son propiedad de la cuenta que realiza la llamada o que se comparten con ella. La opción `--query` limita los resultados a los nombres de recursos de Amazon (ARN) de los servicios.

```
aws vpc-lattice list-services \
    --query items[*].arn
```

Salida:

```
[
    "arn:aws:vpc-lattice:us-east-2:123456789012:service/svc-0285b53b2eEXAMPLE",
    "arn:aws:vpc-lattice:us-east-2:111122223333:service/svc-0b8ac96550EXAMPLE"
]
```

Para obtener más información, consulte Services en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte ListServices en la Referencia de comandos de la AWS CLI.

`list-target-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-target-groups`.

AWS CLI

Para enumerar sus grupos de destino

En el siguiente ejemplo de `list-target-groups`, se enumeran los grupos de destino con un tipo de destino `LAMBDA`.

```
aws vpc-lattice list-target-groups \
    --target-group-type LAMBDA
```

Salida:

```
{
    "items": [
        {
            "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:targetgroup/
tg-045c1b7d9dEXAMPLE",
            "createdAt": "2023-05-06T05:22:16.637Z",
            "id": "tg-045c1b7d9dEXAMPLE",
            "lastUpdatedAt": "2023-05-06T05:22:16.637Z",
            "name": "my-target-group-lam",
            "serviceArns": [
                "arn:aws:vpc-lattice:us-east-2:123456789012:service/
svc-0285b53b2eEXAMPLE"
            ],
            "status": "ACTIVE",
            "type": "LAMBDA"
        }
    ]
}
```

Para obtener más información, consulte Target groups en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte ListTargetGroups en la Referencia de comandos de la AWS CLI.

`list-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-targets`.

AWS CLI

Para enumerar los destinos de un grupo de destino

En el siguiente ejemplo de `list-targets`, se enumeran los destinos del grupo de destino especificado.

```
aws vpc-lattice list-targets \
    --target-group-identifier tg-0eaa4b9ab4EXAMPLE
```

Salida:

```
{
    "items": [
        {
            "id": "i-07dd579bc5EXAMPLE",
            "port": 443,
            "status": "HEALTHY"
        },
        {
            "id": "i-047b3c9078EXAMPLE",
            "port": 443,
            "reasonCode": "HealthCheckFailed",
            "status": "UNHEALTHY"
        }
    ]
}
```

Para obtener más información, consulte Target groups en la Guía del usuario de Amazon VPC Lattice.

- Para obtener detalles sobre la API, consulte ListTargets en la Referencia de comandos de la AWS CLI.

`put-auth-policy`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-auth-policy`.

AWS CLI

Para crear una política de autenticación para un servicio

En el siguiente ejemplo de `put-auth-policy`, se concede acceso a las solicitudes de cualquier entidad principal autenticada que utilice el rol de IAM especificado. El recurso es el ARN del servicio al que está asociado la política.

```
aws vpc-lattice put-auth-policy \
    --resource-identifier svc-0285b53b2eEXAMPLE \
    --policy file://auth-policy.json
```

Contenido de `auth-policy.json`:

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:role/my-clients"
            },
            "Action": "vpc-lattice-svcs:Invoke",
            "Resource": "arn:aws:vpc-lattice:us-east-2:123456789012:service/
svc-0285b53b2eEXAMPLE"
        }
    ]
}
```

Salida:

```
{
    "policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":\"arn:aws:iam::123456789012:role/my-clients\"},
\"Action\":\"vpc-lattice-svcs:Invoke\",\"Resource\":\"arn:aws:vpc-lattice:us-
east-2:123456789012:service/svc-0285b53b2eEXAMPLE\"}]}",
    "state": "Active"
}
```

Para obtener más información, consulte Auth policies en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información acerca de la API, consulte PutAuthPolicy en la Referencia de comandos de la AWS CLI.

`register-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-targets`.

AWS CLI

Para registrar un destino

En el siguiente ejemplo de `register-targets`, se registran los destinos especificados con el grupo de destino indicado.

```
aws vpc-lattice register-targets \
    --targets id=i-047b3c9078EXAMPLE id=i-07dd579bc5EXAMPLE \
```

```
    --target-group-identifier tg-0eaa4b9ab4EXAMPLE
```

Salida:

```
{
    "successful": [
        {
            "id": "i-07dd579bc5EXAMPLE",
            "port": 443
        }
    ],
    "unsuccessful": [
        {
            "failureCode": "UnsupportedTarget",
            "failureMessage": "Instance targets must be in the same VPC as their
 target group",
            "id": "i-047b3c9078EXAMPLE",
            "port": 443
        }
    ]
}
```

Para obtener más información, consulte Register targets en la Guía del usuario de Amazon VPC Lattice.

- Para obtener información sobre la API, consulte RegisterTargets en la Referencia de comandos de la AWS CLI.

AWS WAF Classic Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS WAF Classic.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`put-logging-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-logging-configuration`.

AWS CLI

Para crear una configuración de registro para el ARN de ACL web con el ARN de flujo de Kinesis Firehose especificado

En el siguiente ejemplo de `put-logging-configuration`, se muestra la configuración de registro para WAF con CloudFront.

```
aws waf put-logging-configuration \
    --logging-configuration ResourceArn=arn:aws:waf::123456789012:webacl/3bffd3ed-fa2e-445e-869f-a6a7cf153fd3,LogDestinationConfigs=arn:aws:firehose:us-east-1:123456789012:deliverystream/aws-waf-logs-firehose-stream,RedactedFields=[]
```

Salida:

```
{
    "LoggingConfiguration": {
        "ResourceArn": "arn:aws:waf::123456789012:webacl/3bffd3ed-fa2e-445e-869f-a6a7cf153fd3",
        "LogDestinationConfigs": [
            "arn:aws:firehose:us-east-1:123456789012:deliverystream/aws-waf-logs-firehose-stream"
        ]
    }
}
```

- Para obtener información sobre la API, consulte PutLoggingConfiguration en la Referencia de comandos de la AWS CLI.

`update-byte-match-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-byte-match-set`.

AWS CLI

Para actualizar un conjunto de coincidencias de bytes

El siguiente comando `update-byte-match-set` elimina un objeto ByteMatchTuple (filtro) de un ByteMatchSet:

```
aws waf update-byte-match-set --byte-match-set-id a123fae4-
b567-8e90-1234-5ab67ac8ca90 --change-token 12cs345-67cd-890b-1cd2-c3a4567d89f1 --
updates
 Action="DELETE",ByteMatchTuple={FieldToMatch={Type="HEADER",Data="referer"},TargetString="b
```

Para obtener más información, consulte Trabajar con condiciones de coincidencia de cadena en la Guía para desarrolladores de AWS WAF.

- Para obtener información acerca de la API, consulte UpdateByteMatchSet en la Referencia de comandos de la AWS CLI.

`update-ip-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-ip-set`.

AWS CLI

Para actualizar un conjunto de IP

El siguiente comando `update-ip-set` actualiza un IPSet con una dirección IPv4 y elimina una dirección IPv6:

```
aws waf update-ip-set --ip-set-id a123fae4-b567-8e90-1234-5ab67ac8ca90
 --change-token 12cs345-67cd-890b-1cd2-c3a4567d89f1 --updates
 Action="INSERT",IPSetDescriptor={Type="IPV4",Value="12.34.56.78/16"},Action="DELETE",IPSetD
```

Como alternativa, puede utilizar un archivo JSON para especificar la entrada. Por ejemplo:

```
aws waf update-ip-set --ip-set-id a123fae4-b567-8e90-1234-5ab67ac8ca90 --change-
token 12cs345-67cd-890b-1cd2-c3a4567d89f1  --updates file://change.json
```

Este es el contenido del archivo JSON:

```
[
```

```
{
"Action": "INSERT",
"IPSetDescriptor":
{
"Type": "IPV4",
"Value": "12.34.56.78/16"
}
},
{
"Action": "DELETE",
"IPSetDescriptor":
{
"Type": "IPV6",
"Value": "1111:0000:0000:0000:0000:0000:0000:0111/128"
}
}
]
```

Para obtener más información, consulte Trabajar con condiciones de coincidencia de IP en la Guía para desarrolladores de AWS WAF.

- Para obtener información sobre la API, consulte UpdateIpSet en la Referencia de comandos de la AWS CLI.

`update-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-rule`.

AWS CLI

Para actualizar una regla

El siguiente comando `update-rule` elimina un objeto Predicate de una regla:

```
aws waf update-rule --rule-id a123fae4-b567-8e90-1234-5ab67ac8ca90
 --change-token 12cs345-67cd-890b-1cd2-c3a4567d89f1 --updates
 Action="DELETE",Predicate={Negated=false,Type="ByteMatch",DataId="MyByteMatchSetID"}
```

Para obtener más información, consulte Trabajar con reglas en la Guía para desarrolladores de AWS WAF.

- Para obtener información sobre la API, consulte UpdateRule en la Referencia de comandos de la AWS CLI.

update-size-constraint-set

En el siguiente ejemplo de código, se muestra cómo utilizar `update-size-constraint-set`.

AWS CLI

Para actualizar un conjunto de restricciones de tamaño

El siguiente comando `update-size-constraint-set` elimina un objeto SizeConstraint (filtros) de un conjunto de restricciones de tamaño:

```
aws waf update-size-constraint-set --size-constraint-set-id a123fae4-
b567-8e90-1234-5ab67ac8ca90 --change-token 12cs345-67cd-890b-1cd2-c3a4567d89f1 --
updates
 Action="DELETE",SizeConstraint={FieldToMatch={Type="QUERY_STRING"},TextTransformation="NONE
```

Para obtener más información, consulte Trabajar con condiciones de restricción de tamaño en la Guía para desarrolladores de AWS WAF.

- Para obtener información sobre la API, consulte UpdateSizeConstraintSet en la Referencia de comandos de la AWS CLI.

update-sql-injection-match-set

En el siguiente ejemplo de código, se muestra cómo utilizar `update-sql-injection-match-set`.

AWS CLI

Para actualizar un conjunto de coincidencias de inyección de código SQL

El siguiente comando `update-sql-injection-match-set` elimina un objeto SqlInjectionMatchTuple (filtros) de un conjunto de coincidencias de inyección de código SQL:

```
aws waf update-sql-injection-match-set --sql-injection-
match-set-id a123fae4-b567-8e90-1234-5ab67ac8ca90 --
change-token 12cs345-67cd-890b-1cd2-c3a4567d89f1 --updates
 Action="DELETE",SqlInjectionMatchTuple={FieldToMatch={Type="QUERY_STRING"},TextTransformati
```

Para obtener más información, consulte Trabajar con condiciones de coincidencia de inyección de código SQL en la Guía para desarrolladores de AWS WAF.

- Para obtener información sobre la API, consulte UpdateSqlInjectionMatchSet en la Referencia de comandos de la AWS CLI.

`update-web-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-web-acl`.

AWS CLI

Para actualizar una ACL web

El siguiente comando `update-web-acl` elimina un objeto `ActivatedRule` de una WebACL.

```
aws waf update-web-acl --web-acl-id a123fae4-b567-8e90-1234-5ab67ac8ca90
--change-token 12cs345-67cd-890b-1cd2-c3a4567d89f1 --updates
Action="DELETE",ActivatedRule='{Priority=1,RuleId="WAFRule-1-
Example",Action={Type="ALLOW"},Type="REGULAR"}'
```

Salida:

```
{
    "ChangeToken": "12cs345-67cd-890b-1cd2-c3a4567d89f1"
}
```

Para obtener más información, consulte Trabajar con ACL web en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte UpdateWebAcl en la Referencia de comandos de la AWS CLI.

`update-xss-match-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-xss-match-set`.

AWS CLI

Para actualizar un XSSMatchSet

El siguiente comando `update-xss-match-set` elimina un objeto XssMatchTuple (filtros) de un XssMatchSet:

```
aws waf update-xss-match-set --xss-match-set-id a123fae4-b567-8e90-1234-5ab67ac8ca90
 --change-token 12cs345-67cd-890b-1cd2-c3a4567d89f1 --updates
 Action="DELETE",XssMatchTuple={FieldToMatch={Type="QUERY_STRING"},TextTransformation="URL_D
```

Para obtener más información, consulte Trabajar con condiciones de coincidencia de scripting entre sitios en la Guía para desarrolladores de AWS WAF.

- Para obtener información sobre la API, consulte UpdateXssMatchSet en la Referencia de comandos de la AWS CLI.

AWS WAF Classic Regional Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS WAF Classic Regional.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-web-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-web-acl`.

AWS CLI

Para asociar una ACL web con un recurso

El siguiente comando `associate-web-acl` asocia una ACL web, especificada por web-acl-id, con un recurso, especificado por resource-arn. El ARN del recurso puede hacer referencia a un Equilibrador de carga de aplicación o a una puerta de enlace de la API:

```
aws waf-regional associate-web-acl \
    --web-acl-id a123fae4-b567-8e90-1234-5ab67ac8ca90 \
    --resource-arn 12cs345-67cd-890b-1cd2-c3a4567d89f1
```

Para obtener más información, consulte Trabajar con ACL web en la Guía para desarrolladores de AWS WAF.

- Para obtener información sobre la API, consulte AssociateWebAcl en la Referencia de comandos de la AWS CLI.

`put-logging-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-logging-configuration`.

AWS CLI

Para crear una configuración de registro para el ARN de ACL web con el ARN de flujo de Kinesis Firehose especificado

En el siguiente ejemplo de `put-logging-configuration`, se muestra la configuración de registro para WAF con ALB/APIGateway en la región `us-east-1`.

```
aws waf-regional put-logging-configuration \
    --logging-configuration ResourceArn=arn:aws:waf-
regional:us-east-1:123456789012:webacl/3bffd3ed-fa2e-445e-869f-
a6a7cf153fd3,LogDestinationConfigs=arn:aws:firehose:us-
east-1:123456789012:deliverystream/aws-waf-logs-firehose-stream,RedactedFields=[] \
    --region us-east-1
```

Salida:

```
{
    "LoggingConfiguration": {
        "ResourceArn": "arn:aws:waf-regional:us-east-1:123456789012:webacl/3bffd3ed-
fa2e-445e-869f-a6a7cf153fd3",
        "LogDestinationConfigs": [
            "arn:aws:firehose:us-east-1:123456789012:deliverystream/aws-waf-logs-
firehose-stream"
        ]
    }
}
```

- Para obtener información sobre la API, consulte PutLoggingConfiguration en la Referencia de comandos de la AWS CLI.

update-byte-match-set

En el siguiente ejemplo de código, se muestra cómo utilizar `update-byte-match-set`.

AWS CLI

Para actualizar un conjunto de coincidencias de bytes

El siguiente comando `update-byte-match-set` elimina un objeto `ByteMatchTuple` (filtro) de un `ByteMatchSet`. Como el valor `updates` tiene comillas dobles incrustadas, debe escribir el valor entre comillas simples.

```
aws waf-regional update-byte-match-set \
    --byte-match-set-id a123fae4-b567-8e90-1234-5ab67ac8ca90 \
    --change-token 12cs345-67cd-890b-1cd2-c3a4567d89f1 \
    --updates
 'Action="DELETE",ByteMatchTuple={FieldToMatch={Type="HEADER",Data="referer"},TargetString="
```

Para obtener más información, consulte Trabajar con condiciones de coincidencia de cadena en la Guía para desarrolladores de AWS WAF.

- Para obtener información acerca de la API, consulte UpdateByteMatchSet en la Referencia de comandos de la AWS CLI.

update-ip-set

En el siguiente ejemplo de código, se muestra cómo utilizar `update-ip-set`.

AWS CLI

Para actualizar un conjunto de IP

El siguiente comando `update-ip-set` actualiza un IPSet con una dirección IPv4 y elimina una dirección IPv6. Para obtener el valor de `change-token`, ejecute el comando `get-change-token`. Como el valor para las actualizaciones tiene comillas dobles incrustadas, debe escribir el valor entre comillas simples.

```
aws waf update-ip-set \
```

```
    --ip-set-id a123fae4-b567-8e90-1234-5ab67ac8ca90 \
    --change-token 12cs345-67cd-890b-1cd2-c3a4567d89f1 \
    --updates
 'Action="INSERT",IPSetDescriptor={Type="IPV4",Value="12.34.56.78/16"},Action="DELETE",IPSet
```

Como alternativa, puede utilizar un archivo JSON para especificar la entrada. Por ejemplo:

```
aws waf-regional update-ip-set \
    --ip-set-id a123fae4-b567-8e90-1234-5ab67ac8ca90 \
    --change-token 12cs345-67cd-890b-1cd2-c3a4567d89f1  \
    --updates file://change.json
```

Contenido del `change.json`

```
[
    {
        "Action": "INSERT",
        "IPSetDescriptor":
        {
            "Type": "IPV4",
            "Value": "12.34.56.78/16"
        }
    },
    {
        "Action": "DELETE",
        "IPSetDescriptor":
        {
            "Type": "IPV6",
            "Value": "1111:0000:0000:0000:0000:0000:0000:0111/128"
        }
    }
]
```

Para obtener más información, consulte Trabajar con condiciones de coincidencia de IP en la Guía para desarrolladores de AWS WAF.

- Para obtener información sobre la API, consulte UpdateIpSet en la Referencia de comandos de la AWS CLI.

`update-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-rule`.

AWS CLI

Para actualizar una regla

El siguiente comando `update-rule` elimina un objeto `Predicate` de una regla. Como el valor `updates` tiene comillas dobles incrustadas, debe escribir el valor entero entre comillas simples.

```
aws waf-regional update-rule \
    --rule-id a123fae4-b567-8e90-1234-5ab67ac8ca90 \
    --change-token 12cs345-67cd-890b-1cd2-c3a4567d89f1 \
    --updates
 'Action="DELETE",Predicate={Negated=false,Type="ByteMatch",DataId="MyByteMatchSetID"}'
```

Para obtener más información, consulte Trabajar con reglas en la Guía para desarrolladores de AWS WAF.

- Para obtener información sobre la API, consulte UpdateRule en la Referencia de comandos de la AWS CLI.

update-size-constraint-set

En el siguiente ejemplo de código, se muestra cómo utilizar `update-size-constraint-set`.

AWS CLI

Para actualizar un conjunto de restricciones de tamaño

El siguiente comando `update-size-constraint-set` elimina un objeto SizeConstraint (filtros) de un conjunto de restricciones de tamaño. Como el valor `updates` tiene comillas dobles incrustadas, debe escribir el valor entero entre comillas simples.

```
aws waf-regional update-size-constraint-set \
    --size-constraint-set-id a123fae4-b567-8e90-1234-5ab67ac8ca90 \
    --change-token 12cs345-67cd-890b-1cd2-c3a4567d89f1 \
    --updates
 'Action="DELETE",SizeConstraint={FieldToMatch={Type="QUERY_STRING"},TextTransformation="NON
```

Para obtener más información, consulte Trabajar con condiciones de restricción de tamaño en la Guía para desarrolladores de AWS WAF.

- Para obtener información sobre la API, consulte UpdateSizeConstraintSet en la Referencia de comandos de la AWS CLI.

update-sql-injection-match-set

En el siguiente ejemplo de código, se muestra cómo utilizar `update-sql-injection-match-set`.

AWS CLI

Para actualizar un conjunto de coincidencias de inyección de código SQL

El siguiente comando `update-sql-injection-match-set` elimina un objeto `SqlInjectionMatchTuple` (filtros) de un conjunto de coincidencias de inyección de código SQL. Como el valor `updates` tiene comillas dobles incrustadas, debe escribir el valor entero entre comillas simples.

aws waf-regional update-sql-injection-match-set --sql-injection-match-set-id a123fae4-b567-8e90-1234-5ab67ac8ca90 --change-token 12cs345-67cd-890b-1cd2-c3a4567d89f1 --updates 'Action="DELETE",SqlInjectionMatchTuple={FieldToMatch={Type="QUERY_STRING"},TextTransformatic

Para obtener más información, consulte Trabajar con condiciones de coincidencia de inyección de código SQL en la Guía para desarrolladores de AWS WAF.

- Para obtener información sobre la API, consulte UpdateSqlInjectionMatchSet en la Referencia de comandos de la AWS CLI.

update-web-acl

En el siguiente ejemplo de código, se muestra cómo utilizar `update-web-acl`.

AWS CLI

Para actualizar una ACL web

El siguiente comando `update-web-acl` elimina un objeto `ActivatedRule` de una WebACL. Como el valor `updates` tiene comillas dobles incrustadas, debe escribir el valor entero entre comillas simples.

```
aws waf-regional update-web-acl \
    --web-acl-id a123fae4-b567-8e90-1234-5ab67ac8ca90 \
    --change-token 12cs345-67cd-890b-1cd2-c3a4567d89f1 \
    --updates Action="DELETE",ActivatedRule='{Priority=1,RuleId="WAFRule-1-
Example",Action={Type="ALLOW"},Type="ALLOW"}'
```

Para obtener más información, consulte Trabajar con ACL web en la Guía para desarrolladores de AWS WAF.

- Para obtener información sobre la API, consulte UpdateWebAcl en la Referencia de comandos de la AWS CLI.

`update-xss-match-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-xss-match-set`.

AWS CLI

Para actualizar un XSSMatchSet

El siguiente comando `update-xss-match-set` elimina un objeto `XssMatchTuple` (filtros) de un `XssMatchSet`. Como el valor `updates` tiene comillas dobles incrustadas, debe escribir el valor entero entre comillas simples.

```
aws waf-regional update-xss-match-set \
    --xss-match-set-id a123fae4-b567-8e90-1234-5ab67ac8ca90 \
    --change-token 12cs345-67cd-890b-1cd2-c3a4567d89f1 \
    --updates
 'Action="DELETE",XssMatchTuple={FieldToMatch={Type="QUERY_STRING"},TextTransformation="URL_
```

Para obtener más información, consulte Trabajar con condiciones de coincidencia de scripting entre sitios en la Guía para desarrolladores de AWS WAF.

- Para obtener información sobre la API, consulte UpdateXssMatchSet en la Referencia de comandos de la AWS CLI.

AWS WAFV2 Ejemplos de usando AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con AWS WAFV2.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-web-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-web-acl`.

AWS CLI

Para asociar una ACL web con un recurso de AWS regional

En el siguiente ejemplo de `associate-web-acl`, se asocia la ACL web especificada con el recurso del equilibrador de carga de aplicación.

```
aws wafv2 associate-web-acl \
    --web-acl-arn arn:aws:wafv2:us-west-2:123456789012:regional/webacl/test-cli/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --resource-arn arn:aws:elasticloadbalancing:us-west-2:123456789012:loadbalancer/
app/waf-cli-alb/1ea17125f8b25a2a \
    --region us-west-2
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Asociar o disociar una ACL web con un recurso de AWS en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte AssociateWebAcl en la Referencia de comandos de la AWS CLI.

`check-capacity`

En el siguiente ejemplo de código, se muestra cómo utilizar `check-capacity`.

AWS CLI

Para obtener la capacidad utilizada por un conjunto de reglas

En el siguiente ejemplo de `check-capacity`, se recuperan los requisitos de capacidad de un conjunto de reglas que contiene una instrucción de regla basada en tasas y una instrucción de regla AND que contiene reglas anidadas.

```
aws wafv2 check-capacity \
    --scope REGIONAL \
    --rules file://waf-rule-list.json \
    --region us-west-2
```

Contenido del archivo //waf-rule-list.json:

```
[
    {
        "Name":"basic-rule",
        "Priority":0,
        "Statement":{
            "AndStatement":{
                "Statements":[
                    {
                        "ByteMatchStatement":{
                            "SearchString":"example.com",
                            "FieldToMatch":{
                                "SingleHeader":{
                                    "Name":"host"
                                }
                            },
                            "TextTransformations":[
                                {
                                    "Priority":0,
                                    "Type":"LOWERCASE"
                                }
                            ],
                            "PositionalConstraint":"EXACTLY"
                        }
                    },
                    {
                        "GeoMatchStatement":{
                            "CountryCodes":[
                                "US",
                                "IN"
                            ]
                        }
                    }
                ]
            }
        },
        "Action":{
```

```
            "Allow":{

            }
        },
        "VisibilityConfig":{
            "SampledRequestsEnabled":true,
            "CloudWatchMetricsEnabled":true,
            "MetricName":"basic-rule"
        }
    },
    {
        "Name":"rate-rule",
        "Priority":1,
        "Statement":{
            "RateBasedStatement":{
                "Limit":1000,
                "AggregateKeyType":"IP"
            }
        },
        "Action":{
            "Block":{

            }
        },
        "VisibilityConfig":{
            "SampledRequestsEnabled":true,
            "CloudWatchMetricsEnabled":true,
            "MetricName":"rate-rule"
        }
    }
]
```

Salida:

```
{
    "Capacity":15
}
```

Para obtener más información, consulte Cómo funciona AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener más información sobre la API, consulte CheckCapacity en la Referencia de comandos de la AWS CLI.

`create-ip-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-ip-set`.

AWS CLI

Para crear un conjunto de IP para usarlo en sus ACL web y grupos de reglas

El siguiente comando `create-ip-set` crea un conjunto de direcciones IP con una sola especificación de rango de direcciones.

```
aws wafv2 create-ip-set \
    --name testip \
    --scope REGIONAL \
    --ip-address-version IPV4 \
    --addresses 198.51.100.0/16
```

Salida:

```
{
    "Summary":{
        "ARN":"arn:aws:wafv2:us-west-2:123456789012:regional/ipset/testip/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "Description":"",
        "Name":"testip",
        "LockToken":"447e55ac-0000-0000-0000-86b67c17f8b5",
        "Id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    }
}
```

Para obtener más información, consulte Creación y administración de los conjuntos de direcciones IP y los conjuntos de patrones de expresiones regulares en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte CreateIpSet en la Referencia de comandos de la AWS CLI.

`create-regex-pattern-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-regex-pattern-set`.

AWS CLI

Para crear un conjunto de patrones de expresiones regulares para usarlo en sus ACL web y grupos de reglas

El siguiente comando `create-regex-pattern-set` crea un conjunto de patrones de expresiones regulares con dos patrones de expresiones regulares especificados.

```
aws wafv2 create-regex-pattern-set \
    --name regexPatterSet01 \
    --scope REGIONAL \
    --description 'Test web-acl' \
    --regular-expression-list '[{"RegexString": "/[0-9]*/"},{"RegexString": "/[a-
z]*/"}]'
```

Salida:

```
{
    "Summary":{
        "ARN":"arn:aws:wafv2:us-west-2:123456789012:regional/regexpatternset/
regexPatterSet01/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "Description":"Test web-acl",
        "Name":"regexPatterSet01",
        "LockToken":"0bc01e21-03c9-4b98-9433-6229cbf1ef1c",
        "Id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    }
}
```

Para obtener más información, consulte Creación y administración de los conjuntos de direcciones IP y los conjuntos de patrones de expresiones regulares en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte CreateRegexPatternSet en la Referencia de comandos de la AWS CLI.

`create-rule-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-rule-group`.

AWS CLI

Para crear un grupo de reglas personalizado para usarlo en las ACL web

El siguiente comando `create-rule-group` crea un grupo de reglas personalizado para uso regional. Las instrucciones de reglas del grupo se proporcionan en un archivo con formato JSON.

```
aws wafv2 create-rule-group \
    --name "TestRuleGroup" \
    --scope REGIONAL \
    --capacity 250 \
    --rules file://waf-rule.json \
    --visibility-
config SampledRequestsEnabled=true,CloudWatchMetricsEnabled=true,MetricName=TestRuleGroupMet
 \
    --region us-west-2
```

Contenido del archivo //waf-rule.json:

```
[
    {
        "Name":"basic-rule",
        "Priority":0,
        "Statement":{
            "AndStatement":{
                "Statements":[
                    {
                        "ByteMatchStatement":{
                            "SearchString":"example.com",
                            "FieldToMatch":{
                                "SingleHeader":{
                                    "Name":"host"
                                }
                            },
                            "TextTransformations":[
                                {
                                    "Priority":0,
                                    "Type":"LOWERCASE"
                                }
                            ],
                            "PositionalConstraint":"EXACTLY"
                        }
                    },
                    {
                        "GeoMatchStatement":{
                            "CountryCodes":[
                                "US",
```

```
                                "IN"
                            ]
                        }
                    }
                ]
            }
        },
        "Action":{
            "Allow":{

            }
        },
        "VisibilityConfig":{
            "SampledRequestsEnabled":true,
            "CloudWatchMetricsEnabled":true,
            "MetricName":"basic-rule"
        }
    }
]
```

Salida:

```
{
    "Summary":{
        "ARN":"arn:aws:wafv2:us-west-2:123456789012:regional/rulegroup/
TestRuleGroup/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "Description":"",
        "Name":"TestRuleGroup",
        "LockToken":"7b3bcec2-374e-4c5a-b2b9-563bf47249f0",
        "Id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    }
}
```

Para obtener más información, consulte Administrar sus propios grupos de reglas en la Guía para desarrolladores AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte CreateRuleGroup en la Referencia de comandos de la AWS CLI.

`create-web-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-web-acl`.

AWS CLI

Para crear una ACL web

El siguiente comando `create-web-acl` crea una ACL web para uso regional. Las instrucciones de reglas de la ACL web se proporcionan en un archivo con formato JSON.

```
aws wafv2 create-web-acl \
    --name TestWebAcl \
    --scope REGIONAL \
    --default-action Allow={} \
    --visibility-
config SampledRequestsEnabled=true,CloudWatchMetricsEnabled=true,MetricName=TestWebAclMetric
 \
    --rules file://waf-rule.json \
    --region us-west-2
```

Contenido del archivo //waf-rule.json:

```
[
    {
        "Name":"basic-rule",
        "Priority":0,
        "Statement":{
            "AndStatement":{
                "Statements":[
                    {
                        "ByteMatchStatement":{
                            "SearchString":"example.com",
                            "FieldToMatch":{
                                "SingleHeader":{
                                    "Name":"host"
                                }
                            },
                            "TextTransformations":[
                                {
                                    "Priority":0,
                                    "Type":"LOWERCASE"
                                }
                            ],
                            "PositionalConstraint":"EXACTLY"
                        }
                    },
```

```
                    {
                        "GeoMatchStatement":{
                            "CountryCodes":[
                                "US",
                                "IN"
                            ]
                        }
                    }
                ]
            }
        },
        "Action":{
            "Allow":{

            }
        },
        "VisibilityConfig":{
            "SampledRequestsEnabled":true,
            "CloudWatchMetricsEnabled":true,
            "MetricName":"basic-rule"
        }
    }
]
```

Salida:

```
{
    "Summary":{
        "ARN":"arn:aws:wafv2:us-west-2:123456789012:regional/webacl/TestWebAcl/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "Description":"",
        "Name":"TestWebAcl",
        "LockToken":"2294b3a1-eb60-4aa0-a86f-a3ae04329de9",
        "Id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    }
}
```

Para obtener más información, consulte El uso de las ACL web en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte CreateWebAcl en la Referencia de comandos de AWS CLI.

`delete-ip-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-ip-set`.

AWS CLI

Para eliminar un conjunto de IP

En el siguiente ejemplo de `delete-ip-set`, se elimina el conjunto de IP especificado. Esta llamada requiere un ID, que puede obtener de la llamada a `list-ip-sets` y de un token de bloqueo, que puede obtener de las llamadas a `list-ip-sets` y `get-ip-set`.

```
aws wafv2 delete-ip-set \
    --name test1 \
    --scope REGIONAL \
    --id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --lock-token 46851772-db6f-459d-9385-49428812e357
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación y administración de los conjuntos de direcciones IP y los conjuntos de patrones de expresiones regulares en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte DeleteIpSet en la Referencia de comandos de la AWS CLI.

`delete-logging-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-logging-configuration`.

AWS CLI

Para deshabilitar el registro para una ACL web

En el siguiente ejemplo de `delete-logging-configuration`, se elimina cualquier configuración de registro de la ACL web especificada.

```
aws wafv2 delete-logging-configuration \
    --resource-arn arn:aws:wafv2:us-west-2:123456789012:regional/webacl/test/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Registro AWS WAF del tráfico en la ACL web en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte DeleteLoggingConfiguration en la Referencia de comandos de la AWS CLI.

`delete-regex-pattern-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-regex-pattern-set`.

AWS CLI

Para eliminar un conjunto de patrones de expresiones regulares

En el siguiente ejemplo de `delete-regex-pattern-set`, se actualiza la configuración del conjunto de patrones de expresiones regulares especificado. Esta llamada requiere un ID, que se puede obtener de la llamada a `list-regex-pattern-sets` y de un token de bloqueo, que puede obtener de la llamada a `list-regex-pattern-sets` o de la llamada a `get-regex-pattern-set`.

```
aws wafv2 delete-regex-pattern-set \
    --name regexPatterSet01 \
    --scope REGIONAL \
    --id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --lock-token 0bc01e21-03c9-4b98-9433-6229cbf1ef1c
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Creación y administración de los conjuntos de direcciones IP y los conjuntos de patrones de expresiones regulares en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte DeleteRegexPatternSet en la Referencia de comandos de la AWS CLI.

`delete-rule-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-rule-group`.

AWS CLI

Para eliminar un grupo de reglas personalizadas

En el siguiente ejemplo de `delete-rule-group`, se elimina el grupo de reglas personalizadas especificado. Esta llamada requiere un ID, que se puede obtener de la llamada a `list-rule-groups` y de un token de bloqueo, que puede obtener de la llamada a `list-rule-groups` o de la llamada a `get-rule-group`.

```
aws wafv2 delete-rule-group \
    --name TestRuleGroup \
    --scope REGIONAL \
    --id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --lock-token 7b3bcec2-0000-0000-0000-563bf47249f0
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Administrar sus propios grupos de reglas en la Guía para desarrolladores AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte DeleteRuleGroup en la Referencia de comandos de la AWS CLI.

`delete-web-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-web-acl`.

AWS CLI

Para eliminar una ACL web

En el siguiente ejemplo de `delete-web-acl`, se elimina la ACL web especificada de su cuenta. Una ACL web solo se puede eliminar si no está asociada a ningún recurso. Esta llamada requiere un ID, que se puede obtener de la llamada a `list-web-acls` y de un token de bloqueo, que puede obtener de la llamada a `list-web-acls` o de la llamada a `get-web-acl`.

```
aws wafv2 delete-web-acl \
    --name test \
    --scope REGIONAL \
    --id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --lock-token ebab4ed2-155e-4c9a-9efb-e4c45665b1f5
```

Este comando no genera ninguna salida.

Para obtener más información, consulte El uso de las ACL web en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte DeleteWebAcl en la Referencia de comandos de la AWS CLI.

`describe-managed-rule-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-managed-rule-group`.

AWS CLI

Para recuperar la descripción de un grupo de reglas administrado

En el siguiente ejemplo de `describe-managed-rule-group`, se recupera la descripción de un grupo de reglas administrado por AWS.

```
aws wafv2 describe-managed-rule-group \
    --vendor-name AWS \
    --name AWSManagedRulesCommonRuleSet \
    --scope REGIONAL
```

Salida:

```
{
    "Capacity": 700,
    "Rules": [
        {
            "Name": "NoUserAgent_HEADER",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "UserAgent_BadBots_HEADER",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "SizeRestrictions_QUERYSTRING",
```

```
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "SizeRestrictions_Cookie_HEADER",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "SizeRestrictions_BODY",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "SizeRestrictions_URIPATH",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "EC2MetaDataSSRF_BODY",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "EC2MetaDataSSRF_COOKIE",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "EC2MetaDataSSRF_URIPATH",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "EC2MetaDataSSRF_QUERYARGUMENTS",
            "Action": {
                "Block": {}
```

```
            }
        },
        {
            "Name": "GenericLFI_QUERYARGUMENTS",
            "Action": {
                "Block": {}
            }
        },
        {
            }
            "Name": "GenericLFI_URIPATH",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "GenericLFI_BODY",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "RestrictedExtensions_URIPATH",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "RestrictedExtensions_QUERYARGUMENTS",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "GenericRFI_QUERYARGUMENTS",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "GenericRFI_BODY",
            "Action": {
                "Block": {}
            }
```

```
        },
        {
            "Name": "GenericRFI_URIPATH",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "CrossSiteScripting_COOKIE",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "CrossSiteScripting_QUERYARGUMENTS",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "CrossSiteScripting_BODY",
            "Action": {
                "Block": {}
            }
        },
        {
            "Name": "CrossSiteScripting_URIPATH",
            "Action": {
                "Block": {}
            }
        }
    ]
}
```

Para obtener más información, consulte Uso de grupos de reglas administrados en AWS WAF en la Guía para desarrolladores AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte DescribeManagedRuleGroup en la Referencia de comandos de la AWS CLI.

`disassociate-web-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-web-acl`.

AWS CLI

Para desasociar una ACL web de un recurso de AWS regional

En el siguiente ejemplo de `disassociate-web-acl`, se elimina cualquier asociación de ACL web especificada del recurso del equilibrador de carga de aplicación.

```
aws wafv2 disassociate-web-acl \
    --resource-arn arn:aws:elasticloadbalancing:us-west-2:123456789012:loadbalancer/app/waf-cli-alb/1ea17125f8b25a2a \
    --region us-west-2
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Asociar o disociar una ACL web con un recurso de AWS en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte DisassociateWebAcl en la Referencia de comandos de la AWS CLI.

`get-ip-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-ip-set`.

AWS CLI

Para recuperar un conjunto de IP específico

En el siguiente ejemplo de `get-ip-set`, se recupera el conjunto de direcciones IP con el nombre, el alcance y el ID especificados. Puede obtener el ID de un conjunto de direcciones IP mediante los comandos `create-ip-set` y `list-ip-sets`.

```
aws wafv2 get-ip-set \
    --name testip \
    --scope REGIONAL \
    --id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "IPSet":{
        "Description":"",
```

```
        "Name":"testip",
        "IPAddressVersion":"IPV4",
        "Id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE1111",
        "ARN":"arn:aws:wafv2:us-west-2:123456789012:regional/ipset/testip/
a1b2c3d4-5678-90ab-cdef-EXAMPLE1111",
        "Addresses":[
            "192.0.2.0/16"
        ]
    },
    "LockToken":"447e55ac-2396-4c6d-b9f9-86b67c17f8b5"
}
```

Para obtener más información, consulte Creación y administración de los conjuntos de direcciones IP y los conjuntos de patrones de expresiones regulares en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte GetIpSet en la Referencia de comandos de la AWS CLI.

`get-logging-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-logging-configuration`.

AWS CLI

Para recuperar las configuraciones de registro para una ACL web

En el siguiente ejemplo de `get-logging-configuration`, se recupera la configuración de registro de la ACL web especificada.

```
aws wafv2 get-logging-configuration \
    --resource-arn arn:aws:wafv2:us-west-2:123456789012:regional/webacl/test/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
    --region us-west-2
```

Salida:

```
{
    "LoggingConfiguration":{
        "ResourceArn":"arn:aws:wafv2:us-west-2:123456789012:regional/webacl/test/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "RedactedFields":[
```

```
            {
                "Method":{

                }
            }
        ],
        "LogDestinationConfigs":[
            "arn:aws:firehose:us-west-2:123456789012:deliverystream/aws-waf-logs-
custom-transformation"
        ]
    }
}
```

Para obtener más información, consulte Registro AWS WAF del tráfico en la ACL web en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte GetLoggingConfiguration en la Referencia de comandos de la AWS CLI.

`get-rate-based-statement-managed-keys`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-rate-based-statement-managed-keys`.

AWS CLI

Para recuperar una lista de direcciones IP que están bloqueadas por una regla basada en tasas

En el siguiente ejemplo de `get-rate-based-statement-managed-keys`, se recuperan las direcciones IP actualmente bloqueadas por una regla basada en tasas que se utiliza para una aplicación regional.

```
aws wafv2 get-rate-based-statement-managed-keys \
    --scope REGIONAL \
    --web-acl-name testwebacl2 \
    --web-acl-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --rule-name ratebasedtest
```

Salida:

```
{
    "ManagedKeysIPV4":{
```

```
        "IPAddressVersion":"IPV4",
        "Addresses":[
            "198.51.100.0/32"
        ]
    },
    "ManagedKeysIPV6":{
        "IPAddressVersion":"IPV6",
        "Addresses":[

        ]
    }
}
```

Para obtener más información, consulte Uso de instrucciones de regla basada en tasas en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte GetRateBasedStatementManagedKeys en la Referencia de comandos de la AWS CLI.

`get-regex-pattern-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-regex-pattern-set`.

AWS CLI

Para recuperar un conjunto de patrones de expresiones regulares específico

En el siguiente ejemplo de `get-regex-pattern-set`, se recupera el conjunto de patrones de expresiones regulares con el nombre, el alcance, la región y el ID especificados. Puede obtener el ID de un conjunto de patrones de expresiones regulares mediante los comandos `create-regex-pattern-set` y `list-regex-pattern-sets`.

```
aws wafv2 get-regex-pattern-set \
    --name regexPatterSet01 \
    --scope REGIONAL \
    --id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --region us-west-2
```

Salida:

```
{
```

```
    "RegexPatternSet":{
        "Description":"Test web-acl",
        "RegularExpressionList":[
            {
                "RegexString":"/[0-9]*/"
            },
            {
                "RegexString":"/[a-z]*/"
            }
        ],
        "Name":"regexPatterSet01",
        "ARN":"arn:aws:wafv2:us-west-2:123456789012:regional/regexpatternset/
regexPatterSet01/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "Id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    },
    "LockToken":"c8abf33f-b6fc-46ae-846e-42f994d57b29"
}
```

Para obtener más información, consulte Creación y administración de los conjuntos de direcciones IP y los conjuntos de patrones de expresiones regulares en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte GetRegexPatternSet en la Referencia de comandos de la AWS CLI.

`get-rule-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-rule-group`.

AWS CLI

Para recuperar un grupo de reglas personalizado específico

En el siguiente ejemplo de `get-rule-group`, se recupera el grupo de reglas personalizado con el nombre, el alcance y el ID especificados. Puede obtener el ID de un grupo de reglas mediante los comandos `create-rule-group` y `list-rule-groups`.

```
aws wafv2 get-rule-group \
    --name ff \
    --scope REGIONAL \
    --id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:


```
{
    "RuleGroup":{
        "Capacity":1,
        "Description":"",
        "Rules":[
            {
                "Priority":0,
                "Action":{
                    "Block":{

                    }
                },
                "VisibilityConfig":{
                    "SampledRequestsEnabled":true,
                    "CloudWatchMetricsEnabled":true,
                    "MetricName":"jj"
                },
                "Name":"jj",
                "Statement":{
                    "SizeConstraintStatement":{
                        "ComparisonOperator":"LE",
                        "TextTransformations":[
                            {
                                "Priority":0,
                                "Type":"NONE"
                            }
                        ],
                        "FieldToMatch":{
                            "UriPath":{

                            }
                        },
                        "Size":7
                    }
                }
            }
        ],
        "VisibilityConfig":{
            "SampledRequestsEnabled":true,
            "CloudWatchMetricsEnabled":true,
            "MetricName":"ff"
        },
```

```
        "Id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "ARN":"arn:aws:wafv2:us-west-2:123456789012:regional/rulegroup/ff/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "Name":"ff"
    },
    "LockToken":"485458c9-1830-4234-af31-ec4d52ced1b3"
}
```

Para obtener más información, consulte Administrar sus propios grupos de reglas en la Guía para desarrolladores AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte GetRuleGroup en la Referencia de comandos de la AWS CLI.

`get-sampled-requests`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-sampled-requests`.

AWS CLI

Para recuperar una muestra de solicitudes web para una ACL web

En el siguiente ejemplo de `get-sampled-requests`, se recuperan las solicitudes web de muestra para la ACL web, la métrica de reglas y el período de tiempo especificados.

```
aws wafv2 get-sampled-requests \
    --web-acl-arn arn:aws:wafv2:us-west-2:123456789012:regional/webacl/test-cli/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --rule-metric-name AWS-AWSManagedRulesSQLiRuleSet \
    --scope=REGIONAL \
    --time-window StartTime=2020-02-12T20:00Z,EndTime=2020-02-12T21:10Z \
    --max-items 100
```

Salida:

```
{
    "TimeWindow": {
    "EndTime": 1581541800.0,
    "StartTime": 1581537600.0
    },
    "SampledRequests": [
        {
            "Action": "BLOCK",
```

```
            "Timestamp": 1581541799.564,
            "RuleNameWithinRuleGroup": "AWS#AWSManagedRulesSQLiRuleSet#SQLi_BODY",
            "Request": {
                "Country": "US",
                "URI": "/",
                "Headers": [
                    {
                        "Name": "Host",
                        "Value": "alb-test-1EXAMPLE1.us-east-1.elb.amazonaws.com"
                    },
                    {
                        "Name": "Content-Length",
                        "Value": "7456"
                    },
                    {
                        "Name": "User-Agent",
                        "Value": "curl/7.53.1"
                    },
                    {
                        "Name": "Accept",
                        "Value": "/"
                    },
                    {
                        "Name": "Content-Type",
                        "Value": "application/x-www-form-urlencoded"
                    }
                ],
                "ClientIP": "198.51.100.08",
                "Method": "POST",
                "HTTPVersion": "HTTP/1.1"
            },
            "Weight": 1
        },
        {
            "Action": "BLOCK",
            "Timestamp": 1581541799.988,
            "RuleNameWithinRuleGroup": "AWS#AWSManagedRulesSQLiRuleSet#SQLi_BODY",
            "Request": {
                "Country": "US",
                "URI": "/",
                "Headers": [
                    {
                        "Name": "Host",
                        "Value": "alb-test-1EXAMPLE1.us-east-1.elb.amazonaws.com"
```

```
                    },
                    {
                        "Name": "Content-Length",
                        "Value": "7456"
                    },
                    {
                        "Name": "User-Agent",
                        "Value": "curl/7.53.1"
                    },
                    {
                        "Name": "Accept",
                        "Value": "/"
                    },
                    {
                        "Name": "Content-Type",
                        "Value": "application/x-www-form-urlencoded"
                    }
                ],
                "ClientIP": "198.51.100.08",
                "Method": "POST",
                "HTTPVersion": "HTTP/1.1"
            },
            "Weight": 3
        },
        {
            "Action": "BLOCK",
            "Timestamp": 1581541799.846,
            "RuleNameWithinRuleGroup": "AWS#AWSManagedRulesSQLiRuleSet#SQLi_BODY",
            "Request": {
                "Country": "US",
                "URI": "/",
                "Headers": [
                    {
                        "Name": "Host",
                        "Value": "alb-test-1EXAMPLE1.us-east-1.elb.amazonaws.com"
                    },
                    {
                        "Name": "Content-Length",
                        "Value": "7456"
                    },
                    {
                        "Name": "User-Agent",
                        "Value": "curl/7.53.1"
                    },
```

```
                    {
                        "Name": "Accept",
                        "Value": "/"
                    },
                    {
                        "Name": "Content-Type",
                        "Value": "application/x-www-form-urlencoded"
                    }
                ],
                "ClientIP": "198.51.100.08",
                "Method": "POST",
                "HTTPVersion": "HTTP/1.1"
            },
            "Weight": 1
        },
        {
            "Action": "BLOCK",
            "Timestamp": 1581541799.4,
            "RuleNameWithinRuleGroup": "AWS#AWSManagedRulesSQLiRuleSet#SQLi_BODY",
            "Request": {
                "Country": "US",
                "URI": "/",
                "Headers": [
                    {
                        "Name": "Host",
                        "Value": "alb-test-1EXAMPLE1.us-east-1.elb.amazonaws.com"
                    },
                    {
                        "Name": "Content-Length",
                        "Value": "7456"
                    },
                    {
                        "Name": "User-Agent",
                        "Value": "curl/7.53.1"
                    },
                    {
                        "Name": "Accept",
                        "Value": "/"
                    },
                    {
                        "Name": "Content-Type",
                        "Value": "application/x-www-form-urlencoded"
                    }
                ],
```

```
                "ClientIP": "198.51.100.08",
                "Method": "POST",
                "HTTPVersion": "HTTP/1.1"
            },
            "Weight": 1
        }
    ],
    "PopulationSize": 4
}
```

Para obtener más información, consulte Pruebas y ajustes de sus protecciones de AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte GetSampledRequests en la Referencia de comandos de la AWS CLI.

`get-web-acl-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-web-acl-for-resource`.

AWS CLI

Para recuperar la ACL web asociada a un recurso de AWS

En el siguiente ejemplo de `get-web-acl-for-resource`, se recupera el JSON de la ACL web que está asociada al recurso especificado.

```
aws wafv2 get-web-acl-for-resource \
    --resource-arn arn:aws:elasticloadbalancing:us-west-2:123456789012:loadbalancer/
app/waf-cli-alb/1ea17125f8b25a2a
```

Salida:

```
{
    "WebACL":{
        "Capacity":3,
        "Description":"",
        "Rules":[
            {
                "Priority":1,
                "Action":{
                    "Block":{
```

```
                    }
                },
                "VisibilityConfig":{
                    "SampledRequestsEnabled":true,
                    "CloudWatchMetricsEnabled":true,
                    "MetricName":"testrule01"
                },
                "Name":"testrule01",
                "Statement":{
                    "AndStatement":{
                        "Statements":[
                            {
                                "ByteMatchStatement":{
                                    "PositionalConstraint":"EXACTLY",
                                    "TextTransformations":[
                                        {
                                            "Priority":0,
                                            "Type":"NONE"
                                        }
                                    ],
                                    "SearchString":"dGVzdHN0cmluZw==",
                                    "FieldToMatch":{
                                        "UriPath":{

                                        }
                                    }
                                }
                            },
                            {
                                "SizeConstraintStatement":{
                                    "ComparisonOperator":"EQ",
                                    "TextTransformations":[
                                        {
                                            "Priority":0,
                                            "Type":"NONE"
                                        }
                                    ],
                                    "FieldToMatch":{
                                        "QueryString":{

                                       }
                                    },
                                    "Size":0
                                }
```

```
                            }
                        ]
                    }
                }
            }
        ],
        "VisibilityConfig":{
            "SampledRequestsEnabled":true,
            "CloudWatchMetricsEnabled":true,
            "MetricName":"test01"
        },
        "DefaultAction":{
            "Allow":{

            }
        },
        "Id":"9a1b2c3d4-5678-90ab-cdef-EXAMPLE11111  ",
        "ARN":"arn:aws:wafv2:us-west-2:123456789012:regional/webacl/test01/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111  ",
        "Name":"test01"
    }
}
```

Para obtener más información, consulte Asociar o disociar una ACL web con un recurso de AWS en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte GetWebAclForResource en la Referencia de comandos de la AWS CLI.

`get-web-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-web-acl`.

AWS CLI

Para recuperar una ACL web

En el siguiente ejemplo de `get-web-acl`, se recupera la ACL web con el nombre, el alcance y el ID especificados. Puede obtener el ID de una ACL web mediante los comandos `create-web-acl` y `list-web-acls`.

```
aws wafv2 get-web-acl \
```

```
    --name test01 \
    --scope REGIONAL \
    --id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "WebACL":{
        "Capacity":3,
        "Description":"",
        "Rules":[
            {
                "Priority":1,
                "Action":{
                    "Block":{

                    }
                },
                "VisibilityConfig":{
                   "SampledRequestsEnabled":true,
                    "CloudWatchMetricsEnabled":true,
                    "MetricName":"testrule01"
                },
                "Name":"testrule01",
                "Statement":{
                    "AndStatement":{
                        "Statements":[
                            {
                                "ByteMatchStatement":{
                                    "PositionalConstraint":"EXACTLY",
                                    "TextTransformations":[
                                        {
                                            "Priority":0,
                                            "Type":"NONE"
                                        }
                                    ],
                                    "SearchString":"dGVzdHN0cmluZw==",
                                    "FieldToMatch":{
                                        "UriPath":{

                                        }
                                    }
                                }
```

```
                            },
                            {
                                "SizeConstraintStatement":{
                                    "ComparisonOperator":"EQ",
                                    "TextTransformations":[
                                        {
                                            "Priority":0,
                                            "Type":"NONE"
                                        }
                                    ],
                                    "FieldToMatch":{
                                        "QueryString":{

                                        }
                                    },
                                    "Size":0
                                }
                            }
                        ]
                    }
                }
            }
        ],
        "VisibilityConfig":{
            "SampledRequestsEnabled":true,
            "CloudWatchMetricsEnabled":true,
            "MetricName":"test01"
        },
        "DefaultAction":{
            "Allow":{

            }
        },
        "Id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "ARN":"arn:aws:wafv2:us-west-2:123456789012:regional/webacl/test01/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "Name":"test01"
    },
    "LockToken":"e3db7e2c-d58b-4ee6-8346-6aec5511c6fb"
}
```

Para obtener más información, consulte El uso de las ACL web en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte GetWebAcl en la Referencia de comandos de AWS CLI.

`list-available-managed-rule-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-available-managed-rule-groups`.

AWS CLI

Para recuperar los grupos de reglas administrados

En el siguiente ejemplo de `list-available-managed-rule-groups`, se muestra la lista de todos los grupos de reglas administrados que actualmente están disponibles para su uso en las ACL web.

```
aws wafv2 list-available-managed-rule-groups \
    --scope REGIONAL
```

Salida:

```
{
   "ManagedRuleGroups": [
       {
           "VendorName": "AWS",
           "Name": "AWSManagedRulesCommonRuleSet",
           "Description": "Contains rules that are generally applicable to web
applications. This provides protection against exploitation of a wide range of
vulnerabilities, including those described in OWASP publications and common Common
Vulnerabilities and Exposures (CVE)."
       },
       {
           "VendorName": "AWS",
           "Name": "AWSManagedRulesAdminProtectionRuleSet",
           "Description": "Contains rules that allow you to block external access
to exposed admin pages. This may be useful if you are running third-party software
or would like to reduce the risk of a malicious actor gaining administrative access
to your application."
       },
       {
           "VendorName": "AWS",
           "Name": "AWSManagedRulesKnownBadInputsRuleSet",
```

```
            "Description": "Contains rules that allow you to block request patterns
that are known to be invalid and are associated with exploitation or discovery of
vulnerabilities. This can help reduce the risk of a malicious actor discovering a
vulnerable application."
        },
        {
            "VendorName": "AWS",
            "Name": "AWSManagedRulesSQLiRuleSet",
            "Description": "Contains rules that allow you to block request patterns
associated with exploitation of SQL databases, like SQL injection attacks. This can
help prevent remote injection of unauthorized queries."
        },
        {
            "VendorName": "AWS",
            "Name": "AWSManagedRulesLinuxRuleSet",
            "Description": "Contains rules that block request patterns associated
with exploitation of vulnerabilities specific to Linux, including LFI attacks. This
can help prevent attacks that expose file contents or execute code for which the
attacker should not have had access."
        },
        {
            "VendorName": "AWS",
            "Name": "AWSManagedRulesUnixRuleSet",
            "Description": "Contains rules that block request patterns associated
with exploiting vulnerabilities specific to POSIX/POSIX-like OS, including LFI
attacks. This can help prevent attacks that expose file contents or execute code
for which access should not been allowed."
        },
        {
            "VendorName": "AWS",
            "Name": "AWSManagedRulesWindowsRuleSet",
            "Description": "Contains rules that block request patterns associated
with exploiting vulnerabilities specific to Windows, (e.g., PowerShell commands).
This can help prevent exploits that allow attacker to run unauthorized commands or
execute malicious code."
        },
        {
            "VendorName": "AWS",
            "Name": "AWSManagedRulesPHPRuleSet",
            "Description": "Contains rules that block request patterns associated
with exploiting vulnerabilities specific to the use of the PHP, including injection
of unsafe PHP functions. This can help prevent exploits that allow an attacker to
remotely execute code or commands."
        },
```

```
        {
            "VendorName": "AWS",
            "Name": "AWSManagedRulesWordPressRuleSet",
            "Description": "The WordPress Applications group contains rules that
 block request patterns associated with the exploitation of vulnerabilities specific
 to WordPress sites."
        },
        {
            "VendorName": "AWS",
            "Name": "AWSManagedRulesAmazonIpReputationList",
            "Description": "This group contains rules that are based on Amazon
 threat intelligence. This is useful if you would like to block sources associated
 with bots or other threats."
        }
    ]
}
```

Para obtener más información, consulte Uso de grupos de reglas administrados en AWS WAF en la Guía para desarrolladores AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte ListAvailableManagedRuleGroups en la Referencia de comandos de la AWS CLI.

`list-ip-sets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-ip-sets`.

AWS CLI

Para recuperar una lista de conjuntos de IP

En el siguiente ejemplo de `list-ip-sets`, se recuperan todos los conjuntos de direcciones IP de la cuenta que tienen alcance regional.

```
aws wafv2 list-ip-sets \
    --scope REGIONAL
```

Salida:

```
{
    "IPSets":[
```

```
        {
            "ARN":"arn:aws:wafv2:us-west-2:123456789012:regional/ipset/testip/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "Description":"",
            "Name":"testip",
            "LockToken":"0674c84b-0304-47fe-8728-c6bff46af8fc",
            "Id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111  "
        }
    ],
    "NextMarker":"testip"
}
```

Para obtener más información, consulte Creación y administración de los conjuntos de direcciones IP y los conjuntos de patrones de expresiones regulares en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte ListIpSets en la Referencia de comandos de la AWS CLI.

`list-logging-configurations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-logging-configurations`.

AWS CLI

Para recuperar una lista de todas las configuraciones de registro de una región

En el siguiente ejemplo de `list-logging-configurations`, se recuperan todas las configuraciones de registro de las ACL web de alcance regional en la región de `us-west-2`.

```
aws wafv2 list-logging-configurations \
    --scope REGIONAL \
    --region us-west-2
```

Salida:

```
{
    "LoggingConfigurations":[
        {
            "ResourceArn":"arn:aws:wafv2:us-west-2:123456789012:regional/webacl/
test-2/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
            "RedactedFields":[
                {
                    "QueryString":{

                    }
                }
            ],
            "LogDestinationConfigs":[
                "arn:aws:firehose:us-west-2:123456789012:deliverystream/aws-waf-
logs-test"
            ]
        },
        {
            "ResourceArn":"arn:aws:wafv2:us-west-2:123456789012:regional/webacl/
test/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "RedactedFields":[
                {
                    "Method":{

                    }
                }
            ],
            "LogDestinationConfigs":[
                "arn:aws:firehose:us-west-2:123456789012:deliverystream/aws-waf-
logs-custom-transformation"
            ]
        }
    ]
}
```

Para obtener más información, consulte Registro AWS WAF del tráfico en la ACL web en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener más información sobre la API, consulte ListLoggingConfigurations en la Referencia de comandos de la AWS CLI.

`list-regex-pattern-sets`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-regex-pattern-sets`.

AWS CLI

Para recuperar una lista de los conjuntos de patrones de expresiones regulares

En el siguiente ejemplo de `list-regex-pattern-sets`, se recuperan todos los conjuntos de patrones de expresiones regulares de la cuenta que están definidos en la región `us-west-2`.

```
aws wafv2 list-regex-pattern-sets \
--scope REGIONAL \
--region us-west-2
```

Salida:

```
{
    "NextMarker":"regexPatterSet01",
    "RegexPatternSets":[
        {
            "ARN":"arn:aws:wafv2:us-west-2:123456789012:regional/regexpatternset/
regexPatterSet01/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "Description":"Test web-acl",
            "Name":"regexPatterSet01",
            "LockToken":"f17743f7-0000-0000-0000-19a8b93bfb01",
            "Id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
        }
    ]
}
```

Para obtener más información, consulte Creación y administración de los conjuntos de direcciones IP y los conjuntos de patrones de expresiones regulares en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte ListRegexPatternSets en la Referencia de comandos de la AWS CLI.

`list-resources-for-web-acl`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resources-for-web-acl`.

AWS CLI

Para recuperar los recursos asociados a una ACL web

En el siguiente ejemplo de `list-resources-for-web-acl`, se recuperan los recursos de la API de REST de API Gateway que están actualmente asociados a la ACL web especificada en la región `us-west-2`.

```
aws wafv2 list-resources-for-web-acl \
    --web-acl-arn arn:aws:wafv2:us-west-2:123456789012:regional/webacl/TestWebAcl/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --resource-type API_GATEWAY \
    --region us-west-2
```

Salida:

```
{
    "ResourceArns": [
        "arn:aws:apigateway:us-west-2::/restapis/EXAMPLE111/stages/testing"
    ]
}
```

Para obtener más información, consulte Asociar o disociar una ACL web con un recurso de AWS en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte ListResourcesForWebAcl en la Referencia de comandos de la AWS CLI.

`list-rule-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-rule-groups`.

AWS CLI

Para recuperar una lista de grupos de reglas administrados

En el siguiente ejemplo de `list-rule-groups`, se recuperan todos los grupos de reglas personalizados que están definidos para la cuenta para el alcance y la ubicación de la región especificados.

```
aws wafv2 list-rule-groups \
    --scope REGIONAL \
    --region us-west-2
```

Salida:

```
{
    "RuleGroups":[
```

```
        {
            "ARN":"arn:aws:wafv2:us-west-2:123456789012:regional/rulegroup/
TestRuleGroup/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "Description":"",
            "Name":"TestRuleGroup",
            "LockToken":"1eb5ec48-0000-0000-0000-ee9b906c541e",
            "Id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
        },
        {
            "ARN":"arn:aws:wafv2:us-west-2:123456789012:regional/rulegroup/test/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "Description":"",
            "Name":"test",
            "LockToken":"b0f4583e-998b-4880-9069-3fbe45738b43",
            "Id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
        }
    ],
    "NextMarker":"test"
}
```

Para obtener más información, consulte Administrar sus propios grupos de reglas en la Guía para desarrolladores AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener detalles de la API, consulte ListRuleGroups en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para recuperar todas las etiquetas de un recurso de AWS WAF

En el siguiente ejemplo de `list-tags-for-resource`, se recupera la lista de todos los pares de etiquetas, clave y valor de la ACL web especificada.

```
aws wafv2 list-tags-for-resource \
    --resource-arn arn:aws:wafv2:us-west-2:123456789012:regional/webacl/testwebacl2/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
    "NextMarker":"",
    "TagInfoForResource":{
        "ResourceARN":"arn:aws:wafv2:us-west-2:123456789012:regional/webacl/
testwebacl2/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "TagList":[

        ]
    }
}
```

Para obtener más información, consulte Configuración de AWS WAF y sus componentes en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-web-acls`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-web-acls`.

AWS CLI

Para recuperar las ACL web para un alcance

En el siguiente ejemplo de `list-web-acls`, se recuperan todas las ACL web que están definidas para la cuenta para el alcance especificado.

```
aws wafv2 list-web-acls \
    --scope REGIONAL
```

Salida:

```
{
    "NextMarker":"Testt",
    "WebACLs":[
        {
            "ARN":"arn:aws:wafv2:us-west-2:123456789012:regional/webacl/Testt/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "Description":"sssss",
            "Name":"Testt",
```

```
            "LockToken":"7f36cb30-74ef-4cff-8cd4-a77e1aba1746",
            "Id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
        }
    ]
}
```

Para obtener más información, consulte El uso de las ACL web en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte ListWebAcls en la Referencia de comandos de la AWS CLI.

`put-logging-configuration`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-logging-configuration`.

AWS CLI

Para agregar una configuración de registro a una ACL web

En el siguiente ejemplo de `put-logging-configuration`, se añade la configuración de registro de Amazon Kinesis Data Firehose `aws-waf-logs-custom-transformation` a la ACL web especificada, sin campo redactados a partir de los registros.

```
aws wafv2 put-logging-configuration \
    --logging-configuration ResourceArn=arn:aws:wafv2:us-
west-2:123456789012:regional/webacl/test-cli/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111,LogDestinationConfigs=arn:aws:firehose:us-
west-2:123456789012:deliverystream/aws-waf-logs-custom-transformation \
            --region us-west-2
```

Salida:

```
{
    "LoggingConfiguration":{
        "ResourceArn":"arn:aws:wafv2:us-west-2:123456789012:regional/webacl/test-
cli/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "LogDestinationConfigs":[
            "arn:aws:firehose:us-west-2:123456789012:deliverystream/aws-waf-logs-
custom-transformation"
        ]
    }
```

```
}
```

Para obtener más información, consulte Registro AWS WAF del tráfico en la ACL web en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte PutLoggingConfiguration en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para agregar etiquetas a un recurso de AWS WAF

En el siguiente ejemplo de `tag-resource`, se agrega una etiqueta con una clave `Name` y un valor definido en `AWSWAF` a la ACL web especificada.

```
aws wafv2 tag-resource \
    --resource-arn arn:aws:wafv2:us-west-2:123456789012:regional/webacl/
apiGatewayWebAcl/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --tags Key=Name,Value=AWSWAF
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de AWS WAF y sus componentes en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para eliminar etiquetas de un recurso de AWS WAF

En el siguiente ejemplo de `untag-resource`, se elimina la etiqueta con la clave `KeyName` de la ACL web especificada.

```
aws wafv2 untag-resource \
    --resource-arn arn:aws:wafv2:us-west-2:123456789012:regional/webacl/
apiGatewayWebAcl/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --tag-keys "KeyName"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuración de AWS WAF y sus componentes en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

update-ip-set

En el siguiente ejemplo de código, se muestra cómo utilizar `update-ip-set`.

AWS CLI

Para modificar la configuración de un conjunto de IP existente

En el siguiente ejemplo de `update-ip-set`, se actualiza la configuración del conjunto de direcciones IP especificado. Esta llamada requiere un ID, que puede obtener de la llamada a `list-ip-sets` y de un token de bloqueo, que puede obtener de las llamadas a `list-ip-sets` y `get-ip-set`. Esta llamada también devuelve un token de bloqueo que puede usar para una actualización posterior.

```
aws wafv2 update-ip-set \
    --name testip \
    --scope REGIONAL \
    --id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --addresses 198.51.100.0/16 \
    --lock-token 447e55ac-2396-4c6d-b9f9-86b67c17f8b5
```

Salida:

```
{
    "NextLockToken": "0674c84b-0304-47fe-8728-c6bff46af8fc"
}
```

Para obtener más información, consulte Creación y administración de los conjuntos de direcciones IP y los conjuntos de patrones de expresiones regulares en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte UpdateIpSet en la Referencia de comandos de la AWS CLI.

`update-regex-pattern-set`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-regex-pattern-set`.

AWS CLI

Para modificar la configuración de un conjunto de patrones de expresiones regulares existente

En el siguiente ejemplo de `update-regex-pattern-set`, se actualiza la configuración del conjunto de patrones de expresiones regulares especificado. Esta llamada requiere un ID, que puede obtener de la llamada a `list-regex-pattern-sets` y de un token de bloqueo, que puede obtener de las llamadas a `list-regex-pattern-sets` y `get-regex-pattern-set`. Esta llamada también devuelve un token de bloqueo que puede usar para una actualización posterior.

```
aws wafv2 update-regex-pattern-set \
    --name ExampleRegex \
    --scope REGIONAL \
    --id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --regular-expression-list RegexString="^.+$"  \
    --lock-token ed207e9c-82e9-4a77-aadd-81e6173ab7eb
```

Salida:

```
{
    "NextLockToken": "12ebc73e-fa68-417d-a9b8-2bdd761a4fa5"
}
```

Para obtener más información, consulte Creación y administración de los conjuntos de direcciones IP y los conjuntos de patrones de expresiones regulares en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte UpdateRegexPatternSet en la Referencia de comandos de la AWS CLI.

update-rule-group

En el siguiente ejemplo de código, se muestra cómo utilizar `update-rule-group`.

AWS CLI

Para actualizar un grupo de reglas personalizado

En el siguiente ejemplo de `update-rule-group`, se cambia la configuración de visibilidad de un grupo de reglas personalizado existente. Esta llamada requiere un ID, que puede obtener de la llamada a `list-rule-groups` y de un token de bloqueo, que puede obtener de las llamadas a `list-rule-groups` y `get-rule-group`. Esta llamada también devuelve un token de bloqueo que puede usar para una actualización posterior.

```
aws wafv2 update-rule-group \
    --name TestRuleGroup \
    --scope REGIONAL \
    --id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --lock-token 7b3bcec2-0000-0000-0000-563bf47249f0 \
    --visibility-
config SampledRequestsEnabled=false,CloudWatchMetricsEnabled=false,MetricName=TestMetricsFor
 \
    --region us-west-2
```

Salida:

```
{
    "NextLockToken": "1eb5ec48-0000-0000-0000-ee9b906c541e"
}
```

Para obtener más información, consulte Administrar sus propios grupos de reglas en la Guía para desarrolladores AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte UpdateRuleGroup en la Referencia de la API de la AWS CLI.

update-web-acl

En el siguiente ejemplo de código, se muestra cómo utilizar `update-web-acl`.

AWS CLI

Para actualizar una ACL web

En el siguiente ejemplo de `update-web-acl`, se modifica la configuración de una ACL web existente. Esta llamada requiere un ID, que puede obtener de la llamada a `list-web-acls` y de un token de bloqueo y otros ajustes, que puede obtener de la llamada a `get-web-acl`. Esta llamada también devuelve un token de bloqueo que puede usar para una actualización posterior.

```
aws wafv2 update-web-acl \
    --name TestWebAcl \
    --scope REGIONAL \
    --id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --lock-token 2294b3a1-0000-0000-0000-a3ae04329de9 \
    --default-action Block={} \
    --visibility-
config SampledRequestsEnabled=false,CloudWatchMetricsEnabled=false,MetricName=NewMetricTestW
 \
    --rules file://waf-rule.json \
    --region us-west-2
```

Salida:

```
{
    "NextLockToken": "714a0cfb-0000-0000-0000-2959c8b9a684"
}
```

Para obtener más información, consulte El uso de las ACL web en AWS WAF en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Avanzado.

- Para obtener información sobre la API, consulte UpdateWebAcl en la Referencia de comandos de la AWS CLI.

Ejemplos de WorkDocs que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon WorkDocs.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`abort-document-version-upload`

En el siguiente ejemplo de código, se muestra cómo utilizar `abort-document-version-upload`.

AWS CLI

Para detener la carga de una versión de documento

En este ejemplo se detiene la carga de una versión de documento iniciada anteriormente.

Comando:

```
aws workdocs abort-document-version-upload --document-
id feaba64d4efdf271c2521b60a2a44a8f057e84beaabbe22f012673132098 35f2 --version-
id 1536773972914-ddb67663e782e7ce8455ebc962217cf9f9e47b5a9a702e5c84dcccd417da9313
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte AbortDocumentVersionUpload en la Referencia de comandos de la AWS CLI.

`activate-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `activate-user`.

AWS CLI

Para activar un usuario

En este ejemplo, se activa un usuario inactivo.

Comando:

```
aws workdocs activate-user --user-
id "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c"
```

Salida:

```
{
  "User": {
      "Id": "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
      "Username": "exampleUser",
      "EmailAddress": "exampleUser@site.awsapps.com",
      "GivenName": "Example",
      "Surname": "User",
      "OrganizationId": "d-926726012c",
      "RootFolderId":
 "75f67c183aa1217409ac87576a45c03a5df5e6d8c51c35c01669970538e86cd0",
      "RecycleBinFolderId":
 "642b7dd3e60b14204534f3df7b1959e01b5d170f8c2707f410e40a8149120a57",
      "Status": "ACTIVE",
      "Type": "MINIMALUSER",
      "CreatedTimestamp": 1521226107.747,
      "ModifiedTimestamp": 1525297406.462,
      "Storage": {
          "StorageUtilizedInBytes": 0,
          "StorageRule": {
              "StorageAllocatedInBytes": 0,
              "StorageType": "QUOTA"
          }
      }
  }
}
```

- Para obtener información sobre la API, consulte ActivateUser en la Referencia de comandos de la AWS CLI.

`add-resource-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `add-resource-permissions`.

AWS CLI

Para añadir permisos a un recurso

En este ejemplo, se agregan permisos al recurso para las entidades principales especificadas.

Comando:

```
aws workdocs add-resource-permissions --resource-
id d90d93c1fe44bad0c8471e973ebaab339090401a95e777cffa58e977d2983b65 --
principals Id=anonymous,Type=ANONYMOUS,Role=VIEWER
```

Salida:

```
{
  "ShareResults": [
      {
          "PrincipalId": "anonymous",
          "Role": "VIEWER",
          "Status": "SUCCESS",
          "ShareId":
 "d90d93c1fe44bad0c8471e973ebaab339090401a95e777cffa58e977d2983b65",
          "StatusMessage": ""
      }
  ]
}
```

- Para obtener detalles de la API, consulte AddResourcePermissions en la Referencia de comandos de la AWS CLI.

`create-comment`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-comment`.

AWS CLI

Para agregar un comentario nuevo

En este ejemplo, se agrega un nuevo comentario a la versión del documento especificada.

Comando:

```
aws workdocs create-comment --document-
id 15df51e0335cfcc6a2e4de9dd8be9f22ee40545ad9176f54758dcf903be982d3 --version-
id 1521672507741-9f7df0ea5dd0b121c4f3564a0c7c0b4da95cd12c635d3c442af337a88e297920 --
text "This is a comment."
```

Salida:

```
{
  "Comment": {
      "CommentId": "1534799058197-
c7f5c84de9115875bbca93e0367bbebac609541d461636b760849b88b1609dd5",
      "ThreadId": "1534799058197-
c7f5c84de9115875bbca93e0367bbebac609541d461636b760849b88b1609dd5",
      "Text": "This is a comment.",
      "Contributor": {
          "Id": "arn:aws:iam::123456789123:user/exampleUser",
          "Username": "exampleUser",
          "GivenName": "Example",
          "Surname": "User",
          "Status": "ACTIVE"
      },
      "CreatedTimestamp": 1534799058.197,
      "Status": "PUBLISHED",
      "Visibility": "PUBLIC"
  }
}
```

- Para obtener información sobre la API, consulte CreateComment en la Referencia de comandos de la AWS CLI.

`create-custom-metadata`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-custom-metadata`.

AWS CLI

Para crear metadatos personalizados

En este ejemplo, se crean metadatos personalizados para el documento especificado.

Comando:

```
aws workdocs create-custom-metadata --resource-
id d90d93c1fe44bad0c8471e973ebaab339090401a95e777cffa58e977d2983b65 --custom-
metadata KeyName1=example,KeyName2=example2
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte CreateCustomMetadata en la Referencia de comandos de la AWS CLI.

`create-folder`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-folder`.

AWS CLI

Para crear una carpeta

En este ejemplo, se crea una carpeta.

Comando:

```
aws workdocs create-folder --name documents --parent-folder-
id 1ece93e5fe75315c7407c4967918b4fd9da87ddb2a588e67b7fdaf4a98fde678
```

Salida:

```
{
  "Metadata": {
      "Id": "50893c0af679524d1a0e0651130ed6d073e1a05f95bd12c42dcde5d35634ed08",
      "Name": "documents",
      "CreatorId": "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
      "ParentFolderId":
 "1ece93e5fe75315c7407c4967918b4fd9da87ddb2a588e67b7fdaf4a98fde678",
      "CreatedTimestamp": 1534450467.622,
      "ModifiedTimestamp": 1534450467.622,
      "ResourceState": "ACTIVE",
      "Signature": "",
      "Size": 0,
      "LatestVersionSize": 0
  }
}
```

- Para obtener información sobre la API, consulte CreateFolder en la Referencia de comandos de la AWS CLI.

`create-labels`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-labels`.

AWS CLI

Para crear etiquetas

En este ejemplo, se crea una serie de etiquetas para un documento.

Comando:

```
aws workdocs create-labels --resource-
id d90d93c1fe44bad0c8471e973ebaab339090401a95e777cffa58e977d2983b65 --
labels "documents" "examples" "my_documents"
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte CreateLabels en la Referencia de comandos de la AWS CLI.

`create-notification-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-notification-subscription`.

AWS CLI

Para crear una suscripción de notificaciones

En el siguiente ejemplo de `create-notification-subscription`, se configura una suscripción de notificaciones para la organización de Amazon WorkDocs especificada.

```
aws workdocs create-notification-subscription \
    --organization-id d-123456789c \
    --protocol HTTPS \
    --subscription-type ALL \
    --notification-endpoint "https://example.com/example"
```

Salida:

```
{
    "Subscription": {
        "SubscriptionId": "123ab4c5-678d-901e-f23g-45h6789j0123",
        "EndPoint": "https://example.com/example",
        "Protocol": "HTTPS"
    }
}
```

Para obtener más información, consulte Subscribe to Notifications en la Guía para desarrolladores de Amazon WorkDocs.

- Para obtener información sobre la API, consulte CreateNotificationSubscription en la Referencia de comandos de la AWS CLI.

`create-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-user`.

AWS CLI

Para crear un nuevo usuario

En este ejemplo, se crea un nuevo usuario en un directorio de Simple AD o de Microsoft AD.

Comando:

```
aws workdocs create-user --organization-id d-926726012c --username exampleUser2
 --email-address exampleUser2@site.awsapps.com --given-name example2Name --
surname example2Surname --password examplePa$$w0rd
```

Salida:

```
{
  "User": {
      "Id": "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
      "Username": "exampleUser2",
      "EmailAddress": "exampleUser2@site.awsapps.com",
      "GivenName": "example2Name",
      "Surname": "example2Surname",
      "OrganizationId": "d-926726012c",
```

```
      "RootFolderId":
 "35b886cb17198cbd547655e58b025dff0cf34aaed638be52009567e23dc67390",
      "RecycleBinFolderId":
 "9858c3e9ed4c2460dde9aadb4c69fde998070dd46e5e985bd08ec6169ea249ff",
      "Status": "ACTIVE",
      "Type": "MINIMALUSER",
      "CreatedTimestamp": 1535478836.584,
      "ModifiedTimestamp": 1535478836.584,
      "Storage": {
          "StorageUtilizedInBytes": 0,
          "StorageRule": {
              "StorageAllocatedInBytes": 0,
              "StorageType": "QUOTA"
          }
      }
  }
}
```

- Para obtener información sobre la API, consulte CreateUser en la Referencia de comandos de la AWS CLI.

`deactivate-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `deactivate-user`.

AWS CLI

Para desactivar un usuario

En este ejemplo, se desactiva un usuario activo.

Comando:

```
aws workdocs deactivate-user --user-
id "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c"
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte DeactivateUser en la Referencia de comandos de la AWS CLI.

`delete-comment`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-comment`.

AWS CLI

Para eliminar un comentario específico de la versión de un documento

En este ejemplo, se elimina el comentario especificado de la versión del documento indicada.

Comando:

```
aws workdocs delete-comment --document-
id 15df51e0335cfcc6a2e4de9dd8be9f22ee40545ad9176f54758dcf903be982d3 --version-
id 1521672507741-9f7df0ea5dd0b121c4f3564a0c7c0b4da95cd12c635d3c442af337a88e297920 --
comment-id 1534799058197-
c7f5c84de9115875bbca93e0367bbebac609541d461636b760849b88b1609dd5
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte DeleteComment en la Referencia de comandos de la AWS CLI.

`delete-custom-metadata`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-custom-metadata`.

AWS CLI

Para eliminar los metadatos personalizados de un recurso

En este ejemplo, se eliminan todos los metadatos personalizados del recurso especificado.

Comando:

```
aws workdocs delete-custom-metadata --resource-
id d90d93c1fe44bad0c8471e973ebaab339090401a95e777cffa58e977d2983b65 --delete-all
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte DeleteCustomMetadata en la Referencia de comandos de la AWS CLI.

`delete-document`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-document`.

AWS CLI

Eliminación de un documento

En este ejemplo, se elimina el documento especificado.

Comando:

```
aws workdocs delete-document --document-
id b83ed5e5b167b65ef69de9d597627ff1a0d4f07a45e67f1fab7d26b54427de0a
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte DeleteDocument en la Referencia de comandos de la AWS CLI.

`delete-folder-contents`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-folder-contents`.

AWS CLI

Para eliminar el contenido de una carpeta

En este ejemplo, se elimina el contenido de la carpeta especificada.

Comando:

```
aws workdocs delete-folder-contents --folder-
id 26fa8aa4ba2071447c194f7b150b07149dbdb9e1c8a301872dcd93a4735ce65d
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte DeleteFolderContents en la Referencia de comandos de la AWS CLI.

`delete-folder`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-folder`.

AWS CLI

Para eliminar una carpeta

En este ejemplo, se elimina la carpeta especificada.

Comando:

```
aws workdocs delete-folder --folder-
id 26fa8aa4ba2071447c194f7b150b07149dbdb9e1c8a301872dcd93a4735ce65d
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte DeleteFolder en la Referencia de comandos de la AWS CLI.

`delete-labels`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-labels`.

AWS CLI

Para eliminar etiquetas

En este ejemplo, se eliminan las etiquetas especificadas de un documento.

Comando:

```
aws workdocs delete-labels --resource-
id d90d93c1fe44bad0c8471e973ebaab339090401a95e777cffa58e977d2983b65 --
labels "documents" "examples"
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte DeleteLabels en la Referencia de comandos de la AWS CLI.

`delete-notification-subscription`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-notification-subscription`.

AWS CLI

Para eliminar una suscripción a notificaciones

En el siguiente ejemplo de `delete-notification-subscription`, se elimina la suscripción a las notificaciones especificada.

```
aws workdocs delete-notification-subscription \
    --subscription-id 123ab4c5-678d-901e-f23g-45h6789j0123 \
    --organization-id d-123456789c
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Subscribe to Notifications en la Guía para desarrolladores de Amazon WorkDocs.

- Para obtener información sobre la API, consulte DeleteNotificationSubscription en la Referencia de comandos de la AWS CLI.

`delete-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-user`.

AWS CLI

Para eliminar un usuario

En este ejemplo se elimina un usuario.

Comando:

```
aws workdocs delete-user --user-
id "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c"
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte DeleteUser en la Referencia de comandos de la AWS CLI.

`describe-activities`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-activities`.

AWS CLI

Para obtener una lista de las actividades de los usuarios

En este ejemplo, se devuelve una lista de las últimas actividades de los usuarios de la organización especificada, con un límite establecido a las dos últimas actividades.

Comando:

```
aws workdocs describe-activities --organization-id d-926726012c --limit 2
```

Salida:

```
{
  "UserActivities": [
      {
          "Type": "DOCUMENT_VERSION_DOWNLOADED",
          "TimeStamp": 1534800122.17,
          "Initiator": {
```

```
                "Id": "arn:aws:iam::123456789123:user/exampleUser"
            },
            "ResourceMetadata": {
                "Type": "document",
                "Name": "updatedDoc",
                "Id":
 "15df51e0335cfcc6a2e4de9dd8be9f22ee40545ad9176f54758dcf903be982d3",
                "Owner": {
                    "Id":
 "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
                    "GivenName": "exampleName",
                    "Surname": "exampleSurname"
                }
            }
        },
        {
            "Type": "DOCUMENT_VERSION_VIEWED",
            "TimeStamp": 1534799079.207,
            "Initiator": {
                "Id": "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
                "GivenName": "exampleName",
                "Surname": "exampleSurname"
            },
            "ResourceMetadata": {
                "Type": "document",
                "Name": "updatedDoc",
                "Id":
 "15df51e0335cfcc6a2e4de9dd8be9f22ee40545ad9176f54758dcf903be982d3",
                "Owner": {
                    "Id":
 "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
                    "GivenName": "exampleName",
                    "Surname": "exampleSurname"
                }
            }
        }
    ],
    "Marker":
 "DnF1ZXJ5VGhlbkZldGNoAgAAAAAAAAS7FmlTaU1OdlFTU1h1UU00VVFIbDlRWHcAAAAAAAAJTRY3bWh5eUgzaVF1ZX
}
```

- Para obtener información sobre la API, consulte DescribeActivities en la Referencia de comandos de la AWS CLI.

describe-comments

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-comments`.

AWS CLI

Para obtener una lista de todos los comentarios de la versión del documento especificada

En este ejemplo, se enumeran todos los comentarios de la versión del documento especificada.

Comando:

```
aws workdocs describe-comments --document-
id 15df51e0335cfcc6a2e4de9dd8be9f22ee40545ad9176f54758dcf903be982d3 --version-
id 1521672507741-9f7df0ea5dd0b121c4f3564a0c7c0b4da95cd12c635d3c442af337a88e297920
```

Salida:

```
{
  "Comments": [
      {
          "CommentId": "1534799058197-
c7f5c84de9115875bbca93e0367bbebac609541d461636b760849b88b1609dd5",
          "ThreadId": "1534799058197-
c7f5c84de9115875bbca93e0367bbebac609541d461636b760849b88b1609dd5",
          "Text": "This is a comment.",
          "Contributor": {
              "Username": "arn:aws:iam::123456789123:user/exampleUser",
              "Type": "USER"
          },
          "CreatedTimestamp": 1534799058.197,
          "Status": "PUBLISHED",
          "Visibility": "PUBLIC"
      }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeComments en la Referencia de comandos de la AWS CLI.

describe-document-versions

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-document-versions`.

AWS CLI

Para recuperar las versiones de un documento

En este ejemplo, se recuperan las versiones del documento especificado, incluidas las versiones inicializadas y una URL del documento de origen.

Comando:

```
aws workdocs describe-document-versions --document-
id d90d93c1fe44bad0c8471e973ebaab339090401a95e777cffa58e977d2983b65 --fields SOURCE
```

Salida:

```
{
  "DocumentVersions": [
      {
          "Id":
 "1534452029587-15e129dfc187505c407588df255be83de2920d733859f1d2762411d22a83e3ef",
          "Name": "exampleDoc.docx",
          "ContentType": "application/vnd.openxmlformats-
officedocument.wordprocessingml.document",
          "Size": 13922,
          "Signature": "1a23456b78901c23d4ef56gh7EXAMPLE",
          "Status": "ACTIVE",
          "CreatedTimestamp": 1534452029.587,
          "ModifiedTimestamp": 1534452029.849,
          "CreatorId":
 "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
          "Source": {
              "ORIGINAL": "https://gb-us-west-2-prod-doc-source.s3.us-
west-2.amazonaws.com/
d90d93c1fe44bad0c8471e973ebaab339090401a95e777cffa58e977d2983b65/1534452029587-15e129dfc1875
response-content-disposition=attachment%3B%20filename%2A
%3DUTF-8%27%27exampleDoc29.docx&X-Amz-Algorithm=AWS1-ABCD-EFG234&X-Amz-
Date=20180816T204149Z&X-Amz-SignedHeaders=host&X-Amz-Expires=900&X-Amz-
Credential=AKIAIOSFODNN7EXAMPLE%2F20180816%2Fus-west-2%2Fs3%2Faws1_request&X-Amz-
Signature=01Ab2c34d567e8f90123g456hi78j901k2345678l901234mno56pqr78EXAMPLE"
          }
      },
      {
          "Id": "1529005196082-
bb75fa19abc287699cb07147f75816dce43a53a10f28dc001bf61ef2fab01c59",
```

```
            "Name": "exampleDoc.pdf",
            "ContentType": "application/pdf",
            "Size": 425916,
            "Signature": "1a23456b78901c23d4ef56gh7EXAMPLE",
            "Status": "ACTIVE",
            "CreatedTimestamp": 1529005196.082,
            "ModifiedTimestamp": 1529005196.796,
            "CreatorId":
 "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
            "Source": {
                "ORIGINAL": "https://gb-us-west-2-prod-doc-source.s3.us-
west-2.amazonaws.com/
d90d93c1fe44bad0c8471e973ebaab339090401a95e777cffa58e977d2983b65/1529005196082-
bb75fa19abc287699cb07147f75816dce43a53a10f28dc001bf61ef2fab01c59?
response-content-disposition=attachment%3B%20filename%2A
%3DUTF-8%27%27exampleDoc29.pdf&X-Amz-Algorithm=AWS1-ABCD-EFG234&X-Amz-
Date=20180816T204149Z&X-Amz-SignedHeaders=host&X-Amz-Expires=900&X-Amz-
Credential=AKIAIOSFODNN7EXAMPLE%2F20180816%2Fus-west-2%2Fs3%2Faws1_request&X-Amz-
Signature=01Ab2c34d567e8f90123g456hi78j901k2345678l901234mno56pqr78EXAMPLE"
            }
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeDocumentVersions en la Referencia de comandos de la AWS CLI.

`describe-folder-contents`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-folder-contents`.

AWS CLI

Para describir el contenido de una carpeta

En este ejemplo, se describe todo el contenido activo de la carpeta especificada, incluidos sus documentos y subcarpetas, ordenados por fecha en orden ascendente.

Comando:

```
aws workdocs describe-folder-contents --folder-
id 1ece93e5fe75315c7407c4967918b4fd9da87ddb2a588e67b7fdaf4a98fde678 --sort DATE --
order ASCENDING --type ALL
```

Salida:

```
{
  "Folders": [
      {
          "Id": "50893c0af679524d1a0e0651130ed6d073e1a05f95bd12c42dcde5d35634ed08",
          "Name": "testing",
          "CreatorId":
 "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
          "ParentFolderId":
 "1ece93e5fe75315c7407c4967918b4fd9da87ddb2a588e67b7fdaf4a98fde678",
          "CreatedTimestamp": 1534450467.622,
          "ModifiedTimestamp": 1534451113.504,
          "ResourceState": "ACTIVE",
          "Signature": "1a23456b78901c23d4ef56gh7EXAMPLE",
          "Size": 23019,
          "LatestVersionSize": 11537
      }
  ],
  "Documents": [
      {
          "Id": "d90d93c1fe44bad0c8471e973ebaab339090401a95e777cffa58e977d2983b65",
          "CreatorId":
 "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
          "ParentFolderId":
 "1ece93e5fe75315c7407c4967918b4fd9da87ddb2a588e67b7fdaf4a98fde678",
          "CreatedTimestamp": 1529005196.082,
          "ModifiedTimestamp": 1534452483.01,
          "LatestVersionMetadata": {
              "Id":
 "1534452029587-15e129dfc187505c407588df255be83de2920d733859f1d2762411d22a83e3ef",
              "Name": "exampleDoc.docx",
              "ContentType": "application/vnd.openxmlformats-
officedocument.wordprocessingml.document",
              "Size": 13922,
              "Signature": "1a23456b78901c23d4ef56gh7EXAMPLE",
              "Status": "ACTIVE",
              "CreatedTimestamp": 1534452029.587,
              "ModifiedTimestamp": 1534452029.587,
```

```
                "CreatorId":
 "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c"
            },
            "ResourceState": "ACTIVE"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeFolderContents en la Referencia de comandos de la AWS CLI.

`describe-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-groups`.

AWS CLI

Para recuperar una lista de grupos

En el siguiente ejemplo de `describe-groups`, se enumeran los grupos asociados a la organización de Amazon WorkDocs especificada.

```
aws workdocs describe-groups \
    --search-query "e" \
    --organization-id d-123456789c
```

Salida:

```
{
    "Groups": [
        {
            "Id": "S-1-1-11-1122222222-2222233333-3333334444-4444&d-123456789c",
            "Name": "Example Group 1"
        },
        {
            "Id": "S-1-1-11-1122222222-2222233333-3333334444-5555&d-123456789c",
            "Name": "Example Group 2"
        }
    ]
}
```

Para obtener más información, consulte Introducción a WorkDocs en la Guía del administrador de Amazon WorkDocs.

- Para obtener información sobre la API, consulte DescribeGroups en la Referencia de comandos de la AWS CLI.

`describe-notification-subscriptions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-notification-subscriptions`.

AWS CLI

Para recuperar una lista de suscripciones de notificaciones

En el siguiente ejemplo de `describe-notification-subscriptions`, se recuperan las suscripciones de notificaciones de la organización de Amazon WorkDocs especificada.

```
aws workdocs describe-notification-subscriptions \
    --organization-id d-123456789c
```

Salida:

```
{
    "Subscriptions": [
        {
            "SubscriptionId": "123ab4c5-678d-901e-f23g-45h6789j0123",
            "EndPoint": "https://example.com/example",
            "Protocol": "HTTPS"
        }
    ]
}
```

Para obtener más información, consulte Subscribe to Notifications en la Guía para desarrolladores de Amazon WorkDocs.

- Para obtener información sobre la API, consulte DescribeNotificationSubscriptions en la Referencia de comandos de la AWS CLI.

`describe-resource-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-resource-permissions`.

AWS CLI

Para obtener una lista de permisos para un recurso

En este ejemplo, se devuelve una lista de los permisos del recurso (documento o carpeta) especificado.

Comando:

```
aws workdocs describe-resource-permissions --resource-
id 15df51e0335cfcc6a2e4de9dd8be9f22ee40545ad9176f54758dcf903be982d3
```

Salida:

```
{
  "Principals": [
      {
          "Id": "anonymous",
          "Type": "ANONYMOUS",
          "Roles": [
              {
                  "Role": "VIEWER",
                  "Type": "DIRECT"
              }
          ]
      },
      {
          "Id": "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
          "Type": "USER",
          "Roles": [
              {
                  "Role": "OWNER",
                  "Type": "DIRECT"
              }
          ]
      },
      {
          "Id": "d-926726012c",
          "Type": "ORGANIZATION",
          "Roles": [
              {
                  "Role": "VIEWER",
                  "Type": "INHERITED"
```

```
            }
        ]
    }
  ]
}
```

- Para obtener información sobre la API, consulte DescribeResourcePermissions en la Referencia de comandos de la AWS CLI.

`describe-users`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-users`.

AWS CLI

Para recuperar los detalles de los usuarios especificados

En este ejemplo, se recuperan los detalles de todos los usuarios de la organización especificada.

Comando:

```
aws workdocs describe-users --organization-id d-926726012c
```

Salida:

```
{
  "Users": [
      {
          "Id": "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
          "Username": "example1User",
          "OrganizationId": "d-926726012c",
          "RootFolderId":
 "3c0e3f849dd20a9771d937b9bbcc97e18796150ae56c26d64a4fa0320a2dedc9",
          "RecycleBinFolderId":
 "c277f4c4d647be1f5147b3184ffa96e1e2bf708278b696cacba68ba13b91f4fe",
          "Status": "INACTIVE",
          "Type": "USER",
          "CreatedTimestamp": 1535478999.452,
          "ModifiedTimestamp": 1535478999.452
      },
      {
```

```
            "Id": "S-1-1-11-1111111111-2222222222-3333333333-4444&d-926726012c",
            "Username": "example2User",
            "EmailAddress": "example2User@site.awsapps.com",
            "GivenName": "example2Name",
            "Surname": "example2Surname",
            "OrganizationId": "d-926726012c",
            "RootFolderId":
 "35b886cb17198cbd547655e58b025dff0cf34aaed638be52009567e23dc67390",
            "RecycleBinFolderId":
 "9858c3e9ed4c2460dde9aadb4c69fde998070dd46e5e985bd08ec6169ea249ff",
            "Status": "ACTIVE",
            "Type": "MINIMALUSER",
            "CreatedTimestamp": 1535478836.584,
            "ModifiedTimestamp": 1535478836.584
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeUsers en la Referencia de comandos de la AWS CLI.

`get-document-path`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-document-path`.

AWS CLI

Para recuperar la información de la ruta de un documento

En este ejemplo, se recupera la información de ruta (jerarquía de la carpeta raíz) del documento especificado e incluye los nombres de las carpetas principales.

Comando:

```
aws workdocs get-document-path --document-
id d90d93c1fe44bad0c8471e973ebaab339090401a95e777cffa58e977d2983b65 --fields NAME
```

Salida:

```
{
  "Path": {
```

```
      "Components": [
          {
              "Id":
 "a43d29cbb8e7c4d25cfee8b803a504b0dc63e760b55ad0c611c6b87691eb6ff3",
              "Name": "/"
          },
          {
              "Id":
 "1ece93e5fe75315c7407c4967918b4fd9da87ddb2a588e67b7fdaf4a98fde678",
              "Name": "Top Level Folder"
          },
          {
              "Id":
 "d90d93c1fe44bad0c8471e973ebaab339090401a95e777cffa58e977d2983b65",
              "Name": "exampleDoc.docx"
          }
      ]
  }
}
```

- Para obtener información sobre la API, consulte GetDocumentPath en la Referencia de comandos de la AWS CLI.

`get-document-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-document-version`.

AWS CLI

Para recuperar los metadatos de la versión del documento especificado

En este ejemplo, se recuperan los metadatos de la versión del documento especificado, incluida la URL de origen y los metadatos personalizados.

Comando:

```
aws workdocs get-document-version --document-
id 15df51e0335cfcc6a2e4de9dd8be9f22ee40545ad9176f54758dcf903be982d3 --version-
id 1521672507741-9f7df0ea5dd0b121c4f3564a0c7c0b4da95cd12c635d3c442af337a88e297920 --
fields SOURCE --include-custom-metadata
```

Salida:

```
{
  "Metadata": {
      "Id":
 "1521672507741-9f7df0ea5dd0b121c4f3564a0c7c0b4da95cd12c635d3c442af337a88e297920",
      "Name": "exampleDoc",
      "ContentType": "application/vnd.openxmlformats-
officedocument.wordprocessingml.document",
      "Size": 11537,
      "Signature": "1a23456b78901c23d4ef56gh7EXAMPLE",
      "Status": "ACTIVE",
      "CreatedTimestamp": 1521672507.741,
      "ModifiedTimestamp": 1534451113.504,
      "CreatorId": "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
      "Source": {
          "ORIGINAL": "https://gb-us-west-2-prod-doc-source.s3.us-
west-2.amazonaws.com/15df51e0335cfcc6a2e4de9dd8be9f22ee40545ad9176f54758dcf903be982d3/152167
response-content-disposition=attachment%3B%20filename%2A
%3DUTF-8%27%27exampleDoc&X-Amz-Algorithm=AWS1-ABCD-EFG234&X-Amz-
Date=20180820T212202Z&X-Amz-SignedHeaders=host&X-Amz-Expires=900&X-Amz-
Credential=AKIAIOSFODNN7EXAMPLE%2F20180820%2Fus-west-2%2Fs3%2Faws1_request&X-Amz-
Signature=01Ab2c34d567e8f90123g456hi78j901k2345678l901234mno56pqr78EXAMPLE"
      }
  }
}
```

- Para obtener información sobre la API, consulte GetDocumentVersion en la Referencia de comandos de la AWS CLI.

`get-document`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-document`.

AWS CLI

Para recuperar los detalles del documento

En este ejemplo, se recuperan los detalles del documento especificado.

Comando:

```
aws workdocs get-document --document-
id d90d93c1fe44bad0c8471e973ebaab339090401a95e777cffa58e977d2983b65
```

Salida:

```
{
  "Metadata": {
      "Id": "d90d93c1fe44bad0c8471e973ebaab339090401a95e777cffa58e977d2983b65",
      "CreatorId": "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
      "ParentFolderId":
 "1ece93e5fe75315c7407c4967918b4fd9da87ddb2a588e67b7fdaf4a98fde678",
      "CreatedTimestamp": 1529005196.082,
      "ModifiedTimestamp": 1534452483.01,
      "LatestVersionMetadata": {
          "Id":
 "1534452029587-15e129dfc187505c407588df255be83de2920d733859f1d2762411d22a83e3ef",
          "Name": "exampleDoc.docx",
          "ContentType": "application/vnd.openxmlformats-
officedocument.wordprocessingml.document",
          "Size": 13922,
          "Signature": "1a23456b78901c23d4ef56gh7EXAMPLE",
          "Status": "ACTIVE",
          "CreatedTimestamp": 1534452029.587,
          "ModifiedTimestamp": 1534452029.587,
          "CreatorId": "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c"
      },
      "ResourceState": "ACTIVE"
  }
}
```

- Para obtener información sobre la API, consulte GetDocument en la Referencia de comandos de la AWS CLI.

`get-folder-path`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-folder-path`.

AWS CLI

Para recuperar la información de la ruta de una carpeta

En este ejemplo, se recupera la información de ruta (jerarquía de la carpeta raíz) de la carpeta especificada e incluye los nombres de las carpetas principales.

Comando:

```
aws workdocs get-folder-path --folder-
id 50893c0af679524d1a0e0651130ed6d073e1a05f95bd12c42dcde5d35634ed08 --fields NAME
```

Salida:

```
{
  "Path": {
      "Components": [
          {
              "Id":
 "a43d29cbb8e7c4d25cfee8b803a504b0dc63e760b55ad0c611c6b87691eb6ff3",
              "Name": "/"
          },
          {
              "Id":
 "1ece93e5fe75315c7407c4967918b4fd9da87ddb2a588e67b7fdaf4a98fde678",
              "Name": "Top Level Folder"
          },
          {
              "Id":
 "50893c0af679524d1a0e0651130ed6d073e1a05f95bd12c42dcde5d35634ed08",
              "Name": "Sublevel Folder"
          }
      ]
  }
}
```

- Para obtener información sobre la API, consulte GetFolderPath en la Referencia de comandos de la AWS CLI.

`get-folder`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-folder`.

AWS CLI

Para recuperar los metadatos de una carpeta

En este ejemplo, se recuperan los metadatos de la carpeta especificada.

Comando:

```
aws workdocs get-folder --folder-
id 50893c0af679524d1a0e0651130ed6d073e1a05f95bd12c42dcde5d35634ed08
```

Salida:

```
{
  "Metadata": {
      "Id": "50893c0af679524d1a0e0651130ed6d073e1a05f95bd12c42dcde5d35634ed08",
      "Name": "exampleFolder",
      "CreatorId": "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
      "ParentFolderId":
 "1ece93e5fe75315c7407c4967918b4fd9da87ddb2a588e67b7fdaf4a98fde678",
      "CreatedTimestamp": 1534450467.622,
      "ModifiedTimestamp": 1534451113.504,
      "ResourceState": "ACTIVE",
      "Signature": "1a23456b78901c23d4ef56gh7EXAMPLE",
      "Size": 23019,
      "LatestVersionSize": 11537
  }
}
```

- Para obtener información sobre la API, consulte GetFolder en la Referencia de comandos de la AWS CLI.

`get-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-resources`.

AWS CLI

Para recuperar los recursos compartidos

En el siguiente ejemplo de `get-resources`, se recuperan los recursos compartidos con el usuario de Amazon WorkDocs especificado.

```
aws workdocs get-resources \
    --user-id "S-1-1-11-1111111111-2222222222-3333333333-3333" \
    --collection-type SHARED_WITH_ME
```

Salida:

```
{
"Folders": [],
"Documents": []
}
```

Para obtener más información, consulte Compartir archivos y carpetas en la Guía del usuario de Amazon WorkDocs.

- Para obtener detalles sobre la API, consulte GetResources en la Referencia de comandos de la AWS CLI.

`initiate-document-version-upload`

En el siguiente ejemplo de código, se muestra cómo utilizar `initiate-document-version-upload`.

AWS CLI

Para iniciar la carga de una versión de un documento

En el siguiente ejemplo de `initiate-document-upload`, se crea un nuevo objeto de documento y objeto de versión.

```
aws workdocs initiate-document-version-upload \
    --name exampledocname \
    --parent-folder-
id eacd546d952531c633452ed67cac23161aa0d5df2e8061223a59e8f67e7b6189
```

Salida:

```
{
    "Metadata": {
        "Id": "feaba64d4efdf271c2521b60a2a44a8f057e84beaabbe22f01267313209835f2",
        "CreatorId": "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
        "ParentFolderId":
 "eacd546d952531c633452ed67cac23161aa0d5df2e8061223a59e8f67e7b6189",
        "CreatedTimestamp": 1536773972.914,
        "ModifiedTimestamp": 1536773972.914,
        "LatestVersionMetadata": {
            "Id": "1536773972914-
ddb67663e782e7ce8455ebc962217cf9f9e47b5a9a702e5c84dcccd417da9313",
```

```
            "Name": "exampledocname",
            "ContentType": "application/octet-stream",
            "Size": 0,
            "Status": "INITIALIZED",
            "CreatedTimestamp": 1536773972.914,
            "ModifiedTimestamp": 1536773972.914,
            "CreatorId": "arn:aws:iam::123456789123:user/EXAMPLE"
        },
        "ResourceState": "ACTIVE"
    },
    "UploadMetadata": {
        "UploadUrl": "https://gb-us-west-2-prod-doc-source.s3.us-
west-2.amazonaws.com/
feaba64d4efdf271c2521b60a2a44a8f057e84beaabbe22f01267313209835f2/1536773972914-
ddb67663e782e7ce8455ebc962217cf9f9e47b5a9a702e5c84dcccd417da9313?X-Amz-
Algorithm=AWS1-ABCD-EFG234&X-Amz-Date=20180912T173932Z&X-Amz-SignedHeaders=content-
type%3Bhost%3Bx-amz-server-side-encryption&X-Amz-Expires=899&X-Amz-
Credential=AKIAIOSFODNN7EXAMPLE%2F20180912%2Fus-west-2%2Fs3%2Faws1_request&X-Amz-
Signature=01Ab2c34d567e8f90123g456hi78j901k2345678l901234mno56pqr78EXAMPLE",
        "SignedHeaders": {
            "Content-Type": "application/octet-stream",
            "x-amz-server-side-encryption": "ABC123"
        }
    }
}
```

- Para obtener información sobre la API, consulte InitiateDocumentVersionUpload en la Referencia de comandos de la AWS CLI.

`remove-all-resource-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-all-resource-permissions`.

AWS CLI

Para eliminar todos los permisos de un recurso especificado

En este ejemplo, se eliminan todos los permisos del recurso especificado.

Comando:

```
aws workdocs remove-all-resource-permissions --resource-
id 1ece93e5fe75315c7407c4967918b4fd9da87ddb2a588e67b7fdaf4a98fde678
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte RemoveAllResourcePermissions en la Referencia de comandos de la AWS CLI.

`remove-resource-permission`

En el siguiente ejemplo de código, se muestra cómo utilizar `remove-resource-permission`.

AWS CLI

Para retirar permisos de un recurso

En este ejemplo, se eliminan todos los permisos del recurso de la entidad principal especificada.

Comando:

```
aws workdocs remove-resource-permission --resource-
id 1ece93e5fe75315c7407c4967918b4fd9da87ddb2a588e67b7fdaf4a98fde678 --principal-
id anonymous
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte RemoveResourcePermission en la Referencia de comandos de la AWS CLI.

`update-document-version`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-document-version`.

AWS CLI

Para cambiar el estado de la versión de un documento a Active

En este ejemplo, se cambia el estado de la versión del documento a ACTIVE.

Comando:

```
aws workdocs update-document-version --document-
id 15df51e0335cfcc6a2e4de9dd8be9f22ee40545ad9176f54758dcf903be982d3 --version-
id 1521672507741-9f7df0ea5dd0b121c4f3564a0c7c0b4da95cd12c635d3c442af337a88e297920 --
version-status ACTIVE
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte UpdateDocumentVersion en la Referencia de comandos de la AWS CLI.

`update-document`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-document`.

AWS CLI

Para actualizar un documento

En este ejemplo, se actualizan el nombre y la carpeta principal de un documento.

Comando:

```
aws workdocs update-document --document-
id 15df51e0335cfcc6a2e4de9dd8be9f22ee40545ad9176f54758dcf903be982d3 --
name updatedDoc --parent-folder-
id 50893c0af679524d1a0e0651130ed6d073e1a05f95bd12c42dcde5d35634ed08
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte UpdateDocument en la Referencia de la API de la AWS CLI.

update-folder

En el siguiente ejemplo de código, se muestra cómo utilizar `update-folder`.

AWS CLI

Para actualizar una carpeta

En este ejemplo, se actualiza la carpeta principal y el nombre de una carpeta.

Comando:

```
aws workdocs update-folder --folder-
id 50893c0af679524d1a0e0651130ed6d073e1a05f95bd12c42dcde5d35634ed08 --
name exampleFolder1 --parent-folder-
id 1ece93e5fe75315c7407c4967918b4fd9da87ddb2a588e67b7fdaf4a98fde678
```

Salida:

```
None
```

- Para obtener información sobre la API, consulte UpdateFolder en la Referencia de comandos de la AWS CLI.

update-user

En el siguiente ejemplo de código, se muestra cómo utilizar `update-user`.

AWS CLI

Para actualizar un usuario

En este ejemplo, se actualiza la zona horaria del usuario especificado.

Comando:

```
aws workdocs update-user --user-
id "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c" --time-zone-
id "America/Los_Angeles"
```

Salida:

```
{
```

```
  "User": {
      "Id": "S-1-1-11-1111111111-2222222222-3333333333-3333&d-926726012c",
      "Username": "exampleUser",
      "EmailAddress": "exampleUser@site.awsapps.com",
      "GivenName": "Example",
      "Surname": "User",
      "OrganizationId": "d-926726012c",
      "RootFolderId":
 "c5eceb5e1a2d1d460c9d1af8330ae117fc8d39bb1d3ed6acd0992d5ff192d986",
      "RecycleBinFolderId":
 "6ca20102926ad15f04b1d248d6d6e44f2449944eda5c758f9a1e9df6a6b7fa66",
      "Status": "ACTIVE",
      "Type": "USER",
      "TimeZoneId": "America/Los_Angeles",
      "Storage": {
          "StorageUtilizedInBytes": 0,
          "StorageRule": {
              "StorageAllocatedInBytes": 53687091200,
              "StorageType": "QUOTA"
          }
      }
  }
}
```

- Para obtener información sobre la API, consulte UpdateUser en la Referencia de comandos de la AWS CLI.

Ejemplos de Amazon WorkMail que utilizan la AWS CLI

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con Amazon WorkMail.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`associate-delegate-to-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-delegate-to-resource`.

AWS CLI

Para añadir un delegado a un recurso

El siguiente comando `associate-delegate-to-resource` agrega un delegado a un recurso.

```
aws workmail associate-delegate-to-resource \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --resource-id r-68bf2d3b1c0244aab7264c24b9217443 \
    --entity-id S-1-1-11-1111111111-2222222222-3333333333-3333
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte AssociateDelegateToResource en la Referencia de comandos de la AWS CLI.

`associate-member-to-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `associate-member-to-group`.

AWS CLI

Para agregar un miembro a un grupo

El siguiente comando `associate-member-to-group` agrega el miembro especificado a un grupo.

```
aws workmail associate-member-to-group \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --group-id S-1-1-11-1122222222-2222233333-3333334444-4444 \
    --member-id S-1-1-11-1111111111-2222222222-3333333333-3333
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte AssociateMemberToGroup en la Referencia de comandos de la AWS CLI.

`create-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-alias`.

AWS CLI

Para crear un alias

El siguiente comando `create-alias` crea un alias para la entidad especificada (usuario o grupo).

```
aws workmail create-alias \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --entity-id S-1-1-11-1122222222-2222233333-3333334444-4444 \
    --alias exampleAlias@site.awsapps.com
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte CreateAlias en la Referencia de comandos de la AWS CLI.

`create-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-group`.

AWS CLI

Para crear un grupo nuevo

El siguiente comando `create-group` crea un nuevo grupo en la organización especificada.

```
aws workmail create-group \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --name exampleGroup1
```

Salida:

```
{
    "GroupId": "S-1-1-11-1122222222-2222233333-3333334444-4444"
}
```

- Para obtener información sobre la API, consulte CreateGroup en la Referencia de comandos de la AWS CLI.

`create-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-resource`.

AWS CLI

Para crear un nuevo recurso

El siguiente comando `create-resource` crea un nuevo recurso (sala de reuniones) para la organización especificada.

```
aws workmail create-resource \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --name exampleRoom1 \
    --type ROOM
```

Salida:

```
{
    "ResourceId": "r-7afe0efbade843a58cdc10251fce992c"
}
```

- Para obtener información sobre la API, consulte CreateResource en la Referencia de comandos de la AWS CLI.

`create-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-user`.

AWS CLI

Para crear un nuevo usuario

El siguiente comando `create-user` crea un nuevo usuario.

```
aws workmail create-user \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --name exampleName \
```

```
    --display-name exampleDisplayName \
    --password examplePa$$w0rd
```

Salida:

```
{
    "UserId": "S-1-1-11-1111111111-2222222222-3333333333-3333"
}
```

- Para obtener información sobre la API, consulte CreateUser en la Referencia de comandos de la AWS CLI.

`delete-access-control-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-access-control-rule`.

AWS CLI

Para eliminar una regla de control de acceso

En el siguiente ejemplo de `delete-access-control-rule`, se elimina la regla de control de acceso especificada de la organización de Amazon WorkMail indicada.

```
aws workmail delete-access-control-rule \
    --organization-id m-n1pq2345678r901st2u3vx45x6789yza \
    --name "myRule"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with Access Control Rules en la Guía del administrador de Amazon WorkMail.

- Para obtener información sobre la API, consulte DeleteAccessControlRule en la Referencia de comandos de la AWS CLI.

`delete-alias`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-alias`.

AWS CLI

Para eliminar un alias

El siguiente comando `delete-alias` elimina un alias para la entidad especificada (usuario o grupo).

```
aws workmail delete-alias \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --entity-id S-1-1-11-1122222222-2222233333-3333334444-4444 \
    --alias exampleAlias@site.awsapps.com
```

Este comando no genera ninguna salida.

- Para ver los detalles de la API, consulte DeleteTopic en la Referencia de comandos de la AWS CLI.

`delete-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-group`.

AWS CLI

Para eliminar un grupo existente

El siguiente comando `delete-group` elimina un grupo existente de Amazon WorkMail.

```
aws workmail delete-group \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --group-id S-1-1-11-1122222222-2222233333-3333334444-4444
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteGroup en la Referencia de comandos de la AWS CLI.

`delete-mailbox-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-mailbox-permissions`.

AWS CLI

Para eliminar los permisos del buzón de correo

El siguiente comando `delete-mailbox-permissions` elimina los permisos de buzón de correo que se han concedido anteriormente a un usuario o grupo. La entidad representa al

usuario propietario del buzón de correo y el concesionario representa al usuario o grupo para el que se van a eliminar los permisos.

```
aws workmail delete-mailbox-permissions \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --entity-id S-1-1-11-1122222222-2222233333-3333334444-4444 \
    --grantee-id S-1-1-11-1111111111-2222222222-3333333333-3333
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteMailboxPermissions en la Referencia de comandos de la AWS CLI.

`delete-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-resource`.

AWS CLI

Para eliminar un recurso existente

El siguiente comando `delete-resource` elimina un recurso existente de Amazon WorkMail.

```
aws workmail delete-resource \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --resource-id r-7afe0efbade843a58cdc10251fce992c
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteResource en la Referencia de comandos de la AWS CLI.

`delete-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-user`.

AWS CLI

Cómo eliminar un usuario

El siguiente comando `delete-user` elimina el usuario especificado de Amazon WorkMail y de todos los sistemas posteriores.

```
aws workmail delete-user \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --user-id S-1-1-11-1111111111-2222222222-3333333333-3333
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeleteUser en la Referencia de comandos de la AWS CLI.

`deregister-from-work-mail`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-from-work-mail`.

AWS CLI

Para deshabilitar una entidad existente

El siguiente comando `deregister-from-work-mail` impide que una entidad existente (usuario, grupo o recurso) utilice Amazon WorkMail.

```
aws workmail deregister-from-work-mail \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --entity-id S-1-1-11-1111111111-2222222222-3333333333-3333
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DeregisterFromWorkMail en la Referencia de comandos de la AWS CLI.

`describe-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-group`.

AWS CLI

Para recuperar información de un grupo

El siguiente comando `describe-group` recupera información acerca del grupo especificado.

```
aws workmail describe-group \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
```

```
    --group-id S-1-1-11-1122222222-2222233333-3333334444-4444
```

Salida:

```
{
    "GroupId": "S-1-1-11-1122222222-2222233333-3333334444-4444",
    "Name": "exampleGroup1",
    "State": "ENABLED"
}
```

- Para obtener información sobre la API, consulte DescribeGroup en la Referencia de comandos de la AWS CLI.

`describe-organization`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-organization`.

AWS CLI

Para recuperar la información de una organización

El siguiente comando `describe-organization` recupera información de la organización de Amazon WorkMail especificada.

```
aws workmail describe-organization \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27
```

Salida:

```
{
    "OrganizationId": "m-d281d0a2fd824be5b6cd3d3ce909fd27",
    "Alias": "alias",
    "State": "Active",
    "DirectoryId": "d-926726012c",
    "DirectoryType": "VpcDirectory",
    "DefaultMailDomain": "site.awsapps.com",
    "CompletedDate": 1522693605.468,
    "ARN": "arn:aws:workmail:us-west-2:111122223333:organization/m-
n1pq2345678r901st2u3vx45x6789yza"
}
```

Para obtener más información, consulte Working with Organizations en la Guía del administrador de Amazon WorkMail.

- Para obtener información sobre la API, consulte DescribeOrganization en la Referencia de comandos de la AWS CLI.

`describe-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-resource`.

AWS CLI

Para recuperar información de un recurso

El siguiente comando `describe-resource` recupera información acerca del recurso especificado.

```
aws workmail describe-resource \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --resource-id r-7afe0efbade843a58cdc10251fce992c
```

Salida:

```
{
    "ResourceId": "r-7afe0efbade843a58cdc10251fce992c",
    "Name": "exampleRoom1",
    "Type": "ROOM",
    "BookingOptions": {
        "AutoAcceptRequests": true,
        "AutoDeclineRecurringRequests": false,
        "AutoDeclineConflictingRequests": true
    },
    "State": "ENABLED"
}
```

- Para obtener información sobre la API, consulte DescribeResource en la Referencia de comandos de la AWS CLI.

`describe-user`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-user`.

AWS CLI

Para recuperar información del usuario

El siguiente comando `describe-user` recupera información acerca del usuario especificado.

```
aws workmail describe-user \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --user-id S-1-1-11-1111111111-2222222222-3333333333-3333
```

Salida:

```
{
    "UserId": "S-1-1-11-1111111111-2222222222-3333333333-3333",
    "Name": "exampleUser1",
    "Email": "exampleUser1@site.awsapps.com",
    "DisplayName": "",
    "State": "ENABLED",
    "UserRole": "USER",
    "EnabledDate": 1532459261.827
}
```

- Para obtener detalles sobre la API, consulte DescribeUser en la Referencia de comandos de la AWS CLI.

`disassociate-delegate-from-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-delegate-from-resource`.

AWS CLI

Para eliminar un miembro de un recurso

El siguiente comando `disassociate-delegate-from-resource` elimina el miembro especificado de un recurso.

```
ws workmail disassociate-delegate-from-resource \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --resource-id r-68bf2d3b1c0244aab7264c24b9217443 \
```

```
    --entity-id S-1-1-11-1111111111-2222222222-3333333333-3333
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DisassociateDelegateFromResource en la Referencia de comandos de la AWS CLI.

`disassociate-member-from-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `disassociate-member-from-group`.

AWS CLI

Para eliminar un miembro de un grupo

El siguiente comando `disassociate-member-from-group` elimina el miembro especificado de un grupo.

```
aws workmail disassociate-member-from-group \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --group-id S-1-1-11-1122222222-2222233333-3333334444-4444 \
    --member-id S-1-1-11-1111111111-2222222222-3333333333-3333
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte DisassociateMemberFromGroup en la Referencia de comandos de la AWS CLI.

`get-access-control-effect`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-access-control-effect`.

AWS CLI

Para obtener el efecto de las reglas de control de acceso

En el siguiente ejemplo de `get-access-control-effect`, se recupera el efecto de las reglas de control de acceso de la organización de Amazon WorkMail especificadas para la dirección IP, la acción de protocolo de acceso y el ID de usuario especificados.

```
aws workmail get-access-control-effect \
```

```
    --organization-id m-n1pq2345678r901st2u3vx45x6789yza \
    --ip-address "192.0.2.0" \
    --action "WindowsOutlook" \
    --user-id "S-1-1-11-1111111111-2222222222-3333333333-3333"
```

Salida:

```
{
    "Effect": "DENY",
    "MatchedRules": [
        "myRule"
    ]
}
```

Para obtener más información, consulte Working with Access Control Rules en la Guía del administrador de Amazon WorkMail.

- Para obtener más información sobre la API, consulte GetAccessControlEffect en la Referencia de comandos de la AWS CLI.

`get-mailbox-details`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-mailbox-details`.

AWS CLI

Para obtener los detalles del buzón de correo de un usuario

El siguiente comando `get-mailbox-details` recupera detalles acerca del buzón de correo del usuario especificado.

```
aws workmail get-mailbox-details \
    --organization-id m-n1pq2345678r901st2u3vx45x6789yza \
    --user-id S-1-1-11-1111111111-2222222222-3333333333-3333
```

Salida:

```
{
    "MailboxQuota": 51200,
    "MailboxSize": 0.03890800476074219
}
```

Para obtener más información, consulte Managing User Accounts en la Guía del administrador de Amazon WorkMail.

- Para obtener información sobre la API, consulte GetMailboxDetails en la Referencia de comandos de la AWS CLI.

`list-access-control-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-access-control-rules`.

AWS CLI

Para enumerar las reglas de control de acceso

En el siguiente ejemplo de `list-access-control-rules`, se enumeran las reglas de control de acceso especificadas para la organización de Amazon WorkMail indicada.

```
aws workmail list-access-control-rules \
    --organization-id m-n1pq2345678r901st2u3vx45x6789yza
```

Salida:

```
{
    "Rules": [
        {
            "Name": "default",
            "Effect": "ALLOW",
            "Description": "Default WorkMail Rule",
            "DateCreated": 0.0,
            "DateModified": 0.0
        },
        {
            "Name": "myRule",
            "Effect": "DENY",
            "Description": "my rule",
            "UserIds": [
            "S-1-1-11-1111111111-2222222222-3333333333-3333"
            ],
            "DateCreated": 1581635628.0,
            "DateModified": 1581635628.0
        }
    ]
```

```
}
```

Para obtener más información, consulte Working with Access Control Rules en la Guía del administrador de Amazon WorkMail.

- Para obtener información sobre la API, consulte ListAccessControlRules en la Referencia de comandos de la AWS CLI.

`list-aliases`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-aliases`.

AWS CLI

Para enumerar los alias de un miembro

El siguiente comando `list-aliases` enumera los alias para el miembro especificado (usuario o grupo).

```
aws workmail list-aliases \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --entity-id S-1-1-11-1111111111-2222222222-3333333333-3333
```

Salida:

```
{
    "Aliases": [
        "exampleAlias@site.awsapps.com",
        "exampleAlias1@site.awsapps.com"
    ]
}
```

- Para ver los detalles de la API, consulte ListAliases en la Referencia de comandos de la AWS CLI.

`list-group-members`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-group-members`.

AWS CLI

Para ver una lista de los miembros del grupo

El siguiente comando `list-group-members` enumera los miembros del grupo especificado.

```
aws workmail list-group-members \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --group-id S-1-1-11-1122222222-2222233333-3333334444-4444
```

Salida:

```
{
    "Members": [
        {
            "Id": "S-1-1-11-1111111111-2222222222-3333333333-3333",
            "Name": "exampleUser1",
            "Type": "USER",
            "State": "ENABLED",
            "EnabledDate": 1532459261.827
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListGroupMembers en la Referencia de comandos de la AWS CLI.

`list-groups`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-groups`.

AWS CLI

Para recuperar una lista de grupos

El siguiente comando `list-groups` recupera los resúmenes de los grupos de la organización especificada.

```
aws workmail list-groups \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27
```

Salida:

```
{
    "Groups": [
```

```
        {
            "Id": "S-1-1-11-1122222222-2222233333-3333334444-4444",
            "Name": "exampleGroup1",
            "State": "DISABLED"
        },
        {
            "Id": "S-4-4-44-1122222222-2222233333-3333334444-4444",
            "Name": "exampleGroup2",
            "State": "ENABLED"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListGroups en la Referencia de comandos de la AWS CLI.

`list-mailbox-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-mailbox-permissions`.

AWS CLI

Para recuperar permisos de buzón de correo

El siguiente comando `list-mailbox-permissions` recupera los permisos de buzón de correo asociados al buzón de correo de la entidad especificada.

```
aws workmail list-mailbox-permissions \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --entity-id S-1-1-11-1111111111-2222222222-3333333333-3333
```

Salida:

```
{
    "Permissions": [
        {
            "GranteeId": "S-1-1-11-1122222222-2222233333-3333334444-4444",
            "GranteeType": "USER",
            "PermissionValues": [
                "FULL_ACCESS"
            ]
        }
```

```
    ]
}
```

- Para obtener información sobre la API, consulte ListMailboxPermissions en la Referencia de comandos de la AWS CLI.

`list-organizations`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-organizations`.

AWS CLI

Para recuperar una lista de organizaciones

El siguiente comando `list-organizations` recupera los resúmenes de las organizaciones del cliente.

```
aws workmail list-organizations
```

Salida:

```
{
    "OrganizationSummaries": [
        {
            "OrganizationId": "m-d281d0a2fd824be5b6cd3d3ce909fd27",
            "Alias": "exampleAlias",
            "State": "Active"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListOrganizations en la Referencia de comandos de la AWS CLI.

`list-resource-delegates`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resource-delegates`.

AWS CLI

Para enumerar los delegados de un recurso

El siguiente comando `list-resource-delegates` recupera los delegados asociados al rol especificado.

```
aws workmail list-resource-delegates \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --resource-id r-68bf2d3b1c0244aab7264c24b9217443
```

Salida:

```
{
    "Delegates": [
        {
            "Id": "S-1-1-11-1111111111-2222222222-3333333333-3333",
            "Type": "USER"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListResourceDelegates en la Referencia de comandos de la AWS CLI.

`list-resources`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-resources`.

AWS CLI

Para recuperar una lista de recursos

El siguiente comando `list-resources` recupera los resúmenes de los recursos de la organización especificada.

```
aws workmail list-resources \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27
```

Salida:

```
{
    "Resources": [
        {
            "Id": "r-7afe0efbade843a58cdc10251fce992c",
```

```
            "Name": "exampleRoom1",
            "Type": "ROOM",
            "State": "ENABLED"
        }
    ]
}
```

- Para obtener más información sobre la API, consulte ListResources en la Referencia de comandos de la AWS CLI.

`list-tags-for-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-tags-for-resource`.

AWS CLI

Para enumerar las etiquetas de un recurso

En el siguiente ejemplo de `list-tags-for-resource`, se enumeran las etiquetas para la organización de Amazon WorkMail indicada.

```
aws workmail list-tags-for-resource \
    --resource-arn arn:aws:workmail:us-west-2:111122223333:organization/m-n1pq2345678r901st2u3vx45x6789yza
```

Salida:

```
{
    "Tags": [
        {
            "Key": "priority",
            "Value": "1"
        }
    ]
}
```

Para obtener más información, consulte Tagging an Organization en la Guía del administrador de Amazon WorkMail.

- Para ver los detalles de la API, consulte ListTagsForResource en la Referencia de comandos de la AWS CLI.

`list-users`

En el siguiente ejemplo de código, se muestra cómo utilizar `list-users`.

AWS CLI

Para recuperar una lista de usuarios

El siguiente comando `list-users` recupera los resúmenes de los usuarios de la organización especificada.

```
aws workmail list-users \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27
```

Salida:

```
{
    "Users": [
        {
            "Id": "S-1-1-11-1111111111-2222222222-3333333333-3333",
            "Email": "exampleUser1@site.awsapps.com",
            "Name": "exampleUser1",
            "State": "ENABLED",
            "UserRole": "USER",
            "EnabledDate": 1532459261.827
        },
        {
            "Id": "S-1-1-11-1122222222-2222233333-3333334444-4444",
            "Name": "exampleGuestUser",
            "State": "DISABLED",
            "UserRole": "SYSTEM_USER"
        }
    ]
}
```

- Para obtener información sobre la API, consulte ListUsers en la Referencia de comandos de la AWS CLI.

`put-access-control-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-access-control-rule`.

AWS CLI

Para crear una nueva regla de control de acceso

En el siguiente ejemplo de `put-access-control-rule`, se rechaza el acceso de usuario especificado de la organización de Amazon WorkMail indicada.

```
aws workmail put-access-control-rule \
    --name "myRule" \
    --effect "DENY" \
    --description "my rule" \
    --user-ids "S-1-1-11-1111111111-2222222222-3333333333-3333" \
    --organization-id m-n1pq2345678r901st2u3vx45x6789yza
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Working with Access Control Rules en la Guía del administrador de Amazon WorkMail.

- Para obtener información sobre la API, consulte PutAccessControlRule en la Referencia de comandos de la AWS CLI.

`put-mailbox-permissions`

En el siguiente ejemplo de código, se muestra cómo utilizar `put-mailbox-permissions`.

AWS CLI

Para definir permisos de buzón de correo

El siguiente comando `put-mailbox-permissions` establece los permisos de acceso total para el concesionario especificado (usuario o grupo). La entidad representa al propietario del buzón de correo.

```
aws workmail put-mailbox-permissions \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --entity-id S-1-1-11-1111111111-2222222222-3333333333-3333 \
    --grantee-id S-1-1-11-1122222222-2222233333-3333334444-4444 \
    --permission-values FULL_ACCESS
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte PutMailboxPermissions en la Referencia de comandos de la AWS CLI.

`register-to-work-mail`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-to-work-mail`.

AWS CLI

Para registrar una entidad existente o deshabilitada

El siguiente comando `register-to-work-mail` permite que la entidad existente especificada (usuario, grupo o recurso) utilice Amazon WorkMail.

```
aws workmail register-to-work-mail \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --entity-id S-1-1-11-1122222222-2222233333-3333334444-4444 \
    --email exampleGroup1@site.awsapps.com
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte RegisterToWorkMail en la Referencia de comandos de la AWS CLI.

`reset-password`

En el siguiente ejemplo de código, se muestra cómo utilizar `reset-password`.

AWS CLI

Para restablecer la contraseña de un usuario

El siguiente comando `reset-password` restablece la contraseña del usuario especificado.

```
aws workmail reset-password \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --user-id S-1-1-11-1111111111-2222222222-3333333333-3333 \
    --password examplePa$$w0rd
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte ResetPassword en la Referencia de comandos de la AWS CLI.

`tag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `tag-resource`.

AWS CLI

Para aplicar una etiqueta a un recurso

En el siguiente ejemplo de `tag-resource`, se aplica una etiqueta con la clave priority y el valor 1 a la organización de Amazon WorkMail especificada.

```
aws workmail tag-resource \
    --resource-arn arn:aws:workmail:us-west-2:111122223333:organization/m-n1pq2345678r901st2u3vx45x6789yza \
    --tags "Key=priority,Value=1"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging an Organization en la Guía del administrador de Amazon WorkMail.

- Para ver los detalles de la API, consulte TagResource en la Referencia de comandos de la AWS CLI.

`untag-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `untag-resource`.

AWS CLI

Para retirar la etiqueta de un recurso

En el siguiente ejemplo de `untag-resource`, se rechaza la etiqueta especificada de la organización de Amazon WorkMail indicada.

```
aws workmail untag-resource \
    --resource-arn arn:aws:workmail:us-west-2:111122223333:organization/m-n1pq2345678r901st2u3vx45x6789yza \
    --tag-keys "priority"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tagging an Organization en la Guía del administrador de Amazon WorkMail.

- Para ver los detalles de la API, consulte UntagResource en la Referencia de comandos de la AWS CLI.

`update-mailbox-quota`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-mailbox-quota`.

AWS CLI

Para actualizar la cuota de buzón de correo de un usuario

El siguiente comando `update-mailbox-quota` cambia la cuota de buzón de correo del usuario especificado.

```
aws workmail update-mailbox-quota \
    --organization-id m-n1pq2345678r901st2u3vx45x6789yza \
    --user-id S-1-1-11-1111111111-2222222222-3333333333-3333 \
    --mailbox-quota 40000
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Managing User Accounts en la Guía del administrador de Amazon WorkMail.

- Para obtener información acerca de la API, consulte UpdateMailboxQuota en la Referencia de comandos de la AWS CLI.

`update-primary-email-address`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-primary-email-address`.

AWS CLI

Para actualizar una dirección de correo electrónico principal

El siguiente comando `update-primary-email-address` actualiza la dirección de correo electrónico principal de la entidad especificada (usuario, grupo o recurso).

```
aws workmail update-primary-email-address \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --entity-id S-1-1-11-1111111111-2222222222-3333333333-3333 \
    --email exampleUser2@site.awsapps.com
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte UpdatePrimaryEmailAddress en la Referencia de comandos de la AWS CLI.

`update-resource`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-resource`.

AWS CLI

Para actualizar un recurso

El siguiente comando `update-resource` actualiza el nombre del recurso especificado.

```
aws workmail update-resource \
    --organization-id m-d281d0a2fd824be5b6cd3d3ce909fd27 \
    --resource-id r-7afe0efbade843a58cdc10251fce992c \
    --name exampleRoom2
```

Este comando no genera ninguna salida.

- Para obtener información sobre la API, consulte UpdateResource en la Referencia de comandos de la AWS CLI.

Ejemplos de flujo de mensajes de Amazon WorkMail que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando la AWS Command Line Interface con Amazon WorkMail Message Flow.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`get-raw-message-content`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-raw-message-content`.

AWS CLI

Para obtener el contenido sin procesar de un mensaje de correo electrónico

En el siguiente ejemplo de `get-raw-message-content`, se obtiene el contenido sin procesar de un mensaje de correo electrónico en tránsito y se envía a un archivo de texto denominado `test`.

```
aws workmailmessageflow get-raw-message-content \
    --message-id a1b2cd34-ef5g-6h7j-kl8m-npq9012345rs \
    test
```

Contenido del archivo `test` después de ejecutar el comando:

```
Subject: Hello World
From: =?UTF-8?Q?marymajor_marymajor?= <marymajor@example.com>
To: =?UTF-8?Q?mateojackson=40example=2Enet?= <mateojackson@example.net>
Date: Thu, 7 Nov 2019 19:22:46 +0000
Mime-Version: 1.0
Content-Type: multipart/alternative;
 boundary="=_EXAMPLE+"
References: <mail.1ab23c45.5de6.7f890g123hj45678@storage.wm.amazon.com>
X-Priority: 3 (Normal)
X-Mailer: Amazon WorkMail
Thread-Index: EXAMPLE
Thread-Topic: Hello World
Message-Id: <mail.1ab23c45.5de6.7f890g123hj45678@storage.wm.amazon.com>

This is a multi-part message in MIME format. Your mail reader does not
understand MIME message format.
```

```
--=_EXAMPLE+
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

hello world


--=_EXAMPLE+
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML><html>
<head>
<meta name=3D"Generator" content=3D"Amazon WorkMail v3.0-4510">
<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dutf-8">=

<title>testing</title>
</head>
<body>
<p style=3D"margin: 0px; font-family: Arial, Tahoma, Helvetica, sans-seri=
f; font-size: small;">hello world</p>
</body>
</html>
--=_EXAMPLE+--
```

Para obtener más información, consulte Retrieving Message Content with AWS Lambda en la Guía del administrador de Amazon WorkMail.

- Para obtener información sobre la API, consulte GetRawMessageContent en la Referencia de comandos de la AWS CLI.

Ejemplos de WorkSpaces que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con WorkSpaces.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`create-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-tags`.

AWS CLI

Para añadir etiquetas a un WorkSpace

En el siguiente ejemplo de `create-tags`, se agregan las etiquetas especificadas al WorkSpace indicado.

```
aws workspaces create-tags \
    --resource-id ws-dk1xzr417 \
    --tags Key=Department,Value=Finance
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tag WorkSpaces resources en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte CreateTags en la Referencia de comandos de la AWS CLI.

`create-workspaces`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-workspaces`.

AWS CLI

Ejemplo 1: creación de un WorkSpace AlwaysOn

En el siguiente ejemplo de `create-workspaces`, se crea un WorkSpace AlwaysOn para el usuario especificado con el directorio y el paquete indicados.

```
aws workspaces create-workspaces \
```

```
    --workspaces DirectoryId=d-926722edaf,UserName=Mateo,BundleId=wsb-0zsvgp8fc
```

Salida:

```
{
    "FailedRequests": [],
    "PendingRequests": [
        {
            "WorkspaceId": "ws-kcqms853t",
            "DirectoryId": "d-926722edaf",
            "UserName": "Mateo",
            "State": "PENDING",
            "BundleId": "wsb-0zsvgp8fc"
        }
    ]
}
```

Ejemplo 2: creación de un AutoStop WorkSpace

En el siguiente ejemplo de `create-workspaces`, se crea un AutoStop WorkSpace para el usuario especificado con el directorio y el paquete indicados.

```
aws workspaces create-workspaces \
    --
workspaces DirectoryId=d-926722edaf,UserName=Mary,BundleId=wsb-0zsvgp8fc,WorkspaceProperties
```

Salida:

```
{
    "FailedRequests": [],
    "PendingRequests": [
        {
            "WorkspaceId": "ws-dk1xzr417",
            "DirectoryId": "d-926722edaf",
            "UserName": "Mary",
            "State": "PENDING",
            "BundleId": "wsb-0zsvgp8fc"
        }
    ]
}
```

Ejemplo 3: creación de un WorkSpace desacoplado por el usuario

En el siguiente ejemplo de `create-workspaces`, se crea un WorkSpace desacoplado por el usuario. Para ello, se establece el nombre de usuario en `[UNDEFINED]` y se especifica un nombre de WorkSpace, un ID de directorio y un ID de paquete.

```
aws workspaces create-workspaces \
    --workspaces
 DirectoryId=d-926722edaf,UserName='"[UNDEFINED]"',WorkspaceName=MaryWorkspace1,BundleId=wsb
```

Salida:

```
{
    "FailedRequests": [],
    "PendingRequests": [
        {
            "WorkspaceId": "ws-abcd1234",
            "DirectoryId": "d-926722edaf",
            "UserName": "[UNDEFINED]",
            "State": "PENDING",
            "BundleId": "wsb-0zsvgp8fc",
            "WorkspaceName": "MaryWorkspace1"
        }
    ]
}
```

Para obtener más información, consulte Launch a virtual desktop en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte CreateWorkspaces en la Referencia de comandos de la AWS CLI.

`delete-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-tags`.

AWS CLI

Para eliminar una etiqueta de un WorkSpace

En el siguiente ejemplo de `delete-tags`, se elimina la etiqueta especificada del WorkSpace indicado.

```
aws workspaces delete-tags \
```

```
    --resource-id ws-dk1xzr417 \
    --tag-keys Department
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Tag WorkSpaces resources en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte DeleteTags en la Referencia de comandos de la AWS CLI.

`deregister-workspace-directory`

En el siguiente ejemplo de código, se muestra cómo utilizar `deregister-workspace-directory`.

AWS CLI

Para anular el registro de un directorio

En el siguiente ejemplo de `deregister-workspace-directory` se anula el registro del directorio indicado.

```
aws workspaces deregister-workspace-directory \
    --directory-id d-926722edaf
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Register a directory with WorkSpaces en la Guía de administración de Amazon WorkSpaces.

- Para obtener más información sobre la API, consulte DeregisterWorkspaceDirectory en la Referencia de comandos de la AWS CLI.

`describe-tags`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-tags`.

AWS CLI

Para describir las etiquetas para un WorkSpace

En el siguiente ejemplo de `describe-tags` se describen las etiquetas del WorkSpace especificado.

```
aws workspaces describe-tags \
    --resource-id ws-dk1xzr417
```

Salida:

```
{
    "TagList": [
        {
            "Key": "Department",
            "Value": "Finance"
        }
    ]
}
```

Para obtener más información, consulte Tag WorkSpaces resources en la Guía de administración de Amazon WorkSpaces.

- Para obtener detalles sobre la API, consulte DescribeTags en la Referencia de comandos de la AWS CLI.

`describe-workspace-bundles`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-workspace-bundles`.

AWS CLI

Para enumerar los paquetes proporcionados por Amazon

En el siguiente ejemplo de `describe-workspace-bundles`, se muestran los nombres e ID de los paquetes proporcionados por Amazon, en formato de tabla y ordenados por nombre.

```
aws workspaces describe-workspace-bundles \
    --owner AMAZON \
    --query "Bundles[*].[Name, BundleId]"
```

Salida:

```
[
```

```
    [
        "Standard with Amazon Linux 2",
        "wsb-clj85qzj1"
    ],
    [
        "Performance with Windows 10 (Server 2016 based)",
        "wsb-gm4d5tx2v"
    ],
    [
        "PowerPro with Windows 7",
        "wsb-1pzkp0bx4"
    ],
    [
        "Power with Amazon Linux 2",
        "wsb-2bs6k5lgn"
    ],
    [
        "Graphics with Windows 10 (Server 2019 based)",
        "wsb-03gyjnfyy"
    ],
    ...
]
```

Para obtener más información, consulte WorkSpaces bundles and images en la Guía de administración e Amazon WorkSpaces.

- Para obtener información sobre la API, consulte DescribeWorkspaceBundles en la Referencia de comandos de la AWS CLI.

`describe-workspace-directories`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-workspace-directories`.

AWS CLI

Para describir un directorio registrado

En el siguiente ejemplo de `describe-workspace-directories`, se describe el directorio registrado indicado.

```
aws workspaces describe-workspace-directories \
    --directory-ids d-926722edaf
```

Salida:


```
{
    "Directories": [
        {
            "DirectoryId": "d-926722edaf",
            "Alias": "d-926722edaf",
            "DirectoryName": "example.com",
            "RegistrationCode": "WSpdx+9RJ8JT",
            "SubnetIds": [
                "subnet-9d19c4c6",
                "subnet-500d5819"
            ],
            "DnsIpAddresses": [
                "172.16.1.140",
                "172.16.0.30"
            ],
            "CustomerUserName": "Administrator",
            "IamRoleId": "arn:aws:iam::123456789012:role/workspaces_DefaultRole",
            "DirectoryType": "SIMPLE_AD",
            "WorkspaceSecurityGroupId": "sg-0d89e927e5645d7c5",
            "State": "REGISTERED",
            "WorkspaceCreationProperties": {
                "EnableInternetAccess": false,
                "UserEnabledAsLocalAdministrator": true,
                "EnableMaintenanceMode": true
            },
            "WorkspaceAccessProperties": {
                "DeviceTypeWindows": "ALLOW",
                "DeviceTypeOsx": "ALLOW",
                "DeviceTypeWeb": "DENY",
                "DeviceTypeIos": "ALLOW",
                "DeviceTypeAndroid": "ALLOW",
                "DeviceTypeChromeOs": "ALLOW",
                "DeviceTypeZeroClient": "ALLOW",
                "DeviceTypeLinux": "DENY"
            },
            "Tenancy": "SHARED",
            "SelfservicePermissions": {
                "RestartWorkspace": "ENABLED",
                "IncreaseVolumeSize": "DISABLED",
                "ChangeComputeType": "DISABLED",
                "SwitchRunningMode": "DISABLED",
                "RebuildWorkspace": "DISABLED"
```

```
            }
        }
    ]
}
```

Para obtener más información, consulte Administrar directorios para WorkSpaces Personal en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte DescribeWorkspaceDirectories en la Referencia de comandos de la AWS CLI.

`describe-workspaces-connection-status`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-workspaces-connection-status`.

AWS CLI

Para describir el estado de la conexión de un WorkSpace

En el siguiente ejemplo de `describe-workspaces-connection-status`, se describe el estado de conexión del WorkSpace especificado.

```
aws workspaces describe-workspaces-connection-status \
    --workspace-ids ws-dk1xzr417
```

Salida:

```
{
    "WorkspacesConnectionStatus": [
        {
            "WorkspaceId": "ws-dk1xzr417",
            "ConnectionState": "CONNECTED",
            "ConnectionStateCheckTimestamp": 1662526214.744
        }
    ]
}
```

Para obtener más información, consulte Administer your WorkSpaces en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte DescribeWorkspacesConnectionStatus en la Referencia de comandos de la AWS CLI.

`describe-workspaces`

En el siguiente ejemplo de código, se muestra cómo utilizar `describe-workspaces`.

AWS CLI

Para describir un WorkSpace

En el siguiente ejemplo de `describe-workspaces`, se describe el WorkSpace especificado.

```
aws workspaces describe-workspaces \
    --workspace-ids ws-dk1xzr417
```

Salida:

```
{
    "Workspaces": [
        {
            "WorkspaceId": "ws-dk1xzr417",
            "DirectoryId": "d-926722edaf",
            "UserName": "Mary",
            "IpAddress": "172.16.0.175",
            "State": "STOPPED",
            "BundleId": "wsb-0zsvgp8fc",
            "SubnetId": "subnet-500d5819",
            "ComputerName": "WSAMZN-RBSLTTD9",
            "WorkspaceProperties": {
                "RunningMode": "AUTO_STOP",
                "RunningModeAutoStopTimeoutInMinutes": 60,
                "RootVolumeSizeGib": 80,
                "UserVolumeSizeGib": 10,
                "ComputeTypeName": "VALUE"
            },
            "ModificationStates": []
        }
    ]
}
```

Para obtener más información, consulte Administer your WorkSpaces en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte DescribeWorkspaces en la Referencia de comandos de la AWS CLI.

`migrate-workspace`

En el siguiente ejemplo de código, se muestra cómo utilizar `migrate-workspace`.

AWS CLI

Para migrar un WorkSpace

En el siguiente ejemplo de `migrate-workspace`, se migra el WorkSpace indicado al paquete especificado.

```
aws workspaces migrate-workspace \
    --source-workspace-id ws-dk1xzr417 \
    --bundle-id wsb-j4dky1gs4
```

Salida:

```
{
    "SourceWorkspaceId": "ws-dk1xzr417",
    "TargetWorkspaceId": "ws-x5h1lbkp5"
}
```

Para obtener más información, consulte Migrate a WorkSpace en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte MigrateWorkspace en la Referencia de comandos de la AWS CLI.

`modify-workspace-creation-properties`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-workspace-creation-properties`.

AWS CLI

Para modificar una propiedad de creación de WorkSpace de un directorio

En el siguiente ejemplo de `modify-workspace-creation-properties`, se habilita la propiedad `EnableInternetAccess` para el directorio especificado. Esto permite la asignación automática de direcciones IP públicas para los WorkSpaces creados para el directorio.

```
aws workspaces modify-workspace-creation-properties \
    --resource-id d-926722edaf \
    --workspace-creation-properties EnableInternetAccess=true
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Update directory details for your WorkSpaces en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte ModifyWorkspaceCreationProperties en la Referencia de comandos de la AWS CLI.

`modify-workspace-properties`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-workspace-properties`.

AWS CLI

Para modificar el modo de ejecución de un WorkSpaces

En el siguiente ejemplo de `modify-workspace-properties`, se establece el modo de ejecución del WorkSpace especificado en `AUTO_STOP`.

```
aws workspaces modify-workspace-properties \
    --workspace-id ws-dk1xzr417 \
    --workspace-properties RunningMode=AUTO_STOP
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Modify a WorkSpace en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte ModifyWorkspaceProperties en la Referencia de comandos de la AWS CLI.

`modify-workspace-state`

En el siguiente ejemplo de código, se muestra cómo utilizar `modify-workspace-state`.

AWS CLI

Para modificar el estado de un WorkSpace

En el siguiente ejemplo de `modify-workspace-state`, se establece el estado del WorkSpace especificado en `ADMIN_MAINTENANCE`.

```
aws workspaces modify-workspace-state \
    --workspace-id ws-dk1xzr417 \
    --workspace-state ADMIN_MAINTENANCE
```

Este comando no genera ninguna salida.

Para obtener más información, consulte WorkSpace maintenance en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte ModifyWorkspaceState en la Referencia de comandos de la AWS CLI.

`reboot-workspaces`

En el siguiente ejemplo de código, se muestra cómo utilizar `reboot-workspaces`.

AWS CLI

Para reiniciar un WorkSpace

En el siguiente ejemplo de `reboot-workspaces`, se reinicia el WorkSpace especificado.

```
aws workspaces reboot-workspaces \
    --reboot-workspace-requests ws-dk1xzr417
```

Salida:

```
{
    "FailedRequests": []
}
```

Para obtener más información, consulte Reboot a WorkSpace en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte RebootWorkspaces en la Referencia de comandos de la AWS CLI.

`rebuild-workspaces`

En el siguiente ejemplo de código, se muestra cómo utilizar `rebuild-workspaces`.

AWS CLI

Para reconstruir un WorkSpace

En el siguiente ejemplo de `rebuild-workspaces`, se reconstruye el WorkSpace especificado.

```
aws workspaces rebuild-workspaces \
    --rebuild-workspace-requests ws-dk1xzr417
```

Salida:

```
{
    "FailedRequests": []
}
```

Para obtener más información, consulte Rebuild a WorkSpace en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte RebuildWorkspaces en la referencia de comandos de la AWS CLI.

`register-workspace-directory`

En el siguiente ejemplo de código, se muestra cómo utilizar `register-workspace-directory`.

AWS CLI

Para registrar un directorio

En el siguiente ejemplo de `register-workspace-directory`, se registra el directorio especificado para usarlo con Amazon WorkSpaces.

```
aws workspaces register-workspace-directory \
    --directory-id d-926722edaf
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Registrar un directorio de AWS Directory Service existente con WorkSpaces Personal en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte RegisterWorkspaceDirectory en la Referencia de comandos de la AWS CLI.

`restore-workspace`

En el siguiente ejemplo de código, se muestra cómo utilizar `restore-workspace`.

AWS CLI

Para restaurar un WorkSpace

En el siguiente ejemplo de `restore-workspace`, se restablece el WorkSpace especificado.

```
aws workspaces restore-workspace \
    --workspace-id ws-dk1xzr417
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Restore a WorkSpace en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte RestoreWorkspace en la Referencia de comandos de la AWS CLI.

`start-workspaces`

En el siguiente ejemplo de código, se muestra cómo utilizar `start-workspaces`.

AWS CLI

Para iniciar un AutoStop WorkSpace

En el siguiente ejemplo de `start-workspaces`, se reinicia el WorkSpace especificado. El WorkSpace debe tener un modo de ejecución `AutoStop`.

```
aws workspaces start-workspaces \
    --start-workspace-requests WorkspaceId=ws-dk1xzr417
```

Salida:

```
{
    "FailedRequests": []
}
```

Para obtener más información, consulte Stop and start an AutoStop WorkSpace en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte StartWorkspaces en la Referencia de comandos de la AWS CLI.

`stop-workspaces`

En el siguiente ejemplo de código, se muestra cómo utilizar `stop-workspaces`.

AWS CLI

Para detener un AutoStop WorkSpace

En el siguiente ejemplo de `stop-workspaces`, se detiene el WorkSpace especificado. El WorkSpace debe tener un modo de ejecución `AutoStop`.

```
aws workspaces stop-workspaces \
    --stop-workspace-requests WorkspaceId=ws-dk1xzr417
```

Salida:

```
{
    "FailedRequests": []
}
```

Para obtener más información, consulte Stop and start an AutoStop WorkSpace en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte StopWorkspaces en la Referencia de comandos de la AWS CLI.

`terminate-workspaces`

En el siguiente ejemplo de código, se muestra cómo utilizar `terminate-workspaces`.

AWS CLI

Para terminar un WorkSpace

En el siguiente ejemplo de `terminate-workspaces`, finaliza el WorkSpace especificado.

```
aws workspaces terminate-workspaces \
    --terminate-workspace-requests ws-dk1xzr417
```

Salida:

```
{
    "FailedRequests": []
}
```

Para obtener más información, consulte Delete a WorkSpace en la Guía de administración de Amazon WorkSpaces.

- Para obtener información sobre la API, consulte TerminateWorkspaces en la Referencia de comandos de la AWS CLI.

Ejemplos de X-Ray que utilizan la AWS CLI

En los siguientes ejemplos de código se muestra cómo realizar acciones e implementar escenarios comunes usando AWS Command Line Interface con X-Ray.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`batch-traces-get`

En el siguiente ejemplo de código, se muestra cómo utilizar `batch-traces-get`.

AWS CLI

Para obtener una lista de rastros

En el siguiente ejemplo de `batch-get-traces`, se recupera una lista de rastros identificada por ID. El registro de seguimiento completo incluye un documento para cada segmento, compilado a partir de todos los documentos de segmento recibidos que tienen el mismo ID de registro de seguimiento.

```
aws xray batch-get-traces \
    --trace-ids 1-5d82881a-0a9126e92a73e971eed891b9
```

Salida:

```
{
    "Traces": [
        {
            "Id": "1-5d82881a-0a9126e92a73e971eed891b9",
            "Duration": 0.232,
            "Segments": [
                {
                    "Id": "54aff5735b12dd28",
                    "Document": "{\"id\":\"54aff5735b12dd28\",\"name\":
\"Scorekeep\",\"start_time\":1.568835610432E9,\"end_time\":1.568835610664E9,
\"http\":{\"request\":{\"url\":\"http://scorekeep-env-1.m4fg2pfzpv.us-
east-2.elasticbeanstalk.com/api/user\",\"method\":\"POST\",\"user_agent\":
\"curl/7.59.0\",\"client_ip\":\"52.95.4.28\",\"x_forwarded_for\":true},
\"response\":{\"status\":200}},\"aws\":{\"elastic_beanstalk\":{\"version_label
\":\"Sample Application-1\",\"deployment_id\":3,\"environment_name\":\"Scorekeep-
env-1\"},\"ec2\":{\"availability_zone\":\"us-east-2b\",\"instance_id\":
\"i-0e3cf4d2de0f3f37a\"},\"xray\":{\"sdk_version\":\"1.1.0\",\"sdk\":\"X-Ray for
 Java\"}},\"service\":{\"runtime\":\"OpenJDK 64-Bit Server VM\",\"runtime_version
\":\"1.8.0_222\"},\"trace_id\":\"1-5d82881a-0a9126e92a73e971eed891b9\",
\"origin\":\"AWS::ElasticBeanstalk::Environment\",\"subsegments\":[{\"id\":
\"2d6900034ccfe558\",\"name\":\"DynamoDB\",\"start_time\":1.568835610658E9,
\"end_time\":1.568835610664E9,\"http\":{\"response\":{\"status\":200,
\"content_length\":61}},\"aws\":{\"table_name\":\"scorekeep-user\",\"operation\":
\"UpdateItem\",\"request_id\":\"TPEIDNDUROMLPOV17U4A79555NVV4KQNSO5AEMVJF66Q9ASUAAJG
\",\"resource_names\":[\"scorekeep-user\"]},\"namespace\":\"aws\"}]}"
                },
                {
                    "Id": "0f278b6334c34e6b",
```

```
                    "Document": "{\"id\":\"0f278b6334c34e6b\",\"name\":
\"DynamoDB\",\"start_time\":1.568835610658E9,\"end_time\":1.568835610664E9,
\"parent_id\":\"2d6900034ccfe558\",\"inferred\":true,\"http\":{\"response
\":{\"status\":200,\"content_length\":61}},\"aws\":{\"table_name
\":\"scorekeep-user\",\"operation\":\"UpdateItem\",\"request_id\":
\"TPEIDNDUROMLPOV17U4A79555NVV4KQNSO5AEMVJF66Q9ASUAAJG\",\"resource_names\":
[\"scorekeep-user\"]},\"trace_id\":\"1-5d82881a-0a9126e92a73e971eed891b9\",\"origin
\":\"AWS::DynamoDB::Table\"}"
                }
            ]
        }
    ],
    "UnprocessedTraceIds": []
}
```

Para obtener más información, consulte Using the AWS X-Ray API with the AWS CLI en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información de la API, consulte BatchTracesGet en la Referencia de comandos de la AWS CLI.

`create-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-group`.

AWS CLI

Para crear un grupo

En el siguiente ejemplo de `create-group`, se crea un recurso de grupo llamado `AdminGroup`. El grupo obtiene una expresión de filtro que define los criterios del grupo como un segmento relacionado con un servicio específico que genera un error.

```
aws xray create-group \
   --group-name "AdminGroup" \
   --filter-expression "service(\"mydomain.com\") {fault OR error}"
```

Salida:

```
{
    "GroupName": "AdminGroup",
    "GroupARN": "arn:aws:xray:us-west-2:123456789012:group/AdminGroup/123456789",
```

```
    "FilterExpression": "service(\"mydomain.com\") {fault OR error}"
}
```

Para obtener más información, consulte Configuring Sampling, Groups, and Encryption Settings with the AWS X-Ray API en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información sobre la API, consulte CreateGroup en la Referencia de comandos de la AWS CLI.

`create-sampling-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `create-sampling-rule`.

AWS CLI

Para crear una regla de muestreo

En el siguiente ejemplo de `create-sampling-rule`, se crea una regla para controlar el comportamiento de muestreo para aplicaciones instrumentadas. Las reglas se proporcionan en un archivo JSON. La mayoría de los campos de la regla de muestreo son obligatorios para poder crear la regla.

```
aws xray create-sampling-rule \
    --cli-input-json file://9000-base-scorekeep.json
```

Contenido de `9000-base-scorekeep.json`:

```
{
    "SamplingRule": {
        "RuleName": "base-scorekeep",
        "ResourceARN": "*",
        "Priority": 9000,
        "FixedRate": 0.1,
        "ReservoirSize": 5,
        "ServiceName": "Scorekeep",
        "ServiceType": "*",
        "Host": "*",
        "HTTPMethod": "*",
        "URLPath": "*",
        "Version": 1
    }
}
```

Salida:

```
{
    "SamplingRuleRecord": {
        "SamplingRule": {
            "RuleName": "base-scorekeep",
            "RuleARN": "arn:aws:xray:us-west-2:123456789012:sampling-rule/base-
scorekeep",
            "ResourceARN": "*",
            "Priority": 9000,
            "FixedRate": 0.1,
            "ReservoirSize": 5,
            "ServiceName": "Scorekeep",
            "ServiceType": "*",
            "Host": "*",
            "HTTPMethod": "*",
            "URLPath": "*",
            "Version": 1,
            "Attributes": {}
        },
        "CreatedAt": 1530574410.0,
        "ModifiedAt": 1530574410.0
    }
}
```

Para obtener más información, consulte Configuring Sampling, Groups, and Encryption Settings with the AWS X-Ray API en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información sobre la API, consulte CreateSamplingRule en la Referencia de comandos de la AWS CLI.

`delete-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-group`.

AWS CLI

Para eliminar un grupo

En el siguiente ejemplo de `delete-group`, se elimina el recurso de grupo especificado.

```
aws xray delete-group \
```

```
    --group-name "AdminGroup" \
    --group-arn "arn:aws:xray:us-east-2:123456789012:group/AdminGroup/123456789"
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Configuring Sampling, Groups, and Encryption Settings with the AWS X-Ray API en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información sobre la API, consulte DeleteGroup en la Referencia de comandos de la AWS CLI.

`delete-sampling-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `delete-sampling-rule`.

AWS CLI

Para eliminar una regla de muestreo

En el siguiente ejemplo de `delete-sampling-rule`, se elimina la regla de muestreo especificada. Puede especificar el grupo mediante el nombre del grupo o el ARN del grupo.

```
aws xray delete-sampling-rule \
    --rule-name polling-scorekeep
```

Salida:

```
{
    "SamplingRuleRecord": {
        "SamplingRule": {
            "RuleName": "polling-scorekeep",
            "RuleARN": "arn:aws:xray:us-west-2:123456789012:sampling-rule/polling-
scorekeep",
            "ResourceARN": "*",
            "Priority": 5000,
            "FixedRate": 0.003,
            "ReservoirSize": 0,
            "ServiceName": "Scorekeep",
            "ServiceType": "*",
            "Host": "*",
            "HTTPMethod": "GET",
            "URLPath": "/api/state/*",
```

```
            "Version": 1,
            "Attributes": {}
        },
        "CreatedAt": 1530574399.0,
        "ModifiedAt": 1530574399.0
    }
}
```

Para obtener más información, consulte Configuring Sampling, Groups, and Encryption Settings with the AWS X-Ray API en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información sobre la API, consulte DeleteSamplingRule en la Referencia de comandos de la AWS CLI.

`get-encryption-config`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-encryption-config`.

AWS CLI

Para recuperar la configuración de cifrado

En el siguiente ejemplo de `get-encryption-config`, se recupera la configuración de cifrado actual para datos de AWS X-Ray.

```
aws xray get-encryption-config
```

Salida:

```
{
    "EncryptionConfig": {
        "KeyId": "ae4aa6d49-a4d8-9df9-a475-4ff6d7898456",
        "Status": "ACTIVE",
        "Type": "NONE"
    }
}
```

Para obtener más información, consulte Configuring Sampling, Groups, and Encryption Settings with the AWS X-Ray API en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información sobre la API, consulte GetEncryptionConfig en la Referencia de comandos de la AWS CLI.

get-group

En el siguiente ejemplo de código, se muestra cómo utilizar `get-group`.

AWS CLI

Para recuperar un grupo

En el siguiente ejemplo de `get-group`, se muestran los detalles del grupo de grupo especificado. Los detalles incluyen el nombre del grupo, el ARN del grupo y la expresión de filtro que define los criterios de ese grupo. El ARN también puede recuperar los grupos.

```
aws xray get-group \
    --group-name "AdminGroup"
```

Salida:

```
{
    "Group": [
        {
            "GroupName": "AdminGroup",
            "GroupARN": "arn:aws:xray:us-west-2:123456789012:group/
AdminGroup/123456789",
            "FilterExpression": "service(\"mydomain.com\") {fault OR error}"
        }
    ]
}
```

Para obtener más información, consulte Configuring Sampling, Groups, and Encryption Settings with the AWS X-Ray API en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información sobre la API, consulte GetGroup en la Referencia de comandos de la AWS CLI.

get-groups

En el siguiente ejemplo de código, se muestra cómo utilizar `get-groups`.

AWS CLI

Para recuperar todos los grupos

En el siguiente ejemplo, se muestran los detalles de todos los grupos activos.

```
aws xray get-groups
```

Salida:

```
{
    "Groups": [
        {
            "GroupName": "AdminGroup",
            "GroupARN": "arn:aws:xray:us-west-2:123456789012:group/
AdminGroup/123456789",
            "FilterExpression": "service(\"example.com\") {fault OR error}"
        },
        {
            "GroupName": "SDETGroup",
            "GroupARN": "arn:aws:xray:us-west-2:123456789012:group/
SDETGroup/987654321",
            "FilterExpression": "responsetime > 2"
        }
    ]
}
```

Para obtener más información, consulte Configuring Sampling, Groups, and Encryption Settings with the AWS X-Ray API en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información sobre la API, consulte GetGroups en la Referencia de comandos de la AWS CLI.

`get-sampling-rules`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-sampling-rules`.

AWS CLI

Para recuperar todas las reglas de muestreo

En el siguiente ejemplo de `get-sampling-rules`, se muestran los detalles de todas las reglas de muestreo disponibles.

```
aws xray get-sampling-rules
```

Salida:


```
{
    "SamplingRuleRecords": [
        {
            "SamplingRule": {
                "RuleName": "Default",
                "RuleARN": "arn:aws:xray:us-east-1::sampling-rule/Default",
                "ResourceARN": "*",
                "Priority": 10000,
                "FixedRate": 0.01,
                "ReservoirSize": 0,
                "ServiceName": "*",
                "ServiceType": "*",
                "Host": "*",
                "HTTPMethod": "*",
                "URLPath": "*",
                "Version": 1,
                "Attributes": {}
            },
            "CreatedAt": 0.0,
            "ModifiedAt": 1530558121.0
        },
        {
            "SamplingRule": {
                "RuleName": "base-scorekeep",
                "RuleARN": "arn:aws:xray:us-east-1::sampling-rule/base-scorekeep",
                "ResourceARN": "*",
                "Priority": 9000,
                "FixedRate": 0.1,
                "ReservoirSize": 2,
                "ServiceName": "Scorekeep",
                "ServiceType": "*",
                "Host": "*",
                "HTTPMethod": "*",
                "URLPath": "*",
                "Version": 1,
                "Attributes": {}
            },
            "CreatedAt": 1530573954.0,
            "ModifiedAt": 1530920505.0
        },
        {
            "SamplingRule": {
```

```
                "RuleName": "polling-scorekeep",
                "RuleARN": "arn:aws:xray:us-east-1::sampling-rule/polling-
scorekeep",
                "ResourceARN": "*",
                "Priority": 5000,
                "FixedRate": 0.003,
                "ReservoirSize": 0,
                "ServiceName": "Scorekeep",
                "ServiceType": "*",
                "Host": "*",
                "HTTPMethod": "GET",
                "URLPath": "/api/state/*",
                "Version": 1,
                "Attributes": {}
            },
            "CreatedAt": 1530918163.0,
            "ModifiedAt": 1530918163.0
        }
    ]
}
```

Para obtener más información, consulte Using Sampling Rules with the X-Ray API en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información sobre la API, consulte GetSamplingRules en la Referencia de comandos de la AWS CLI.

`get-sampling-targets`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-sampling-targets`.

AWS CLI

Para solicitar una cuota de muestreo

En el siguiente ejemplo de `get-sampling-targets`, se solicita una cuota de muestreo para las reglas que el servicio utiliza para muestrear solicitudes. La respuesta de AWS X-Ray incluye una cuota que se puede utilizar en lugar de tomarla prestada del bucket.

```
aws xray get-sampling-targets \
    --sampling-statistics-documents '[ { "RuleName": "base-scorekeep", "ClientID":
 "ABCDEF1234567890ABCDEF10", "Timestamp": "2018-07-07T00:20:06, "RequestCount": 110,
```

```
 "SampledCount": 20, "BorrowCount": 10 }, { "RuleName": "polling-scorekeep", 31,
 "BorrowCount": 0 } ]'
```

Salida:

```
{
    "SamplingTargetDocuments": [
        {
            "RuleName": "base-scorekeep",
            "FixedRate": 0.1,
            "ReservoirQuota": 2,
            "ReservoirQuotaTTL": 1530923107.0,
            "Interval": 10
        },
        {
            "RuleName": "polling-scorekeep",
            "FixedRate": 0.003,
            "ReservoirQuota": 0,
            "ReservoirQuotaTTL": 1530923107.0,
            "Interval": 10
        }
    ],
    "LastRuleModification": 1530920505.0,
    "UnprocessedStatistics": []
}
```

Para obtener más información, consulte Using Sampling Rules with the X-Ray API en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información sobre la API, consulte GetSamplingTargets en la Referencia de comandos de la AWS CLI.

`get-service-graph`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-service-graph`.

AWS CLI

Para obtener un gráfico de servicio

En el ejemplo siguiente se muestra un documento dentro de un período de tiempo determinado que describe los servicios que procesan solicitudes entrantes y los servicios posteriores a los que llaman como resultado.

```
aws xray get-service-graph \
    --start-time 1568835392.0
    --end-time 1568835446.0
```

Salida:

```
{
    "Services": [
        {
            "ReferenceId": 0,
            "Name": "Scorekeep",
            "Names": [
                "Scorekeep"
            ],
            "Root": true,
            "Type": "AWS::ElasticBeanstalk::Environment",
            "State": "active",
            "StartTime": 1568835392.0,
            "EndTime": 1568835446.0,
            "Edges": [
                {
                    "ReferenceId": 1,
                    "StartTime": 1568835392.0,
                    "EndTime": 1568835446.0,
                    "SummaryStatistics": {
                        "OkCount": 14,
                        "ErrorStatistics": {
                            "ThrottleCount": 0,
                            "OtherCount": 0,
                            "TotalCount": 0
                        },
                        "FaultStatistics": {
                            "OtherCount": 0,
                            "TotalCount": 0
                        },
                        "TotalCount": 14,
                        "TotalResponseTime": 0.13
                    },
                    "ResponseTimeHistogram": [
```

```
                        {
                            "Value": 0.008,
                            "Count": 1
                        },
                        {
                            "Value": 0.005,
                            "Count": 7
                        },
                        {
                            "Value": 0.009,
                            "Count": 1
                        },
                        {
                            "Value": 0.021,
                            "Count": 1
                        },
                        {
                            "Value": 0.038,
                            "Count": 1
                        },
                        {
                            "Value": 0.007,
                            "Count": 1
                        },
                        {
                            "Value": 0.006,
                            "Count": 2
                        }
                    ],
                    "Aliases": []
                },

                ... TRUNCATED FOR BREVITY ...

            ]
        }
    ],
    "StartTime": 1568835392.0,
    "EndTime": 1568835446.0,
    "ContainsOldGroupVersions": false
}
```

Para obtener más información, consulte Using the AWS X-Ray API with the AWS CLI en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información sobre la API, consulte GetServiceGraph en la Referencia de comandos de la AWS CLI.

`get-trace-summaries`

En el siguiente ejemplo de código, se muestra cómo utilizar `get-trace-summaries`.

AWS CLI

Para obtener un resumen del rastro

En el siguiente ejemplo de `get-trace-summaries`, se recuperan los ID y los metadatos de los rastros disponibles dentro de un período de tiempo determinado.

```
aws xray get-trace-summaries \
    --start-time 1568835392.0 \
    --end-time 1568835446.0
```

Salida:

```
[
    "http://scorekeep-env-1.123456789.us-east-2.elasticbeanstalk.com/api/move/
VSAE93HF/GSSD2NTB/DP0PCC09",
    "http://scorekeep-env-1.123456789.us-east-2.elasticbeanstalk.com/api/move/
GCQ2B35P/FREELDFT/4LRE643M",
    "http://scorekeep-env-1.123456789.us-east-2.elasticbeanstalk.com/api/game/
VSAE93HF/GSSD2NTB/starttime/1568835513",
    "http://scorekeep-env-1.123456789.us-east-2.elasticbeanstalk.com/api/
move/4MQNA5NN/L99KK2RF/null"
]
```

Para obtener más información, consulte Using the AWS X-Ray API with the AWS CLI en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información sobre la API, consulte GetTraceSummaries en la Referencia de comandos de la AWS CLI.

put-encryption-config

En el siguiente ejemplo de código, se muestra cómo utilizar `put-encryption-config`.

AWS CLI

Para actualizar la configuración de cifrado

El siguiente `put-encryption-config``example updates the encryption configuration for AWS X-Ray data to use the default AWS managed KMS key ``aws/xray`.

```
aws xray put-encryption-config \
    --type KMS \
    --key-id alias/aws/xray
```

Salida:

```
{
    "EncryptionConfig": {
        "KeyId": "arn:aws:kms:us-west-2:123456789012:key/c234g4e8-39e9-4gb0-84e2-
b0ea215cbba5",
        "Status": "UPDATING",
        "Type": "KMS"
    }
}
```

Para obtener más información, consulte Configuring Sampling, Groups, and Encryption Settings with the AWS X-Ray API en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información sobre la API, consulte PutEncryptionConfig en la Referencia de comandos de la AWS CLI.

put-trace-segments

En el siguiente ejemplo de código, se muestra cómo utilizar `put-trace-segments`.

AWS CLI

Para cargar un segmento

En el siguiente ejemplo de `put-trace-segments`, se cargan documentos segmentados a AWS X-Ray. El documento segmentado se consume como una lista de documentos segmentados JSON.

```
aws xray put-trace-segments \
    --trace-segment-documents "{\"id\":\"20312a0e2b8809f4\",\"name
\":\"DynamoDB\",\"trace_id\":\"1-5832862d-a43aafded3334a971fe312db\",
\"start_time\":1.479706157195E9,\"end_time\":1.479706157202E9,\"parent_id\":
\"79736b962fe3239e\",\"http\":{\"response\":{\"content_length\":60,\"status
\":200}},\"inferred\":true,\"aws\":{\"consistent_read\":false,\"table_name
\":\"scorekeep-session-xray\",\"operation\":\"GetItem\",\"request_id\":
\"SCAU23OM6M8FO38UASGC7785ARVV4KQNSO5AEMVJF66Q9ASUAAJG\",\"resource_names\":
[\"scorekeep-session-xray\"]},\"origin\":\"AWS::DynamoDB::Table\"}"
```

Salida:

```
{
    "UnprocessedTraceSegments": []
}
```

Para obtener más información, consulte Sending Trace Data to AWS X-Ray en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información sobre la API, consulte PutTraceSegments en la Referencia de comandos de la AWS CLI.

`update-group`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-group`.

AWS CLI

Para actualizar un grupo

En el siguiente ejemplo de `update-group`, se actualizan los criterios para aceptar los rastros en el grupo denominado `AdminGroup`. Puede especificar el grupo deseado mediante el nombre del grupo o el ARN del grupo.

```
aws xray update-group \
    --group-name "AdminGroup" \
```

```
    --group-arn "arn:aws:xray:us-west-2:123456789012:group/AdminGroup/123456789" \
    --filter-expression "service(\"mydomain.com\") {fault}"
```

Salida:

```
{
    "GroupName": "AdminGroup",
    "GroupARN": "arn:aws:xray:us-east-2:123456789012:group/AdminGroup/123456789",
    "FilterExpression": "service(\"mydomain.com\") {fault}"
}
```

Para obtener más información, consulte Configuring Sampling, Groups, and Encryption Settings with the AWS X-Ray API en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información sobre la API, consulte UpdateGroup en la Referencia de comandos de la AWS CLI.

`update-sampling-rule`

En el siguiente ejemplo de código, se muestra cómo utilizar `update-sampling-rule`.

AWS CLI

Para actualizar una regla de muestreo

En el siguiente ejemplo de `update-sampling-rule`, se modifica la configuración de una regla de muestreo. Las reglas se consumen desde un archivo JSON. Solo son obligatorios los campos que se están actualizando.

```
aws xray update-sampling-rule \
   --cli-input-json file://1000-default.json
```

Contenido de `1000-default.json`:

```
{
    "SamplingRuleUpdate": {
        "RuleName": "Default",
        "FixedRate": 0.01,
        "ReservoirSize": 0
    }
```

```
}
```

Salida:

```
{
    "SamplingRuleRecords": [
        {
            "SamplingRule": {
                "RuleName": "Default",
                "RuleARN": "arn:aws:xray:us-west-2:123456789012:sampling-rule/
Default",
                "ResourceARN": "*",
                "Priority": 10000,
                "FixedRate": 0.01,
                "ReservoirSize": 0,
                "ServiceName": "*",
                "ServiceType": "*",
                "Host": "*",
                "HTTPMethod": "*",
                "URLPath": "*",
                "Version": 1,
                "Attributes": {}
            },
            "CreatedAt": 0.0,
            "ModifiedAt": 1529959993.0
        }
   ]
}
```

Para obtener más información, consulte Configuring Sampling, Groups, and Encryption Settings with the AWS X-Ray API en la Guía para desarrolladores de AWS X-Ray.

- Para obtener información acerca de la API, consulte UpdateSamplingRule en la Referencia de comandos de la AWS CLI.

Ejemplos de código de la AWS CLI con script Bash

Los ejemplos de código de este tema muestran cómo utilizar AWS Command Line Interface con script Bash con AWS.

Los conceptos básicos son ejemplos de código que muestran cómo realizar las operaciones esenciales dentro de un servicio.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica a través de llamadas a varias funciones dentro del servicio o combinado con otros Servicios de AWS.

Algunos servicios contienen categorías de ejemplo adicionales que muestran cómo aprovechar las bibliotecas o funciones específicas del servicio.

Services

- Ejemplos de AWS Batch que utilizan la AWS CLI con el script Bash
- Ejemplos de AWS Cloud Map que utilizan la AWS CLI con el script Bash
- Ejemplos de CloudFront que utilizan la AWS CLI con el script Bash
- Ejemplos de DynamoDB que utilizan la AWS CLI con el script Bash
- Ejemplos de Amazon EC2 que utilizan la AWS CLI con el script Bash
- Ejemplos de HealthImaging que utilizan la AWS CLI con el script Bash
- Ejemplos de IAM que utilizan la AWS CLI con el script Bash
- Ejemplos de AWS KMS que utilizan la AWS CLI con el script Bash
- Ejemplos de Lightsail que utilizan la AWS CLI con el script Bash
- Ejemplos de Amazon S3 que utilizan la AWS CLI con el script Bash
- Ejemplos de AWS STS que utilizan la AWS CLI con el script Bash

Ejemplos de AWS Batch que utilizan la AWS CLI con el script Bash

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante AWS Command Line Interface con el script Bash con AWS Batch.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica a través de llamadas a varias funciones dentro del servicio o combinado con otros Servicios de AWS.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Escenarios

Escenarios

Introducción a Batch y Fargate

En el siguiente ejemplo de código, se muestra cómo:

- Creación de un rol de ejecución de tareas para tareas de ECS
- Creación de un entorno informático de Fargate administrado
- Creación de una cola de trabajos con ajustes de prioridad
- Registro de una definición de trabajo para cargas de trabajo en contenedores
- Envío y supervisión de la ejecución de un trabajo por lotes
- Visualización de resultados de trabajos en registros de CloudWatch
- Eliminación de los recursos en el orden de dependencia adecuado

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Encuentre el ejemplo completo y obtenga información sobre cómo configurarlo y ejecutarlo en el repositorio de Tutoriales para desarrolladores de ejemplo.

```
#!/bin/bash

# AWS Batch Fargate Getting Started Script - Fixed Version
# This script demonstrates creating AWS Batch resources with Fargate orchestration
#
# HIGH SEVERITY FIXES APPLIED:
# 1. Added IAM role propagation delay after role creation
# 2. Added resource state validation before deletion attempts

set -e  # Exit on any error

# Configuration
SCRIPT_NAME="batch-fargate-tutorial"
LOG_FILE="${SCRIPT_NAME}-$(date +%Y%m%d-%H%M%S).log"
RANDOM_SUFFIX=$(openssl rand -hex 6)
COMPUTE_ENV_NAME="batch-fargate-compute-${RANDOM_SUFFIX}"
JOB_QUEUE_NAME="batch-fargate-queue-${RANDOM_SUFFIX}"
```

```
JOB_DEF_NAME="batch-fargate-jobdef-${RANDOM_SUFFIX}"
JOB_NAME="batch-hello-world-${RANDOM_SUFFIX}"
ROLE_NAME="BatchEcsTaskExecutionRole-${RANDOM_SUFFIX}"
TRUST_POLICY_FILE="batch-trust-policy-${RANDOM_SUFFIX}.json"

# Array to track created resources for cleanup
CREATED_RESOURCES=()

# Logging function
log() {
    echo "[$(date '+%Y-%m-%d %H:%M:%S')] $1" | tee -a "$LOG_FILE"
}

# Error handling function
handle_error() {
    log "ERROR: Script failed at line $1"
    log "Attempting to clean up resources created so far..."
    cleanup_resources
    exit 1
}

# Set up error handling
trap 'handle_error $LINENO' ERR

# Function to wait for resource to be ready
wait_for_compute_env() {
    local env_name=$1
    log "Waiting for compute environment $env_name to be VALID..."

    while true; do
        local status=$(aws batch describe-compute-environments \
            --compute-environments "$env_name" \
            --query 'computeEnvironments[0].status' \
            --output text 2>/dev/null || echo "NOT_FOUND")

        if [ "$status" = "VALID" ]; then
            log "Compute environment $env_name is ready"
            break
        elif [ "$status" = "INVALID" ] || [ "$status" = "NOT_FOUND" ]; then
            log "ERROR: Compute environment $env_name failed to create properly"
            return 1
        fi

        log "Compute environment status: $status. Waiting 10 seconds..."
```

```
        sleep 10
    done
}

# Function to wait for job queue to be ready
wait_for_job_queue() {
    local queue_name=$1
    log "Waiting for job queue $queue_name to be VALID..."

    while true; do
        local state=$(aws batch describe-job-queues \
            --job-queues "$queue_name" \
            --query 'jobQueues[0].state' \
            --output text 2>/dev/null || echo "NOT_FOUND")

        if [ "$state" = "ENABLED" ]; then
            log "Job queue $queue_name is ready"
            break
        elif [ "$state" = "DISABLED" ] || [ "$state" = "NOT_FOUND" ]; then
            log "ERROR: Job queue $queue_name failed to create properly"
            return 1
        fi

        log "Job queue state: $state. Waiting 10 seconds..."
        sleep 10
    done
}

# Function to wait for job completion
wait_for_job() {
    local job_id=$1
    log "Waiting for job $job_id to complete..."

    while true; do
        local status=$(aws batch describe-jobs \
            --jobs "$job_id" \
            --query 'jobs[0].status' \
            --output text 2>/dev/null || echo "NOT_FOUND")

        if [ "$status" = "SUCCEEDED" ]; then
            log "Job $job_id completed successfully"
            break
        elif [ "$status" = "FAILED" ]; then
            log "ERROR: Job $job_id failed"
```

```
            return 1
        fi

        log "Job status: $status. Waiting 30 seconds..."
        sleep 30
    done
}

# FIXED: Added function to wait for resource state before deletion
wait_for_resource_state() {
    local resource_type=$1
    local resource_name=$2
    local expected_state=$3
    local max_attempts=30
    local attempt=0

    log "Waiting for $resource_type $resource_name to reach state: $expected_state"

    while [ $attempt -lt $max_attempts ]; do
        local current_state=""

        case $resource_type in
            "JOB_QUEUE")
                current_state=$(aws batch describe-job-queues \
                    --job-queues "$resource_name" \
                    --query 'jobQueues[0].state' \
                    --output text 2>/dev/null || echo "NOT_FOUND")
                ;;
            "COMPUTE_ENV")
                current_state=$(aws batch describe-compute-environments \
                    --compute-environments "$resource_name" \
                    --query 'computeEnvironments[0].status' \
                    --output text 2>/dev/null || echo "NOT_FOUND")
                ;;
        esac

        if [ "$current_state" = "$expected_state" ]; then
            log "$resource_type $resource_name is now in state: $expected_state"
            return 0
        fi

        log "$resource_type $resource_name state: $current_state (waiting for
 $expected_state)"
        sleep 10
```

```
        ((attempt++))
    done

    log "WARNING: $resource_type $resource_name did not reach expected state after
 $max_attempts attempts"
    return 1
}

# Cleanup function
cleanup_resources() {
    log "Starting cleanup of created resources..."

    # Clean up in reverse order of creation
    for ((i=${#CREATED_RESOURCES[@]}-1; i>=0; i--)); do
        local resource="${CREATED_RESOURCES[i]}"
        local resource_type=$(echo "$resource" | cut -d: -f1)
        local resource_name=$(echo "$resource" | cut -d: -f2)

        log "Cleaning up $resource_type: $resource_name"

        case $resource_type in
            "JOB_QUEUE")
                # FIXED: Validate state before deletion
                aws batch update-job-queue --job-queue "$resource_name" --state
 DISABLED 2>/dev/null || true
                wait_for_resource_state "JOB_QUEUE" "$resource_name" "DISABLED" ||
 true
                aws batch delete-job-queue --job-queue "$resource_name" 2>/dev/null
 || true
                ;;
            "COMPUTE_ENV")
                # FIXED: Validate state before deletion
                aws batch update-compute-environment --compute-environment
 "$resource_name" --state DISABLED 2>/dev/null || true
                wait_for_resource_state "COMPUTE_ENV" "$resource_name" "DISABLED" ||
 true
                aws batch delete-compute-environment --compute-environment
 "$resource_name" 2>/dev/null || true
                ;;
            "IAM_ROLE")
                aws iam detach-role-policy --role-name "$resource_name" --policy-arn
 "arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy" 2>/dev/null
 || true
                aws iam delete-role --role-name "$resource_name" 2>/dev/null || true
```

```
                ;;
            "FILE")
                rm -f "$resource_name" 2>/dev/null || true
                ;;
        esac
    done

    log "Cleanup completed"
}

# Main script execution
main() {
    log "Starting AWS Batch Fargate tutorial script - Fixed Version"
    log "Log file: $LOG_FILE"

    # Get AWS account ID
    log "Getting AWS account ID..."
    ACCOUNT_ID=$(aws sts get-caller-identity --query Account --output text)
    log "Account ID: $ACCOUNT_ID"

    # Get default VPC and subnets
    log "Getting default VPC and subnets..."
    DEFAULT_VPC=$(aws ec2 describe-vpcs \
        --filters "Name=is-default,Values=true" \
        --query 'Vpcs[0].VpcId' \
        --output text)

    if [ "$DEFAULT_VPC" = "None" ] || [ "$DEFAULT_VPC" = "null" ]; then
        log "ERROR: No default VPC found. Please create a VPC first."
        exit 1
    fi

    log "Default VPC: $DEFAULT_VPC"

    # Get subnets in the default VPC
    SUBNETS=$(aws ec2 describe-subnets \
        --filters "Name=vpc-id,Values=$DEFAULT_VPC" \
        --query 'Subnets[*].SubnetId' \
        --output text)

    if [ -z "$SUBNETS" ]; then
        log "ERROR: No subnets found in default VPC"
        exit 1
    fi
```

```
    # Convert tab/space-separated subnets to JSON array format
    SUBNET_ARRAY=$(echo "$SUBNETS" | tr '\t ' '\n' | sed 's/^/"/;s/$/"/' | paste -sd
 ',' -)
    log "Subnets: $SUBNETS"
    log "Subnet array: [$SUBNET_ARRAY]"

    # Get default security group for the VPC
    DEFAULT_SG=$(aws ec2 describe-security-groups \
        --filters "Name=vpc-id,Values=$DEFAULT_VPC" "Name=group-name,Values=default"
 \
        --query 'SecurityGroups[0].GroupId' \
        --output text)

    if [ "$DEFAULT_SG" = "None" ] || [ "$DEFAULT_SG" = "null" ]; then
        log "ERROR: No default security group found in VPC"
        exit 1
    fi

    log "Default security group: $DEFAULT_SG"

    # Step 1: Create IAM execution role
    log "Step 1: Creating IAM execution role..."

    # Create trust policy document
    cat > "$TRUST_POLICY_FILE" << EOF
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ecs-tasks.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
    CREATED_RESOURCES+=("FILE:$TRUST_POLICY_FILE")

    # Create the role
    aws iam create-role \
        --role-name "$ROLE_NAME" \
```

```
        --assume-role-policy-document "file://$TRUST_POLICY_FILE"
    CREATED_RESOURCES+=("IAM_ROLE:$ROLE_NAME")

    # Attach policy
    aws iam attach-role-policy \
        --role-name "$ROLE_NAME" \
        --policy-arn "arn:aws:iam::aws:policy/service-role/
AmazonECSTaskExecutionRolePolicy"

    log "IAM role created: $ROLE_NAME"

    # FIXED: Wait for IAM role propagation
    log "Waiting for IAM role propagation (15 seconds)..."
    sleep 15

    # Step 2: Create compute environment
    log "Step 2: Creating Fargate compute environment..."

    aws batch create-compute-environment \
        --compute-environment-name "$COMPUTE_ENV_NAME" \
        --type MANAGED \
        --state ENABLED \
        --compute-resources "{
            \"type\": \"FARGATE\",
            \"maxvCpus\": 256,
            \"subnets\": [$SUBNET_ARRAY],
            \"securityGroupIds\": [\"$DEFAULT_SG\"]
        }"
    CREATED_RESOURCES+=("COMPUTE_ENV:$COMPUTE_ENV_NAME")

    # Wait for compute environment to be ready
    wait_for_compute_env "$COMPUTE_ENV_NAME"

    # Step 3: Create job queue
    log "Step 3: Creating job queue..."

    aws batch create-job-queue \
        --job-queue-name "$JOB_QUEUE_NAME" \
        --state ENABLED \
        --priority 900 \
        --compute-environment-order order=1,computeEnvironment="$COMPUTE_ENV_NAME"
    CREATED_RESOURCES+=("JOB_QUEUE:$JOB_QUEUE_NAME")

    # Wait for job queue to be ready
```

```
wait_for_job_queue "$JOB_QUEUE_NAME"

# Step 4: Create job definition
log "Step 4: Creating job definition..."

aws batch register-job-definition \
    --job-definition-name "$JOB_DEF_NAME" \
    --type container \
    --platform-capabilities FARGATE \
    --container-properties "{
        \"image\": \"busybox\",
        \"resourceRequirements\": [
            {\"type\": \"VCPU\", \"value\": \"0.25\"},
            {\"type\": \"MEMORY\", \"value\": \"512\"}
        ],
        \"command\": [\"echo\", \"hello world\"],
        \"networkConfiguration\": {
            \"assignPublicIp\": \"ENABLED\"
        },
        \"executionRoleArn\": \"arn:aws:iam::${ACCOUNT_ID}:role/${ROLE_NAME}\"
    }"

log "Job definition created: $JOB_DEF_NAME"

# Step 5: Submit job
log "Step 5: Submitting job..."

JOB_ID=$(aws batch submit-job \
    --job-name "$JOB_NAME" \
    --job-queue "$JOB_QUEUE_NAME" \
    --job-definition "$JOB_DEF_NAME" \
    --query 'jobId' \
    --output text)

log "Job submitted with ID: $JOB_ID"

# Step 6: Wait for job completion and view output
log "Step 6: Waiting for job completion..."
wait_for_job "$JOB_ID"

# Get log stream name
log "Getting job logs..."
LOG_STREAM=$(aws batch describe-jobs \
    --jobs "$JOB_ID" \
```

```
        --query 'jobs[0].attempts[0].taskProperties.containers[0].logStreamName' \
        --output text)

    if [ "$LOG_STREAM" != "None" ] && [ "$LOG_STREAM" != "null" ]; then
        log "Log stream: $LOG_STREAM"
        log "Job output:"
        aws logs get-log-events \
            --log-group-name "/aws/batch/job" \
            --log-stream-name "$LOG_STREAM" \
            --query 'events[*].message' \
            --output text | tee -a "$LOG_FILE"
    else
        log "No log stream available for job"
    fi

    log "Tutorial completed successfully!"

    # Show created resources
    echo ""
    echo "========================================="
    echo "CREATED RESOURCES"
    echo "========================================="
    echo "The following resources were created:"
    for resource in "${CREATED_RESOURCES[@]}"; do
        echo "  - $resource"
    done
    echo ""
    echo "========================================="
    echo "CLEANUP CONFIRMATION"
    echo "========================================="
    echo "Do you want to clean up all created resources? (y/n): "
    read -r CLEANUP_CHOICE

    if [[ "$CLEANUP_CHOICE" =~ ^[Yy]$ ]]; then
        cleanup_resources
        log "All resources have been cleaned up"
    else
        log "Resources left intact. You can clean them up manually later."
        echo "To clean up manually, run the following commands:"
        echo "aws batch update-job-queue --job-queue $JOB_QUEUE_NAME --state
DISABLED"
        echo "aws batch delete-job-queue --job-queue $JOB_QUEUE_NAME"
        echo "aws batch update-compute-environment --compute-environment
$COMPUTE_ENV_NAME --state DISABLED"
```

```
        echo "aws batch delete-compute-environment --compute-environment
 $COMPUTE_ENV_NAME"
        echo "aws iam detach-role-policy --role-name $ROLE_NAME --policy-arn
 arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy"
        echo "aws iam delete-role --role-name $ROLE_NAME"
    fi
}

# Run main function
main "$@"
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreateComputeEnvironment
  - CreateJobQueue
  - DeleteComputeEnvironment
  - DeleteJobQueue
  - DescribeComputeEnvironments
  - DescribeJobQueues
  - DescribeJobs
  - RegisterJobDefinition
  - SubmitJob
  - UpdateComputeEnvironment
  - UpdateJobQueue

Ejemplos de AWS Cloud Map que utilizan la AWS CLI con el script Bash

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante AWS Command Line Interface con el script Bash con AWS Cloud Map.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica a través de llamadas a varias funciones dentro del servicio o combinado con otros Servicios de AWS.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Escenarios

Escenarios

Atributos personalizados de Cloud Map

En el siguiente ejemplo de código, se muestra cómo:

- Creación de un espacio de nombres HTTP para la detección de servicios basada en API
- Creación de una tabla de DynamoDB y registro de la misma como un servicio de datos con atributos personalizados
- Creación de funciones de Lambda para lectura y escritura de datos
- Registro de las funciones de Lambda como instancias de servicio con atributos personalizados para una detección basada en acciones
- Creación de aplicaciones de clientes que detectan servicios mediante atributos personalizados
- Eliminación de todos los recursos, incluidas las funciones de Lambda, la tabla de DynamoDB y los servicios de Cloud Map

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Encuentre el ejemplo completo y obtenga información sobre cómo configurarlo y ejecutarlo en el repositorio de Tutoriales para desarrolladores de ejemplo.

```
#!/bin/bash

# AWS Cloud Map Tutorial Script
# This script demonstrates how to use AWS Cloud Map for service discovery with
 custom attributes

# Set up logging
LOG_FILE="cloudmap-tutorial.log"
echo "AWS Cloud Map Tutorial Script" > $LOG_FILE
echo "Started at $(date)" >> $LOG_FILE
```

```
# Array to track created resources for cleanup
CREATED_RESOURCES=()

# Function to log commands and their output
log_cmd() {
  echo "$ $1" | tee -a $LOG_FILE
  eval "$1" | tee -a $LOG_FILE
}

# Function to handle errors
handle_error() {
  local LINE=$1
  echo "An error occurred at line $LINE" | tee -a $LOG_FILE
  echo "Resources created so far:" | tee -a $LOG_FILE
  for resource in "${CREATED_RESOURCES[@]}"; do
    echo "- $resource" | tee -a $LOG_FILE
  done
  echo "Attempting to clean up resources..." | tee -a $LOG_FILE
  cleanup
  exit 1
}

# Set up error handling
trap 'handle_error $LINENO' ERR

# Helper function to wait for Cloud Map operations to complete
wait_for_operation() {
  local OPERATION_ID=$1
  local TIMEOUT=300  # 5 minutes timeout
  local START_TIME=$(date +%s)

  while true; do
    local STATUS=$(aws servicediscovery get-operation --operation-id $OPERATION_ID
 --query 'Operation.Status' --output text)

    if [ "$STATUS" == "SUCCESS" ]; then
      echo "Operation completed successfully" | tee -a $LOG_FILE
      break
    elif [ "$STATUS" == "FAIL" ]; then
      echo "Operation failed" | tee -a $LOG_FILE
      return 1
    fi

    local CURRENT_TIME=$(date +%s)
```

```
    if [ $((CURRENT_TIME - START_TIME)) -gt $TIMEOUT ]; then
      echo "Operation timed out" | tee -a $LOG_FILE
      return 1
    fi

    sleep 5
  done

  return 0
}

# Function to clean up resources
cleanup() {
  echo "Cleaning up resources..." | tee -a $LOG_FILE

  # Reverse the order of created resources for proper deletion
  for ((i=${#CREATED_RESOURCES[@]}-1; i>=0; i--)); do
    resource="${CREATED_RESOURCES[$i]}"
    echo "Deleting $resource..." | tee -a $LOG_FILE

    if [[ $resource == "instance:"* ]]; then
      # Extract service ID and instance ID
      SERVICE_ID=$(echo $resource | cut -d':' -f2)
      INSTANCE_ID=$(echo $resource | cut -d':' -f3)

      # Check if instance exists before trying to deregister
      INSTANCE_EXISTS=$(aws servicediscovery list-instances --service-id $SERVICE_ID
 --query "Instances[?Id=='$INSTANCE_ID'].Id" --output text 2>/dev/null || echo "")
      if [[ -n "$INSTANCE_EXISTS" ]]; then
        OPERATION_ID=$(aws servicediscovery deregister-instance --service-id
 $SERVICE_ID --instance-id $INSTANCE_ID --query 'OperationId' --output text)

        # Wait for deregistration to complete
        echo "Waiting for instance deregistration to complete..." | tee -a $LOG_FILE
        wait_for_operation $OPERATION_ID
      else
        echo "Instance $INSTANCE_ID already deregistered" | tee -a $LOG_FILE
      fi
    elif [[ $resource == "lambda:"* ]]; then
      # Extract function name
      FUNCTION_NAME=$(echo $resource | cut -d':' -f2)
      aws lambda delete-function --function-name $FUNCTION_NAME
    elif [[ $resource == "role:"* ]]; then
      # Extract role name
```

```
      ROLE_NAME=$(echo $resource | cut -d':' -f2)

      # Detach all policies first
      for POLICY_ARN in $(aws iam list-attached-role-policies --role-name $ROLE_NAME
 --query 'AttachedPolicies[*].PolicyArn' --output text); do
        aws iam detach-role-policy --role-name $ROLE_NAME --policy-arn $POLICY_ARN
      done

      # Delete the role
      aws iam delete-role --role-name $ROLE_NAME
    elif [[ $resource == "dynamodb:"* ]]; then
      # Extract table name
      TABLE_NAME=$(echo $resource | cut -d':' -f2)
      aws dynamodb delete-table --table-name $TABLE_NAME

      # Wait for table deletion to complete
      echo "Waiting for DynamoDB table deletion to complete..." | tee -a $LOG_FILE
      aws dynamodb wait table-not-exists --table-name $TABLE_NAME
    fi
  done

  # Handle services separately to ensure all instances are deregistered first
  for ((i=${#CREATED_RESOURCES[@]}-1; i>=0; i--)); do
    resource="${CREATED_RESOURCES[$i]}"
    if [[ $resource == "service:"* ]]; then
      # Extract service ID
      SERVICE_ID=$(echo $resource | cut -d':' -f2)
      echo "Deleting service $SERVICE_ID..." | tee -a $LOG_FILE

      # Make sure all instances are deregistered
      INSTANCES=$(aws servicediscovery list-instances --service-id $SERVICE_ID --
query 'Instances[*].Id' --output text)
      if [[ -n "$INSTANCES" ]]; then
        echo "Service still has instances. Waiting before deletion..." | tee -a
 $LOG_FILE
        sleep 10
      fi

      # Try to delete the service
      aws servicediscovery delete-service --id $SERVICE_ID
      sleep 5
    fi
  done
```

```
  # Handle namespaces last to ensure all services are deleted first
  for ((i=${#CREATED_RESOURCES[@]}-1; i>=0; i--)); do
    resource="${CREATED_RESOURCES[$i]}"
    if [[ $resource == "namespace:"* ]]; then
      # Extract namespace ID
      NAMESPACE_ID=$(echo $resource | cut -d':' -f2)
      echo "Deleting namespace $NAMESPACE_ID..." | tee -a $LOG_FILE

      # Check if namespace still has services
      SERVICES=$(aws servicediscovery list-services --filters
 "Name=NAMESPACE_ID,Values=$NAMESPACE_ID,Condition=EQ" --query 'Services[*].Id' --
output text)
      if [[ -n "$SERVICES" ]]; then
        echo "Namespace still has services. Deleting them first..." | tee -a
 $LOG_FILE
        for SERVICE_ID in $SERVICES; do
          echo "Deleting service $SERVICE_ID..." | tee -a $LOG_FILE
          aws servicediscovery delete-service --id $SERVICE_ID
        done
        sleep 5
      fi

      # Try to delete the namespace
      OPERATION_ID=$(aws servicediscovery delete-namespace --id $NAMESPACE_ID --
query 'OperationId' --output text 2>/dev/null || echo "")
      if [[ -n "$OPERATION_ID" ]]; then
        echo "Waiting for namespace deletion to complete..." | tee -a $LOG_FILE
        wait_for_operation $OPERATION_ID
      else
        echo "Failed to delete namespace or namespace already deleted" | tee -a
 $LOG_FILE
      fi
    fi
  done

  echo "Cleanup complete" | tee -a $LOG_FILE
}

# Step 1: Create an AWS Cloud Map namespace
echo "Step 1: Creating AWS Cloud Map namespace..." | tee -a $LOG_FILE

# Check if namespace already exists
NAMESPACE_ID=$(aws servicediscovery list-namespaces --query "Namespaces[?
Name=='cloudmap-tutorial'].Id" --output text)
```

```
if [[ -z "$NAMESPACE_ID" || "$NAMESPACE_ID" == "None" ]]; then
  log_cmd "aws servicediscovery create-http-namespace --name cloudmap-tutorial --
creator-request-id namespace-request"
  OPERATION_ID=$(aws servicediscovery create-http-namespace --name cloudmap-tutorial
 --creator-request-id namespace-request --query 'OperationId' --output text)

  # Wait for namespace creation to complete
  echo "Waiting for namespace creation to complete..." | tee -a $LOG_FILE
  wait_for_operation $OPERATION_ID

  # Get the namespace ID
  NAMESPACE_ID=$(aws servicediscovery list-namespaces --query "Namespaces[?
Name=='cloudmap-tutorial'].Id" --output text)
  echo "Namespace created with ID: $NAMESPACE_ID" | tee -a $LOG_FILE
else
  echo "Namespace cloudmap-tutorial already exists with ID: $NAMESPACE_ID" | tee -a
 $LOG_FILE
fi

CREATED_RESOURCES+=("namespace:$NAMESPACE_ID")

# Step 2: Create a DynamoDB table
echo "Step 2: Creating DynamoDB table..." | tee -a $LOG_FILE

# Check if table already exists
TABLE_EXISTS=$(aws dynamodb describe-table --table-name cloudmap 2>&1 || echo
 "NOT_EXISTS")

if [[ $TABLE_EXISTS == *"ResourceNotFoundException"* || $TABLE_EXISTS ==
 "NOT_EXISTS" ]]; then
  log_cmd "aws dynamodb create-table --table-name cloudmap --attribute-definitions
 AttributeName=id,AttributeType=S --key-schema AttributeName=id,KeyType=HASH --
billing-mode PAY_PER_REQUEST"

  # Wait for DynamoDB table to become active
  echo "Waiting for DynamoDB table to become active..." | tee -a $LOG_FILE
  aws dynamodb wait table-exists --table-name cloudmap
else
  echo "DynamoDB table cloudmap already exists" | tee -a $LOG_FILE
fi

CREATED_RESOURCES+=("dynamodb:cloudmap")
```

```
# Step 3: Create an AWS Cloud Map data service
echo "Step 3: Creating AWS Cloud Map data service..." | tee -a $LOG_FILE

# Get all services in the namespace
echo "Listing all services in namespace $NAMESPACE_ID..." | tee -a $LOG_FILE
SERVICES=$(aws servicediscovery list-services --filters "Name=NAMESPACE_ID,Values=
$NAMESPACE_ID,Condition=EQ" --query 'Services[*].[Id,Name]' --output text)
echo "Services found: $SERVICES" | tee -a $LOG_FILE

# Check if data service already exists
DATA_SERVICE_ID=""
while read -r id name || [[ -n "$id" ]]; do
  echo "Checking service: ID=$id, Name=$name" | tee -a $LOG_FILE
  if [[ "$name" == "data-service" ]]; then
    DATA_SERVICE_ID="$id"
    break
  fi
done <<< "$SERVICES"

if [[ -z "$DATA_SERVICE_ID" ]]; then
  echo "Data service does not exist, creating it..." | tee -a $LOG_FILE
  # Create the service and capture the ID directly
  echo "$ aws servicediscovery create-service --name data-service --namespace-id
 $NAMESPACE_ID --creator-request-id data-service-request" | tee -a $LOG_FILE
  CREATE_OUTPUT=$(aws servicediscovery create-service --name data-service --
namespace-id $NAMESPACE_ID --creator-request-id data-service-request)
  echo "$CREATE_OUTPUT" | tee -a $LOG_FILE

  # Extract the service ID using AWS CLI query
  DATA_SERVICE_ID=$(aws servicediscovery list-services --filters
 "Name=NAMESPACE_ID,Values=$NAMESPACE_ID,Condition=EQ" --query "Services[?
Name=='data-service'].Id" --output text)
  echo "Data service created with ID: $DATA_SERVICE_ID" | tee -a $LOG_FILE
else
  echo "Data service already exists with ID: $DATA_SERVICE_ID" | tee -a $LOG_FILE
fi

CREATED_RESOURCES+=("service:$DATA_SERVICE_ID")

# Register DynamoDB table as a service instance
echo "Registering DynamoDB table as a service instance..." | tee -a $LOG_FILE

# Check if instance already exists
```

```
INSTANCE_EXISTS=$(aws servicediscovery list-instances --service-id $DATA_SERVICE_ID
 --query "Instances[?Id=='data-instance'].Id" --output text)

if [[ -z "$INSTANCE_EXISTS" ]]; then
  log_cmd "aws servicediscovery register-instance --service-id $DATA_SERVICE_ID --
instance-id data-instance --attributes tablename=cloudmap,region=$(aws configure get
 region)"
  OPERATION_ID=$(aws servicediscovery register-instance --service-
id $DATA_SERVICE_ID --instance-id data-instance --attributes
 tablename=cloudmap,region=$(aws configure get region) --query 'OperationId' --
output text)

  # Wait for instance registration to complete
  echo "Waiting for instance registration to complete..." | tee -a $LOG_FILE
  wait_for_operation $OPERATION_ID
else
  echo "Instance data-instance already exists" | tee -a $LOG_FILE
fi

CREATED_RESOURCES+=("instance:$DATA_SERVICE_ID:data-instance")

# Step 4: Create an IAM role for Lambda
echo "Step 4: Creating IAM role for Lambda..." | tee -a $LOG_FILE

# Create a trust policy for Lambda
cat > lambda-trust-policy.json << EOF
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF

# Check if role already exists
echo "Checking if IAM role already exists..." | tee -a $LOG_FILE
ROLE_EXISTS=$(aws iam get-role --role-name cloudmap-tutorial-role 2>&1 || echo
 "NOT_EXISTS")
```

```
if [[ $ROLE_EXISTS == *"NoSuchEntity"* || $ROLE_EXISTS == "NOT_EXISTS" ]]; then
    log_cmd "aws iam create-role --role-name cloudmap-tutorial-role --assume-role-
policy-document file://lambda-trust-policy.json"
else
    echo "Role cloudmap-tutorial-role already exists, using existing role" | tee -a
 $LOG_FILE
fi

# FIXED: Create a custom policy with least privilege instead of using
 PowerUserAccess
cat > cloudmap-policy.json << EOF
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:PutItem",
        "dynamodb:GetItem",
        "dynamodb:Scan"
      ],
      "Resource": "arn:aws:dynamodb:*:*:table/cloudmap"
    },
    {
      "Effect": "Allow",
      "Action": [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource": "*"
    }
  ]
}
EOF
```

```
# Check if policy already exists
POLICY_ARN=$(aws iam list-policies --query "Policies[?
PolicyName=='CloudMapTutorialPolicy'].Arn" --output text)

if [[ -z "$POLICY_ARN" ]]; then
  echo "Creating CloudMapTutorialPolicy..." | tee -a $LOG_FILE
  echo "$ aws iam create-policy --policy-name CloudMapTutorialPolicy --policy-
document file://cloudmap-policy.json" | tee -a $LOG_FILE
  CREATE_OUTPUT=$(aws iam create-policy --policy-name CloudMapTutorialPolicy --
policy-document file://cloudmap-policy.json)
  echo "$CREATE_OUTPUT" | tee -a $LOG_FILE
  POLICY_ARN=$(aws iam list-policies --query "Policies[?
PolicyName=='CloudMapTutorialPolicy'].Arn" --output text)
else
  echo "Policy CloudMapTutorialPolicy already exists with ARN: $POLICY_ARN" | tee -a
 $LOG_FILE
fi

echo "$ aws iam attach-role-policy --role-name cloudmap-tutorial-role --policy-arn
 $POLICY_ARN" | tee -a $LOG_FILE
aws iam attach-role-policy --role-name cloudmap-tutorial-role --policy-arn
 $POLICY_ARN | tee -a $LOG_FILE

echo "$ aws iam attach-role-policy --role-name cloudmap-tutorial-role --policy-
arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole" | tee -a
 $LOG_FILE
aws iam attach-role-policy --role-name cloudmap-tutorial-role --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole | tee -a $LOG_FILE

# Wait for role to propagate
echo "Waiting for IAM role to propagate..." | tee -a $LOG_FILE
sleep 10

ROLE_ARN=$(aws iam get-role --role-name cloudmap-tutorial-role --query 'Role.Arn' --
output text)
CREATED_RESOURCES+=("role:cloudmap-tutorial-role")

# Step 5: Create an AWS Cloud Map app service
echo "Step 5: Creating AWS Cloud Map app service..." | tee -a $LOG_FILE

# Get all services in the namespace
SERVICES=$(aws servicediscovery list-services --filters "Name=NAMESPACE_ID,Values=
$NAMESPACE_ID,Condition=EQ" --query 'Services[*].[Id,Name]' --output text)
```

```
# Check if app service already exists
APP_SERVICE_ID=""
while read -r id name || [[ -n "$id" ]]; do
  if [[ "$name" == "app-service" ]]; then
    APP_SERVICE_ID="$id"
    break
  fi
done <<< "$SERVICES"

if [[ -z "$APP_SERVICE_ID" ]]; then
  echo "App service does not exist, creating it..." | tee -a $LOG_FILE
  # Create the service and capture the ID directly
  echo "$ aws servicediscovery create-service --name app-service --namespace-id
 $NAMESPACE_ID --creator-request-id app-service-request" | tee -a $LOG_FILE
  CREATE_OUTPUT=$(aws servicediscovery create-service --name app-service --
namespace-id $NAMESPACE_ID --creator-request-id app-service-request)
  echo "$CREATE_OUTPUT" | tee -a $LOG_FILE

  # Extract the service ID using AWS CLI query
  APP_SERVICE_ID=$(aws servicediscovery list-services --filters
 "Name=NAMESPACE_ID,Values=$NAMESPACE_ID,Condition=EQ" --query "Services[?
Name=='app-service'].Id" --output text)
  echo "App service created with ID: $APP_SERVICE_ID" | tee -a $LOG_FILE
else
  echo "App service already exists with ID: $APP_SERVICE_ID" | tee -a $LOG_FILE
fi

CREATED_RESOURCES+=("service:$APP_SERVICE_ID")

# Step 6: Create a Lambda function to write data
echo "Step 6: Creating Lambda function to write data..." | tee -a $LOG_FILE

# Create Lambda function code
cat > writefunction.py << EOF
import boto3
import json
import random

def lambda_handler(event, context):
    # Use AWS Cloud Map to discover the DynamoDB table
    serviceclient = boto3.client('servicediscovery')

    # Discover the data service instance
    response = serviceclient.discover_instances(
```

```
        NamespaceName='cloudmap-tutorial',
        ServiceName='data-service'
    )

    # Extract table name and region from the instance attributes
    tablename = response['Instances'][0]['Attributes']['tablename']
    region = response['Instances'][0]['Attributes']['region']

    # Create DynamoDB client in the specified region
    dynamodb = boto3.resource('dynamodb', region_name=region)
    table = dynamodb.Table(tablename)

    # Write data to the table
    table.put_item(
        Item={
            'id': str(random.randint(1,100)),
            'todo': event
        }
    )

    return {
        'statusCode': 200,
        'body': json.dumps('Data written successfully!')
    }
EOF

# Zip the function code
log_cmd "zip writefunction.zip writefunction.py"

# Create the Lambda function
FUNCTION_EXISTS=$(aws lambda list-functions --query "Functions[?
FunctionName=='writefunction'].FunctionName" --output text)
if [[ -z "$FUNCTION_EXISTS" ]]; then
  log_cmd "aws lambda create-function --function-name writefunction --runtime
 python3.12 --role $ROLE_ARN --handler writefunction.lambda_handler --zip-file
 fileb://writefunction.zip --architectures x86_64"

  # Wait for the Lambda function to be active before updating
  echo "Waiting for Lambda function to become active..." | tee -a $LOG_FILE
  function_state="Pending"
  while [ "$function_state" == "Pending" ]; do
      sleep 5
      function_state=$(aws lambda get-function --function-name writefunction --query
 'Configuration.State' --output text)
```

```
      echo "Current function state: $function_state" | tee -a $LOG_FILE
  done

  # Update the function timeout
  log_cmd "aws lambda update-function-configuration --function-name writefunction --
timeout 5"
else
  echo "Lambda function writefunction already exists" | tee -a $LOG_FILE
fi
CREATED_RESOURCES+=("lambda:writefunction")

# Step 7: Register the Lambda write function as an AWS Cloud Map service instance
echo "Step 7: Registering Lambda write function as a service instance..." | tee -a
 $LOG_FILE

# Check if instance already exists
INSTANCE_EXISTS=$(aws servicediscovery list-instances --service-id $APP_SERVICE_ID
 --query "Instances[?Id=='write-instance'].Id" --output text)

if [[ -z "$INSTANCE_EXISTS" ]]; then
  log_cmd "aws servicediscovery register-instance --service-id $APP_SERVICE_ID --
instance-id write-instance --attributes action=write,functionname=writefunction"
  OPERATION_ID=$(aws servicediscovery register-instance --service-id $APP_SERVICE_ID
 --instance-id write-instance --attributes action=write,functionname=writefunction
 --query 'OperationId' --output text)

  # Wait for instance registration to complete
  echo "Waiting for write instance registration to complete..." | tee -a $LOG_FILE
  wait_for_operation $OPERATION_ID
else
  echo "Instance write-instance already exists" | tee -a $LOG_FILE
fi

CREATED_RESOURCES+=("instance:$APP_SERVICE_ID:write-instance")

# Step 8: Create a Lambda function to read data
echo "Step 8: Creating Lambda function to read data..." | tee -a $LOG_FILE

# Create Lambda function code
cat > readfunction.py << EOF
import boto3
import json

def lambda_handler(event, context):
```

```
    # Use AWS Cloud Map to discover the DynamoDB table
    serviceclient = boto3.client('servicediscovery')

    # Discover the data service instance
    response = serviceclient.discover_instances(
        NamespaceName='cloudmap-tutorial',
        ServiceName='data-service'
    )

    # Extract table name and region from the instance attributes
    tablename = response['Instances'][0]['Attributes']['tablename']
    region = response['Instances'][0]['Attributes']['region']

    # Create DynamoDB client in the specified region
    dynamodb = boto3.resource('dynamodb', region_name=region)
    table = dynamodb.Table(tablename)

    # Read data from the table
    response = table.scan()

    return {
        'statusCode': 200,
        'body': json.dumps(response['Items'])
    }
EOF

# Zip the function code
log_cmd "zip readfunction.zip readfunction.py"

# Create the Lambda function
FUNCTION_EXISTS=$(aws lambda list-functions --query "Functions[?
FunctionName=='readfunction'].FunctionName" --output text)
if [[ -z "$FUNCTION_EXISTS" ]]; then
  log_cmd "aws lambda create-function --function-name readfunction --runtime
 python3.12 --role $ROLE_ARN --handler readfunction.lambda_handler --zip-file
 fileb://readfunction.zip --architectures x86_64"

  # Wait for the Lambda function to be active before updating
  echo "Waiting for Lambda function to become active..." | tee -a $LOG_FILE
  function_state="Pending"
  while [ "$function_state" == "Pending" ]; do
      sleep 5
      function_state=$(aws lambda get-function --function-name readfunction --query
 'Configuration.State' --output text)
```

```
      echo "Current function state: $function_state" | tee -a $LOG_FILE
  done

  # Update the function timeout
  log_cmd "aws lambda update-function-configuration --function-name readfunction --
timeout 5"
else
  echo "Lambda function readfunction already exists" | tee -a $LOG_FILE
fi
CREATED_RESOURCES+=("lambda:readfunction")

# Step 9: Register the Lambda read function as an AWS Cloud Map service instance
echo "Step 9: Registering Lambda read function as a service instance..." | tee -a
 $LOG_FILE

# Check if instance already exists
INSTANCE_EXISTS=$(aws servicediscovery list-instances --service-id $APP_SERVICE_ID
 --query "Instances[?Id=='read-instance'].Id" --output text)

if [[ -z "$INSTANCE_EXISTS" ]]; then
  log_cmd "aws servicediscovery register-instance --service-id $APP_SERVICE_ID --
instance-id read-instance --attributes action=read,functionname=readfunction"
  OPERATION_ID=$(aws servicediscovery register-instance --service-id $APP_SERVICE_ID
 --instance-id read-instance --attributes action=read,functionname=readfunction --
query 'OperationId' --output text)

  # Wait for read instance registration to complete
  echo "Waiting for read instance registration to complete..." | tee -a $LOG_FILE
  wait_for_operation $OPERATION_ID
else
  echo "Instance read-instance already exists" | tee -a $LOG_FILE
fi

CREATED_RESOURCES+=("instance:$APP_SERVICE_ID:read-instance")

# Step 10: Create Python clients to interact with the services
echo "Step 10: Creating Python clients..." | tee -a $LOG_FILE

cat > writeclient.py << EOF
import boto3

serviceclient = boto3.client('servicediscovery')
```

```
response = serviceclient.discover_instances(NamespaceName='cloudmap-tutorial',
 ServiceName='app-service', QueryParameters={ 'action': 'write' })

functionname = response["Instances"][0]["Attributes"]["functionname"]

lambdaclient = boto3.client('lambda')

resp = lambdaclient.invoke(FunctionName=functionname, Payload='"This is a test
 data"')

print(resp["Payload"].read())
EOF

cat > readclient.py << EOF
import boto3

serviceclient = boto3.client('servicediscovery')

response = serviceclient.discover_instances(NamespaceName='cloudmap-tutorial',
 ServiceName='app-service', QueryParameters={ 'action': 'read' })

functionname = response["Instances"][0]["Attributes"]["functionname"]

lambdaclient = boto3.client('lambda')

resp = lambdaclient.invoke(FunctionName=functionname,
 InvocationType='RequestResponse')

print(resp["Payload"].read())
EOF

echo "Running write client..." | tee -a $LOG_FILE
log_cmd "python3 writeclient.py"

echo "Running read client..." | tee -a $LOG_FILE
log_cmd "python3 readclient.py"

# Step 11: Clean up resources
echo "Resources created:" | tee -a $LOG_FILE
for resource in "${CREATED_RESOURCES[@]}"; do
  echo "- $resource" | tee -a $LOG_FILE
done

echo "" | tee -a $LOG_FILE
```

```
echo "==========================================" | tee -a $LOG_FILE
echo "CLEANUP CONFIRMATION" | tee -a $LOG_FILE
echo "==========================================" | tee -a $LOG_FILE
echo "Do you want to clean up all created resources? (y/n): " | tee -a $LOG_FILE
read -r CLEANUP_CONFIRM
if [[ $CLEANUP_CONFIRM == "y" || $CLEANUP_CONFIRM == "Y" ]]; then
  cleanup
else
  echo "Resources were not cleaned up. You can manually clean them up later." | tee
 -a $LOG_FILE
fi

echo "Script completed at $(date)" | tee -a $LOG_FILE
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreateHttpNamespace
  - CreateService
  - DeleteNamespace
  - DeleteService
  - DeregisterInstance
  - GetOperation
  - ListNamespaces
  - ListServices
  - RegisterInstance

Detección de servicios de Cloud Map

En el siguiente ejemplo de código, se muestra cómo:

- Creación de un espacio de nombres DNS público con la integración de zonas alojadas de Route 53
- Creación de servicios que puedan detectarse mediante consultas de DNS y llamadas a la API
- Registro de instancias de servicio con diferentes configuraciones de detección
- Detección de servicios mediante consultas de DNS y la API de Cloud Map
- Verificación de detección de servicios mediante el comando dig y las llamadas a la API

- Eliminación de los recursos en el orden correcto (instancias, servicios, espacio de nombres)

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Encuentre el ejemplo completo y obtenga información sobre cómo configurarlo y ejecutarlo en el repositorio de Tutoriales para desarrolladores de ejemplo.

```
#!/bin/bash

# AWS Cloud Map Private Namespace Tutorial Script
# This script demonstrates how to use AWS Cloud Map for service discovery
# with DNS queries and API calls

# Exit on error
set -e

# Configuration
REGION="us-east-2"
NAMESPACE_NAME="cloudmap-tutorial.com"
LOG_FILE="cloudmap-tutorial.log"
CREATOR_REQUEST_ID=$(date +%s)

# Function to log messages
log() {
    local message="$1"
    echo "$(date '+%Y-%m-%d %H:%M:%S') - $message" | tee -a "$LOG_FILE"
}

# Function to check operation status
check_operation() {
    local operation_id="$1"
    local status=""

    log "Checking operation status for $operation_id..."

    while [[ "$status" != "SUCCESS" ]]; do
        sleep 5
        status=$(aws servicediscovery get-operation \
            --operation-id "$operation_id" \
```

```
            --region "$REGION" \
            --query "Operation.Status" \
            --output text)

        log "Operation status: $status"

        if [[ "$status" == "FAIL" ]]; then
            log "Operation failed. Exiting."
            exit 1
        fi
    done

    log "Operation completed successfully."
}

# Function to clean up resources
cleanup() {
    log "Starting cleanup process..."

    if [[ -n "$FIRST_INSTANCE_ID" ]]; then
        log "Deregistering first service instance..."
        aws servicediscovery deregister-instance \
            --service-id "$PUBLIC_SERVICE_ID" \
            --instance-id "$FIRST_INSTANCE_ID" \
            --region "$REGION" || log "Failed to deregister first instance"
    fi

    if [[ -n "$SECOND_INSTANCE_ID" ]]; then
        log "Deregistering second service instance..."
        aws servicediscovery deregister-instance \
            --service-id "$BACKEND_SERVICE_ID" \
            --instance-id "$SECOND_INSTANCE_ID" \
            --region "$REGION" || log "Failed to deregister second instance"
    fi

    if [[ -n "$PUBLIC_SERVICE_ID" ]]; then
        log "Deleting public service..."
        aws servicediscovery delete-service \
            --id "$PUBLIC_SERVICE_ID" \
            --region "$REGION" || log "Failed to delete public service"
    fi

    if [[ -n "$BACKEND_SERVICE_ID" ]]; then
        log "Deleting backend service..."
```

```
        aws servicediscovery delete-service \
            --id "$BACKEND_SERVICE_ID" \
            --region "$REGION" || log "Failed to delete backend service"
    fi

    if [[ -n "$NAMESPACE_ID" ]]; then
        log "Deleting namespace..."
        aws servicediscovery delete-namespace \
            --id "$NAMESPACE_ID" \
            --region "$REGION" || log "Failed to delete namespace"
    fi

    log "Cleanup completed."
}

# Set up trap for cleanup on script exit
trap cleanup EXIT INT TERM

# Initialize log file
> "$LOG_FILE"
log "Starting AWS Cloud Map tutorial script"

# Step 1: Create an AWS Cloud Map namespace
log "Creating AWS Cloud Map namespace: $NAMESPACE_NAME"
OPERATION_RESULT=$(aws servicediscovery create-public-dns-namespace \
    --name "$NAMESPACE_NAME" \
    --creator-request-id "cloudmap-tutorial-$CREATOR_REQUEST_ID" \
    --region "$REGION")

OPERATION_ID=$(echo "$OPERATION_RESULT" | jq -r '.OperationId')
log "Namespace creation initiated. Operation ID: $OPERATION_ID"

# Check operation status
check_operation "$OPERATION_ID"

# Get the namespace ID
log "Getting namespace ID..."
NAMESPACE_ID=$(aws servicediscovery list-namespaces \
    --region "$REGION" \
    --query "Namespaces[?Name=='$NAMESPACE_NAME'].Id" \
    --output text)

log "Namespace ID: $NAMESPACE_ID"
```

```
# Get the hosted zone ID
log "Getting Route 53 hosted zone ID..."
HOSTED_ZONE_ID=$(aws route53 list-hosted-zones-by-name \
    --dns-name "$NAMESPACE_NAME" \
    --query "HostedZones[0].Id" \
    --output text | sed 's|/hostedzone/||')

log "Hosted Zone ID: $HOSTED_ZONE_ID"

# Step 2: Create the AWS Cloud Map services
log "Creating public service..."
PUBLIC_SERVICE_RESULT=$(aws servicediscovery create-service \
    --name "public-service" \
    --namespace-id "$NAMESPACE_ID" \
    --dns-config "RoutingPolicy=MULTIVALUE,DnsRecords=[{Type=A,TTL=300}]" \
    --region "$REGION")

PUBLIC_SERVICE_ID=$(echo "$PUBLIC_SERVICE_RESULT" | jq -r '.Service.Id')
log "Public service created. Service ID: $PUBLIC_SERVICE_ID"

log "Creating backend service..."
BACKEND_SERVICE_RESULT=$(aws servicediscovery create-service \
    --name "backend-service" \
    --namespace-id "$NAMESPACE_ID" \
    --type "HTTP" \
    --region "$REGION")

BACKEND_SERVICE_ID=$(echo "$BACKEND_SERVICE_RESULT" | jq -r '.Service.Id')
log "Backend service created. Service ID: $BACKEND_SERVICE_ID"

# Step 3: Register the AWS Cloud Map service instances
log "Registering first service instance..."
FIRST_INSTANCE_RESULT=$(aws servicediscovery register-instance \
    --service-id "$PUBLIC_SERVICE_ID" \
    --instance-id "first" \
    --attributes "AWS_INSTANCE_IPV4=192.168.2.1" \
    --region "$REGION")

FIRST_INSTANCE_ID="first"
FIRST_OPERATION_ID=$(echo "$FIRST_INSTANCE_RESULT" | jq -r '.OperationId')
log "First instance registration initiated. Operation ID: $FIRST_OPERATION_ID"

# Check operation status
check_operation "$FIRST_OPERATION_ID"
```

```
log "Registering second service instance..."
SECOND_INSTANCE_RESULT=$(aws servicediscovery register-instance \
    --service-id "$BACKEND_SERVICE_ID" \
    --instance-id "second" \
    --attributes "service-name=backend" \
    --region "$REGION")

SECOND_INSTANCE_ID="second"
SECOND_OPERATION_ID=$(echo "$SECOND_INSTANCE_RESULT" | jq -r '.OperationId')
log "Second instance registration initiated. Operation ID: $SECOND_OPERATION_ID"

# Check operation status
check_operation "$SECOND_OPERATION_ID"

# Step 4: Discover the AWS Cloud Map service instances
log "Getting Route 53 name servers..."
NAME_SERVERS=$(aws route53 get-hosted-zone \
    --id "$HOSTED_ZONE_ID" \
    --query "DelegationSet.NameServers[0]" \
    --output text)

log "Name server: $NAME_SERVERS"

log "Using dig to query DNS records (this will be simulated)..."
log "Command: dig @$NAME_SERVERS public-service.$NAMESPACE_NAME"
log "Expected output would show: public-service.$NAMESPACE_NAME. 300 IN A
 192.168.2.1"

log "Using AWS CLI to discover backend service instances..."
DISCOVER_RESULT=$(aws servicediscovery discover-instances \
    --namespace-name "$NAMESPACE_NAME" \
    --service-name "backend-service" \
    --region "$REGION")

log "Discovery result: $(echo "$DISCOVER_RESULT" | jq -c '.')"

# Display created resources
log "Resources created:"
log "- Namespace: $NAMESPACE_NAME (ID: $NAMESPACE_ID)"
log "- Public Service: public-service (ID: $PUBLIC_SERVICE_ID)"
log "- Backend Service: backend-service (ID: $BACKEND_SERVICE_ID)"
log "- Service Instance: first (Service: public-service)"
log "- Service Instance: second (Service: backend-service)"
```

```
# Ask user if they want to clean up resources
read -p "Do you want to clean up all created resources? (y/n): " CLEANUP_RESPONSE

if [[ "$CLEANUP_RESPONSE" == "y" || "$CLEANUP_RESPONSE" == "Y" ]]; then
    log "User confirmed cleanup. Proceeding with resource deletion."
    # Cleanup function will be called automatically on exit
else
    log "User chose not to clean up resources. Exiting without cleanup."
    trap - EXIT
    exit 0
fi
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreatePublicDnsNamespace
  - CreateService
  - DeleteNamespace
  - DeleteService
  - DeregisterInstance
  - DiscoverInstances
  - GetOperation
  - ListNamespaces
  - RegisterInstance

Ejemplos de CloudFront que utilizan la AWS CLI con el script Bash

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante la AWS Command Line Interface con el script Bash con CloudFront.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica a través de llamadas a varias funciones dentro del servicio o combinado con otros Servicios de AWS.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Escenarios

Escenarios

Introducción a CloudFront

En el siguiente ejemplo de código, se muestra cómo:

- Creación de un bucket de Amazon S3 para el almacenamiento de contenido
- Carga del contenido de ejemplo en el bucket de S3
- Creación de un control de acceso de origen (OAC) para el acceso seguro a S3
- Creación de una distribución de CloudFront con S3 como origen
- Actualización de la política de bucket de S3 para permitir el acceso de CloudFront
- Espera para la implementación de la distribución y prueba del acceso al contenido
- Eliminación de los recursos, incluidos la distribución, el OAC y el bucket de S3

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Encuentre el ejemplo completo y obtenga información sobre cómo configurarlo y ejecutarlo en el repositorio de Tutoriales para desarrolladores de ejemplo.

```
#!/bin/bash

# CloudFront Getting Started Tutorial Script
# This script creates an S3 bucket, uploads sample content, creates a CloudFront
 distribution with OAC,
# and demonstrates how to access content through CloudFront.

# Set up logging
LOG_FILE="cloudfront-tutorial.log"
exec > >(tee -a "$LOG_FILE") 2>&1

echo "Starting CloudFront Getting Started Tutorial at $(date)"

# Function to handle errors
```

```
handle_error() {
    echo "ERROR: $1"
    echo "Resources created before error:"
    if [ -n "$BUCKET_NAME" ]; then
        echo "- S3 Bucket: $BUCKET_NAME"
    fi
    if [ -n "$OAC_ID" ]; then
        echo "- CloudFront Origin Access Control: $OAC_ID"
    fi
    if [ -n "$DISTRIBUTION_ID" ]; then
        echo "- CloudFront Distribution: $DISTRIBUTION_ID"
    fi

    echo "Attempting to clean up resources..."
    cleanup
    exit 1
}

# Function to clean up resources
cleanup() {
    echo "Cleaning up resources..."

    if [ -n "$DISTRIBUTION_ID" ]; then
        echo "Disabling CloudFront distribution $DISTRIBUTION_ID..."

        # Get the current configuration and ETag
        ETAG=$(aws cloudfront get-distribution-config --id "$DISTRIBUTION_ID" --
query 'ETag' --output text)
        if [ $? -ne 0 ]; then
            echo "Failed to get distribution config. Continuing with cleanup..."
        else
            # Create a modified configuration with Enabled=false
            aws cloudfront get-distribution-config --id "$DISTRIBUTION_ID" | \
            jq '.DistributionConfig.Enabled = false' > temp_disabled_config.json

            # Update the distribution to disable it
            aws cloudfront update-distribution \
                --id "$DISTRIBUTION_ID" \
                --distribution-config file://<(jq '.DistributionConfig'
 temp_disabled_config.json) \
                --if-match "$ETAG"

            if [ $? -ne 0 ]; then
                echo "Failed to disable distribution. Continuing with cleanup..."
```

```
            else
                echo "Waiting for distribution to be disabled (this may take several
 minutes)..."
                aws cloudfront wait distribution-deployed --id "$DISTRIBUTION_ID"

                # Delete the distribution
                ETAG=$(aws cloudfront get-distribution-config --id
 "$DISTRIBUTION_ID" --query 'ETag' --output text)
                aws cloudfront delete-distribution --id "$DISTRIBUTION_ID" --if-
match "$ETAG"
                if [ $? -ne 0 ]; then
                    echo "Failed to delete distribution. You may need to delete it
 manually."
                else
                    echo "CloudFront distribution deleted."
                fi
            fi
        fi
    fi

    if [ -n "$OAC_ID" ]; then
        echo "Deleting Origin Access Control $OAC_ID..."
        OAC_ETAG=$(aws cloudfront get-origin-access-control --id "$OAC_ID" --query
 'ETag' --output text 2>/dev/null)
        if [ $? -ne 0 ]; then
            echo "Failed to get Origin Access Control ETag. You may need to delete
 it manually."
        else
            aws cloudfront delete-origin-access-control --id "$OAC_ID" --if-match
 "$OAC_ETAG"
            if [ $? -ne 0 ]; then
                echo "Failed to delete Origin Access Control. You may need to delete
 it manually."
            else
                echo "Origin Access Control deleted."
            fi
        fi
    fi

    if [ -n "$BUCKET_NAME" ]; then
        echo "Deleting S3 bucket $BUCKET_NAME and its contents..."
        aws s3 rm "s3://$BUCKET_NAME" --recursive
        if [ $? -ne 0 ]; then
```

```
            echo "Failed to remove bucket contents. Continuing with bucket
 deletion..."
        fi

        aws s3 rb "s3://$BUCKET_NAME"
        if [ $? -ne 0 ]; then
            echo "Failed to delete bucket. You may need to delete it manually."
        else
            echo "S3 bucket deleted."
        fi
    fi

    # Clean up temporary files
    rm -f temp_disabled_config.json
    rm -rf temp_content
}

# Generate a random identifier for the bucket name
RANDOM_ID=$(openssl rand -hex 6)
BUCKET_NAME="cloudfront-${RANDOM_ID}"
echo "Using bucket name: $BUCKET_NAME"

# Create a temporary directory for content
TEMP_DIR="temp_content"
mkdir -p "$TEMP_DIR/css"
if [ $? -ne 0 ]; then
    handle_error "Failed to create temporary directory"
fi

# Step 1: Create an S3 bucket
echo "Creating S3 bucket: $BUCKET_NAME"
aws s3 mb "s3://$BUCKET_NAME"
if [ $? -ne 0 ]; then
    handle_error "Failed to create S3 bucket"
fi

# Step 2: Create sample content
echo "Creating sample content..."
cat > "$TEMP_DIR/index.html" << 'EOF'
<!DOCTYPE html>
<html>
<head>
    <title>Hello World</title>
    <link rel="stylesheet" type="text/css" href="css/styles.css">
```

```
</head>
<body>
    <h1>Hello world!</h1>
</body>
</html>
EOF

cat > "$TEMP_DIR/css/styles.css" << 'EOF'
body {
    font-family: Arial, sans-serif;
    margin: 40px;
    background-color: #f5f5f5;
}
h1 {
    color: #333;
    text-align: center;
}
EOF

# Step 3: Upload content to the S3 bucket
echo "Uploading content to S3 bucket..."
aws s3 cp "$TEMP_DIR/" "s3://$BUCKET_NAME/" --recursive
if [ $? -ne 0 ]; then
    handle_error "Failed to upload content to S3 bucket"
fi

# Step 4: Create Origin Access Control
echo "Creating Origin Access Control..."
OAC_RESPONSE=$(aws cloudfront create-origin-access-control \
    --origin-access-control-config Name="oac-for-
$BUCKET_NAME",SigningProtocol=sigv4,SigningBehavior=always,OriginAccessControlOriginType=s3)

if [ $? -ne 0 ]; then
    handle_error "Failed to create Origin Access Control"
fi

OAC_ID=$(echo "$OAC_RESPONSE" | jq -r '.OriginAccessControl.Id')
echo "Created Origin Access Control with ID: $OAC_ID"

# Step 5: Create CloudFront distribution
echo "Creating CloudFront distribution..."

# Get AWS account ID for bucket policy
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)
```

```
if [ $? -ne 0 ]; then
    handle_error "Failed to get AWS account ID"
fi

# Create distribution configuration
cat > distribution-config.json << EOF
{
    "CallerReference": "cli-tutorial-$(date +%s)",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "S3-$BUCKET_NAME",
                "DomainName": "$BUCKET_NAME.s3.amazonaws.com",
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                },
                "OriginAccessControlId": "$OAC_ID"
            }
        ]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "S3-$BUCKET_NAME",
        "ViewerProtocolPolicy": "redirect-to-https",
        "AllowedMethods": {
            "Quantity": 2,
            "Items": ["GET", "HEAD"],
            "CachedMethods": {
                "Quantity": 2,
                "Items": ["GET", "HEAD"]
            }
        },
        "DefaultTTL": 86400,
        "MinTTL": 0,
        "MaxTTL": 31536000,
        "Compress": true,
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            }
        }
    },
    "Comment": "CloudFront distribution for tutorial",
```

```
    "Enabled": true,
    "WebACLId": ""
}
EOF

DIST_RESPONSE=$(aws cloudfront create-distribution --distribution-config file://
distribution-config.json)
if [ $? -ne 0 ]; then
    handle_error "Failed to create CloudFront distribution"
fi

DISTRIBUTION_ID=$(echo "$DIST_RESPONSE" | jq -r '.Distribution.Id')
DOMAIN_NAME=$(echo "$DIST_RESPONSE" | jq -r '.Distribution.DomainName')

echo "Created CloudFront distribution with ID: $DISTRIBUTION_ID"
echo "CloudFront domain name: $DOMAIN_NAME"

# Step 6: Update S3 bucket policy
echo "Updating S3 bucket policy..."
cat > bucket-policy.json << EOF
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontServicePrincipal",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::$BUCKET_NAME/*",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn": "arn:aws:cloudfront::$ACCOUNT_ID:distribution/
$DISTRIBUTION_ID"
                }
            }
        }
    ]
}
EOF

aws s3api put-bucket-policy --bucket "$BUCKET_NAME" --policy file://bucket-
policy.json
```

```
if [ $? -ne 0 ]; then
    handle_error "Failed to update S3 bucket policy"
fi

# Step 7: Wait for distribution to deploy
echo "Waiting for CloudFront distribution to deploy (this may take 5-10 minutes)..."
aws cloudfront wait distribution-deployed --id "$DISTRIBUTION_ID"
if [ $? -ne 0 ]; then
    echo "Warning: Distribution deployment wait timed out. The distribution may
 still be deploying."
else
    echo "CloudFront distribution is now deployed."
fi

# Step 8: Display access information
echo ""
echo "===== CloudFront Distribution Setup Complete ====="
echo "You can access your content at: https://$DOMAIN_NAME/index.html"
echo ""
echo "Resources created:"
echo "- S3 Bucket: $BUCKET_NAME"
echo "- CloudFront Origin Access Control: $OAC_ID"
echo "- CloudFront Distribution: $DISTRIBUTION_ID"
echo ""

# Ask user if they want to clean up resources
read -p "Do you want to clean up all resources created by this script? (y/n): "
 CLEANUP_RESPONSE
if [[ "$CLEANUP_RESPONSE" =~ ^[Yy] ]]; then
    cleanup
    echo "All resources have been cleaned up."
else
    echo "Resources will not be cleaned up. You can manually delete them later."
    echo "To access your content, visit: https://$DOMAIN_NAME/index.html"
fi

echo "Tutorial completed at $(date)"
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreateDistribution

- CreateOriginAccessControl
- DeleteDistribution
- DeleteOriginAccessControl
- GetDistribution
- GetDistributionConfig
- GetOriginAccessControl
- UpdateDistribution
- WaitDistributionDeployed

Ejemplos de DynamoDB que utilizan la AWS CLI con el script Bash

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante AWS Command Line Interface con el script Bash con DynamoDB.

Los conceptos básicos son ejemplos de código que muestran cómo realizar las operaciones esenciales dentro de un servicio.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica a través de llamadas a varias funciones dentro del servicio o combinado con otros Servicios de AWS.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Conceptos básicos
- Acciones
- Escenarios

Conceptos básicos

Conceptos básicos

En el siguiente ejemplo de código, se muestra cómo:

- Creación de una tabla que pueda contener datos de películas.
- Colocar, obtener y actualizar una sola película en la tabla.
- Escribir los datos de películas en la tabla a partir de un archivo JSON de ejemplo.
- Consultar películas que se hayan estrenado en un año determinado.
- Buscar películas que se hayan estrenado en un intervalo de años.
- Eliminación de una película de la tabla y, a continuación, eliminar la tabla.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

El escenario de introducción a DynamoDB.

```
###############################################################################
# function dynamodb_getting_started_movies
#
# Scenario to create an Amazon DynamoDB table and perform a series of operations on
 the table.
#
# Returns:
#       0 - If successful.
#       1 - If an error occurred.
###############################################################################
function dynamodb_getting_started_movies() {

  source ./dynamodb_operations.sh

  key_schema_json_file="dynamodb_key_schema.json"
  attribute_definitions_json_file="dynamodb_attr_def.json"
  item_json_file="movie_item.json"
  key_json_file="movie_key.json"
  batch_json_file="batch.json"
  attribute_names_json_file="attribute_names.json"
  attributes_values_json_file="attribute_values.json"

  echo_repeat "*" 88
```

```
  echo
  echo "Welcome to the Amazon DynamoDB getting started demo."
  echo
  echo_repeat "*" 88
  echo

  local table_name
  echo -n "Enter a name for a new DynamoDB table: "
  get_input
  table_name=$get_input_result

  echo '[
  {"AttributeName": "year", "KeyType": "HASH"},
   {"AttributeName": "title", "KeyType": "RANGE"}
  ]' >"$key_schema_json_file"

  echo '[
  {"AttributeName": "year", "AttributeType": "N"},
   {"AttributeName": "title", "AttributeType": "S"}
  ]' >"$attribute_definitions_json_file"

  if dynamodb_create_table -n "$table_name" -a "$attribute_definitions_json_file" \
    -k "$key_schema_json_file" 1>/dev/null; then
    echo "Created a DynamoDB table named $table_name"
  else
    errecho "The table failed to create. This demo will exit."
    clean_up
    return 1
  fi

  echo "Waiting for the table to become active...."

  if dynamodb_wait_table_active -n "$table_name"; then
    echo "The table is now active."
  else
    errecho "The table failed to become active. This demo will exit."
    cleanup "$table_name"
    return 1
  fi

  echo
  echo_repeat "*" 88
  echo
```

```
  echo -n "Enter the title of a movie you want to add to the table: "
  get_input
  local added_title
  added_title=$get_input_result

  local added_year
  get_int_input "What year was it released? "
  added_year=$get_input_result

  local rating
  get_float_input "On a scale of 1 - 10, how do you rate it? " "1" "10"
  rating=$get_input_result

  local plot
  echo -n "Summarize the plot for me: "
  get_input
  plot=$get_input_result

  echo '{
    "year": {"N" :"'"$added_year"'"},
    "title": {"S" :  "'"$added_title"'"},
    "info": {"M" : {"plot": {"S" : "'"$plot"'"}, "rating": {"N" :"'"$rating"'"} } }
   }' >"$item_json_file"

  if dynamodb_put_item -n "$table_name" -i "$item_json_file"; then
    echo "The movie '$added_title' was successfully added to the table
'$table_name'."
  else
    errecho "Put item failed. This demo will exit."
    clean_up "$table_name"
    return 1
  fi

  echo
  echo_repeat "*" 88
  echo

  echo "Let's update your movie '$added_title'."
  get_float_input "You rated it $rating, what new rating would you give it? " "1"
"10"
  rating=$get_input_result

  echo -n "You summarized the plot as '$plot'."
  echo "What would you say now? "
```

```
  get_input
  plot=$get_input_result

  echo '{
    "year": {"N" :"'"$added_year"'"},
    "title": {"S" :  "'"$added_title"'"}
    }' >"$key_json_file"

  echo '{
    ":r": {"N" :"'"$rating"'"},
    ":p": {"S" : "'"$plot"'"}
   }' >"$item_json_file"

  local update_expression="SET info.rating = :r, info.plot = :p"

  if dynamodb_update_item -n "$table_name" -k "$key_json_file" -e
"$update_expression" -v "$item_json_file"; then
    echo "Updated '$added_title' with new attributes."
  else
    errecho "Update item failed. This demo will exit."
    clean_up "$table_name"
    return 1
  fi

  echo
  echo_repeat "*" 88
  echo

  echo "We will now use batch write to upload 150 movie entries into the table."

  local batch_json
  for batch_json in movie_files/movies_*.json; do
    echo "{ \"$table_name\" : $(<"$batch_json") }" >"$batch_json_file"
    if dynamodb_batch_write_item -i "$batch_json_file" 1>/dev/null; then
      echo "Entries in $batch_json added to table."
    else
      errecho "Batch write failed. This demo will exit."
      clean_up "$table_name"
      return 1
    fi
  done

  local title="The Lord of the Rings: The Fellowship of the Ring"
  local year="2001"
```

```
 if get_yes_no_input "Let's move on...do you want to get info about '$title'? (y/n)
"; then
   echo '{
 "year": {"N" :"'"$year"'"},
 "title": {"S" :  "'"$title"'"}
 }' >"$key_json_file"
   local info
   info=$(dynamodb_get_item -n "$table_name" -k "$key_json_file")

   # shellcheck disable=SC2181
   if [[ ${?} -ne 0 ]]; then
     errecho "Get item failed. This demo will exit."
     clean_up "$table_name"
     return 1
   fi

   echo "Here is what I found:"
   echo "$info"
 fi

 local ask_for_year=true
 while [[ "$ask_for_year" == true ]]; do
   echo "Let's get a list of movies released in a given year."
   get_int_input "Enter a year between 1972 and 2018: " "1972" "2018"
   year=$get_input_result
   echo '{
   "#n": "year"
   }' >"$attribute_names_json_file"

   echo '{
   ":v": {"N" :"'"$year"'"}
   }' >"$attributes_values_json_file"

   response=$(dynamodb_query -n "$table_name" -k "#n=:v" -a
"$attribute_names_json_file" -v "$attributes_values_json_file")

   # shellcheck disable=SC2181
   if [[ ${?} -ne 0 ]]; then
     errecho "Query table failed. This demo will exit."
     clean_up "$table_name"
     return 1
   fi
```

```
    echo "Here is what I found:"
    echo "$response"

    if ! get_yes_no_input "Try another year? (y/n) "; then
      ask_for_year=false
    fi
  done

  echo "Now let's scan for movies released in a range of years. Enter a year: "
  get_int_input "Enter a year between 1972 and 2018: " "1972" "2018"
  local start=$get_input_result

  get_int_input "Enter another year: " "1972" "2018"
  local end=$get_input_result

  echo '{
    "#n": "year"
    }' >"$attribute_names_json_file"

  echo '{
    ":v1": {"N" : "'"$start"'"},
    ":v2": {"N" : "'"$end"'"}
    }' >"$attributes_values_json_file"

  response=$(dynamodb_scan -n "$table_name" -f "#n BETWEEN :v1 AND :v2" -a
"$attribute_names_json_file" -v "$attributes_values_json_file")

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "Scan table failed. This demo will exit."
    clean_up "$table_name"
    return 1
  fi

  echo "Here is what I found:"
  echo "$response"

  echo
  echo_repeat "*" 88
  echo

  echo "Let's remove your movie '$added_title' from the table."

  if get_yes_no_input "Do you want to remove '$added_title'? (y/n) "; then
```

```
    echo '{
  "year": {"N" :"'"$added_year"'"},
  "title": {"S" :  "'"$added_title"'"}
  }' >"$key_json_file"

    if ! dynamodb_delete_item -n "$table_name" -k "$key_json_file"; then
      errecho "Delete item failed. This demo will exit."
      clean_up "$table_name"
      return 1
    fi
  fi

  if get_yes_no_input "Do you want to delete the table '$table_name'? (y/n) "; then
    if ! clean_up "$table_name"; then
      return 1
    fi
  else
    if ! clean_up; then
      return 1
    fi
  fi

  return 0
}
```

Las funciones de DynamoDB utilizadas en este escenario.

```
###############################################################################
# function dynamodb_create_table
#
# This function creates an Amazon DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table to create.
#       -a attribute_definitions -- JSON file path of a list of attributes and their
 types.
#       -k key_schema -- JSON file path of a list of attributes and their key types.
#
#  Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
```

```
function dynamodb_create_table() {
  local table_name attribute_definitions key_schema response
  local option OPTARG # Required to use getopts command in a function.

  ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_create_table"
    echo "Creates an Amazon DynamoDB table with on-demand billing."
    echo " -n table_name  -- The name of the table to create."
    echo " -a attribute_definitions -- JSON file path of a list of attributes and
 their types."
    echo " -k key_schema -- JSON file path of a list of attributes and their key
 types."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:a:k:h" option; do
    case "${option}" in
      n) table_name="${OPTARG}" ;;
      a) attribute_definitions="${OPTARG}" ;;
      k) key_schema="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$table_name" ]]; then
    errecho "ERROR: You must provide a table name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$attribute_definitions" ]]; then
```

```
    errecho "ERROR: You must provide an attribute definitions json file path the -a
 parameter."
    usage
    return 1
  fi

  if [[ -z "$key_schema" ]]; then
    errecho "ERROR: You must provide a key schema json file path the -k parameter."
    usage
    return 1
  fi

  iecho "Parameters:\n"
  iecho "    table_name:   $table_name"
  iecho "    attribute_definitions:   $attribute_definitions"
  iecho "    key_schema:   $key_schema"
  iecho ""

  response=$(aws dynamodb create-table \
    --table-name "$table_name" \
    --attribute-definitions file://"$attribute_definitions" \
    --billing-mode PAY_PER_REQUEST \
    --key-schema file://"$key_schema" )

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-table operation failed.$response"
    return 1
  fi

  return 0
}

###############################################################################
# function dynamodb_describe_table
#
# This function returns the status of a DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table.
#
#  Response:
```

```
#       - TableStatus:
#     And:
#       0 - Table is active.
#       1 - If it fails.
###############################################################################
function dynamodb_describe_table {
  local table_name
  local option OPTARG # Required to use getopts command in a function.

  ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_describe_table"
    echo "Describe the status of a DynamoDB table."
    echo "  -n table_name  -- The name of the table."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:h" option; do
    case "${option}" in
      n) table_name="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$table_name" ]]; then
    errecho "ERROR: You must provide a table name with the -n parameter."
    usage
    return 1
  fi

  local table_status
    table_status=$(
```

```
      aws dynamodb describe-table \
        --table-name "$table_name" \
        --output text \
        --query 'Table.TableStatus'
    )

   local error_code=${?}

    if [[ $error_code -ne 0 ]]; then
      aws_cli_error_log "$error_code"
      errecho "ERROR: AWS reports describe-table operation failed.$table_status"
      return 1
    fi

  echo "$table_status"

  return 0
}

###############################################################################
# function dynamodb_put_item
#
# This function puts an item into a DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table.
#       -i item  -- Path to json file containing the item values.
#
#  Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_put_item() {
  local table_name item response
  local option OPTARG # Required to use getopts command in a function.

  ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_put_item"
    echo "Put an item into a DynamoDB table."
    echo " -n table_name  -- The name of the table."
    echo " -i item  -- Path to json file containing the item values."
```

```
  echo ""
}

while getopts "n:i:h" option; do
  case "${option}" in
    n) table_name="${OPTARG}" ;;
    i) item="${OPTARG}" ;;
    h)
      usage
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$table_name" ]]; then
  errecho "ERROR: You must provide a table name with the -n parameter."
  usage
  return 1
fi

if [[ -z "$item" ]]; then
  errecho "ERROR: You must provide an item with the -i parameter."
  usage
  return 1
fi

iecho "Parameters:\n"
iecho "    table_name:   $table_name"
iecho "    item:   $item"
iecho ""
iecho ""

response=$(aws dynamodb put-item \
  --table-name "$table_name" \
  --item file://"$item")

local error_code=${?}
```

```
  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports put-item operation failed.$response"
    return 1
  fi

  return 0

}

# bashsupport disable=BP5008
function dynamodb_update_item() {
  local table_name keys update_expression values response
  local option OPTARG # Required to use getopts command in a function.

  ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_update_item"
    echo "Update an item in a DynamoDB table."
    echo " -n table_name  -- The name of the table."
    echo " -k keys  -- Path to json file containing the keys that identify the item
 to update."
    echo " -e update expression  -- An expression that defines one or more
 attributes to be updated."
    echo " -v values  -- Path to json file containing the update values."
```

```
  echo ""
}

while getopts "n:k:e:v:h" option; do
  case "${option}" in
    n) table_name="${OPTARG}" ;;
    k) keys="${OPTARG}" ;;
    e) update_expression="${OPTARG}" ;;
    v) values="${OPTARG}" ;;
    h)
      usage
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$table_name" ]]; then
  errecho "ERROR: You must provide a table name with the -n parameter."
  usage
  return 1
fi

if [[ -z "$keys" ]]; then
  errecho "ERROR: You must provide a keys json file path the -k parameter."
  usage
  return 1
fi
if [[ -z "$update_expression" ]]; then
  errecho "ERROR: You must provide an update expression with the -e parameter."
  usage
  return 1
fi

if [[ -z "$values" ]]; then
  errecho "ERROR: You must provide a values json file path the -v parameter."
  usage
  return 1
fi
```

```
  iecho "Parameters:\n"
  iecho "    table_name:   $table_name"
  iecho "    keys:   $keys"
  iecho "    update_expression:   $update_expression"
  iecho "    values:   $values"

  response=$(aws dynamodb update-item \
    --table-name "$table_name" \
    --key file://"$keys" \
    --update-expression "$update_expression" \
    --expression-attribute-values file://"$values")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports update-item operation failed.$response"
    return 1
  fi

  return 0

}

###############################################################################
# function dynamodb_batch_write_item
#
# This function writes a batch of items into a DynamoDB table.
#
# Parameters:
#       -i item  -- Path to json file containing the items to write.
#
#  Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_batch_write_item() {
  local item response
  local option OPTARG # Required to use getopts command in a function.

  ######################################
  # Function usage explanation
  ######################################
```

```
function usage() {
  echo "function dynamodb_batch_write_item"
  echo "Write a batch of items into a DynamoDB table."
  echo " -i item  -- Path to json file containing the items to write."
  echo ""
}
while getopts "i:h" option; do
  case "${option}" in
    i) item="${OPTARG}" ;;
    h)
      usage
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$item" ]]; then
  errecho "ERROR: You must provide an item with the -i parameter."
  usage
  return 1
fi

iecho "Parameters:\n"
iecho "    table_name:   $table_name"
iecho "    item:   $item"
iecho ""

response=$(aws dynamodb batch-write-item \
  --request-items file://"$item")

local error_code=${?}

if [[ $error_code -ne 0 ]]; then
  aws_cli_error_log $error_code
  errecho "ERROR: AWS reports batch-write-item operation failed.$response"
  return 1
fi
```

```
  return 0
}

###############################################################################
# function dynamodb_get_item
#
# This function gets an item from a DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table.
#       -k keys  -- Path to json file containing the keys that identify the item to
 get.
#       [-q query]  -- Optional JMESPath query expression.
#
#  Returns:
#       The item as text output.
#  And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_get_item() {
  local table_name keys query response
  local option OPTARG # Required to use getopts command in a function.

  # ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_get_item"
    echo "Get an item from a DynamoDB table."
    echo " -n table_name  -- The name of the table."
    echo " -k keys  -- Path to json file containing the keys that identify the item
 to get."
    echo " [-q query]  -- Optional JMESPath query expression."
    echo ""
  }
  query=""
  while getopts "n:k:q:h" option; do
    case "${option}" in
      n) table_name="${OPTARG}" ;;
      k) keys="${OPTARG}" ;;
      q) query="${OPTARG}" ;;
      h)
        usage
```

```
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$table_name" ]]; then
  errecho "ERROR: You must provide a table name with the -n parameter."
  usage
  return 1
fi

if [[ -z "$keys" ]]; then
  errecho "ERROR: You must provide a keys json file path the -k parameter."
  usage
  return 1
fi

if [[ -n "$query" ]]; then
  response=$(aws dynamodb get-item \
    --table-name "$table_name" \
    --key file://"$keys" \
    --output text \
    --query "$query")
else
  response=$(
    aws dynamodb get-item \
      --table-name "$table_name" \
      --key file://"$keys" \
      --output text
  )
fi

local error_code=${?}

if [[ $error_code -ne 0 ]]; then
  aws_cli_error_log $error_code
  errecho "ERROR: AWS reports get-item operation failed.$response"
  return 1
```

```
  fi

  if [[ -n "$query" ]]; then
    echo "$response" | sed "/^\t/s/\t//1" # Remove initial tab that the JMSEPath
 query inserts on some strings.
  else
    echo "$response"
  fi

  return 0
}

###############################################################################
# function dynamodb_query
#
# This function queries a DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table.
#       -k key_condition_expression -- The key condition expression.
#       -a attribute_names -- Path to JSON file containing the attribute names.
#       -v attribute_values -- Path to JSON file containing the attribute values.
#       [-p projection_expression]  -- Optional projection expression.
#
#  Returns:
#       The items as json output.
#  And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_query() {
  local table_name key_condition_expression attribute_names attribute_values
 projection_expression response
  local option OPTARG # Required to use getopts command in a function.

  # ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_query"
    echo "Query a DynamoDB table."
    echo " -n table_name  -- The name of the table."
    echo " -k key_condition_expression -- The key condition expression."
    echo " -a attribute_names -- Path to JSON file containing the attribute names."
```

```
    echo " -v attribute_values -- Path to JSON file containing the attribute
values."
    echo " [-p projection_expression]  -- Optional projection expression."
    echo ""
 }

 while getopts "n:k:a:v:p:h" option; do
    case "${option}" in
      n) table_name="${OPTARG}" ;;
      k) key_condition_expression="${OPTARG}" ;;
      a) attribute_names="${OPTARG}" ;;
      v) attribute_values="${OPTARG}" ;;
      p) projection_expression="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
 done
 export OPTIND=1

 if [[ -z "$table_name" ]]; then
    errecho "ERROR: You must provide a table name with the -n parameter."
    usage
    return 1
 fi

 if [[ -z "$key_condition_expression" ]]; then
    errecho "ERROR: You must provide a key condition expression with the -k
parameter."
    usage
    return 1
 fi

 if [[ -z "$attribute_names" ]]; then
    errecho "ERROR: You must provide a attribute names with the -a parameter."
    usage
    return 1
 fi
```

```
  if [[ -z "$attribute_values" ]]; then
    errecho "ERROR: You must provide a attribute values with the -v parameter."
    usage
    return 1
  fi

  if [[ -z "$projection_expression" ]]; then
    response=$(aws dynamodb query \
      --table-name "$table_name" \
      --key-condition-expression "$key_condition_expression" \
      --expression-attribute-names file://"$attribute_names" \
      --expression-attribute-values file://"$attribute_values")
  else
    response=$(aws dynamodb query \
      --table-name "$table_name" \
      --key-condition-expression "$key_condition_expression" \
      --expression-attribute-names file://"$attribute_names" \
      --expression-attribute-values file://"$attribute_values" \
      --projection-expression "$projection_expression")
  fi

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports query operation failed.$response"
    return 1
  fi

  echo "$response"

  return 0
}

###############################################################################
# function dynamodb_scan
#
# This function scans a DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table.
#       -f filter_expression  -- The filter expression.
```

```
#       -a expression_attribute_names -- Path to JSON file containing the expression
 attribute names.
#       -v expression_attribute_values -- Path to JSON file containing the
 expression attribute values.
#       [-p projection_expression]  -- Optional projection expression.
#
#  Returns:
#       The items as json output.
#  And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_scan() {
  local table_name filter_expression expression_attribute_names
 expression_attribute_values projection_expression response
  local option OPTARG # Required to use getopts command in a function.

  # ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_scan"
    echo "Scan a DynamoDB table."
    echo " -n table_name  -- The name of the table."
    echo " -f filter_expression  -- The filter expression."
    echo " -a expression_attribute_names -- Path to JSON file containing the
 expression attribute names."
    echo " -v expression_attribute_values -- Path to JSON file containing the
 expression attribute values."
    echo " [-p projection_expression]  -- Optional projection expression."
    echo ""
  }

  while getopts "n:f:a:v:p:h" option; do
    case "${option}" in
      n) table_name="${OPTARG}" ;;
      f) filter_expression="${OPTARG}" ;;
      a) expression_attribute_names="${OPTARG}" ;;
      v) expression_attribute_values="${OPTARG}" ;;
      p) projection_expression="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
```

```
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$table_name" ]]; then
  errecho "ERROR: You must provide a table name with the -n parameter."
  usage
  return 1
fi

if [[ -z "$filter_expression" ]]; then
  errecho "ERROR: You must provide a filter expression with the -f parameter."
  usage
  return 1
fi

if [[ -z "$expression_attribute_names" ]]; then
  errecho "ERROR: You must provide expression attribute names with the -a
parameter."
  usage
  return 1
fi

if [[ -z "$expression_attribute_values" ]]; then
  errecho "ERROR: You must provide expression attribute values with the -v
parameter."
  usage
  return 1
fi

if [[ -z "$projection_expression" ]]; then
  response=$(aws dynamodb scan \
    --table-name "$table_name" \
    --filter-expression "$filter_expression" \
    --expression-attribute-names file://"$expression_attribute_names" \
    --expression-attribute-values file://"$expression_attribute_values")
else
  response=$(aws dynamodb scan \
    --table-name "$table_name" \
```

```
      --filter-expression "$filter_expression" \
      --expression-attribute-names file://"$expression_attribute_names" \
      --expression-attribute-values file://"$expression_attribute_values" \
      --projection-expression "$projection_expression")
  fi

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports scan operation failed.$response"
    return 1
  fi

  echo "$response"

  return 0
}

###############################################################################
# function dynamodb_delete_item
#
# This function deletes an item from a DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table.
#       -k keys  -- Path to json file containing the keys that identify the item to
 delete.
#
#  Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_delete_item() {
  local table_name keys response
  local option OPTARG # Required to use getopts command in a function.

  # ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_delete_item"
    echo "Delete an item from a DynamoDB table."
    echo " -n table_name  -- The name of the table."
```

```
    echo " -k keys  -- Path to json file containing the keys that identify the item
 to delete."
    echo ""
 }
 while getopts "n:k:h" option; do
    case "${option}" in
      n) table_name="${OPTARG}" ;;
      k) keys="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
 done
 export OPTIND=1

 if [[ -z "$table_name" ]]; then
    errecho "ERROR: You must provide a table name with the -n parameter."
    usage
    return 1
 fi

 if [[ -z "$keys" ]]; then
    errecho "ERROR: You must provide a keys json file path the -k parameter."
    usage
    return 1
 fi

 iecho "Parameters:\n"
 iecho "    table_name:   $table_name"
 iecho "    keys:   $keys"
 iecho ""

 response=$(aws dynamodb delete-item \
    --table-name "$table_name" \
    --key file://"$keys")

 local error_code=${?}
```

```
  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports delete-item operation failed.$response"
    return 1
  fi

  return 0

}

###############################################################################
# function dynamodb_delete_table
#
# This function deletes a DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table to delete.
#
#  Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_delete_table() {
  local table_name response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function dynamodb_delete_table"
    echo "Deletes an Amazon DynamoDB table."
    echo " -n table_name  -- The name of the table to delete."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:h" option; do
    case "${option}" in
      n) table_name="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
```

```
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$table_name" ]]; then
    errecho "ERROR: You must provide a table name with the -n parameter."
    usage
    return 1
  fi

  iecho "Parameters:\n"
  iecho "    table_name:   $table_name"
  iecho ""

  response=$(aws dynamodb delete-table \
    --table-name "$table_name")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports delete-table operation failed.$response"
    return 1
  fi

  return 0
}
```

Las funciones de utilidad usadas en este escenario.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
```

```
  fi
}

############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# See https://docs.aws.amazon.com/cli/latest/topic/return-codes.html#cli-aws-help-
return-codes.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
```

```
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - BatchWriteItem
  - CreateTable
  - DeleteItem
  - DeleteTable
  - DescribeTable
  - GetItem
  - PutItem
  - Query
  - Examen
  - UpdateItem

Acciones

`BatchGetItem`

En el siguiente ejemplo de código, se muestra cómo utilizar `BatchGetItem`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
# function dynamodb_batch_get_item
#
# This function gets a batch of items from a DynamoDB table.
```

```
#
# Parameters:
#       -i item  -- Path to json file containing the keys of the items to get.
#
#  Returns:
#       The items as json output.
#  And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_batch_get_item() {
  local item response
  local option OPTARG # Required to use getopts command in a function.

  ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_batch_get_item"
    echo "Get a batch of items from a DynamoDB table."
    echo " -i item  -- Path to json file containing the keys of the items to get."
    echo ""
  }

  while getopts "i:h" option; do
    case "${option}" in
      i) item="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$item" ]]; then
    errecho "ERROR: You must provide an item with the -i parameter."
    usage
    return 1
```

```
  fi

  response=$(aws dynamodb batch-get-item \
    --request-items file://"$item")
  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports batch-get-item operation failed.$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# See https://docs.aws.amazon.com/cli/latest/topic/return-codes.html#cli-aws-help-
return-codes.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
```

```
###############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información de la API, consulte BatchGetItem en la Referencia de comandos de la AWS CLI.

`BatchWriteItem`

En el siguiente ejemplo de código, se muestra cómo utilizar `BatchWriteItem`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function dynamodb_batch_write_item
```

```
#
# This function writes a batch of items into a DynamoDB table.
#
# Parameters:
#       -i item  -- Path to json file containing the items to write.
#
#  Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_batch_write_item() {
  local item response
  local option OPTARG # Required to use getopts command in a function.

  ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_batch_write_item"
    echo "Write a batch of items into a DynamoDB table."
    echo " -i item  -- Path to json file containing the items to write."
    echo ""
  }
  while getopts "i:h" option; do
    case "${option}" in
      i) item="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$item" ]]; then
    errecho "ERROR: You must provide an item with the -i parameter."
    usage
    return 1
  fi
```

```
  iecho "Parameters:\n"
  iecho "    table_name:   $table_name"
  iecho "    item:   $item"
  iecho ""

  response=$(aws dynamodb batch-write-item \
    --request-items file://"$item")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports batch-write-item operation failed.$response"
    return 1
  fi

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}
```

```
###############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# See https://docs.aws.amazon.com/cli/latest/topic/return-codes.html#cli-aws-help-
return-codes.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
###############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información de la API, consulte BatchWriteItem en la Referencia de comandos de la AWS CLI.

`CreateTable`

En el siguiente ejemplo de código, se muestra cómo utilizar `CreateTable`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function dynamodb_create_table
#
# This function creates an Amazon DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table to create.
#       -a attribute_definitions -- JSON file path of a list of attributes and their
 types.
#       -k key_schema -- JSON file path of a list of attributes and their key types.
#
#  Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_create_table() {
  local table_name attribute_definitions key_schema response
  local option OPTARG # Required to use getopts command in a function.

  ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_create_table"
    echo "Creates an Amazon DynamoDB table with on-demand billing."
    echo " -n table_name  -- The name of the table to create."
    echo " -a attribute_definitions -- JSON file path of a list of attributes and
 their types."
    echo " -k key_schema -- JSON file path of a list of attributes and their key
 types."
    echo ""
```

```
  }

  # Retrieve the calling parameters.
  while getopts "n:a:k:h" option; do
    case "${option}" in
      n) table_name="${OPTARG}" ;;
      a) attribute_definitions="${OPTARG}" ;;
      k) key_schema="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$table_name" ]]; then
    errecho "ERROR: You must provide a table name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$attribute_definitions" ]]; then
    errecho "ERROR: You must provide an attribute definitions json file path the -a
parameter."
    usage
    return 1
  fi

  if [[ -z "$key_schema" ]]; then
    errecho "ERROR: You must provide a key schema json file path the -k parameter."
    usage
    return 1
  fi

  iecho "Parameters:\n"
  iecho "    table_name:   $table_name"
  iecho "    attribute_definitions:   $attribute_definitions"
  iecho "    key_schema:   $key_schema"
```

```
  iecho ""

  response=$(aws dynamodb create-table \
    --table-name "$table_name" \
    --attribute-definitions file://"$attribute_definitions" \
    --billing-mode PAY_PER_REQUEST \
    --key-schema file://"$key_schema" )

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-table operation failed.$response"
    return 1
  fi

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}
```

```
###############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# See https://docs.aws.amazon.com/cli/latest/topic/return-codes.html#cli-aws-help-
return-codes.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
###############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte CreateTable en la Referencia de comandos de la AWS CLI.

`DeleteItem`

En el siguiente ejemplo de código, se muestra cómo utilizar `DeleteItem`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function dynamodb_delete_item
#
# This function deletes an item from a DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table.
#       -k keys  -- Path to json file containing the keys that identify the item to
 delete.
#
#  Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_delete_item() {
  local table_name keys response
  local option OPTARG # Required to use getopts command in a function.

  # ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_delete_item"
    echo "Delete an item from a DynamoDB table."
    echo " -n table_name  -- The name of the table."
    echo " -k keys  -- Path to json file containing the keys that identify the item
 to delete."
    echo ""
  }
  while getopts "n:k:h" option; do
    case "${option}" in
```

```
    n) table_name="${OPTARG}" ;;
    k) keys="${OPTARG}" ;;
    h)
      usage
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$table_name" ]]; then
  errecho "ERROR: You must provide a table name with the -n parameter."
  usage
  return 1
fi

if [[ -z "$keys" ]]; then
  errecho "ERROR: You must provide a keys json file path the -k parameter."
  usage
  return 1
fi

iecho "Parameters:\n"
iecho "    table_name:   $table_name"
iecho "    keys:   $keys"
iecho ""

response=$(aws dynamodb delete-item \
  --table-name "$table_name" \
  --key file://"$keys")

local error_code=${?}

if [[ $error_code -ne 0 ]]; then
  aws_cli_error_log $error_code
  errecho "ERROR: AWS reports delete-item operation failed.$response"
  return 1
fi
```

```
  return 0

}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
################################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
################################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

################################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
################################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

################################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# See https://docs.aws.amazon.com/cli/latest/topic/return-codes.html#cli-aws-help-
return-codes.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
################################################################################
```

```
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte DeleteItem en la Referencia de comandos de la AWS CLI.

`DeleteTable`

En el siguiente ejemplo de código, se muestra cómo utilizar `DeleteTable`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function dynamodb_delete_table
#
```

```
# This function deletes a DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table to delete.
#
#  Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_delete_table() {
  local table_name response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function dynamodb_delete_table"
    echo "Deletes an Amazon DynamoDB table."
    echo " -n table_name  -- The name of the table to delete."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:h" option; do
    case "${option}" in
      n) table_name="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$table_name" ]]; then
    errecho "ERROR: You must provide a table name with the -n parameter."
    usage
    return 1
  fi
```

```
  iecho "Parameters:\n"
  iecho "    table_name:   $table_name"
  iecho ""

  response=$(aws dynamodb delete-table \
    --table-name "$table_name")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports delete-table operation failed.$response"
    return 1
  fi

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
```

```
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# See https://docs.aws.amazon.com/cli/latest/topic/return-codes.html#cli-aws-help-
return-codes.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
################################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte DeleteTable en la Referencia de comandos de la AWS CLI.

`DescribeTable`

En el siguiente ejemplo de código, se muestra cómo utilizar `DescribeTable`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function dynamodb_describe_table
#
# This function returns the status of a DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table.
#
#  Response:
#       - TableStatus:
#     And:
#       0 - Table is active.
#       1 - If it fails.
###############################################################################
function dynamodb_describe_table {
  local table_name
  local option OPTARG # Required to use getopts command in a function.

  ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_describe_table"
    echo "Describe the status of a DynamoDB table."
    echo "  -n table_name  -- The name of the table."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:h" option; do
    case "${option}" in
      n) table_name="${OPTARG}" ;;
      h)
        usage
```

```
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$table_name" ]]; then
    errecho "ERROR: You must provide a table name with the -n parameter."
    usage
    return 1
  fi

  local table_status
    table_status=$(
      aws dynamodb describe-table \
        --table-name "$table_name" \
        --output text \
        --query 'Table.TableStatus'
    )

   local error_code=${?}

    if [[ $error_code -ne 0 ]]; then
      aws_cli_error_log "$error_code"
      errecho "ERROR: AWS reports describe-table operation failed.$table_status"
      return 1
    fi

  echo "$table_status"

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
```

```
#
# This function outputs everything sent to it to STDERR (standard error output).
#############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

#############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# See https://docs.aws.amazon.com/cli/latest/topic/return-codes.html#cli-aws-help-
return-codes.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
#############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte DescribeTable en la Referencia de comandos de la AWS CLI.

`GetItem`

En el siguiente ejemplo de código, se muestra cómo utilizar `GetItem`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function dynamodb_get_item
#
# This function gets an item from a DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table.
#       -k keys  -- Path to json file containing the keys that identify the item to
 get.
#       [-q query]  -- Optional JMESPath query expression.
#
#  Returns:
#       The item as text output.
#  And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_get_item() {
  local table_name keys query response
  local option OPTARG # Required to use getopts command in a function.

  # ######################################
  # Function usage explanation
  ######################################
```

```
 function usage() {
   echo "function dynamodb_get_item"
   echo "Get an item from a DynamoDB table."
   echo " -n table_name  -- The name of the table."
   echo " -k keys  -- Path to json file containing the keys that identify the item
to get."
   echo " [-q query]  -- Optional JMESPath query expression."
   echo ""
 }
 query=""
 while getopts "n:k:q:h" option; do
   case "${option}" in
     n) table_name="${OPTARG}" ;;
     k) keys="${OPTARG}" ;;
     q) query="${OPTARG}" ;;
     h)
       usage
       return 0
       ;;
     \?)
       echo "Invalid parameter"
       usage
       return 1
       ;;
   esac
 done
 export OPTIND=1

 if [[ -z "$table_name" ]]; then
   errecho "ERROR: You must provide a table name with the -n parameter."
   usage
   return 1
 fi

 if [[ -z "$keys" ]]; then
   errecho "ERROR: You must provide a keys json file path the -k parameter."
   usage
   return 1
 fi

 if [[ -n "$query" ]]; then
   response=$(aws dynamodb get-item \
     --table-name "$table_name" \
     --key file://"$keys" \
```

```
      --output text \
      --query "$query")
  else
    response=$(
      aws dynamodb get-item \
        --table-name "$table_name" \
        --key file://"$keys" \
        --output text
    )
  fi

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports get-item operation failed.$response"
    return 1
  fi

  if [[ -n "$query" ]]; then
    echo "$response" | sed "/^\t/s/\t//1" # Remove initial tab that the JMSEPath
 query inserts on some strings.
  else
    echo "$response"
  fi

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function aws_cli_error_log()
```

```
#
# This function is used to log the error messages from the AWS CLI.
#
# See https://docs.aws.amazon.com/cli/latest/topic/return-codes.html#cli-aws-help-
return-codes.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
################################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte GetItem en la Referencia de comandos de la AWS CLI.

`ListTables`

En el siguiente ejemplo de código, se muestra cómo utilizar `ListTables`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
# function dynamodb_list_tables
#
# This function lists all the tables in a DynamoDB.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
##############################################################################
function dynamodb_list_tables() {
  response=$(aws dynamodb list-tables \
    --output text \
    --query "TableNames")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports batch-write-item operation failed.$response"
    return 1
  fi

  echo "$response" | tr -s "[:space:]" "\n"

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
##############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
```

```
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# See https://docs.aws.amazon.com/cli/latest/topic/return-codes.html#cli-aws-help-
return-codes.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
###############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte ListTables en la Referencia de comandos de la AWS CLI.

`PutItem`

En el siguiente ejemplo de código, se muestra cómo utilizar `PutItem`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function dynamodb_put_item
#
# This function puts an item into a DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table.
#       -i item  -- Path to json file containing the item values.
#
#  Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_put_item() {
  local table_name item response
  local option OPTARG # Required to use getopts command in a function.

  ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_put_item"
    echo "Put an item into a DynamoDB table."
    echo " -n table_name  -- The name of the table."
    echo " -i item  -- Path to json file containing the item values."
    echo ""
  }
```

```
while getopts "n:i:h" option; do
  case "${option}" in
    n) table_name="${OPTARG}" ;;
    i) item="${OPTARG}" ;;
    h)
      usage
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$table_name" ]]; then
  errecho "ERROR: You must provide a table name with the -n parameter."
  usage
  return 1
fi

if [[ -z "$item" ]]; then
  errecho "ERROR: You must provide an item with the -i parameter."
  usage
  return 1
fi

iecho "Parameters:\n"
iecho "    table_name:   $table_name"
iecho "    item:   $item"
iecho ""
iecho ""

response=$(aws dynamodb put-item \
  --table-name "$table_name" \
  --item file://"$item")

local error_code=${?}

if [[ $error_code -ne 0 ]]; then
  aws_cli_error_log $error_code
```

```
    errecho "ERROR: AWS reports put-item operation failed.$response"
    return 1
  fi

  return 0

}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# See https://docs.aws.amazon.com/cli/latest/topic/return-codes.html#cli-aws-help-
return-codes.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
```

```
#  Returns:
#          0: - Success.
#
###############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte PutItem en la Referencia de comandos de la AWS CLI.

`Query`

En el siguiente ejemplo de código, se muestra cómo utilizar `Query`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function dynamodb_query
#
# This function queries a DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table.
#       -k key_condition_expression -- The key condition expression.
#       -a attribute_names -- Path to JSON file containing the attribute names.
#       -v attribute_values -- Path to JSON file containing the attribute values.
#       [-p projection_expression]  -- Optional projection expression.
#
#  Returns:
#       The items as json output.
#  And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_query() {
  local table_name key_condition_expression attribute_names attribute_values
 projection_expression response
  local option OPTARG # Required to use getopts command in a function.

  # ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_query"
    echo "Query a DynamoDB table."
    echo " -n table_name  -- The name of the table."
    echo " -k key_condition_expression -- The key condition expression."
    echo " -a attribute_names -- Path to JSON file containing the attribute names."
    echo " -v attribute_values -- Path to JSON file containing the attribute
 values."
    echo " [-p projection_expression]  -- Optional projection expression."
    echo ""
  }

  while getopts "n:k:a:v:p:h" option; do
    case "${option}" in
      n) table_name="${OPTARG}" ;;
      k) key_condition_expression="${OPTARG}" ;;
      a) attribute_names="${OPTARG}" ;;
```

```
      v) attribute_values="${OPTARG}" ;;
      p) projection_expression="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$table_name" ]]; then
    errecho "ERROR: You must provide a table name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$key_condition_expression" ]]; then
    errecho "ERROR: You must provide a key condition expression with the -k
parameter."
    usage
    return 1
  fi

  if [[ -z "$attribute_names" ]]; then
    errecho "ERROR: You must provide a attribute names with the -a parameter."
    usage
    return 1
  fi

  if [[ -z "$attribute_values" ]]; then
    errecho "ERROR: You must provide a attribute values with the -v parameter."
    usage
    return 1
  fi

  if [[ -z "$projection_expression" ]]; then
    response=$(aws dynamodb query \
      --table-name "$table_name" \
      --key-condition-expression "$key_condition_expression" \
```

```
      --expression-attribute-names file://"$attribute_names" \
      --expression-attribute-values file://"$attribute_values")
  else
    response=$(aws dynamodb query \
      --table-name "$table_name" \
      --key-condition-expression "$key_condition_expression" \
      --expression-attribute-names file://"$attribute_names" \
      --expression-attribute-values file://"$attribute_values" \
      --projection-expression "$projection_expression")
  fi

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports query operation failed.$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# See https://docs.aws.amazon.com/cli/latest/topic/return-codes.html#cli-aws-help-
return-codes.
```

```
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
################################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte Query en la Referencia de comandos de la AWS CLI.

Scan

En el siguiente ejemplo de código, se muestra cómo utilizar `Scan`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function dynamodb_scan
#
# This function scans a DynamoDB table.
#
# Parameters:
#       -n table_name  -- The name of the table.
#       -f filter_expression  -- The filter expression.
#       -a expression_attribute_names -- Path to JSON file containing the expression
 attribute names.
#       -v expression_attribute_values -- Path to JSON file containing the
 expression attribute values.
#       [-p projection_expression]  -- Optional projection expression.
#
#  Returns:
#       The items as json output.
#  And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function dynamodb_scan() {
  local table_name filter_expression expression_attribute_names
 expression_attribute_values projection_expression response
  local option OPTARG # Required to use getopts command in a function.

  # ######################################
  # Function usage explanation
  ######################################
  function usage() {
    echo "function dynamodb_scan"
    echo "Scan a DynamoDB table."
    echo " -n table_name  -- The name of the table."
    echo " -f filter_expression  -- The filter expression."
```

```
   echo " -a expression_attribute_names -- Path to JSON file containing the
expression attribute names."
   echo " -v expression_attribute_values -- Path to JSON file containing the
expression attribute values."
   echo " [-p projection_expression]  -- Optional projection expression."
   echo ""
 }

 while getopts "n:f:a:v:p:h" option; do
   case "${option}" in
     n) table_name="${OPTARG}" ;;
     f) filter_expression="${OPTARG}" ;;
     a) expression_attribute_names="${OPTARG}" ;;
     v) expression_attribute_values="${OPTARG}" ;;
     p) projection_expression="${OPTARG}" ;;
     h)
       usage
       return 0
       ;;
     \?)
       echo "Invalid parameter"
       usage
       return 1
       ;;
   esac
 done
 export OPTIND=1

 if [[ -z "$table_name" ]]; then
   errecho "ERROR: You must provide a table name with the -n parameter."
   usage
   return 1
 fi

 if [[ -z "$filter_expression" ]]; then
   errecho "ERROR: You must provide a filter expression with the -f parameter."
   usage
   return 1
 fi

 if [[ -z "$expression_attribute_names" ]]; then
   errecho "ERROR: You must provide expression attribute names with the -a
parameter."
   usage
```

```
    return 1
  fi

  if [[ -z "$expression_attribute_values" ]]; then
    errecho "ERROR: You must provide expression attribute values with the -v
 parameter."
    usage
    return 1
  fi

  if [[ -z "$projection_expression" ]]; then
    response=$(aws dynamodb scan \
      --table-name "$table_name" \
      --filter-expression "$filter_expression" \
      --expression-attribute-names file://"$expression_attribute_names" \
      --expression-attribute-values file://"$expression_attribute_values")
  else
    response=$(aws dynamodb scan \
      --table-name "$table_name" \
      --filter-expression "$filter_expression" \
      --expression-attribute-names file://"$expression_attribute_names" \
      --expression-attribute-values file://"$expression_attribute_values" \
      --projection-expression "$projection_expression")
  fi

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports scan operation failed.$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
```

```
#
# This function outputs everything sent to it to STDERR (standard error output).
#############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

#############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# See https://docs.aws.amazon.com/cli/latest/topic/return-codes.html#cli-aws-help-
return-codes.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
#############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte Scan en la Referencia de comandos de la AWS CLI.

`UpdateItem`

En el siguiente ejemplo de código, se muestra cómo utilizar `UpdateItem`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
# function dynamodb_update_item
#
# This function updates an item in a DynamoDB table.
#
#
# Parameters:
#       -n table_name  -- The name of the table.
#       -k keys  -- Path to json file containing the keys that identify the item to
 update.
#       -e update expression  -- An expression that defines one or more attributes
 to be updated.
#       -v values  -- Path to json file containing the update values.
#
#  Returns:
#       0 - If successful.
#       1 - If it fails.
##############################################################################
function dynamodb_update_item() {
  local table_name keys update_expression values response
  local option OPTARG # Required to use getopts command in a function.

  ######################################
  # Function usage explanation
```

```
 ######################################
 function usage() {
   echo "function dynamodb_update_item"
   echo "Update an item in a DynamoDB table."
   echo " -n table_name  -- The name of the table."
   echo " -k keys  -- Path to json file containing the keys that identify the item
to update."
   echo " -e update expression  -- An expression that defines one or more
attributes to be updated."
   echo " -v values  -- Path to json file containing the update values."
   echo ""
 }

 while getopts "n:k:e:v:h" option; do
   case "${option}" in
     n) table_name="${OPTARG}" ;;
     k) keys="${OPTARG}" ;;
     e) update_expression="${OPTARG}" ;;
     v) values="${OPTARG}" ;;
     h)
       usage
       return 0
       ;;
     \?)
       echo "Invalid parameter"
       usage
       return 1
       ;;
   esac
 done
 export OPTIND=1

 if [[ -z "$table_name" ]]; then
   errecho "ERROR: You must provide a table name with the -n parameter."
   usage
   return 1
 fi

 if [[ -z "$keys" ]]; then
   errecho "ERROR: You must provide a keys json file path the -k parameter."
   usage
   return 1
 fi
 if [[ -z "$update_expression" ]]; then
```

```
    errecho "ERROR: You must provide an update expression with the -e parameter."
    usage
    return 1
  fi

  if [[ -z "$values" ]]; then
    errecho "ERROR: You must provide a values json file path the -v parameter."
    usage
    return 1
  fi

  iecho "Parameters:\n"
  iecho "    table_name:   $table_name"
  iecho "    keys:   $keys"
  iecho "    update_expression:   $update_expression"
  iecho "    values:   $values"

  response=$(aws dynamodb update-item \
    --table-name "$table_name" \
    --key file://"$keys" \
    --update-expression "$update_expression" \
    --expression-attribute-values file://"$values")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports update-item operation failed.$response"
    return 1
  fi

  return 0

}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
```

```
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# See https://docs.aws.amazon.com/cli/latest/topic/return-codes.html#cli-aws-help-
return-codes.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
###############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
```

```
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte UpdateItem en la Referencia de comandos de la AWS CLI.

Escenarios

Escenarios avanzados de índice secundario global

En el siguiente ejemplo de código se muestra cómo trabajar con configuraciones avanzadas de índice secundario global.

- Cree una tabla con varios GSI.
- Cree una tabla con capacidad bajo demanda y GSI.
- Coloque elementos en una tabla con múltiples GSI.
- Consultar múltiples GSI con diferentes condiciones.

AWS CLI con Bash script

Cree una tabla con varios GSI.

```
# Create a table with multiple GSIs
aws dynamodb create-table \
    --table-name MusicLibrary \
    --attribute-definitions \
        AttributeName=Artist,AttributeType=S \
        AttributeName=SongTitle,AttributeType=S \
        AttributeName=AlbumTitle,AttributeType=S \
        AttributeName=Genre,AttributeType=S \
        AttributeName=Year,AttributeType=N \
    --key-schema \
        AttributeName=Artist,KeyType=HASH \
```

```
        AttributeName=SongTitle,KeyType=RANGE \
    --billing-mode PAY_PER_REQUEST \
    --global-secondary-indexes \
        "[
            {
                \"IndexName\": \"AlbumIndex\",
                \"KeySchema\": [{\"AttributeName\":\"AlbumTitle\",\"KeyType\":\"HASH
\"}],
                \"Projection\": {\"ProjectionType\":\"ALL\"}
            },
            {
                \"IndexName\": \"GenreYearIndex\",
                \"KeySchema\": [
                    {\"AttributeName\":\"Genre\",\"KeyType\":\"HASH\"},
                    {\"AttributeName\":\"Year\",\"KeyType\":\"RANGE\"}
                ],
                \"Projection\": {\"ProjectionType\":\"INCLUDE\",\"NonKeyAttributes
\":[\"Artist\",\"SongTitle\"]}
            }
        ]"
```

Cree una tabla con capacidad bajo demanda y GSI.

```
# Create a table with on-demand capacity and GSI
aws dynamodb create-table \
    --table-name MusicOnDemand \
    --attribute-definitions \
        AttributeName=Artist,AttributeType=S \
        AttributeName=SongTitle,AttributeType=S \
        AttributeName=Genre,AttributeType=S \
    --key-schema \
        AttributeName=Artist,KeyType=HASH \
        AttributeName=SongTitle,KeyType=RANGE \
    --billing-mode PAY_PER_REQUEST \
    --global-secondary-indexes \
        "[
            {
                \"IndexName\": \"GenreIndex\",
                \"KeySchema\": [{\"AttributeName\":\"Genre\",\"KeyType\":\"HASH\"}],
                \"Projection\": {\"ProjectionType\":\"ALL\"}
            }
        ]"
```

Coloque elementos en una tabla con múltiples GSI.

```
# Add items to MusicLibrary table
aws dynamodb put-item \
    --table-name MusicLibrary \
    --item '{
        "Artist": {"S": "The Beatles"},
        "SongTitle": {"S": "Hey Jude"},
        "AlbumTitle": {"S": "Past Masters"},
        "Genre": {"S": "Rock"},
        "Year": {"N": "1968"}
    }'

aws dynamodb put-item \
    --table-name MusicLibrary \
    --item '{
        "Artist": {"S": "Miles Davis"},
        "SongTitle": {"S": "So What"},
        "AlbumTitle": {"S": "Kind of Blue"},
        "Genre": {"S": "Jazz"},
        "Year": {"N": "1959"}
    }'
```

Consulte elementos de una tabla con múltiples GSI.

```
# Query the AlbumIndex GSI
echo "Querying AlbumIndex GSI:"
aws dynamodb query \
    --table-name MusicLibrary \
    --index-name AlbumIndex \
    --key-condition-expression "AlbumTitle = :album" \
    --expression-attribute-values '{":album":{"S":"Kind of Blue"}}'

# Query the GenreYearIndex GSI with a range condition
echo "Querying GenreYearIndex GSI with range condition:"
aws dynamodb query \
    --table-name MusicLibrary \
    --index-name GenreYearIndex \
    --key-condition-expression "Genre = :genre AND #yr > :year" \
    --expression-attribute-names '{"#yr": "Year"}' \
```

```
    --expression-attribute-values '{":genre":{"S":"Rock"},":year":{"N":"1965"}}'
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreateTable
  - PutItem
  - Query

Creación y administración de tablas globales de MRSC

En el siguiente ejemplo de código, se muestra cómo crear y administrar las tablas globales de DynamoDB con coherencia alta de varias regiones (MRSC).

- Cree una tabla con coherencia alta de varias regiones.
- Verifique la configuración de MRSC y el estado de la réplica.
- Pruebe la coherencia alta entre regiones con lecturas inmediatas.
- Realice escrituras condicionales con garantías de MRSC.
- Limpie los recursos de la tabla global de MRSC.

AWS CLI con Bash script

Cree una tabla con coherencia alta de varias regiones.

```
# Step 1: Create a new table in us-east-2 (primary region for MRSC)
# Note: Table must be empty when enabling MRSC
aws dynamodb create-table \
    --table-name MusicTable \
    --attribute-definitions \
        AttributeName=Artist,AttributeType=S \
        AttributeName=SongTitle,AttributeType=S \
    --key-schema \
        AttributeName=Artist,KeyType=HASH \
        AttributeName=SongTitle,KeyType=RANGE \
    --billing-mode PAY_PER_REQUEST \
    --region us-east-2

# Wait for table to become active
```

```
aws dynamodb wait table-exists --table-name MusicTable --region us-east-2

# Step 2: Add replica and witness with Multi-Region Strong Consistency
# MRSC requires exactly three replicas in supported regions
aws dynamodb update-table \
    --table-name MusicTable \
    --replica-updates '[{"Create": {"RegionName": "us-east-1"}}]' \
    --global-table-witness-updates '[{"Create": {"RegionName": "us-west-2"}}]' \
    --multi-region-consistency STRONG \
    --region us-east-2
```

Verifique la configuración de MRSC y el estado de la réplica.

```
# Verify the global table configuration and MRSC setting
aws dynamodb describe-table \
    --table-name MusicTable \
    --region us-east-2 \
    --query 'Table.
{TableName:TableName,TableStatus:TableStatus,MultiRegionConsistency:MultiRegionConsistency,R
{Region:RegionName,Status:ReplicaStatus}}'
```

Pruebe la coherencia alta con lecturas inmediatas entre regiones.

```
# Write an item to the primary region
aws dynamodb put-item \
    --table-name MusicTable \
    --item '{"Artist": {"S":"The Beatles"},"SongTitle": {"S":"Hey Jude"},"Album":
 {"S":"The Beatles 1967-1970"},"Year": {"N":"1968"}}' \
    --region us-east-2

# Read the item from replica region to verify strong consistency (cannot read or
 write to witness)
# No wait time needed - MRSC provides immediate consistency
echo "Reading from us-east-1 (immediate consistency):"
aws dynamodb get-item \
    --table-name MusicTable \
    --key '{"Artist": {"S":"The Beatles"},"SongTitle": {"S":"Hey Jude"}}' \
    --consistent-read \
    --region us-east-1
```

Realice escrituras condicionales con garantías de MRSC.

```
# Perform a conditional update from a different region
# This demonstrates that conditions work consistently across all regions
aws dynamodb update-item \
    --table-name MusicTable \
    --key '{"Artist": {"S":"The Beatles"},"SongTitle": {"S":"Hey Jude"}}' \
    --update-expression "SET #rating = :rating" \
    --condition-expression "attribute_exists(Artist)" \
    --expression-attribute-names '{"#rating": "Rating"}' \
    --expression-attribute-values '{":rating": {"N":"5"}}' \
    --region us-east-1
```

Limpie los recursos de la tabla global de MRSC.

```
# Remove replica tables (must be done before deleting the primary table)
aws dynamodb update-table \
    --table-name MusicTable \
    --replica-updates '[{"Delete": {"RegionName": "us-east-1"}}]' \
    --global-table-witness-updates '[{"Delete": {"RegionName": "us-west-2"}}]' \
    --region us-east-2

# Wait for replicas to be deleted
echo "Waiting for replicas to be deleted..."
sleep 30

# Delete the primary table
aws dynamodb delete-table \
    --table-name MusicTable \
    --region us-east-2
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreateTable
  - DeleteTable
  - DescribeTable
  - GetItem
  - PutItem

- UpdateItem
- UpdateTable

Administración de índices secundarios globales

En el siguiente ejemplo de código se muestra cómo administrar el ciclo de vida completo de los índices secundarios globales.

- Cree una tabla con un índice secundario global.
- Agregue un nuevo GSI a una tabla existente.
- Actualice (aumente) el rendimiento en caliente del GSI.
- Consulte datos mediante GSI.
- Elimine un GSI.

AWS CLI con Bash script

Cree una tabla con un índice secundario global.

```
# Create a table with a GSI
aws dynamodb create-table \
    --table-name MusicCollection \
    --attribute-definitions \
        AttributeName=Artist,AttributeType=S \
        AttributeName=SongTitle,AttributeType=S \
        AttributeName=AlbumTitle,AttributeType=S \
    --key-schema \
        AttributeName=Artist,KeyType=HASH \
        AttributeName=SongTitle,KeyType=RANGE \
    --billing-mode PAY_PER_REQUEST \
    --global-secondary-indexes \
        "IndexName=AlbumIndex,\
        KeySchema=[{AttributeName=AlbumTitle,KeyType=HASH}],\
        Projection={ProjectionType=ALL}"
```

Agregue un nuevo GSI (bajo demanda) a una tabla existente.

```
# Add a new GSI to an existing table
aws dynamodb update-table \
```

```
    --table-name MusicCollection \
    --attribute-definitions \
        AttributeName=Genre,AttributeType=S \
    --global-secondary-index-updates \
        "[{\"Create\":{\"IndexName\":\"GenreIndex\",\
        \"KeySchema\":[{\"AttributeName\":\"Genre\",\"KeyType\":\"HASH\"}],\
        \"Projection\":{\"ProjectionType\":\"ALL\"}}}]"
```

Actualice (aumente) el rendimiento en caliente del GSI.

```
# Increase the warm throughput of a GSI (default values are 12k reads, 4k writes)
aws dynamodb update-table \
    --table-name MusicCollection \
    --global-secondary-index-updates \
        "[{\"Update\":{\"IndexName\":\"AlbumIndex\",\
        \"WarmThroughput\":{\"ReadUnitsPerSecond\":15000,\"WriteUnitsPerSecond
\":6000}}}]"
```

Consulte datos mediante GSI.

```
# Query the AlbumIndex GSI
aws dynamodb query \
    --table-name MusicCollection \
    --index-name AlbumIndex \
    --key-condition-expression "AlbumTitle = :album" \
    --expression-attribute-values '{":album":{"S":"Let It Be"}}'

# Query the GenreIndex GSI
aws dynamodb query \
    --table-name MusicCollection \
    --index-name GenreIndex \
    --key-condition-expression "Genre = :genre" \
    --expression-attribute-values '{":genre":{"S":"Jazz"}}'
```

Elimine un GSI.

```
# Delete a GSI from a table
aws dynamodb update-table \
    --table-name MusicCollection \
```

```
    --global-secondary-index-updates \
        "[{\"Delete\":{\"IndexName\":\"GenreIndex\"}}]"
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreateTable
  - DeleteTable
  - Query
  - UpdateTable

Administración de las políticas basadas en recursos

En el siguiente ejemplo de código se muestra cómo administrar el ciclo de vida completo de las políticas basadas en recursos para las tablas de DynamoDB.

- Cree una tabla con una política de recursos.
- Obtenga una política de recursos.
- Actualice una política de recursos.
- Elimine una política de recursos.

AWS CLI con Bash script

Cree una tabla con una política de recursos.

```
# Step 1: Create a DynamoDB table
aws dynamodb create-table \
    --table-name MusicCollection \
    --attribute-definitions \
        AttributeName=Artist,AttributeType=S \
        AttributeName=SongTitle,AttributeType=S \
    --key-schema \
        AttributeName=Artist,KeyType=HASH \
        AttributeName=SongTitle,KeyType=RANGE \
    --billing-mode PAY_PER_REQUEST

# Step 2: Create a resource-based policy document
cat > policy.json << 'EOF'
{
```

```
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/DynamoDBReadOnly"
      },
      "Action": [
        "dynamodb:GetItem",
        "dynamodb:BatchGetItem",
        "dynamodb:Query",
        "dynamodb:Scan"
      ],
      "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection"
    }
  ]
}
EOF

# Step 3: Attach the resource-based policy to the table
aws dynamodb put-resource-policy \
    --resource-arn arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection \
    --policy file://policy.json
```

Obtenga una política de recursos.

```
# Get the resource-based policy attached to a table
aws dynamodb get-resource-policy \
    --resource-arn arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection
```

Actualice una política de recursos.

```
# Step 1: Create an updated policy document
cat > updated-policy.json << 'EOF'
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
```

```
          "arn:aws:iam::123456789012:role/DynamoDBReadOnly",
          "arn:aws:iam::123456789012:role/DynamoDBAnalytics"
        ]
      },
      "Action": [
        "dynamodb:GetItem",
        "dynamodb:BatchGetItem",
        "dynamodb:Query",
        "dynamodb:Scan"
      ],
      "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection"
    }
  ]
}
EOF

# Step 2: Update the resource-based policy on the table
aws dynamodb put-resource-policy \
    --resource-arn arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection \
    --policy file://updated-policy.json
```

Elimine una política de recursos.

```
# Delete the resource-based policy from a table
aws dynamodb delete-resource-policy \
    --resource-arn arn:aws:dynamodb:us-west-2:123456789012:table/MusicCollection
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreateTable
  - DeleteResourcePolicy
  - GetResourcePolicy
  - PutResourcePolicy

Configuración del control de acceso basado en atributos

El siguiente ejemplo de código muestra cómo implementar el control de acceso basado en atributos (ABAC) para DynamoDB.

- Cree una política de IAM para ABAC.
- Cree tablas con etiquetas para diferentes departamentos.
- Enumere y filtre las tablas en función de las etiquetas.

AWS CLI con Bash script

Cree una política de IAM para ABAC.

```
# Step 1: Create a policy document for ABAC
cat > abac-policy.json << 'EOF'
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:GetItem",
        "dynamodb:BatchGetItem",
        "dynamodb:Query",
        "dynamodb:Scan"
      ],
      "Resource": "arn:aws:dynamodb:*:*:table/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "${aws:PrincipalTag/Department}"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:PutItem",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteItem",
        "dynamodb:BatchWriteItem"
      ],
      "Resource": "arn:aws:dynamodb:*:*:table/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "${aws:PrincipalTag/Department}",
          "aws:ResourceTag/Environment": "Development"
        }
```

```
      }
    }
  ]
}
EOF

# Step 2: Create the IAM policy
aws iam create-policy \
    --policy-name DynamoDBDepartmentBasedAccess \
    --policy-document file://abac-policy.json
```

Cree tablas con etiquetas para diferentes departamentos.

```
# Create a DynamoDB table with tags for ABAC
aws dynamodb create-table \
    --table-name FinanceData \
    --attribute-definitions \
        AttributeName=RecordID,AttributeType=S \
    --key-schema \
        AttributeName=RecordID,KeyType=HASH \
    --billing-mode PAY_PER_REQUEST \
    --tags \
        Key=Department,Value=Finance \
        Key=Environment,Value=Development

# Create another table with different tags
aws dynamodb create-table \
    --table-name MarketingData \
    --attribute-definitions \
        AttributeName=RecordID,AttributeType=S \
    --key-schema \
        AttributeName=RecordID,KeyType=HASH \
    --billing-mode PAY_PER_REQUEST \
    --tags \
        Key=Department,Value=Marketing \
        Key=Environment,Value=Production
```

Enumere y filtre las tablas en función de las etiquetas.

```
# List all DynamoDB tables
echo "Listing all tables:"
```

```
aws dynamodb list-tables

# Get ARNs for all tables
echo -e "\nGetting ARNs for all tables:"
TABLE_ARNS=$(aws dynamodb list-tables --query "TableNames[*]" --output text | xargs
 -I {} aws dynamodb describe-table --table-name {} --query "Table.TableArn" --output
 text)

# For each table ARN, list its tags
echo -e "\nListing tags for each table:"
for ARN in $TABLE_ARNS; do
    TABLE_NAME=$(echo $ARN | awk -F/ '{print $2}')
    echo -e "\nTags for table: $TABLE_NAME"
    aws dynamodb list-tags-of-resource --resource-arn $ARN
done

# Example: Find tables with a specific tag
echo -e "\nFinding tables with Environment=Production tag:"
for ARN in $TABLE_ARNS; do
    TABLE_NAME=$(echo $ARN | awk -F/ '{print $2}')
    TAGS=$(aws dynamodb list-tags-of-resource --resource-arn $ARN --query "Tags[?
Key=='Environment' && Value=='Production']" --output text)
    if [ ! -z "$TAGS" ]; then
        echo "Table with Production tag: $TABLE_NAME"
    fi
done
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreatePolicy
  - CreateTable
  - ListTables

Trabajo con índices secundarios locales

En el siguiente ejemplo se muestra cómo crear y consultar tablas con índices secundarios locales.

- Cree una tabla con un índice secundario local (LSI).
- Cree una tabla con varios LSI con diferentes tipos de proyección.
- Consulte datos mediante LSI.

AWS CLI con Bash script

Cree una tabla con un índice secundario local.

```
# Create a table with a Local Secondary Index
aws dynamodb create-table \
    --table-name CustomerOrders \
    --attribute-definitions \
        AttributeName=CustomerID,AttributeType=S \
        AttributeName=OrderID,AttributeType=S \
        AttributeName=OrderDate,AttributeType=S \
    --key-schema \
        AttributeName=CustomerID,KeyType=HASH \
        AttributeName=OrderID,KeyType=RANGE \
    --local-secondary-indexes \
        "IndexName=OrderDateIndex,\
        KeySchema=[{AttributeName=CustomerID,KeyType=HASH},
{AttributeName=OrderDate,KeyType=RANGE}],\
        Projection={ProjectionType=ALL}" \
    --billing-mode PAY_PER_REQUEST
```

Cree una tabla con varios LSI.

```
# Create a table with multiple Local Secondary Indexes
aws dynamodb create-table \
    --table-name CustomerDetails \
    --attribute-definitions \
        AttributeName=CustomerID,AttributeType=S \
        AttributeName=Name,AttributeType=S \
        AttributeName=Email,AttributeType=S \
        AttributeName=RegistrationDate,AttributeType=S \
    --key-schema \
        AttributeName=CustomerID,KeyType=HASH \
        AttributeName=Name,KeyType=RANGE \
    --local-secondary-indexes \
        "[
            {
                \"IndexName\": \"EmailIndex\",
                \"KeySchema\": [
                    {\"AttributeName\":\"CustomerID\",\"KeyType\":\"HASH\"},
                    {\"AttributeName\":\"Email\",\"KeyType\":\"RANGE\"}
                ],
```

```
                \"Projection\": {\"ProjectionType\":\"INCLUDE\",\"NonKeyAttributes
\":[\"Address\",\"Phone\"]}
            },
            {
                \"IndexName\": \"RegistrationIndex\",
                \"KeySchema\": [
                    {\"AttributeName\":\"CustomerID\",\"KeyType\":\"HASH\"},
                    {\"AttributeName\":\"RegistrationDate\",\"KeyType\":\"RANGE\"}
                ],
                \"Projection\": {\"ProjectionType\":\"KEYS_ONLY\"}
            }
        ]" \
    --billing-mode PAY_PER_REQUEST
```

Consulte datos mediante LSI.

```
# Query the OrderDateIndex LSI
aws dynamodb query \
    --table-name CustomerOrders \
    --index-name OrderDateIndex \
    --key-condition-expression "CustomerID = :custId AND OrderDate BETWEEN :date1
 AND :date2" \
    --expression-attribute-values '{
        ":custId": {"S": "C1"},
        ":date1": {"S": "2023-01-01"},
        ":date2": {"S": "2023-02-01"}
    }'

# Query with a filter expression
aws dynamodb query \
    --table-name CustomerOrders \
    --index-name OrderDateIndex \
    --key-condition-expression "CustomerID = :custId" \
    --filter-expression "Amount > :amount" \
    --expression-attribute-values '{
        ":custId": {"S": "C1"},
        ":amount": {"N": "150"}
    }'
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.

- CreateTable
- Query

Trabajo con Streams y tiempo de vida

El siguiente ejemplo de código muestra cómo administrar las características de DynamoDB Streams y tiempo de vida.

- Cree una tabla con Streams habilitado.
- Describa Streams.
- Cree una función de Lambda para procesar Streams.
- Habilite TTL en una tabla.
- Agregue elementos con atributos TTL.
- Describa la configuración de TTL.

AWS CLI con Bash script

Cree una tabla con Streams habilitado.

```
# Create a table with DynamoDB Streams enabled
aws dynamodb create-table \
    --table-name StreamsDemo \
    --attribute-definitions \
        AttributeName=ID,AttributeType=S \
    --key-schema \
        AttributeName=ID,KeyType=HASH \
    --billing-mode PAY_PER_REQUEST \
    --stream-specification StreamEnabled=true,StreamViewType=NEW_AND_OLD_IMAGES
```

Describa Streams.

```
# Get information about the stream
aws dynamodb describe-table \
    --table-name StreamsDemo \
    --query "Table.StreamSpecification"

# Get the stream ARN
```

```
STREAM_ARN=$(aws dynamodb describe-table \
    --table-name StreamsDemo \
    --query "Table.LatestStreamArn" \
    --output text)

echo "Stream ARN: $STREAM_ARN"

# Describe the stream
aws dynamodbstreams describe-stream \
    --stream-arn $STREAM_ARN
```

Cree una función de Lambda para Streams.

```
# Step 1: Create an IAM role for the Lambda function
cat > trust-policy.json << 'EOF'
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF

aws iam create-role \
    --role-name DynamoDBStreamsLambdaRole \
    --assume-role-policy-document file://trust-policy.json

# Step 2: Attach permissions to the role
aws iam attach-role-policy \
    --role-name DynamoDBStreamsLambdaRole \
    --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole

# Step 3: Create a Lambda function (code would be in a separate file)
echo "Lambda function creation would be done separately with appropriate code"

# Step 4: Create an event source mapping
```

```
echo "Example command to create event source mapping:"
echo "aws lambda create-event-source-mapping \\"
echo "    --function-name ProcessDynamoDBRecords \\"
echo "    --event-source $STREAM_ARN \\"
echo "    --batch-size 100 \\"
echo "    --starting-position LATEST"
```

Habilite TTL en una tabla.

```
# Create a table for TTL demonstration
aws dynamodb create-table \
    --table-name TTLDemo \
    --attribute-definitions \
        AttributeName=ID,AttributeType=S \
    --key-schema \
        AttributeName=ID,KeyType=HASH \
    --billing-mode PAY_PER_REQUEST

# Wait for table to become active
aws dynamodb wait table-exists --table-name TTLDemo

# Enable TTL on the table
aws dynamodb update-time-to-live \
    --table-name TTLDemo \
    --time-to-live-specification "Enabled=true, AttributeName=ExpirationTime"
```

Agregue elementos con atributos TTL.

```
# Calculate expiration time (current time + 1 day in seconds)
EXPIRATION_TIME=$(date -d "+1 day" +%s)

# Add an item with TTL attribute
aws dynamodb put-item \
    --table-name TTLDemo \
    --item '{
        "ID": {"S": "item1"},
        "Data": {"S": "This item will expire in 1 day"},
        "ExpirationTime": {"N": "'$EXPIRATION_TIME'"}
    }'

# Add an item that expires in 1 hour
```

```
EXPIRATION_TIME_HOUR=$(date -d "+1 hour" +%s)
aws dynamodb put-item \
    --table-name TTLDemo \
    --item '{
        "ID": {"S": "item2"},
        "Data": {"S": "This item will expire in 1 hour"},
        "ExpirationTime": {"N": "'$EXPIRATION_TIME_HOUR'"}
    }'
```

Describa la configuración de TTL.

```
# Describe TTL settings for a table
aws dynamodb describe-time-to-live \
    --table-name TTLDemo
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - AttachRolePolicy
  - CreateRole
  - CreateTable
  - DescribeTable
  - DescribeTimeToLive
  - PutItem
  - UpdateTimeToLive

Trabajo con tablas globales y coherencia final de replicación de varias regiones (MREC)

En el siguiente ejemplo de código, se muestra cómo administrar las tablas globales de DynamoDB con replicación de varias regiones con coherencia final (MREC).

- Cree una tabla con replicación de varias regiones (MREC).
- Coloque y obtenga elementos de las tablas de réplica.
- Elimine réplicas una por una.
- Efectúe una limpieza eliminando la tabla.

AWS CLI con Bash script

Cree una tabla con replicación de varias regiones.

```
# Step 1: Create a new table (MusicTable) in US East (Ohio), with DynamoDB Streams
 enabled (NEW_AND_OLD_IMAGES)
aws dynamodb create-table \
    --table-name MusicTable \
    --attribute-definitions \
        AttributeName=Artist,AttributeType=S \
        AttributeName=SongTitle,AttributeType=S \
    --key-schema \
        AttributeName=Artist,KeyType=HASH \
        AttributeName=SongTitle,KeyType=RANGE \
    --billing-mode PAY_PER_REQUEST \
    --stream-specification StreamEnabled=true,StreamViewType=NEW_AND_OLD_IMAGES \
    --region us-east-2

# Step 2: Create an identical MusicTable table in US East (N. Virginia)
aws dynamodb update-table --table-name MusicTable --cli-input-json \
'{
  "ReplicaUpdates":
  [
    {
      "Create": {
        "RegionName": "us-east-1"
      }
    }
  ]
}' \
--region us-east-2

# Step 3: Create a table in Europe (Ireland)
aws dynamodb update-table --table-name MusicTable --cli-input-json \
'{
  "ReplicaUpdates":
  [
    {
      "Create": {
        "RegionName": "eu-west-1"
      }
    }
  ]
}' \
```

```
--region us-east-2
```

Describa la tabla de varias regiones.

```
# Step 4: View the list of replicas created using describe-table
aws dynamodb describe-table \
    --table-name MusicTable \
    --region us-east-2 \
    --query 'Table.
{TableName:TableName,TableStatus:TableStatus,MultiRegionConsistency:MultiRegionConsistency,R
{Region:RegionName,Status:ReplicaStatus}}'
```

Coloque elementos en una tabla de réplica.

```
# Step 5: To verify that replication is working, add a new item to the Music table
 in US East (Ohio)
aws dynamodb put-item \
    --table-name MusicTable \
    --item '{"Artist": {"S":"item_1"},"SongTitle": {"S":"Song Value 1"}}' \
    --region us-east-2
```

Obtenga elementos de las tablas de réplica.

```
# Step 6: Wait for a few seconds, and then check to see whether the item has been
# successfully replicated to US East (N. Virginia) and Europe (Ireland)
aws dynamodb get-item \
    --table-name MusicTable \
    --key '{"Artist": {"S":"item_1"},"SongTitle": {"S":"Song Value 1"}}' \
    --region us-east-1

aws dynamodb get-item \
    --table-name MusicTable \
    --key '{"Artist": {"S":"item_1"},"SongTitle": {"S":"Song Value 1"}}' \
    --region eu-west-1
```

Elimine réplicas.

```
# Step 7: Delete the replica table in Europe (Ireland) Region
```

```
aws dynamodb update-table --table-name MusicTable --cli-input-json \
'{
  "ReplicaUpdates":
  [
    {
      "Delete": {
        "RegionName": "eu-west-1"
      }
    }
  ]
}' \
--region us-east-2

# Delete the replica table in US East (N. Virginia) Region
aws dynamodb update-table --table-name MusicTable --cli-input-json \
'{
  "ReplicaUpdates":
  [
    {
      "Delete": {
        "RegionName": "us-east-1"
      }
    }
  ]
}' \
--region us-east-2
```

Efectúe una limpieza eliminando la tabla.

```
# Clean up: Delete the primary table
aws dynamodb delete-table --table-name MusicTable --region us-east-2

echo "Global table demonstration complete."
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreateTable
  - DeleteTable
  - DescribeTable

- GetItem
- PutItem
- UpdateTable

Trabajo con el etiquetado de recursos

En el siguiente ejemplo de código se muestra cómo administrar etiquetas para los recursos de DynamoDB.

- Cree una tabla con etiquetas.
- Enumera las etiquetas de un recurso.
- Agregue etiquetas a un recurso.
- Elimine etiquetas de un recurso.
- Filtre tablas por etiquetas.

AWS CLI con Bash script

Cree una tabla con etiquetas.

```
# Create a table with tags
aws dynamodb create-table \
    --table-name TaggedTable \
    --attribute-definitions \
        AttributeName=ID,AttributeType=S \
    --key-schema \
        AttributeName=ID,KeyType=HASH \
    --billing-mode PAY_PER_REQUEST \
    --tags \
        Key=Environment,Value=Production \
        Key=Project,Value=Analytics \
        Key=Owner,Value=DataTeam
```

Enumera las etiquetas de un recurso.

```
# Get the table ARN
TABLE_ARN=$(aws dynamodb describe-table \
    --table-name TaggedTable \
    --query "Table.TableArn" \
```

```
    --output text)

# List tags for the table
aws dynamodb list-tags-of-resource \
    --resource-arn $TABLE_ARN
```

Agregue etiquetas a un recurso.

```
# Add tags to an existing table
aws dynamodb tag-resource \
    --resource-arn $TABLE_ARN \
    --tags \
        Key=CostCenter,Value=12345 \
        Key=BackupSchedule,Value=Daily
```

Elimine etiquetas de un recurso.

```
# Remove tags from a table
aws dynamodb untag-resource \
    --resource-arn $TABLE_ARN \
    --tag-keys Owner BackupSchedule
```

Filtre tablas por etiquetas.

```
# Create another table with different tags
aws dynamodb create-table \
    --table-name AnotherTaggedTable \
    --attribute-definitions \
        AttributeName=ID,AttributeType=S \
    --key-schema \
        AttributeName=ID,KeyType=HASH \
    --billing-mode PAY_PER_REQUEST \
    --tags \
        Key=Environment,Value=Development \
        Key=Project,Value=Testing

# Wait for table to become active
aws dynamodb wait table-exists --table-name AnotherTaggedTable
```

```
# List all tables
echo "All tables:"
aws dynamodb list-tables

# Get ARNs for all tables
echo -e "\nFiltering tables by Environment=Production tag:"
TABLE_ARNS=$(aws dynamodb list-tables --query "TableNames[*]" --output text | xargs
 -I {} aws dynamodb describe-table --table-name {} --query "Table.TableArn" --output
 text)

# Find tables with specific tag
for ARN in $TABLE_ARNS; do
    TABLE_NAME=$(echo $ARN | awk -F/ '{print $2}')
    TAGS=$(aws dynamodb list-tags-of-resource --resource-arn $ARN --query "Tags[?
Key=='Environment' && Value=='Production']" --output text)
    if [ ! -z "$TAGS" ]; then
        echo "Table with Production tag: $TABLE_NAME"
    fi
done
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreateTable
  - ListTagsOfResource
  - TagResource
  - UntagResource

Trabajo con el cifrado de tablas

En el siguiente ejemplo de código se muestra cómo administrar las opciones de cifrado de las tablas de DynamoDB.

- Cree una tabla con un cifrado predeterminado.
- Cree una tabla con una CMK administrada por el cliente.
- Actualice la configuración de cifrado de la tabla.
- Describa el cifrado de la tabla.

AWS CLI con Bash script

Cree una tabla con un cifrado predeterminado.

```
# Create a table with default encryption (AWS owned key)
aws dynamodb create-table \
    --table-name CustomerData \
    --attribute-definitions \
        AttributeName=CustomerID,AttributeType=S \
    --key-schema \
        AttributeName=CustomerID,KeyType=HASH \
    --billing-mode PAY_PER_REQUEST \
    --sse-specification Enabled=true,SSEType=KMS
```

Cree una tabla con una CMK administrada por el cliente.

```
# Step 1: Create a customer managed key in KMS
aws kms create-key \
    --description "Key for DynamoDB table encryption" \
    --key-usage ENCRYPT_DECRYPT \
    --customer-master-key-spec SYMMETRIC_DEFAULT

# Store the key ID for later use
KEY_ID=$(aws kms list-keys --query "Keys[?contains(KeyArn, 'Key for
 DynamoDB')].KeyId" --output text)

# Step 2: Create a table with the customer managed key
aws dynamodb create-table \
    --table-name SensitiveData \
    --attribute-definitions \
        AttributeName=RecordID,AttributeType=S \
    --key-schema \
        AttributeName=RecordID,KeyType=HASH \
    --billing-mode PAY_PER_REQUEST \
    --sse-specification Enabled=true,SSEType=KMS,KMSMasterKeyId=$KEY_ID
```

Actualice el cifrado de la tabla.

```
# Update a table to use a different KMS key
aws dynamodb update-table \
    --table-name CustomerData \
```

```
    --sse-specification Enabled=true,SSEType=KMS,KMSMasterKeyId=$KEY_ID
```

Describa el cifrado de la tabla.

```
# Describe the table to see encryption settings
aws dynamodb describe-table \
    --table-name CustomerData \
    --query "Table.SSEDescription"
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreateKey
  - CreateTable
  - DescribeTable
  - UpdateTable

Ejemplos de Amazon EC2 que utilizan la AWS CLI con el script Bash

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante la AWS Command Line Interface con el script Bash con Amazon EC2.

Los conceptos básicos son ejemplos de código que muestran cómo realizar las operaciones esenciales dentro de un servicio.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica a través de llamadas a varias funciones dentro del servicio o combinado con otros Servicios de AWS.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Conceptos básicos
- Acciones

- Escenarios

Conceptos básicos

Conceptos básicos

En el siguiente ejemplo de código, se muestra cómo:

- Cree un par de claves y un grupo de seguridad.
- Seleccione una Imagen de máquina de Amazon (AMI) y un tipo de instancia; a continuación, cree una instancia.
- Detenga y vuelva a iniciar la instancia.
- Asocie una dirección IP elástica a su instancia.
- Conéctese a tu instancia con SSH y, a continuación, limpie los recursos.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Ejecutar un escenario interactivo en un símbolo del sistema.

```
###############################################################################
# function get_started_with_ec2_instances
#
# Runs an interactive scenario that shows how to get started using EC2 instances.
#
#     "EC2 access" permissions are needed to run this code.
#
# Returns:
#       0 - If successful.
#       1 - If an error occurred.
###############################################################################
function get_started_with_ec2_instances() {
  # Requires version 4 for mapfile.
  local required_version=4.0
```

```
 # Get the current Bash version
 # Check if BASH_VERSION is set
 local current_version
 if [[ -n "$BASH_VERSION" ]]; then
   # Convert BASH_VERSION to a number for comparison
   current_version=$BASH_VERSION
 else
   # Get the current Bash version using the bash command
   current_version=$(bash --version | head -n 1 | awk '{ print $4 }')
 fi

 # Convert version strings to numbers for comparison
 local required_version_num current_version_num
 required_version_num=$(echo "$required_version" | awk -F. '{ print ($1 * 10000) +
($2 * 100) + $3 }')
 current_version_num=$(echo "$current_version" | awk -F. '{ print ($1 * 10000) +
($2 * 100) + $3 }')

 # Compare versions
 if ((current_version_num < required_version_num)); then
   echo "Error: This script requires Bash version $required_version or higher."
   echo "Your current Bash version is number is $current_version."
   exit 1
 fi

 {
   if [ "$EC2_OPERATIONS_SOURCED" != "True" ]; then

     source ./ec2_operations.sh
   fi
 }

 echo_repeat "*" 88
 echo "Welcome to the Amazon Elastic Compute Cloud (Amazon EC2) get started with
instances demo."
 echo_repeat "*" 88
 echo

 echo "Let's create an RSA key pair that you can be use to securely connect to "
 echo "your EC2 instance."

 echo -n "Enter a unique name for your key: "
 get_input
```

```
  local key_name
  key_name=$get_input_result

  local temp_dir
  temp_dir=$(mktemp -d)
  local key_file_name="$temp_dir/${key_name}.pem"

  if ec2_create_keypair -n "${key_name}" -f "${key_file_name}"; then
    echo "Created a key pair $key_name and saved the private key to $key_file_name"
    echo
  else
    errecho "The key pair failed to create. This demo will exit."
    return 1
  fi

  chmod 400 "${key_file_name}"

  if yes_no_input "Do you want to list some of your key pairs? (y/n) "; then
    local keys_and_fingerprints
    keys_and_fingerprints="$(ec2_describe_key_pairs)" && {
      local image_name_and_id
      while IFS=$'\n' read -r image_name_and_id; do
        local entries
        IFS=$'\t' read -ra entries <<<"$image_name_and_id"
        echo "Found rsa key ${entries[0]} with fingerprint:"
        echo "     ${entries[1]}"
      done <<<"$keys_and_fingerprints"

    }
  fi

  echo_repeat "*" 88
  echo_repeat "*" 88

  echo "Let's create a security group to manage access to your instance."
  echo -n "Enter a unique name for your security group: "
  get_input
  local security_group_name
  security_group_name=$get_input_result
  local security_group_id
  security_group_id=$(ec2_create_security_group -n "$security_group_name" \
    -d "Security group for EC2 instance") || {
    errecho "The security failed to create. This demo will exit."
    clean_up "$key_name" "$key_file_name"
```

```
    return 1
  }

  echo "Security group created with ID $security_group_id"
  echo

  local public_ip
  public_ip=$(curl -s http://checkip.amazonaws.com)

  echo "Let's add a rule to allow SSH only from your current IP address."
  echo "Your public IP address is $public_ip"
  echo -n "press return to add this rule to your security group."
  get_input

  if ! ec2_authorize_security_group_ingress -g "$security_group_id" -i "$public_ip"
-p tcp -f 22 -t 22; then
    errecho "The security group rules failed to update. This demo will exit."
    clean_up "$key_name" "$key_file_name" "$security_group_id"
    return 1
  fi

  echo "Security group rules updated"

  local security_group_description
  security_group_description="$(ec2_describe_security_groups -g
"${security_group_id}")" || {
    errecho "Failed to describe security groups. This demo will exit."
    clean_up "$key_name" "$key_file_name" "$security_group_id"
    return 1
  }

  mapfile -t parameters <<<"$security_group_description"
  IFS=$'\t' read -ra entries <<<"${parameters[0]}"
  echo "Security group: ${entries[0]}"
  echo "    ID: ${entries[1]}"
  echo "    VPC: ${entries[2]}"
  echo "Inbound permissions:"
  IFS=$'\t' read -ra entries <<<"${parameters[1]}"
  echo "    IpProtocol: ${entries[0]}"
  echo "    FromPort: ${entries[1]}"
  echo "    ToPort: ${entries[2]}"
  echo "    CidrIp: ${parameters[2]}"

  local parameters
```

```
  parameters="$(ssm_get_parameters_by_path -p "/aws/service/ami-amazon-linux-
latest")" || {
    errecho "Failed to get parameters. This demo will exit."
    clean_up "$key_name" "$key_file_name" "$security_group_id"
    return 1

  }

  local image_ids=""
  mapfile -t parameters <<<"$parameters"
  for image_name_and_id in "${parameters[@]}"; do
    IFS=$'\t' read -ra values <<<"$image_name_and_id"
    if [[ "${values[0]}" == *"amzn2"* ]]; then
      image_ids+="${values[1]} "
    fi
  done

  local images
  images="$(ec2_describe_images -i "$image_ids")" || {
    errecho "Failed to describe images. This demo will exit."
    clean_up "$key_name" "$key_file_name" "$security_group_id"
    return 1

  }

  new_line_and_tab_to_list "$images"
  local images=("${list_result[@]}")

  # Get the size of the array
  local images_count=${#images[@]}

  if ((images_count == 0)); then
    errecho "No images found. This demo will exit."
    clean_up "$key_name" "$key_file_name" "$security_group_id"
    return 1
  fi

  echo_repeat "*" 88
  echo_repeat "*" 88

  echo "Let's create an instance from an Amazon Linux 2 AMI. Here are some options:"
  for ((i = 0; i < images_count; i += 3)); do
    echo "$(((i / 3) + 1)) - ${images[$i]}"
  done
```

```
  integer_input "Please enter the number of the AMI you want to use: " 1
 "$((images_count / 3))"
  local choice=$get_input_result
  choice=$(((choice - 1) * 3))

  echo "Great choice."
  echo

  local architecture=${images[$((choice + 1))]}
  local image_id=${images[$((choice + 2))]}
  echo "Here are some instance types that support the ${architecture} architecture
 of the image:"
  response="$(ec2_describe_instance_types -a "${architecture}" -t
 "*.micro,*.small")" || {
    errecho "Failed to describe instance types. This demo will exit."
    clean_up "$key_name" "$key_file_name" "$security_group_id"
    return 1
  }

  local instance_types
  mapfile -t instance_types <<<"$response"

  # Get the size of the array
  local instance_types_count=${#instance_types[@]}

  echo "Here are some options:"
  for ((i = 0; i < instance_types_count; i++)); do
    echo "$((i + 1)) - ${instance_types[$i]}"
  done

  integer_input "Which one do you want to use? " 1 "${#instance_types[@]}
"
  choice=$get_input_result
  local instance_type=${instance_types[$((choice - 1))]}
  echo "Another great choice."
  echo

  echo "Creating your instance and waiting for it to start..."
  local instance_id
  instance_id=$(ec2_run_instances -i "$image_id" -t "$instance_type" -k "$key_name"
 -s "$security_group_id") || {
    errecho "Failed to run instance. This demo will exit."
    clean_up "$key_name" "$key_file_name" "$security_group_id"
```

```
    return 1
  }

  ec2_wait_for_instance_running -i "$instance_id"
  echo "Your instance is ready:"
  echo

  local instance_details
  instance_details="$(ec2_describe_instances -i "${instance_id}")"

  echo
  print_instance_details "${instance_details}"

  local public_ip
  public_ip=$(echo "${instance_details}" | awk '{print $6}')
  echo
  echo "You can use SSH to connect to your instance"
  echo "If the connection attempt times out, you might have to manually update the
SSH ingress rule"
  echo "for your IP address in the AWS Management Console."
  connect_to_instance "$key_file_name" "$public_ip"

  echo -n "Press Enter when you're ready to continue the demo: "
  get_input

  echo_repeat "*" 88
  echo_repeat "*" 88

  echo "Let's stop and start your instance to see what changes."
  echo "Stopping your instance and waiting until it's stopped..."
  ec2_stop_instances -i "$instance_id"
  ec2_wait_for_instance_stopped -i "$instance_id"

  echo "Your instance is stopped. Restarting..."

  ec2_start_instances -i "$instance_id"
  ec2_wait_for_instance_running -i "$instance_id"

  echo "Your instance is running again."
  local instance_details
  instance_details="$(ec2_describe_instances -i "${instance_id}")"

  print_instance_details "${instance_details}"
```

```
  public_ip=$(echo "${instance_details}" | awk '{print $6}')

  echo "Every time your instance is restarted, its public IP address changes"
  connect_to_instance "$key_file_name" "$public_ip"

  echo -n "Press Enter when you're ready to continue the demo: "
  get_input

  echo_repeat "*" 88
  echo_repeat "*" 88

  echo "You can allocate an Elastic IP address and associate it with your instance"
  echo "to keep a consistent IP address even when your instance restarts."

  local result
  result=$(ec2_allocate_address -d vpc) || {
    errecho "Failed to allocate an address. This demo will exit."
    clean_up "$key_name" "$key_file_name" "$security_group_id" "$instance_id"
    return 1
  }

  local elastic_ip allocation_id
  elastic_ip=$(echo "$result" | awk '{print $1}')
  allocation_id=$(echo "$result" | awk '{print $2}')

  echo "Allocated static Elastic IP address: $elastic_ip"

  local association_id
  association_id=$(ec2_associate_address -i "$instance_id" -a "$allocation_id") || {
    errecho "Failed to associate an address. This demo will exit."
    clean_up "$key_name" "$key_file_name" "$security_group_id" "$instance_id"
"$allocation_id"
    return 1
  }

  echo "Associated your Elastic IP with your instance."
  echo "You can now use SSH to connect to your instance by using the Elastic IP."
  connect_to_instance "$key_file_name" "$elastic_ip"

  echo -n "Press Enter when you're ready to continue the demo: "
  get_input

  echo_repeat "*" 88
  echo_repeat "*" 88
```

```
  echo "Let's stop and start your instance to see what changes."
  echo "Stopping your instance and waiting until it's stopped..."
  ec2_stop_instances -i "$instance_id"
  ec2_wait_for_instance_stopped -i "$instance_id"

  echo "Your instance is stopped. Restarting..."

  ec2_start_instances -i "$instance_id"
  ec2_wait_for_instance_running -i "$instance_id"

  echo "Your instance is running again."
  local instance_details
  instance_details="$(ec2_describe_instances -i "${instance_id}")"

  print_instance_details "${instance_details}"

  echo "Because you have associated an Elastic IP with your instance, you can"
  echo "connect by using a consistent IP address after the instance restarts."
  connect_to_instance "$key_file_name" "$elastic_ip"

  echo -n "Press Enter when you're ready to continue the demo: "
  get_input

  echo_repeat "*" 88
  echo_repeat "*" 88

  if yes_no_input "Do you want to delete the resources created in this demo: (y/n)
 "; then
    clean_up "$key_name" "$key_file_name" "$security_group_id" "$instance_id" \
      "$allocation_id" "$association_id"
  else
    echo "The following resources were not deleted."
    echo "Key pair: $key_name"
    echo "Key file: $key_file_name"
    echo "Security group: $security_group_id"
    echo "Instance: $instance_id"
    echo "Elastic IP address: $elastic_ip"
  fi
}

################################################################################
# function clean_up
#
```

```
# This function cleans up the created resources.
#     $1 - The name of the ec2 key pair to delete.
#     $2 - The name of the key file to delete.
#     $3 - The ID of the security group to delete.
#     $4 - The ID of the instance to terminate.
#     $5 - The ID of the elastic IP address to release.
#     $6 - The ID of the elastic IP address to disassociate.
#
# Returns:
#       0 - If successful.
#       1 - If an error occurred.
###############################################################################
function clean_up() {
  local result=0
  local key_pair_name=$1
  local key_file_name=$2
  local security_group_id=$3
  local instance_id=$4
  local allocation_id=$5
  local association_id=$6

  if [ -n "$association_id" ]; then
    # bashsupport disable=BP2002
    if (ec2_disassociate_address -a "$association_id"); then
      echo "Disassociated elastic IP address with ID $association_id"
    else
      errecho "The elastic IP address disassociation failed."
      result=1
    fi
  fi

  if [ -n "$allocation_id" ]; then
    # bashsupport disable=BP2002
    if (ec2_release_address -a "$allocation_id"); then
      echo "Released elastic IP address with ID $allocation_id"
    else
      errecho "The elastic IP address release failed."
      result=1
    fi
  fi

  if [ -n "$instance_id" ]; then
    # bashsupport disable=BP2002
    if (ec2_terminate_instances -i "$instance_id"); then
```

```
      echo "Started terminating instance with ID $instance_id"

      ec2_wait_for_instance_terminated -i "$instance_id"
    else
      errecho "The instance terminate failed."
      result=1
    fi
  fi

  if [ -n "$security_group_id" ]; then
    # bashsupport disable=BP2002
    if (ec2_delete_security_group -i "$security_group_id"); then
      echo "Deleted security group with ID $security_group_id"
    else
      errecho "The security group delete failed."
      result=1
    fi
  fi

  if [ -n "$key_pair_name" ]; then
    # bashsupport disable=BP2002
    if (ec2_delete_keypair -n "$key_pair_name"); then
      echo "Deleted key pair named $key_pair_name"
    else
      errecho "The key pair delete failed."
      result=1
    fi
  fi

  if [ -n "$key_file_name" ]; then
    rm -f "$key_file_name"
  fi

  return $result
}

###############################################################################
# function ssm_get_parameters_by_path
#
# This function retrieves one or more parameters from the AWS Systems Manager
 Parameter Store
# by specifying a parameter path.
#
# Parameters:
```

```
#       -p parameter_path - The path of the parameter(s) to retrieve.
#
# And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ssm_get_parameters_by_path() {
  local parameter_path response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ssm_get_parameters_by_path"
    echo "Retrieves one or more parameters from the AWS Systems Manager Parameter
 Store by specifying a parameter path."
    echo "  -p parameter_path - The path of the parameter(s) to retrieve."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "p:h" option; do
    case "${option}" in
      p) parameter_path="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$parameter_path" ]]; then
    errecho "ERROR: You must provide a parameter path with the -p parameter."
    usage
    return 1
  fi

  response=$(aws ssm get-parameters-by-path \
    --path "$parameter_path" \
```

```
    --query "Parameters[*].[Name, Value]" \
    --output text) || {
    aws_cli_error_log $?
    errecho "ERROR: AWS reports get-parameters-by-path operation failed.$response"
    return 1
  }

  echo "$response"

  return 0
}

###############################################################################
# function print_instance_details
#
# This function prints the details of an Amazon Elastic Compute Cloud (Amazon EC2)
 instance.
#
# Parameters:
#       instance_details - The instance details in the format "InstanceId ImageId
 InstanceType KeyName VpcId PublicIpAddress State.Name".
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function print_instance_details() {
  local instance_details="$1"

  if [[ -z "${instance_details}" ]]; then
    echo "Error: Missing required instance details argument."
    return 1
  fi

  local instance_id image_id instance_type key_name vpc_id public_ip state
  instance_id=$(echo "${instance_details}" | awk '{print $1}')
  image_id=$(echo "${instance_details}" | awk '{print $2}')
  instance_type=$(echo "${instance_details}" | awk '{print $3}')
  key_name=$(echo "${instance_details}" | awk '{print $4}')
  vpc_id=$(echo "${instance_details}" | awk '{print $5}')
  public_ip=$(echo "${instance_details}" | awk '{print $6}')
  state=$(echo "${instance_details}" | awk '{print $7}')

  echo "    ID: ${instance_id}"
```

```
  echo "    Image ID: ${image_id}"
  echo "    Instance type: ${instance_type}"
  echo "    Key name: ${key_name}"
  echo "    VPC ID: ${vpc_id}"
  echo "    Public IP: ${public_ip}"
  echo "    State: ${state}"

  return 0
}

################################################################################
# function connect_to_instance
#
# This function displays the public IP address of an Amazon Elastic Compute Cloud
 (Amazon EC2) instance and prompts the user to connect to the instance via SSH.
#
# Parameters:
#       $1 - The name of the key file used to connect to the instance.
#       $2 - The public IP address of the instance.
#
# Returns:
#       None
################################################################################
function connect_to_instance() {
  local key_file_name="$1"
  local public_ip="$2"

  # Validate the input parameters
  if [[ -z "$key_file_name" ]]; then
    echo "ERROR: You must provide a key file name as the first argument." >&2
    return 1
  fi

  if [[ -z "$public_ip" ]]; then
    echo "ERROR: You must provide a public IP address as the second argument." >&2
    return 1
  fi

  # Display the public IP address and connection command
  echo "To connect, run the following command:"
  echo "    ssh -i ${key_file_name} ec2-user@${public_ip}"

  # Prompt the user to connect to the instance
  if yes_no_input "Do you want to connect now? (y/n) "; then
```

```
    echo "After you have connected, you can return to this example by typing 'exit'"
    ssh -i "${key_file_name}" ec2-user@"${public_ip}"
  fi
}

###############################################################################
# function get_input
#
# This function gets user input from the command line.
#
# Outputs:
#   User input to stdout.
#
# Returns:
#       0
###############################################################################
function get_input() {

  if [ -z "${mock_input+x}" ]; then
    read -r get_input_result
  else

    if [ "$mock_input_array_index" -lt ${#mock_input_array[@]} ]; then
      get_input_result="${mock_input_array[$mock_input_array_index]}"
      # bashsupport disable=BP2001
      # shellcheck disable=SC2206
      ((mock_input_array_index++))
      echo -n "$get_input_result"
    else
      echo "MOCK_INPUT_ARRAY has no more elements" 1>&2
      return 1
    fi
  fi

  return 0
}

###############################################################################
# function yes_no_input
#
# This function requests a yes/no answer from the user, following to a prompt.
#
# Parameters:
#       $1 - The prompt.
```

```
#
# Returns:
#       0 - If yes.
#       1 - If no.
###############################################################################
function yes_no_input() {
  if [ -z "$1" ]; then
    echo "Internal error yes_no_input"
    return 1
  fi

  local index=0
  local response="N"
  while [[ $index -lt 10 ]]; do
    index=$((index + 1))
    echo -n "$1"
    if ! get_input; then
      return 1
    fi
    response=$(echo "$get_input_result" | tr '[:upper:]' '[:lower:]')
    if [ "$response" = "y" ] || [ "$response" = "n" ]; then
      break
    else
      echo -e "\nPlease enter or 'y' or 'n'."
    fi
  done

  echo

  if [ "$response" = "y" ]; then
    return 0
  else
    return 1
  fi
}

###############################################################################
# function integer_input
#
# This function prompts the user to enter an integer within a specified range
# and validates the input.
#
# Parameters:
#       $1 - The prompt message to display to the user.
```

```
#       $2 - The minimum value of the accepted range.
#       $3 - The maximum value of the accepted range.
#
# Returns:
#       The valid integer input from the user.
#       If the input is invalid or out of range, the function will continue
#       prompting the user until a valid input is provided.
###############################################################################
function integer_input() {
  local prompt="$1"
  local min_value="$2"
  local max_value="$3"
  local input=""

  while true; do
    # Display the prompt message and wait for user input
    echo -n "$prompt"

    if ! get_input; then
      return 1
    fi

    input="$get_input_result"

    # Check if the input is a valid integer
    if [[ "$input" =~ ^-?[0-9]+$ ]]; then
      # Check if the input is within the specified range
      if ((input >= min_value && input <= max_value)); then
        return 0
      else
        echo "Error: Input, $input, must be between $min_value and $max_value."
      fi
    else
      echo "Error: Invalid input- $input. Please enter an integer."
    fi
  done
}
###############################################################################
# function new_line_and_tab_to_list
#
# This function takes a string input containing newlines and tabs, and
# converts it into a list (array) of elements.
#
# Parameters:
```

```
#       $1 - The input string containing newlines and tabs.
#
# Returns:
#       The resulting list (array) is stored in the global variable
#       'list_result'.
##############################################################################
function new_line_and_tab_to_list() {
  local input=$1
  export list_result

  list_result=()
  mapfile -t lines <<<"$input"
  local line
  for line in "${lines[@]}"; do
    IFS=$'\t' read -ra parameters <<<"$line"
    list_result+=("${parameters[@]}")
  done
}

##############################################################################
# function echo_repeat
#
# This function prints a string 'n' times to stdout.
#
# Parameters:
#       $1 - The string.
#       $2 - Number of times to print the string.
#
# Outputs:
#   String 'n' times to stdout.
#
# Returns:
#       0
##############################################################################
function echo_repeat() {
  local end=$2
  for ((i = 0; i < end; i++)); do
    echo -n "$1"
  done
  echo
}
```

Las funciones de DynamoDB utilizadas en este escenario.

```
###############################################################################
# function ec2_create_keypair
#
# This function creates an Amazon Elastic Compute Cloud (Amazon EC2) ED25519 or
 2048-bit RSA key pair
# and writes it to a file.
#
# Parameters:
#       -n key_pair_name - A key pair name.
#       -f file_path - File to store the key pair.
#
# And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_create_keypair() {
  local key_pair_name file_path response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_create_keypair"
    echo "Creates an Amazon Elastic Compute Cloud (Amazon EC2) ED25519 or 2048-bit
 RSA key pair"
    echo " and writes it to a file."
    echo "  -n key_pair_name - A key pair name."
    echo "  -f file_path - File to store the key pair."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:f:h" option; do
    case "${option}" in
      n) key_pair_name="${OPTARG}" ;;
      f) file_path="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
```

```
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$key_pair_name" ]]; then
    errecho "ERROR: You must provide a key name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$file_path" ]]; then
    errecho "ERROR: You must provide a file path with the -f parameter."
    usage
    return 1
  fi

  response=$(aws ec2 create-key-pair \
    --key-name "$key_pair_name" \
    --query 'KeyMaterial' \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports create-access-key operation failed.$response"
    return 1
  }

  if [[ -n "$file_path" ]]; then
    echo "$response" >"$file_path"
  fi

  return 0
}

###############################################################################
# function ec2_describe_key_pairs
#
# This function describes one or more Amazon Elastic Compute Cloud (Amazon EC2) key
 pairs.
#
# Parameters:
#       -h - Display help.
#
# And:
```

```
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_describe_key_pairs() {
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_describe_key_pairs"
    echo "Describes one or more Amazon Elastic Compute Cloud (Amazon EC2) key
 pairs."
    echo "  -h - Display help."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "h" option; do
    case "${option}" in
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  local response

  response=$(aws ec2 describe-key-pairs \
    --query 'KeyPairs[*].[KeyName, KeyFingerprint]' \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports describe-key-pairs operation failed.$response"
    return 1
  }

  echo "$response"

  return 0
```

```
}

################################################################################
# function ec2_create_security_group
#
# This function creates an Amazon Elastic Compute Cloud (Amazon EC2) security group.
#
# Parameters:
#       -n security_group_name - The name of the security group.
#       -d security_group_description - The description of the security group.
#
# Returns:
#       The ID of the created security group, or an error message if the operation
 fails.
# And:
#       0 - If successful.
#       1 - If it fails.
#
################################################################################
function ec2_create_security_group() {
  local security_group_name security_group_description response

  # Function to display usage information
  function usage() {
    echo "function ec2_create_security_group"
    echo "Creates an Amazon Elastic Compute Cloud (Amazon EC2) security group."
    echo "  -n security_group_name - The name of the security group."
    echo "  -d security_group_description - The description of the security group."
    echo ""
  }

  # Parse the command-line arguments
  while getopts "n:d:h" option; do
    case "${option}" in
      n) security_group_name="${OPTARG}" ;;
      d) security_group_description="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
```

```
        ;;
    esac
  done
  export OPTIND=1

  # Validate the input parameters
  if [[ -z "$security_group_name" ]]; then
    errecho "ERROR: You must provide a security group name with the -n parameter."
    return 1
  fi

  if [[ -z "$security_group_description" ]]; then
    errecho "ERROR: You must provide a security group description with the -d
 parameter."
    return 1
  fi

  # Create the security group
  response=$(aws ec2 create-security-group \
    --group-name "$security_group_name" \
    --description "$security_group_description" \
    --query "GroupId" \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports create-security-group operation failed."
    errecho "$response"
    return 1
  }

  echo "$response"
  return 0
}

################################################################################
# function ec2_describe_security_groups
#
# This function describes one or more Amazon Elastic Compute Cloud (Amazon EC2)
 security groups.
#
# Parameters:
#       -g security_group_id - The ID of the security group to describe (optional).
#
# And:
#       0 - If successful.
```

```
#       1 - If it fails.
###############################################################################
function ec2_describe_security_groups() {
  local security_group_id response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_describe_security_groups"
    echo "Describes one or more Amazon Elastic Compute Cloud (Amazon EC2) security
 groups."
    echo "  -g security_group_id - The ID of the security group to describe
 (optional)."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "g:h" option; do
    case "${option}" in
      g) security_group_id="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  local query="SecurityGroups[*].[GroupName, GroupId, VpcId, IpPermissions[*].
[IpProtocol, FromPort, ToPort, IpRanges[*].CidrIp]]"

  if [[ -n "$security_group_id" ]]; then
    response=$(aws ec2 describe-security-groups --group-ids "$security_group_id" --
query "${query}" --output text)
  else
    response=$(aws ec2 describe-security-groups --query "${query}" --output text)
  fi

  local error_code=${?}
```

```
  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports describe-security-groups operation failed.$response"
    return 1
  fi

  echo "$response"

  return 0
}

###############################################################################
# function ec2_authorize_security_group_ingress
#
# This function authorizes an ingress rule for an Amazon Elastic Compute Cloud
 (Amazon EC2) security group.
#
# Parameters:
#       -g security_group_id - The ID of the security group.
#       -i ip_address - The IP address or CIDR block to authorize.
#       -p protocol - The protocol to authorize (e.g., tcp, udp, icmp).
#       -f from_port - The start of the port range to authorize.
#       -t to_port - The end of the port range to authorize.
#
# And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_authorize_security_group_ingress() {
  local security_group_id ip_address protocol from_port to_port response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_authorize_security_group_ingress"
    echo "Authorizes an ingress rule for an Amazon Elastic Compute Cloud (Amazon
 EC2) security group."
    echo "  -g security_group_id - The ID of the security group."
    echo "  -i ip_address - The IP address or CIDR block to authorize."
    echo "  -p protocol - The protocol to authorize (e.g., tcp, udp, icmp)."
    echo "  -f from_port - The start of the port range to authorize."
    echo "  -t to_port - The end of the port range to authorize."
    echo ""
```

```
  }

  # Retrieve the calling parameters.
  while getopts "g:i:p:f:t:h" option; do
    case "${option}" in
      g) security_group_id="${OPTARG}" ;;
      i) ip_address="${OPTARG}" ;;
      p) protocol="${OPTARG}" ;;
      f) from_port="${OPTARG}" ;;
      t) to_port="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$security_group_id" ]]; then
    errecho "ERROR: You must provide a security group ID with the -g parameter."
    usage
    return 1
  fi

  if [[ -z "$ip_address" ]]; then
    errecho "ERROR: You must provide an IP address or CIDR block with the -i
parameter."
    usage
    return 1
  fi

  if [[ -z "$protocol" ]]; then
    errecho "ERROR: You must provide a protocol with the -p parameter."
    usage
    return 1
  fi

  if [[ -z "$from_port" ]]; then
    errecho "ERROR: You must provide a start port with the -f parameter."
```

```
    usage
    return 1
  fi

  if [[ -z "$to_port" ]]; then
    errecho "ERROR: You must provide an end port with the -t parameter."
    usage
    return 1
  fi

  response=$(aws ec2 authorize-security-group-ingress \
    --group-id "$security_group_id" \
    --cidr "${ip_address}/32" \
    --protocol "$protocol" \
    --port "$from_port-$to_port" \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports authorize-security-group-ingress operation failed.
$response"
    return 1
  }

  return 0
}

###############################################################################
# function ec2_describe_images
#
# This function describes one or more Amazon Elastic Compute Cloud (Amazon EC2)
 images.
#
# Parameters:
#       -i image_ids - A space-separated  list of image IDs (optional).
#       -h - Display help.
#
# And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_describe_images() {
  local image_ids response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
```

```
function usage() {
  echo "function ec2_describe_images"
  echo "Describes one or more Amazon Elastic Compute Cloud (Amazon EC2) images."
  echo "  -i image_ids - A space-separated list of image IDs (optional)."
  echo "  -h - Display help."
  echo ""
}

# Retrieve the calling parameters.
while getopts "i:h" option; do
  case "${option}" in
    i) image_ids="${OPTARG}" ;;
    h)
      usage
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

local aws_cli_args=()

if [[ -n "$image_ids" ]]; then
  # shellcheck disable=SC2206
  aws_cli_args+=("--image-ids" $image_ids)
fi

response=$(aws ec2 describe-images \
  "${aws_cli_args[@]}" \
  --query 'Images[*].[Description,Architecture,ImageId]' \
  --output text) || {
  aws_cli_error_log ${?}
  errecho "ERROR: AWS reports describe-images operation failed.$response"
  return 1
}

echo "$response"

return 0
```

```
}

################################################################################
# ec2_describe_instance_types
#
# This function describes EC2 instance types filtered by processor architecture
# and optionally by instance type. It takes the following arguments:
#
# -a, --architecture ARCHITECTURE  Specify the processor architecture (e.g., x86_64)
# -t, --type INSTANCE_TYPE         Comma-separated list of instance types (e.g.,
 t2.micro)
# -h, --help                       Show the usage help
#
# The function prints the instance type and supported architecture for each
# matching instance type.
################################################################################
function ec2_describe_instance_types() {
  local architecture=""
  local instance_types=""

  # bashsupport disable=BP5008
  function usage() {
    echo "Usage: ec2_describe_instance_types [-a|--architecture ARCHITECTURE] [-t|--
type INSTANCE_TYPE] [-h|--help]"
    echo "  -a, --architecture ARCHITECTURE  Specify the processor architecture
 (e.g., x86_64)"
    echo "  -t, --type INSTANCE_TYPE         Comma-separated list of instance types
 (e.g., t2.micro)"
    echo "  -h, --help                       Show this help message"
  }

  while [[ $# -gt 0 ]]; do
    case "$1" in
      -a | --architecture)
        architecture="$2"
        shift 2
        ;;
      -t | --type)
        instance_types="$2"
        shift 2
        ;;
      -h | --help)
        usage
        return 0
```

```
      ;;
    *)
      echo "Unknown argument: $1"
      return 1
      ;;
  esac
done

if [[ -z "$architecture" ]]; then
  errecho "Error: Architecture not specified."
  usage
  return 1
fi

if [[ -z "$instance_types" ]]; then
  errecho "Error: Instance type not specified."
  usage
  return 1
fi

local tmp_json_file="temp_ec2.json"
echo -n '[
  {
    "Name": "processor-info.supported-architecture",
    "Values": [' >"$tmp_json_file"

local items
IFS=',' read -ra items <<<"$architecture"
local array_size
array_size=${#items[@]}
for i in $(seq 0 $((array_size - 1))); do
  echo -n '"'"${items[$i]}"'"' >>"$tmp_json_file"
  if [[ $i -lt $((array_size - 1)) ]]; then
    echo -n ',' >>"$tmp_json_file"
  fi
done
echo -n ']},
  {
  "Name": "instance-type",
    "Values": [' >>"$tmp_json_file"
IFS=',' read -ra items <<<"$instance_types"
local array_size
array_size=${#items[@]}
for i in $(seq 0 $((array_size - 1))); do
```

```
    echo -n '"'"${items[$i]}"'"' >>"$tmp_json_file"
    if [[ $i -lt $((array_size - 1)) ]]; then
      echo -n ',' >>"$tmp_json_file"
    fi
  done

  echo -n ']}]' >>"$tmp_json_file"

  local response
  response=$(aws ec2 describe-instance-types --filters file://"$tmp_json_file" \
    --query 'InstanceTypes[*].[InstanceType]' --output text)

  local error_code=$?

  rm "$tmp_json_file"

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    echo "ERROR: AWS reports describe-instance-types operation failed."
    return 1
  fi

  echo "$response"
  return 0
}

###############################################################################
# function ec2_run_instances
#
# This function launches one or more Amazon Elastic Compute Cloud (Amazon EC2)
 instances.
#
# Parameters:
#       -i image_id - The ID of the Amazon Machine Image (AMI) to use.
#       -t instance_type - The instance type to use (e.g., t2.micro).
#       -k key_pair_name - The name of the key pair to use.
#       -s security_group_id - The ID of the security group to use.
#       -c count - The number of instances to launch (default: 1).
#       -h - Display help.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
```

```
function ec2_run_instances() {
  local image_id instance_type key_pair_name security_group_id count response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_run_instances"
    echo "Launches one or more Amazon Elastic Compute Cloud (Amazon EC2) instances."
    echo "  -i image_id - The ID of the Amazon Machine Image (AMI) to use."
    echo "  -t instance_type - The instance type to use (e.g., t2.micro)."
    echo "  -k key_pair_name - The name of the key pair to use."
    echo "  -s security_group_id - The ID of the security group to use."
    echo "  -c count - The number of instances to launch (default: 1)."
    echo "  -h - Display help."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "i:t:k:s:c:h" option; do
    case "${option}" in
      i) image_id="${OPTARG}" ;;
      t) instance_type="${OPTARG}" ;;
      k) key_pair_name="${OPTARG}" ;;
      s) security_group_id="${OPTARG}" ;;
      c) count="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$image_id" ]]; then
    errecho "ERROR: You must provide an Amazon Machine Image (AMI) ID with the -i
 parameter."
    usage
    return 1
  fi
```

```
  if [[ -z "$instance_type" ]]; then
    errecho "ERROR: You must provide an instance type with the -t parameter."
    usage
    return 1
  fi

  if [[ -z "$key_pair_name" ]]; then
    errecho "ERROR: You must provide a key pair name with the -k parameter."
    usage
    return 1
  fi

  if [[ -z "$security_group_id" ]]; then
    errecho "ERROR: You must provide a security group ID with the -s parameter."
    usage
    return 1
  fi

  if [[ -z "$count" ]]; then
    count=1
  fi

  response=$(aws ec2 run-instances \
    --image-id "$image_id" \
    --instance-type "$instance_type" \
    --key-name "$key_pair_name" \
    --security-group-ids "$security_group_id" \
    --count "$count" \
    --query 'Instances[*].[InstanceId]' \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports run-instances operation failed.$response"
    return 1
  }

  echo "$response"

  return 0
}

###############################################################################
# function ec2_describe_instances
#
```

```
# This function describes one or more Amazon Elastic Compute Cloud (Amazon EC2)
 instances.
#
# Parameters:
#       -i instance_id - The ID of the instance to describe (optional).
#       -q query - The query to filter the response (optional).
#       -h - Display help.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_describe_instances() {
  local instance_id query response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_describe_instances"
    echo "Describes one or more Amazon Elastic Compute Cloud (Amazon EC2)
 instances."
    echo "  -i instance_id - The ID of the instance to describe (optional)."
    echo "  -q query - The query to filter the response (optional)."
    echo "  -h - Display help."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "i:q:h" option; do
    case "${option}" in
      i) instance_id="${OPTARG}" ;;
      q) query="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1
```

```
  local aws_cli_args=()

  if [[ -n "$instance_id" ]]; then
    # shellcheck disable=SC2206
    aws_cli_args+=("--instance-ids" $instance_id)
  fi

  local query_arg=""
  if [[ -n "$query" ]]; then
    query_arg="--query '$query'"
  else
    query_arg="--query Reservations[*].Instances[*].
[InstanceId,ImageId,InstanceType,KeyName,VpcId,PublicIpAddress,State.Name]"
  fi

  # shellcheck disable=SC2086
  response=$(aws ec2 describe-instances \
    "${aws_cli_args[@]}" \
    $query_arg \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports describe-instances operation failed.$response"
    return 1
  }

  echo "$response"

  return 0
}

###############################################################################
# function ec2_stop_instances
#
# This function stops one or more Amazon Elastic Compute Cloud (Amazon EC2)
 instances.
#
# Parameters:
#       -i instance_id - The ID(s) of the instance(s) to stop (comma-separated).
#       -h - Display help.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
```

```
###############################################################################
function ec2_stop_instances() {
  local instance_ids
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_stop_instances"
    echo "Stops one or more Amazon Elastic Compute Cloud (Amazon EC2) instances."
    echo "  -i instance_id - The ID(s) of the instance(s) to stop (comma-
separated)."
    echo "  -h - Display help."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "i:h" option; do
    case "${option}" in
      i) instance_ids="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$instance_ids" ]]; then
    errecho "ERROR: You must provide one or more instance IDs with the -i
 parameter."
    usage
    return 1
  fi

  response=$(aws ec2 stop-instances \
    --instance-ids "${instance_ids}") || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports stop-instances operation failed with $response."
    return 1
```

```
  }

  return 0
}

###############################################################################
# function ec2_start_instances
#
# This function starts one or more Amazon Elastic Compute Cloud (Amazon EC2)
 instances.
#
# Parameters:
#       -i instance_id - The ID(s) of the instance(s) to start (comma-separated).
#       -h - Display help.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_start_instances() {
  local instance_ids
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_start_instances"
    echo "Starts one or more Amazon Elastic Compute Cloud (Amazon EC2) instances."
    echo "  -i instance_id - The ID(s) of the instance(s) to start (comma-
separated)."
    echo "  -h - Display help."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "i:h" option; do
    case "${option}" in
      i) instance_ids="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
```

```
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$instance_ids" ]]; then
    errecho "ERROR: You must provide one or more instance IDs with the -i
 parameter."
    usage
    return 1
  fi

  response=$(aws ec2 start-instances \
    --instance-ids "${instance_ids}") || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports start-instances operation failed with $response."
    return 1
  }

  return 0
}

###############################################################################
# function ec2_allocate_address
#
# This function allocates an Elastic IP address for use with Amazon Elastic Compute
 Cloud (Amazon EC2) instances in a specific AWS Region.
#
# Parameters:
#       -d domain - The domain for the Elastic IP address (either 'vpc' or
 'standard').
#
# Returns:
#       The allocated Elastic IP address, or an error message if the operation
 fails.
# And:
#       0 - If successful.
#       1 - If it fails.
#
###############################################################################
function ec2_allocate_address() {
  local domain response
```

```
 # Function to display usage information
 function usage() {
   echo "function ec2_allocate_address"
   echo "Allocates an Elastic IP address for use with Amazon Elastic Compute Cloud
(Amazon EC2) instances in a specific AWS Region."
   echo "  -d domain - The domain for the Elastic IP address (either 'vpc' or
'standard')."
   echo ""
 }

 # Parse the command-line arguments
 while getopts "d:h" option; do
   case "${option}" in
     d) domain="${OPTARG}" ;;
     h)
       usage
       return 0
       ;;
     \?)
       echo "Invalid parameter"
       usage
       return 1
       ;;
   esac
 done
 export OPTIND=1

 # Validate the input parameters
 if [[ -z "$domain" ]]; then
   errecho "ERROR: You must provide a domain with the -d parameter (either 'vpc' or
'standard')."
   return 1
 fi

 if [[ "$domain" != "vpc" && "$domain" != "standard" ]]; then
   errecho "ERROR: Invalid domain value. Must be either 'vpc' or 'standard'."
   return 1
 fi

 # Allocate the Elastic IP address
 response=$(aws ec2 allocate-address \
   --domain "$domain" \
   --query "[PublicIp,AllocationId]" \
   --output text) || {
```

```
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports allocate-address operation failed."
    errecho "$response"
    return 1
  }

  echo "$response"
  return 0
}

################################################################################
# function ec2_associate_address
#
# This function associates an Elastic IP address with an Amazon Elastic Compute
 Cloud (Amazon EC2) instance.
#
# Parameters:
#       -a allocation_id - The allocation ID of the Elastic IP address to associate.
#       -i instance_id - The ID of the EC2 instance to associate the Elastic IP
 address with.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
#
################################################################################
function ec2_associate_address() {
  local allocation_id instance_id response

  # Function to display usage information
  function usage() {
    echo "function ec2_associate_address"
    echo "Associates an Elastic IP address with an Amazon Elastic Compute Cloud
 (Amazon EC2) instance."
    echo "  -a allocation_id - The allocation ID of the Elastic IP address to
 associate."
    echo "  -i instance_id - The ID of the EC2 instance to associate the Elastic IP
 address with."
    echo ""
  }

  # Parse the command-line arguments
  while getopts "a:i:h" option; do
    case "${option}" in
```

```
      a) allocation_id="${OPTARG}" ;;
      i) instance_id="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  # Validate the input parameters
  if [[ -z "$allocation_id" ]]; then
    errecho "ERROR: You must provide an allocation ID with the -a parameter."
    return 1
  fi

  if [[ -z "$instance_id" ]]; then
    errecho "ERROR: You must provide an instance ID with the -i parameter."
    return 1
  fi

  # Associate the Elastic IP address
  response=$(aws ec2 associate-address \
    --allocation-id "$allocation_id" \
    --instance-id "$instance_id" \
    --query "AssociationId" \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports associate-address operation failed."
    errecho "$response"
    return 1
  }

  echo "$response"
  return 0
}

################################################################################
# function ec2_disassociate_address
```

```
#
# This function disassociates an Elastic IP address from an Amazon Elastic Compute
 Cloud (Amazon EC2) instance.
#
# Parameters:
#       -a association_id - The association ID that represents the association of
 the Elastic IP address with an instance.
#
# And:
#       0 - If successful.
#       1 - If it fails.
#
###############################################################################
function ec2_disassociate_address() {
  local association_id response

  # Function to display usage information
  function usage() {
    echo "function ec2_disassociate_address"
    echo "Disassociates an Elastic IP address from an Amazon Elastic Compute Cloud
 (Amazon EC2) instance."
    echo "  -a association_id - The association ID that represents the association
 of the Elastic IP address with an instance."
    echo ""
  }

  # Parse the command-line arguments
  while getopts "a:h" option; do
    case "${option}" in
      a) association_id="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  # Validate the input parameters
```

```
  if [[ -z "$association_id" ]]; then
    errecho "ERROR: You must provide an association ID with the -a parameter."
    return 1
  fi

  response=$(aws ec2 disassociate-address \
    --association-id "$association_id") || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports disassociate-address operation failed."
    errecho "$response"
    return 1
  }

  return 0
}

###############################################################################
# function ec2_release_address
#
# This function releases an Elastic IP address from an Amazon Elastic Compute Cloud
 (Amazon EC2) instance.
#
# Parameters:
#       -a allocation_id - The allocation ID of the Elastic IP address to release.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
#
###############################################################################
function ec2_release_address() {
  local allocation_id response

  # Function to display usage information
  function usage() {
    echo "function ec2_release_address"
    echo "Releases an Elastic IP address from an Amazon Elastic Compute Cloud
 (Amazon EC2) instance."
    echo "  -a allocation_id - The allocation ID of the Elastic IP address to
 release."
    echo ""
  }

  # Parse the command-line arguments
```

```
  while getopts "a:h" option; do
    case "${option}" in
      a) allocation_id="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  # Validate the input parameters
  if [[ -z "$allocation_id" ]]; then
    errecho "ERROR: You must provide an allocation ID with the -a parameter."
    return 1
  fi

  response=$(aws ec2 release-address \
    --allocation-id "$allocation_id") || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports release-address operation failed."
    errecho "$response"
    return 1
  }

  return 0
}

###############################################################################
# function ec2_terminate_instances
#
# This function terminates one or more Amazon Elastic Compute Cloud (Amazon EC2)
# instances using the AWS CLI.
#
# Parameters:
#       -i instance_ids - A space-separated list of instance IDs.
#       -h - Display help.
#
# Returns:
```

```
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_terminate_instances() {
  local instance_ids response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_terminate_instances"
    echo "Terminates one or more Amazon Elastic Compute Cloud (Amazon EC2)
 instances."
    echo "  -i instance_ids - A space-separated list of instance IDs."
    echo "  -h - Display help."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "i:h" option; do
    case "${option}" in
      i) instance_ids="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  # Check if instance ID is provided
  if [[ -z "${instance_ids}" ]]; then
    echo "Error: Missing required instance IDs parameter."
    usage
    return 1
  fi

  # shellcheck disable=SC2086
  response=$(aws ec2 terminate-instances \
    "--instance-ids" $instance_ids \
```

```
    --query 'TerminatingInstances[*].[InstanceId,CurrentState.Name]' \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports terminate-instances operation failed.$response"
    return 1
  }

  return 0
}

###############################################################################
# function ec2_delete_security_group
#
# This function deletes an Amazon Elastic Compute Cloud (Amazon EC2) security group.
#
# Parameters:
#       -i security_group_id - The ID of the security group to delete.
#
# And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_delete_security_group() {
  local security_group_id response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_delete_security_group"
    echo "Deletes an Amazon Elastic Compute Cloud (Amazon EC2) security group."
    echo "  -i security_group_id - The ID of the security group to delete."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "i:h" option; do
    case "${option}" in
      i) security_group_id="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
```

```
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$security_group_id" ]]; then
    errecho "ERROR: You must provide a security group ID with the -i parameter."
    usage
    return 1
  fi

  response=$(aws ec2 delete-security-group --group-id "$security_group_id" --output
 text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports delete-security-group operation failed.$response"
    return 1
  }

  return 0
}

################################################################################
# function ec2_delete_keypair
#
# This function deletes an Amazon EC2 ED25519 or 2048-bit RSA key pair.
#
# Parameters:
#       -n key_pair_name - A key pair name.
#
# And:
#       0 - If successful.
#       1 - If it fails.
################################################################################
function ec2_delete_keypair() {
  local key_pair_name response

  local option OPTARG # Required to use getopts command in a function.
  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_delete_keypair"
    echo "Deletes an Amazon EC2 ED25519 or 2048-bit RSA key pair."
    echo "  -n key_pair_name - A key pair name."
```

```
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:h" option; do
    case "${option}" in
      n) key_pair_name="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$key_pair_name" ]]; then
    errecho "ERROR: You must provide a key pair name with the -n parameter."
    usage
    return 1
  fi

  response=$(aws ec2 delete-key-pair \
    --key-name "$key_pair_name") || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports delete-key-pair operation failed.$response"
    return 1
  }

  return 0
}
```

Las funciones de utilidad usadas en este escenario.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
```

```
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
###############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - AllocateAddress

- AssociateAddress
- AuthorizeSecurityGroupIngress
- CreateKeyPair
- CreateSecurityGroup
- DeleteKeyPair
- DeleteSecurityGroup
- DescribeImages
- DescribeInstanceTypes
- DescribeInstances
- DescribeKeyPairs
- DescribeSecurityGroups
- DisassociateAddress
- ReleaseAddress
- RunInstances
- StartInstances
- StopInstances
- TerminateInstances
- UnmonitorInstances

Acciones

`AllocateAddress`

En el siguiente ejemplo de código, se muestra cómo utilizar `AllocateAddress`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
```

```
# function ec2_allocate_address
#
# This function allocates an Elastic IP address for use with Amazon Elastic Compute
 Cloud (Amazon EC2) instances in a specific AWS Region.
#
# Parameters:
#       -d domain - The domain for the Elastic IP address (either 'vpc' or
 'standard').
#
# Returns:
#       The allocated Elastic IP address, or an error message if the operation
 fails.
# And:
#       0 - If successful.
#       1 - If it fails.
#
################################################################################
function ec2_allocate_address() {
  local domain response

  # Function to display usage information
  function usage() {
    echo "function ec2_allocate_address"
    echo "Allocates an Elastic IP address for use with Amazon Elastic Compute Cloud
 (Amazon EC2) instances in a specific AWS Region."
    echo "  -d domain - The domain for the Elastic IP address (either 'vpc' or
 'standard')."
    echo ""
  }

  # Parse the command-line arguments
  while getopts "d:h" option; do
    case "${option}" in
      d) domain="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
```

```
  done
  export OPTIND=1

  # Validate the input parameters
  if [[ -z "$domain" ]]; then
    errecho "ERROR: You must provide a domain with the -d parameter (either 'vpc' or
 'standard')."
    return 1
  fi

  if [[ "$domain" != "vpc" && "$domain" != "standard" ]]; then
    errecho "ERROR: Invalid domain value. Must be either 'vpc' or 'standard'."
    return 1
  fi

  # Allocate the Elastic IP address
  response=$(aws ec2 allocate-address \
    --domain "$domain" \
    --query "[PublicIp,AllocationId]" \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports allocate-address operation failed."
    errecho "$response"
    return 1
  }

  echo "$response"
  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
```

```
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
################################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte AllocateAddress en la Referencia de comandos de la AWS CLI.

`AssociateAddress`

En el siguiente ejemplo de código, se muestra cómo utilizar `AssociateAddress`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function ec2_associate_address
#
# This function associates an Elastic IP address with an Amazon Elastic Compute
 Cloud (Amazon EC2) instance.
#
# Parameters:
#       -a allocation_id - The allocation ID of the Elastic IP address to associate.
#       -i instance_id - The ID of the EC2 instance to associate the Elastic IP
 address with.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
#
###############################################################################
function ec2_associate_address() {
  local allocation_id instance_id response

  # Function to display usage information
  function usage() {
    echo "function ec2_associate_address"
    echo "Associates an Elastic IP address with an Amazon Elastic Compute Cloud
 (Amazon EC2) instance."
    echo "  -a allocation_id - The allocation ID of the Elastic IP address to
 associate."
    echo "  -i instance_id - The ID of the EC2 instance to associate the Elastic IP
 address with."
    echo ""
  }

  # Parse the command-line arguments
  while getopts "a:i:h" option; do
    case "${option}" in
```

```
      a) allocation_id="${OPTARG}" ;;
      i) instance_id="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  # Validate the input parameters
  if [[ -z "$allocation_id" ]]; then
    errecho "ERROR: You must provide an allocation ID with the -a parameter."
    return 1
  fi

  if [[ -z "$instance_id" ]]; then
    errecho "ERROR: You must provide an instance ID with the -i parameter."
    return 1
  fi

  # Associate the Elastic IP address
  response=$(aws ec2 associate-address \
    --allocation-id "$allocation_id" \
    --instance-id "$instance_id" \
    --query "AssociationId" \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports associate-address operation failed."
    errecho "$response"
    return 1
  }

  echo "$response"
  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
#####################################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
#####################################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

#####################################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
#####################################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte AssociateAddress en la Referencia de comandos de la AWS CLI.

`AuthorizeSecurityGroupIngress`

En el siguiente ejemplo de código, se muestra cómo utilizar `AuthorizeSecurityGroupIngress`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function ec2_authorize_security_group_ingress
#
# This function authorizes an ingress rule for an Amazon Elastic Compute Cloud
 (Amazon EC2) security group.
#
# Parameters:
#       -g security_group_id - The ID of the security group.
#       -i ip_address - The IP address or CIDR block to authorize.
#       -p protocol - The protocol to authorize (e.g., tcp, udp, icmp).
#       -f from_port - The start of the port range to authorize.
#       -t to_port - The end of the port range to authorize.
#
# And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_authorize_security_group_ingress() {
  local security_group_id ip_address protocol from_port to_port response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_authorize_security_group_ingress"
```

```
    echo "Authorizes an ingress rule for an Amazon Elastic Compute Cloud (Amazon
EC2) security group."
    echo "  -g security_group_id - The ID of the security group."
    echo "  -i ip_address - The IP address or CIDR block to authorize."
    echo "  -p protocol - The protocol to authorize (e.g., tcp, udp, icmp)."
    echo "  -f from_port - The start of the port range to authorize."
    echo "  -t to_port - The end of the port range to authorize."
    echo ""
 }

 # Retrieve the calling parameters.
 while getopts "g:i:p:f:t:h" option; do
   case "${option}" in
     g) security_group_id="${OPTARG}" ;;
     i) ip_address="${OPTARG}" ;;
     p) protocol="${OPTARG}" ;;
     f) from_port="${OPTARG}" ;;
     t) to_port="${OPTARG}" ;;
     h)
       usage
       return 0
       ;;
     \?)
       echo "Invalid parameter"
       usage
       return 1
       ;;
   esac
 done
 export OPTIND=1

 if [[ -z "$security_group_id" ]]; then
   errecho "ERROR: You must provide a security group ID with the -g parameter."
   usage
   return 1
 fi

 if [[ -z "$ip_address" ]]; then
   errecho "ERROR: You must provide an IP address or CIDR block with the -i
parameter."
   usage
   return 1
 fi
```

```
  if [[ -z "$protocol" ]]; then
    errecho "ERROR: You must provide a protocol with the -p parameter."
    usage
    return 1
  fi

  if [[ -z "$from_port" ]]; then
    errecho "ERROR: You must provide a start port with the -f parameter."
    usage
    return 1
  fi

  if [[ -z "$to_port" ]]; then
    errecho "ERROR: You must provide an end port with the -t parameter."
    usage
    return 1
  fi

  response=$(aws ec2 authorize-security-group-ingress \
    --group-id "$security_group_id" \
    --cidr "${ip_address}/32" \
    --protocol "$protocol" \
    --port "$from_port-$to_port" \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports authorize-security-group-ingress operation failed.
$response"
    return 1
  }

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
```

```
}

#############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
#############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte AuthorizeSecurityGroupIngress en la Referencia de comandos de la AWS CLI.

`CreateKeyPair`

En el siguiente ejemplo de código, se muestra cómo utilizar `CreateKeyPair`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
#############################################################################
# function ec2_create_keypair
#
# This function creates an Amazon Elastic Compute Cloud (Amazon EC2) ED25519 or
 2048-bit RSA key pair
# and writes it to a file.
#
# Parameters:
#       -n key_pair_name - A key pair name.
#       -f file_path - File to store the key pair.
#
# And:
#       0 - If successful.
#       1 - If it fails.
#############################################################################
function ec2_create_keypair() {
  local key_pair_name file_path response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_create_keypair"
    echo "Creates an Amazon Elastic Compute Cloud (Amazon EC2) ED25519 or 2048-bit
 RSA key pair"
    echo " and writes it to a file."
    echo "  -n key_pair_name - A key pair name."
    echo "  -f file_path - File to store the key pair."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:f:h" option; do
    case "${option}" in
      n) key_pair_name="${OPTARG}" ;;
```

```
      f) file_path="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$key_pair_name" ]]; then
    errecho "ERROR: You must provide a key name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$file_path" ]]; then
    errecho "ERROR: You must provide a file path with the -f parameter."
    usage
    return 1
  fi

  response=$(aws ec2 create-key-pair \
    --key-name "$key_pair_name" \
    --query 'KeyMaterial' \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports create-access-key operation failed.$response"
    return 1
  }

  if [[ -n "$file_path" ]]; then
    echo "$response" >"$file_path"
  fi

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
################################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
################################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

################################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
################################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte CreateKeyPair en la Referencia de comandos de la AWS CLI.

`CreateSecurityGroup`

En el siguiente ejemplo de código, se muestra cómo utilizar `CreateSecurityGroup`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function ec2_create_security_group
#
# This function creates an Amazon Elastic Compute Cloud (Amazon EC2) security group.
#
# Parameters:
#       -n security_group_name - The name of the security group.
#       -d security_group_description - The description of the security group.
#
# Returns:
#       The ID of the created security group, or an error message if the operation
 fails.
# And:
#       0 - If successful.
#       1 - If it fails.
#
###############################################################################
function ec2_create_security_group() {
  local security_group_name security_group_description response

  # Function to display usage information
  function usage() {
    echo "function ec2_create_security_group"
    echo "Creates an Amazon Elastic Compute Cloud (Amazon EC2) security group."
```

```
    echo "  -n security_group_name - The name of the security group."
    echo "  -d security_group_description - The description of the security group."
    echo ""
  }

  # Parse the command-line arguments
  while getopts "n:d:h" option; do
    case "${option}" in
      n) security_group_name="${OPTARG}" ;;
      d) security_group_description="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  # Validate the input parameters
  if [[ -z "$security_group_name" ]]; then
    errecho "ERROR: You must provide a security group name with the -n parameter."
    return 1
  fi

  if [[ -z "$security_group_description" ]]; then
    errecho "ERROR: You must provide a security group description with the -d
parameter."
    return 1
  fi

  # Create the security group
  response=$(aws ec2 create-security-group \
    --group-name "$security_group_name" \
    --description "$security_group_description" \
    --query "GroupId" \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports create-security-group operation failed."
    errecho "$response"
```

```
    return 1
  }

  echo "$response"
  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
################################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
################################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

################################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
################################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
```

```
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte CreateSecurityGroup en la Referencia de comandos de la AWS CLI.

`DeleteKeyPair`

En el siguiente ejemplo de código, se muestra cómo utilizar `DeleteKeyPair`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function ec2_delete_keypair
#
# This function deletes an Amazon EC2 ED25519 or 2048-bit RSA key pair.
#
# Parameters:
#       -n key_pair_name - A key pair name.
#
# And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_delete_keypair() {
  local key_pair_name response
```

```
  local option OPTARG # Required to use getopts command in a function.
  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_delete_keypair"
    echo "Deletes an Amazon EC2 ED25519 or 2048-bit RSA key pair."
    echo "  -n key_pair_name - A key pair name."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:h" option; do
    case "${option}" in
      n) key_pair_name="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$key_pair_name" ]]; then
    errecho "ERROR: You must provide a key pair name with the -n parameter."
    usage
    return 1
  fi

  response=$(aws ec2 delete-key-pair \
    --key-name "$key_pair_name") || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports delete-key-pair operation failed.$response"
    return 1
  }

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
#############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
#############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

#############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
#############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte DeleteKeyPair en la Referencia de comandos de la AWS CLI.

`DeleteSecurityGroup`

En el siguiente ejemplo de código, se muestra cómo utilizar `DeleteSecurityGroup`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function ec2_delete_security_group
#
# This function deletes an Amazon Elastic Compute Cloud (Amazon EC2) security group.
#
# Parameters:
#       -i security_group_id - The ID of the security group to delete.
#
# And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_delete_security_group() {
  local security_group_id response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_delete_security_group"
    echo "Deletes an Amazon Elastic Compute Cloud (Amazon EC2) security group."
    echo "  -i security_group_id - The ID of the security group to delete."
    echo ""
  }
```

```
  # Retrieve the calling parameters.
  while getopts "i:h" option; do
    case "${option}" in
      i) security_group_id="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$security_group_id" ]]; then
    errecho "ERROR: You must provide a security group ID with the -i parameter."
    usage
    return 1
  fi

  response=$(aws ec2 delete-security-group --group-id "$security_group_id" --output
 text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports delete-security-group operation failed.$response"
    return 1
  }

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
```

```
}

#############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
#############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte DeleteSecurityGroup en la Referencia de comandos de la AWS CLI.

`DescribeImages`

En el siguiente ejemplo de código, se muestra cómo utilizar `DescribeImages`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
#############################################################################
# function ec2_describe_images
#
# This function describes one or more Amazon Elastic Compute Cloud (Amazon EC2)
 images.
#
# Parameters:
#       -i image_ids - A space-separated  list of image IDs (optional).
#       -h - Display help.
#
# And:
#       0 - If successful.
#       1 - If it fails.
#############################################################################
function ec2_describe_images() {
  local image_ids response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_describe_images"
    echo "Describes one or more Amazon Elastic Compute Cloud (Amazon EC2) images."
    echo "  -i image_ids - A space-separated list of image IDs (optional)."
    echo "  -h - Display help."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "i:h" option; do
    case "${option}" in
      i) image_ids="${OPTARG}" ;;
      h)
        usage
        return 0
```

```
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  local aws_cli_args=()

  if [[ -n "$image_ids" ]]; then
    # shellcheck disable=SC2206
    aws_cli_args+=("--image-ids" $image_ids)
  fi

  response=$(aws ec2 describe-images \
    "${aws_cli_args[@]}" \
    --query 'Images[*].[Description,Architecture,ImageId]' \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports describe-images operation failed.$response"
    return 1
  }

  echo "$response"

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}
```

```
###############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
###############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte DescribeImages en la Referencia de comandos de la AWS CLI.

`DescribeInstanceTypes`

En el siguiente ejemplo de código, se muestra cómo utilizar `DescribeInstanceTypes`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
# ec2_describe_instance_types
#
# This function describes EC2 instance types filtered by processor architecture
# and optionally by instance type. It takes the following arguments:
#
# -a, --architecture ARCHITECTURE  Specify the processor architecture (e.g., x86_64)
# -t, --type INSTANCE_TYPE         Comma-separated list of instance types (e.g.,
 t2.micro)
# -h, --help                       Show the usage help
#
# The function prints the instance type and supported architecture for each
# matching instance type.
##############################################################################
function ec2_describe_instance_types() {
  local architecture=""
  local instance_types=""

  # bashsupport disable=BP5008
  function usage() {
    echo "Usage: ec2_describe_instance_types [-a|--architecture ARCHITECTURE] [-t|--
type INSTANCE_TYPE] [-h|--help]"
    echo "  -a, --architecture ARCHITECTURE  Specify the processor architecture
 (e.g., x86_64)"
    echo "  -t, --type INSTANCE_TYPE         Comma-separated list of instance types
 (e.g., t2.micro)"
    echo "  -h, --help                       Show this help message"
  }

  while [[ $# -gt 0 ]]; do
    case "$1" in
      -a | --architecture)
        architecture="$2"
        shift 2
```

```
      ;;
    -t | --type)
      instance_types="$2"
      shift 2
      ;;
    -h | --help)
      usage
      return 0
      ;;
    *)
      echo "Unknown argument: $1"
      return 1
      ;;
  esac
done

if [[ -z "$architecture" ]]; then
  errecho "Error: Architecture not specified."
  usage
  return 1
fi

if [[ -z "$instance_types" ]]; then
  errecho "Error: Instance type not specified."
  usage
  return 1
fi

local tmp_json_file="temp_ec2.json"
echo -n '[
  {
    "Name": "processor-info.supported-architecture",
    "Values": [' >"$tmp_json_file"

local items
IFS=',' read -ra items <<<"$architecture"
local array_size
array_size=${#items[@]}
for i in $(seq 0 $((array_size - 1))); do
  echo -n '"'"${items[$i]}"'"' >>"$tmp_json_file"
  if [[ $i -lt $((array_size - 1)) ]]; then
    echo -n ',' >>"$tmp_json_file"
  fi
done
```

```
  echo -n ']},
    {
    "Name": "instance-type",
      "Values": [' >>"$tmp_json_file"
  IFS=',' read -ra items <<<"$instance_types"
  local array_size
  array_size=${#items[@]}
  for i in $(seq 0 $((array_size - 1))); do
    echo -n '"'"${items[$i]}"'"' >>"$tmp_json_file"
    if [[ $i -lt $((array_size - 1)) ]]; then
      echo -n ',' >>"$tmp_json_file"
    fi
  done

  echo -n ']}]' >>"$tmp_json_file"

  local response
  response=$(aws ec2 describe-instance-types --filters file://"$tmp_json_file" \
    --query 'InstanceTypes[*].[InstanceType]' --output text)

  local error_code=$?

  rm "$tmp_json_file"

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    echo "ERROR: AWS reports describe-instance-types operation failed."
    return 1
  fi

  echo "$response"
  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
```

```
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
###############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte DescribeInstanceTypes en la Referencia de comandos de la AWS CLI.

`DescribeInstances`

En el siguiente ejemplo de código, se muestra cómo utilizar `DescribeInstances`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function ec2_describe_instances
#
# This function describes one or more Amazon Elastic Compute Cloud (Amazon EC2)
 instances.
#
# Parameters:
#       -i instance_id - The ID of the instance to describe (optional).
#       -q query - The query to filter the response (optional).
#       -h - Display help.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_describe_instances() {
  local instance_id query response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_describe_instances"
    echo "Describes one or more Amazon Elastic Compute Cloud (Amazon EC2)
 instances."
    echo "  -i instance_id - The ID of the instance to describe (optional)."
    echo "  -q query - The query to filter the response (optional)."
    echo "  -h - Display help."
    echo ""
  }

  # Retrieve the calling parameters.
```

```
  while getopts "i:q:h" option; do
    case "${option}" in
      i) instance_id="${OPTARG}" ;;
      q) query="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  local aws_cli_args=()

  if [[ -n "$instance_id" ]]; then
    # shellcheck disable=SC2206
    aws_cli_args+=("--instance-ids" $instance_id)
  fi

  local query_arg=""
  if [[ -n "$query" ]]; then
    query_arg="--query '$query'"
  else
    query_arg="--query Reservations[*].Instances[*].
[InstanceId,ImageId,InstanceType,KeyName,VpcId,PublicIpAddress,State.Name]"
  fi

  # shellcheck disable=SC2086
  response=$(aws ec2 describe-instances \
    "${aws_cli_args[@]}" \
    $query_arg \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports describe-instances operation failed.$response"
    return 1
  }

  echo "$response"
```

```
  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
################################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
################################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

################################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
################################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
```

```
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte DescribeInstances en la Referencia de comandos de la AWS CLI.

`DescribeKeyPairs`

En el siguiente ejemplo de código, se muestra cómo utilizar `DescribeKeyPairs`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function ec2_describe_key_pairs
#
# This function describes one or more Amazon Elastic Compute Cloud (Amazon EC2) key
 pairs.
#
# Parameters:
#       -h - Display help.
#
# And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_describe_key_pairs() {
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_describe_key_pairs"
```

```
    echo "Describes one or more Amazon Elastic Compute Cloud (Amazon EC2) key
 pairs."
    echo "  -h - Display help."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "h" option; do
    case "${option}" in
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  local response

  response=$(aws ec2 describe-key-pairs \
    --query 'KeyPairs[*].[KeyName, KeyFingerprint]' \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports describe-key-pairs operation failed.$response"
    return 1
  }

  echo "$response"

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
```

```
# This function outputs everything sent to it to STDERR (standard error output).
#########################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

#########################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
#########################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte DescribeKeyPairs en la Referencia de comandos de la AWS CLI.

`DescribeSecurityGroups`

En el siguiente ejemplo de código, se muestra cómo utilizar `DescribeSecurityGroups`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function ec2_describe_security_groups
#
# This function describes one or more Amazon Elastic Compute Cloud (Amazon EC2)
 security groups.
#
# Parameters:
#       -g security_group_id - The ID of the security group to describe (optional).
#
# And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_describe_security_groups() {
  local security_group_id response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_describe_security_groups"
    echo "Describes one or more Amazon Elastic Compute Cloud (Amazon EC2) security
 groups."
    echo "  -g security_group_id - The ID of the security group to describe
 (optional)."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "g:h" option; do
    case "${option}" in
      g) security_group_id="${OPTARG}" ;;
```

```
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  local query="SecurityGroups[*].[GroupName, GroupId, VpcId, IpPermissions[*].
[IpProtocol, FromPort, ToPort, IpRanges[*].CidrIp]]"

  if [[ -n "$security_group_id" ]]; then
    response=$(aws ec2 describe-security-groups --group-ids "$security_group_id" --
query "${query}" --output text)
  else
    response=$(aws ec2 describe-security-groups --query "${query}" --output text)
  fi

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports describe-security-groups operation failed.$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
```

```
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
###############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte DescribeSecurityGroups en la Referencia de comandos de la AWS CLI.

`DisassociateAddress`

En el siguiente ejemplo de código, se muestra cómo utilizar `DisassociateAddress`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function ec2_disassociate_address
#
# This function disassociates an Elastic IP address from an Amazon Elastic Compute
 Cloud (Amazon EC2) instance.
#
# Parameters:
#       -a association_id - The association ID that represents the association of
 the Elastic IP address with an instance.
#
# And:
#       0 - If successful.
#       1 - If it fails.
#
###############################################################################
function ec2_disassociate_address() {
  local association_id response

  # Function to display usage information
  function usage() {
    echo "function ec2_disassociate_address"
    echo "Disassociates an Elastic IP address from an Amazon Elastic Compute Cloud
 (Amazon EC2) instance."
    echo "  -a association_id - The association ID that represents the association
 of the Elastic IP address with an instance."
    echo ""
  }

  # Parse the command-line arguments
  while getopts "a:h" option; do
    case "${option}" in
```

```
      a) association_id="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  # Validate the input parameters
  if [[ -z "$association_id" ]]; then
    errecho "ERROR: You must provide an association ID with the -a parameter."
    return 1
  fi

  response=$(aws ec2 disassociate-address \
    --association-id "$association_id") || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports disassociate-address operation failed."
    errecho "$response"
    return 1
  }

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}
```

```
###############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
###############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte DisassociateAddress en la Referencia de comandos de la AWS CLI.

`ReleaseAddress`

En el siguiente ejemplo de código, se muestra cómo utilizar `ReleaseAddress`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function ec2_release_address
#
# This function releases an Elastic IP address from an Amazon Elastic Compute Cloud
 (Amazon EC2) instance.
#
# Parameters:
#       -a allocation_id - The allocation ID of the Elastic IP address to release.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
#
###############################################################################
function ec2_release_address() {
  local allocation_id response

  # Function to display usage information
  function usage() {
    echo "function ec2_release_address"
    echo "Releases an Elastic IP address from an Amazon Elastic Compute Cloud
 (Amazon EC2) instance."
    echo "  -a allocation_id - The allocation ID of the Elastic IP address to
 release."
    echo ""
  }

  # Parse the command-line arguments
  while getopts "a:h" option; do
    case "${option}" in
      a) allocation_id="${OPTARG}" ;;
      h)
        usage
        return 0
```

```
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  # Validate the input parameters
  if [[ -z "$allocation_id" ]]; then
    errecho "ERROR: You must provide an allocation ID with the -a parameter."
    return 1
  fi

  response=$(aws ec2 release-address \
    --allocation-id "$allocation_id") || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports release-address operation failed."
    errecho "$response"
    return 1
  }

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
```

```
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
################################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte ReleaseAddress en la Referencia de comandos de la AWS CLI.

`RunInstances`

En el siguiente ejemplo de código, se muestra cómo utilizar `RunInstances`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function ec2_run_instances
#
# This function launches one or more Amazon Elastic Compute Cloud (Amazon EC2)
 instances.
#
# Parameters:
#       -i image_id - The ID of the Amazon Machine Image (AMI) to use.
#       -t instance_type - The instance type to use (e.g., t2.micro).
#       -k key_pair_name - The name of the key pair to use.
#       -s security_group_id - The ID of the security group to use.
#       -c count - The number of instances to launch (default: 1).
#       -h - Display help.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_run_instances() {
  local image_id instance_type key_pair_name security_group_id count response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_run_instances"
    echo "Launches one or more Amazon Elastic Compute Cloud (Amazon EC2) instances."
    echo "  -i image_id - The ID of the Amazon Machine Image (AMI) to use."
    echo "  -t instance_type - The instance type to use (e.g., t2.micro)."
    echo "  -k key_pair_name - The name of the key pair to use."
    echo "  -s security_group_id - The ID of the security group to use."
    echo "  -c count - The number of instances to launch (default: 1)."
    echo "  -h - Display help."
    echo ""
  }
```

```
 # Retrieve the calling parameters.
 while getopts "i:t:k:s:c:h" option; do
   case "${option}" in
     i) image_id="${OPTARG}" ;;
     t) instance_type="${OPTARG}" ;;
     k) key_pair_name="${OPTARG}" ;;
     s) security_group_id="${OPTARG}" ;;
     c) count="${OPTARG}" ;;
     h)
       usage
       return 0
       ;;
     \?)
       echo "Invalid parameter"
       usage
       return 1
       ;;
   esac
 done
 export OPTIND=1

 if [[ -z "$image_id" ]]; then
   errecho "ERROR: You must provide an Amazon Machine Image (AMI) ID with the -i
parameter."
   usage
   return 1
 fi

 if [[ -z "$instance_type" ]]; then
   errecho "ERROR: You must provide an instance type with the -t parameter."
   usage
   return 1
 fi

 if [[ -z "$key_pair_name" ]]; then
   errecho "ERROR: You must provide a key pair name with the -k parameter."
   usage
   return 1
 fi

 if [[ -z "$security_group_id" ]]; then
   errecho "ERROR: You must provide a security group ID with the -s parameter."
   usage
```

```
    return 1
  fi

  if [[ -z "$count" ]]; then
    count=1
  fi

  response=$(aws ec2 run-instances \
    --image-id "$image_id" \
    --instance-type "$instance_type" \
    --key-name "$key_pair_name" \
    --security-group-ids "$security_group_id" \
    --count "$count" \
    --query 'Instances[*].[InstanceId]' \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports run-instances operation failed.$response"
    return 1
  }

  echo "$response"

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
```

```
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
################################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte RunInstances en la Referencia de comandos de la AWS CLI.

`StartInstances`

En el siguiente ejemplo de código, se muestra cómo utilizar `StartInstances`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function ec2_start_instances
#
# This function starts one or more Amazon Elastic Compute Cloud (Amazon EC2)
 instances.
#
# Parameters:
#       -i instance_id - The ID(s) of the instance(s) to start (comma-separated).
#       -h - Display help.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_start_instances() {
  local instance_ids
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_start_instances"
    echo "Starts one or more Amazon Elastic Compute Cloud (Amazon EC2) instances."
    echo "  -i instance_id - The ID(s) of the instance(s) to start (comma-
separated)."
    echo "  -h - Display help."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "i:h" option; do
    case "${option}" in
      i) instance_ids="${OPTARG}" ;;
      h)
        usage
```

```
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$instance_ids" ]]; then
    errecho "ERROR: You must provide one or more instance IDs with the -i
 parameter."
    usage
    return 1
  fi

  response=$(aws ec2 start-instances \
    --instance-ids "${instance_ids}") || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports start-instances operation failed with $response."
    return 1
  }

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function aws_cli_error_log()
#
```

```
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
################################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte StartInstances en la Referencia de comandos de la AWS CLI.

`StopInstances`

En el siguiente ejemplo de código, se muestra cómo utilizar `StopInstances`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
# function ec2_stop_instances
#
# This function stops one or more Amazon Elastic Compute Cloud (Amazon EC2)
 instances.
#
# Parameters:
#       -i instance_id - The ID(s) of the instance(s) to stop (comma-separated).
#       -h - Display help.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
##############################################################################
function ec2_stop_instances() {
  local instance_ids
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_stop_instances"
    echo "Stops one or more Amazon Elastic Compute Cloud (Amazon EC2) instances."
    echo "  -i instance_id - The ID(s) of the instance(s) to stop (comma-
separated)."
    echo "  -h - Display help."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "i:h" option; do
    case "${option}" in
      i) instance_ids="${OPTARG}" ;;
      h)
        usage
```

```
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$instance_ids" ]]; then
    errecho "ERROR: You must provide one or more instance IDs with the -i
 parameter."
    usage
    return 1
  fi

  response=$(aws ec2 stop-instances \
    --instance-ids "${instance_ids}") || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports stop-instances operation failed with $response."
    return 1
  }

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function aws_cli_error_log()
#
```

```
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
################################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte StopInstances en la Referencia de comandos de la AWS CLI.

`TerminateInstances`

En el siguiente ejemplo de código, se muestra cómo utilizar `TerminateInstances`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function ec2_terminate_instances
#
# This function terminates one or more Amazon Elastic Compute Cloud (Amazon EC2)
# instances using the AWS CLI.
#
# Parameters:
#       -i instance_ids - A space-separated list of instance IDs.
#       -h - Display help.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function ec2_terminate_instances() {
  local instance_ids response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function ec2_terminate_instances"
    echo "Terminates one or more Amazon Elastic Compute Cloud (Amazon EC2)
 instances."
    echo "  -i instance_ids - A space-separated list of instance IDs."
    echo "  -h - Display help."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "i:h" option; do
    case "${option}" in
      i) instance_ids="${OPTARG}" ;;
      h)
        usage
```

```
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  # Check if instance ID is provided
  if [[ -z "${instance_ids}" ]]; then
    echo "Error: Missing required instance IDs parameter."
    usage
    return 1
  fi

  # shellcheck disable=SC2086
  response=$(aws ec2 terminate-instances \
    "--instance-ids" $instance_ids \
    --query 'TerminatingInstances[*].[InstanceId,CurrentState.Name]' \
    --output text) || {
    aws_cli_error_log ${?}
    errecho "ERROR: AWS reports terminate-instances operation failed.$response"
    return 1
  }

  return 0
}
```

Las funciones de utilidad utilizadas en este ejemplo.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}
```

```
###############################################################################
# function aws_cli_error_log()
#
# This function is used to log the error messages from the AWS CLI.
#
# The function expects the following argument:
#         $1 - The error code returned by the AWS CLI.
#
#  Returns:
#          0: - Success.
#
###############################################################################
function aws_cli_error_log() {
  local err_code=$1
  errecho "Error code : $err_code"
  if [ "$err_code" == 1 ]; then
    errecho "  One or more S3 transfers failed."
  elif [ "$err_code" == 2 ]; then
    errecho "  Command line failed to parse."
  elif [ "$err_code" == 130 ]; then
    errecho "  Process received SIGINT."
  elif [ "$err_code" == 252 ]; then
    errecho "  Command syntax invalid."
  elif [ "$err_code" == 253 ]; then
    errecho "  The system environment or configuration was invalid."
  elif [ "$err_code" == 254 ]; then
    errecho "  The service returned an error."
  elif [ "$err_code" == 255 ]; then
    errecho "  255 is a catch-all error."
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte TerminateInstances en la Referencia de comandos de la AWS CLI.

Escenarios

Creación de una VPC con subredes privadas y puertas de enlace NAT

En el siguiente ejemplo de código, se muestra cómo:

- Creación de una VPC con subredes privadas y puertas de enlace NAT mediante la CLI.
- Configure los componentes necesarios, incluidas la VPC, las subredes, las tablas de enrutamiento y las puertas de enlace NAT.
- Configure los grupos de seguridad y los roles de IAM para garantizar un acceso y una seguridad adecuados.
- Utilice los comandos de la CLI para automatizar la creación y configuración de estos recursos.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Encuentre el ejemplo completo y obtenga información sobre cómo configurarlo y ejecutarlo en el repositorio de Tutoriales para desarrolladores de ejemplo.

```
#!/bin/bash

# VPC with Private Subnets and NAT Gateways (IMDSv2 Compliant Version)
# This script creates a VPC with public and private subnets in two Availability
 Zones,
# NAT gateways, an internet gateway, route tables, a VPC endpoint for S3,
# security groups, a launch template, an Auto Scaling group, and an Application Load
 Balancer.

# Set up logging
LOG_FILE="vpc-private-subnets-nat.log"
exec > >(tee -a "$LOG_FILE") 2>&1

# Cleanup function to delete all created resources
cleanup_resources() {
  echo "Cleaning up resources..."

  # Delete Auto Scaling group if it exists
  if [ -n "${ASG_NAME:-}" ]; then
    echo "Deleting Auto Scaling group: $ASG_NAME"
    aws autoscaling delete-auto-scaling-group --auto-scaling-group-name "$ASG_NAME"
 --force-delete
    echo "Waiting for Auto Scaling group to be deleted..."
```

```
  aws autoscaling wait auto-scaling-groups-deleted --auto-scaling-group-names
"$ASG_NAME"
 fi

 # Delete load balancer if it exists
 if [ -n "${LB_ARN:-}" ]; then
   echo "Deleting load balancer: $LB_ARN"
   aws elbv2 delete-load-balancer --load-balancer-arn "$LB_ARN"
   # Wait for load balancer to be deleted
   sleep 30
 fi

 # Delete target group if it exists
 if [ -n "${TARGET_GROUP_ARN:-}" ]; then
   echo "Deleting target group: $TARGET_GROUP_ARN"
   aws elbv2 delete-target-group --target-group-arn "$TARGET_GROUP_ARN"
 fi

 # Delete launch template if it exists
 if [ -n "${LAUNCH_TEMPLATE_NAME:-}" ]; then
   echo "Deleting launch template: $LAUNCH_TEMPLATE_NAME"
   aws ec2 delete-launch-template --launch-template-name "$LAUNCH_TEMPLATE_NAME"
 fi

 # Delete NAT Gateways if they exist
 if [ -n "${NAT_GW1_ID:-}" ]; then
   echo "Deleting NAT Gateway 1: $NAT_GW1_ID"
   aws ec2 delete-nat-gateway --nat-gateway-id "$NAT_GW1_ID"
 fi

 if [ -n "${NAT_GW2_ID:-}" ]; then
   echo "Deleting NAT Gateway 2: $NAT_GW2_ID"
   aws ec2 delete-nat-gateway --nat-gateway-id "$NAT_GW2_ID"
 fi

 # Wait for NAT Gateways to be deleted
 if [ -n "${NAT_GW1_ID:-}" ] || [ -n "${NAT_GW2_ID:-}" ]; then
   echo "Waiting for NAT Gateways to be deleted..."
   sleep 60
 fi

 # Release Elastic IPs if they exist
 if [ -n "${EIP1_ALLOC_ID:-}" ]; then
   echo "Releasing Elastic IP 1: $EIP1_ALLOC_ID"
```

```
    aws ec2 release-address --allocation-id "$EIP1_ALLOC_ID"
  fi

  if [ -n "${EIP2_ALLOC_ID:-}" ]; then
    echo "Releasing Elastic IP 2: $EIP2_ALLOC_ID"
    aws ec2 release-address --allocation-id "$EIP2_ALLOC_ID"
  fi

  # Delete VPC endpoint if it exists
  if [ -n "${VPC_ENDPOINT_ID:-}" ]; then
    echo "Deleting VPC endpoint: $VPC_ENDPOINT_ID"
    aws ec2 delete-vpc-endpoints --vpc-endpoint-ids "$VPC_ENDPOINT_ID"
  fi

  # Delete security groups if they exist
  if [ -n "${APP_SG_ID:-}" ]; then
    echo "Deleting application security group: $APP_SG_ID"
    aws ec2 delete-security-group --group-id "$APP_SG_ID"
  fi

  if [ -n "${LB_SG_ID:-}" ]; then
    echo "Deleting load balancer security group: $LB_SG_ID"
    aws ec2 delete-security-group --group-id "$LB_SG_ID"
  fi

  # Detach and delete Internet Gateway if it exists
  if [ -n "${IGW_ID:-}" ] && [ -n "${VPC_ID:-}" ]; then
    echo "Detaching Internet Gateway: $IGW_ID from VPC: $VPC_ID"
    aws ec2 detach-internet-gateway --internet-gateway-id "$IGW_ID" --vpc-id
"$VPC_ID"
    echo "Deleting Internet Gateway: $IGW_ID"
    aws ec2 delete-internet-gateway --internet-gateway-id "$IGW_ID"
  fi

  # Delete route table associations and route tables if they exist
  if [ -n "${PUBLIC_RT_ASSOC1_ID:-}" ]; then
    echo "Disassociating public route table from subnet 1: $PUBLIC_RT_ASSOC1_ID"
    aws ec2 disassociate-route-table --association-id "$PUBLIC_RT_ASSOC1_ID"
  fi

  if [ -n "${PUBLIC_RT_ASSOC2_ID:-}" ]; then
    echo "Disassociating public route table from subnet 2: $PUBLIC_RT_ASSOC2_ID"
    aws ec2 disassociate-route-table --association-id "$PUBLIC_RT_ASSOC2_ID"
  fi
```

```
if [ -n "${PRIVATE_RT1_ASSOC_ID:-}" ]; then
  echo "Disassociating private route table 1: $PRIVATE_RT1_ASSOC_ID"
  aws ec2 disassociate-route-table --association-id "$PRIVATE_RT1_ASSOC_ID"
fi

if [ -n "${PRIVATE_RT2_ASSOC_ID:-}" ]; then
  echo "Disassociating private route table 2: $PRIVATE_RT2_ASSOC_ID"
  aws ec2 disassociate-route-table --association-id "$PRIVATE_RT2_ASSOC_ID"
fi

if [ -n "${PUBLIC_RT_ID:-}" ]; then
  echo "Deleting public route table: $PUBLIC_RT_ID"
  aws ec2 delete-route-table --route-table-id "$PUBLIC_RT_ID"
fi

if [ -n "${PRIVATE_RT1_ID:-}" ]; then
  echo "Deleting private route table 1: $PRIVATE_RT1_ID"
  aws ec2 delete-route-table --route-table-id "$PRIVATE_RT1_ID"
fi

if [ -n "${PRIVATE_RT2_ID:-}" ]; then
  echo "Deleting private route table 2: $PRIVATE_RT2_ID"
  aws ec2 delete-route-table --route-table-id "$PRIVATE_RT2_ID"
fi

# Delete subnets if they exist
if [ -n "${PUBLIC_SUBNET1_ID:-}" ]; then
  echo "Deleting public subnet 1: $PUBLIC_SUBNET1_ID"
  aws ec2 delete-subnet --subnet-id "$PUBLIC_SUBNET1_ID"
fi

if [ -n "${PUBLIC_SUBNET2_ID:-}" ]; then
  echo "Deleting public subnet 2: $PUBLIC_SUBNET2_ID"
  aws ec2 delete-subnet --subnet-id "$PUBLIC_SUBNET2_ID"
fi

if [ -n "${PRIVATE_SUBNET1_ID:-}" ]; then
  echo "Deleting private subnet 1: $PRIVATE_SUBNET1_ID"
  aws ec2 delete-subnet --subnet-id "$PRIVATE_SUBNET1_ID"
fi

if [ -n "${PRIVATE_SUBNET2_ID:-}" ]; then
  echo "Deleting private subnet 2: $PRIVATE_SUBNET2_ID"
```

```
    aws ec2 delete-subnet --subnet-id "$PRIVATE_SUBNET2_ID"
  fi

  # Delete VPC if it exists
  if [ -n "${VPC_ID:-}" ]; then
    echo "Deleting VPC: $VPC_ID"
    aws ec2 delete-vpc --vpc-id "$VPC_ID"
  fi

  echo "Cleanup completed."
}

# Error handling function
handle_error() {
  echo "ERROR: $1"
  echo "Attempting to clean up resources..."
  cleanup_resources
  exit 1
}

# Function to check command success
check_command() {
  if [ $? -ne 0 ]; then
    handle_error "$1"
  fi
}

# Generate a random identifier for resource names
RANDOM_ID=$(openssl rand -hex 4)
echo "Using random identifier: $RANDOM_ID"

# Create VPC
echo "Creating VPC..."
VPC_RESULT=$(aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications
 "ResourceType=vpc,Tags=[{Key=Name,Value=ProductionVPC-$RANDOM_ID}]")
check_command "Failed to create VPC"

VPC_ID=$(echo "$VPC_RESULT" | jq -r '.Vpc.VpcId')
echo "VPC created with ID: $VPC_ID"

# Get Availability Zones
echo "Getting Availability Zones..."
AZ_RESULT=$(aws ec2 describe-availability-zones --query
 'AvailabilityZones[0:2].ZoneName' --output text)
```

```
check_command "Failed to get Availability Zones"

# Convert space-separated output to array
read -r -a AZS <<< "$AZ_RESULT"
AZ1=${AZS[0]}
AZ2=${AZS[1]}
echo "Using Availability Zones: $AZ1 and $AZ2"

# Create subnets
echo "Creating subnets..."
PUBLIC_SUBNET1_RESULT=$(aws ec2 create-subnet --vpc-id "$VPC_ID" --
cidr-block 10.0.0.0/24 --availability-zone "$AZ1" --tag-specifications
 "ResourceType=subnet,Tags=[{Key=Name,Value=PublicSubnet1-$RANDOM_ID}]")
check_command "Failed to create public subnet 1"
PUBLIC_SUBNET1_ID=$(echo "$PUBLIC_SUBNET1_RESULT" | jq -r '.Subnet.SubnetId')

PRIVATE_SUBNET1_RESULT=$(aws ec2 create-subnet --vpc-id "$VPC_ID" --
cidr-block 10.0.1.0/24 --availability-zone "$AZ1" --tag-specifications
 "ResourceType=subnet,Tags=[{Key=Name,Value=PrivateSubnet1-$RANDOM_ID}]")
check_command "Failed to create private subnet 1"
PRIVATE_SUBNET1_ID=$(echo "$PRIVATE_SUBNET1_RESULT" | jq -r '.Subnet.SubnetId')

PUBLIC_SUBNET2_RESULT=$(aws ec2 create-subnet --vpc-id "$VPC_ID" --
cidr-block 10.0.2.0/24 --availability-zone "$AZ2" --tag-specifications
 "ResourceType=subnet,Tags=[{Key=Name,Value=PublicSubnet2-$RANDOM_ID}]")
check_command "Failed to create public subnet 2"
PUBLIC_SUBNET2_ID=$(echo "$PUBLIC_SUBNET2_RESULT" | jq -r '.Subnet.SubnetId')

PRIVATE_SUBNET2_RESULT=$(aws ec2 create-subnet --vpc-id "$VPC_ID" --
cidr-block 10.0.3.0/24 --availability-zone "$AZ2" --tag-specifications
 "ResourceType=subnet,Tags=[{Key=Name,Value=PrivateSubnet2-$RANDOM_ID}]")
check_command "Failed to create private subnet 2"
PRIVATE_SUBNET2_ID=$(echo "$PRIVATE_SUBNET2_RESULT" | jq -r '.Subnet.SubnetId')

echo "Subnets created with IDs:"
echo "Public Subnet 1: $PUBLIC_SUBNET1_ID"
echo "Private Subnet 1: $PRIVATE_SUBNET1_ID"
echo "Public Subnet 2: $PUBLIC_SUBNET2_ID"
echo "Private Subnet 2: $PRIVATE_SUBNET2_ID"

# Create Internet Gateway
echo "Creating Internet Gateway..."
IGW_RESULT=$(aws ec2 create-internet-gateway --tag-specifications
 "ResourceType=internet-gateway,Tags=[{Key=Name,Value=ProductionIGW-$RANDOM_ID}]")
```

```
check_command "Failed to create Internet Gateway"
IGW_ID=$(echo "$IGW_RESULT" | jq -r '.InternetGateway.InternetGatewayId')
echo "Internet Gateway created with ID: $IGW_ID"

# Attach Internet Gateway to VPC
echo "Attaching Internet Gateway to VPC..."
aws ec2 attach-internet-gateway --internet-gateway-id "$IGW_ID" --vpc-id "$VPC_ID"
check_command "Failed to attach Internet Gateway to VPC"

# Create route tables
echo "Creating route tables..."
PUBLIC_RT_RESULT=$(aws ec2 create-route-table --vpc-id "$VPC_ID" --tag-
specifications "ResourceType=route-table,Tags=[{Key=Name,Value=PublicRouteTable-
$RANDOM_ID}]")
check_command "Failed to create public route table"
PUBLIC_RT_ID=$(echo "$PUBLIC_RT_RESULT" | jq -r '.RouteTable.RouteTableId')

PRIVATE_RT1_RESULT=$(aws ec2 create-route-table --vpc-id "$VPC_ID" --tag-
specifications "ResourceType=route-table,Tags=[{Key=Name,Value=PrivateRouteTable1-
$RANDOM_ID}]")
check_command "Failed to create private route table 1"
PRIVATE_RT1_ID=$(echo "$PRIVATE_RT1_RESULT" | jq -r '.RouteTable.RouteTableId')

PRIVATE_RT2_RESULT=$(aws ec2 create-route-table --vpc-id "$VPC_ID" --tag-
specifications "ResourceType=route-table,Tags=[{Key=Name,Value=PrivateRouteTable2-
$RANDOM_ID}]")
check_command "Failed to create private route table 2"
PRIVATE_RT2_ID=$(echo "$PRIVATE_RT2_RESULT" | jq -r '.RouteTable.RouteTableId')

echo "Route tables created with IDs:"
echo "Public Route Table: $PUBLIC_RT_ID"
echo "Private Route Table 1: $PRIVATE_RT1_ID"
echo "Private Route Table 2: $PRIVATE_RT2_ID"

# Add route to Internet Gateway in public route table
echo "Adding route to Internet Gateway in public route table..."
aws ec2 create-route --route-table-id "$PUBLIC_RT_ID" --destination-cidr-block
 0.0.0.0/0 --gateway-id "$IGW_ID"
check_command "Failed to add route to Internet Gateway"

# Associate subnets with route tables
echo "Associating subnets with route tables..."
PUBLIC_RT_ASSOC1_RESULT=$(aws ec2 associate-route-table --route-table-id
 "$PUBLIC_RT_ID" --subnet-id "$PUBLIC_SUBNET1_ID")
```

```
check_command "Failed to associate public subnet 1 with route table"
PUBLIC_RT_ASSOC1_ID=$(echo "$PUBLIC_RT_ASSOC1_RESULT" | jq -r '.AssociationId')

PUBLIC_RT_ASSOC2_RESULT=$(aws ec2 associate-route-table --route-table-id
 "$PUBLIC_RT_ID" --subnet-id "$PUBLIC_SUBNET2_ID")
check_command "Failed to associate public subnet 2 with route table"
PUBLIC_RT_ASSOC2_ID=$(echo "$PUBLIC_RT_ASSOC2_RESULT" | jq -r '.AssociationId')

PRIVATE_RT1_ASSOC_RESULT=$(aws ec2 associate-route-table --route-table-id
 "$PRIVATE_RT1_ID" --subnet-id "$PRIVATE_SUBNET1_ID")
check_command "Failed to associate private subnet 1 with route table"
PRIVATE_RT1_ASSOC_ID=$(echo "$PRIVATE_RT1_ASSOC_RESULT" | jq -r '.AssociationId')

PRIVATE_RT2_ASSOC_RESULT=$(aws ec2 associate-route-table --route-table-id
 "$PRIVATE_RT2_ID" --subnet-id "$PRIVATE_SUBNET2_ID")
check_command "Failed to associate private subnet 2 with route table"
PRIVATE_RT2_ASSOC_ID=$(echo "$PRIVATE_RT2_ASSOC_RESULT" | jq -r '.AssociationId')

echo "Route table associations created with IDs:"
echo "Public Subnet 1 Association: $PUBLIC_RT_ASSOC1_ID"
echo "Public Subnet 2 Association: $PUBLIC_RT_ASSOC2_ID"
echo "Private Subnet 1 Association: $PRIVATE_RT1_ASSOC_ID"
echo "Private Subnet 2 Association: $PRIVATE_RT2_ASSOC_ID"

# Create NAT Gateways
echo "Creating NAT Gateways..."

# Allocate Elastic IPs for NAT Gateways
echo "Allocating Elastic IPs for NAT Gateways..."
EIP1_RESULT=$(aws ec2 allocate-address --domain vpc --tag-specifications
 "ResourceType=elastic-ip,Tags=[{Key=Name,Value=NAT1-EIP-$RANDOM_ID}]")
check_command "Failed to allocate Elastic IP 1"
EIP1_ALLOC_ID=$(echo "$EIP1_RESULT" | jq -r '.AllocationId')

EIP2_RESULT=$(aws ec2 allocate-address --domain vpc --tag-specifications
 "ResourceType=elastic-ip,Tags=[{Key=Name,Value=NAT2-EIP-$RANDOM_ID}]")
check_command "Failed to allocate Elastic IP 2"
EIP2_ALLOC_ID=$(echo "$EIP2_RESULT" | jq -r '.AllocationId')

echo "Elastic IPs allocated with IDs:"
echo "EIP 1 Allocation ID: $EIP1_ALLOC_ID"
echo "EIP 2 Allocation ID: $EIP2_ALLOC_ID"

# Create NAT Gateways
```

```
echo "Creating NAT Gateway in public subnet 1..."
NAT_GW1_RESULT=$(aws ec2 create-nat-gateway --subnet-id
 "$PUBLIC_SUBNET1_ID" --allocation-id "$EIP1_ALLOC_ID" --tag-specifications
 "ResourceType=natgateway,Tags=[{Key=Name,Value=NAT-Gateway1-$RANDOM_ID}]")
check_command "Failed to create NAT Gateway 1"
NAT_GW1_ID=$(echo "$NAT_GW1_RESULT" | jq -r '.NatGateway.NatGatewayId')

echo "Creating NAT Gateway in public subnet 2..."
NAT_GW2_RESULT=$(aws ec2 create-nat-gateway --subnet-id
 "$PUBLIC_SUBNET2_ID" --allocation-id "$EIP2_ALLOC_ID" --tag-specifications
 "ResourceType=natgateway,Tags=[{Key=Name,Value=NAT-Gateway2-$RANDOM_ID}]")
check_command "Failed to create NAT Gateway 2"
NAT_GW2_ID=$(echo "$NAT_GW2_RESULT" | jq -r '.NatGateway.NatGatewayId')

echo "NAT Gateways created with IDs:"
echo "NAT Gateway 1: $NAT_GW1_ID"
echo "NAT Gateway 2: $NAT_GW2_ID"

# Wait for NAT Gateways to be available
echo "Waiting for NAT Gateways to be available..."
aws ec2 wait nat-gateway-available --nat-gateway-ids "$NAT_GW1_ID"
check_command "NAT Gateway 1 did not become available"
aws ec2 wait nat-gateway-available --nat-gateway-ids "$NAT_GW2_ID"
check_command "NAT Gateway 2 did not become available"
echo "NAT Gateways are now available"

# Add routes to NAT Gateways in private route tables
echo "Adding routes to NAT Gateways in private route tables..."
aws ec2 create-route --route-table-id "$PRIVATE_RT1_ID" --destination-cidr-block
 0.0.0.0/0 --nat-gateway-id "$NAT_GW1_ID"
check_command "Failed to add route to NAT Gateway 1"

aws ec2 create-route --route-table-id "$PRIVATE_RT2_ID" --destination-cidr-block
 0.0.0.0/0 --nat-gateway-id "$NAT_GW2_ID"
check_command "Failed to add route to NAT Gateway 2"

# Create VPC Endpoint for S3
echo "Creating VPC Endpoint for S3..."
S3_PREFIX_LIST_ID=$(aws ec2 describe-prefix-lists --filters "Name=prefix-
list-name,Values=com.amazonaws.$(aws configure get region).s3" --query
 'PrefixLists[0].PrefixListId' --output text)
check_command "Failed to get S3 prefix list ID"
```

```
VPC_ENDPOINT_RESULT=$(aws ec2 create-vpc-endpoint --vpc-id "$VPC_ID" --
service-name "com.amazonaws.$(aws configure get region).s3" --route-table-ids
 "$PRIVATE_RT1_ID" "$PRIVATE_RT2_ID" --tag-specifications "ResourceType=vpc-
endpoint,Tags=[{Key=Name,Value=S3-Endpoint-$RANDOM_ID}]")
check_command "Failed to create VPC endpoint for S3"
VPC_ENDPOINT_ID=$(echo "$VPC_ENDPOINT_RESULT" | jq -r '.VpcEndpoint.VpcEndpointId')
echo "VPC Endpoint created with ID: $VPC_ENDPOINT_ID"

# Create security groups
echo "Creating security groups..."
LB_SG_RESULT=$(aws ec2 create-security-group --group-name "LoadBalancerSG-
$RANDOM_ID" --description "Security group for the load balancer"
 --vpc-id "$VPC_ID" --tag-specifications "ResourceType=security-
group,Tags=[{Key=Name,Value=LoadBalancerSG-$RANDOM_ID}]")
check_command "Failed to create load balancer security group"
LB_SG_ID=$(echo "$LB_SG_RESULT" | jq -r '.GroupId')

# Allow inbound HTTP traffic from anywhere to the load balancer
aws ec2 authorize-security-group-ingress --group-id "$LB_SG_ID" --protocol tcp --
port 80 --cidr 0.0.0.0/0
check_command "Failed to authorize ingress to load balancer security group"

APP_SG_RESULT=$(aws ec2 create-security-group --group-name "AppServerSG-$RANDOM_ID"
 --description "Security group for the application servers" --vpc-id "$VPC_ID" --
tag-specifications "ResourceType=security-group,Tags=[{Key=Name,Value=AppServerSG-
$RANDOM_ID}]")
check_command "Failed to create application server security group"
APP_SG_ID=$(echo "$APP_SG_RESULT" | jq -r '.GroupId')

# Allow inbound HTTP traffic from the load balancer security group to the
 application servers
aws ec2 authorize-security-group-ingress --group-id "$APP_SG_ID" --protocol tcp --
port 80 --source-group "$LB_SG_ID"
check_command "Failed to authorize ingress to application server security group"

echo "Security groups created with IDs:"
echo "Load Balancer Security Group: $LB_SG_ID"
echo "Application Server Security Group: $APP_SG_ID"

# Create a launch template
echo "Creating launch template..."

# Create user data script with IMDSv2 support
cat > user-data.sh << 'EOF'
```

```
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd

# Use IMDSv2 with session token
TOKEN=$(curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600")
AZ=$(curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/latest/
meta-data/placement/availability-zone)
HOSTNAME=$(hostname -f)

echo "<h1>Hello from $HOSTNAME in $AZ</h1>" > /var/www/html/index.html
EOF

# Encode user data
USER_DATA=$(base64 -w 0 user-data.sh)

# Get latest Amazon Linux 2 AMI
echo "Getting latest Amazon Linux 2 AMI..."
AMI_ID=$(aws ec2 describe-images --owners amazon --filters "Name=name,Values=amzn2-
ami-hvm-*-x86_64-gp2" "Name=state,Values=available" --query 'sort_by(Images,
 &CreationDate)[-1].ImageId' --output text)
check_command "Failed to get latest Amazon Linux 2 AMI"
echo "Using AMI: $AMI_ID"

# Create launch template with IMDSv2 required
LAUNCH_TEMPLATE_NAME="AppServerTemplate-$RANDOM_ID"
echo "Creating launch template: $LAUNCH_TEMPLATE_NAME"

aws ec2 create-launch-template \
  --launch-template-name "$LAUNCH_TEMPLATE_NAME" \
  --version-description "Initial version" \
  --tag-specifications "ResourceType=launch-template,Tags=[{Key=Name,Value=
$LAUNCH_TEMPLATE_NAME}]" \
  --launch-template-data "{
    \"NetworkInterfaces\": [{
      \"DeviceIndex\": 0,
      \"Groups\": [\"$APP_SG_ID\"],
      \"DeleteOnTermination\": true
    }],
    \"ImageId\": \"$AMI_ID\",
    \"InstanceType\": \"t3.micro\",
```

```
    \"UserData\": \"$USER_DATA\",
    \"MetadataOptions\": {
      \"HttpTokens\": \"required\",
      \"HttpEndpoint\": \"enabled\"
    },
    \"TagSpecifications\": [{
      \"ResourceType\": \"instance\",
      \"Tags\": [{
        \"Key\": \"Name\",
        \"Value\": \"AppServer-$RANDOM_ID\"
      }]
    }]
  }"
check_command "Failed to create launch template"

# Create target group
echo "Creating target group..."
TARGET_GROUP_NAME="AppTargetGroup-$RANDOM_ID"
TARGET_GROUP_RESULT=$(aws elbv2 create-target-group \
  --name "$TARGET_GROUP_NAME" \
  --protocol HTTP \
  --port 80 \
  --vpc-id "$VPC_ID" \
  --target-type instance \
  --health-check-protocol HTTP \
  --health-check-path "/" \
  --health-check-port traffic-port)
check_command "Failed to create target group"
TARGET_GROUP_ARN=$(echo "$TARGET_GROUP_RESULT" | jq -r
 '.TargetGroups[0].TargetGroupArn')
echo "Target group created with ARN: $TARGET_GROUP_ARN"

# Create load balancer
echo "Creating load balancer..."
LB_NAME="AppLoadBalancer-$RANDOM_ID"
LB_RESULT=$(aws elbv2 create-load-balancer \
  --name "$LB_NAME" \
  --subnets "$PUBLIC_SUBNET1_ID" "$PUBLIC_SUBNET2_ID" \
  --security-groups "$LB_SG_ID" \
  --tags "Key=Name,Value=$LB_NAME")
check_command "Failed to create load balancer"
LB_ARN=$(echo "$LB_RESULT" | jq -r '.LoadBalancers[0].LoadBalancerArn')
echo "Load balancer created with ARN: $LB_ARN"
```

```
# Wait for load balancer to be active
echo "Waiting for load balancer to be active..."
aws elbv2 wait load-balancer-available --load-balancer-arns "$LB_ARN"
check_command "Load balancer did not become available"

# Create listener
echo "Creating listener..."
LISTENER_RESULT=$(aws elbv2 create-listener \
  --load-balancer-arn "$LB_ARN" \
  --protocol HTTP \
  --port 80 \
  --default-actions "Type=forward,TargetGroupArn=$TARGET_GROUP_ARN")
check_command "Failed to create listener"
LISTENER_ARN=$(echo "$LISTENER_RESULT" | jq -r '.Listeners[0].ListenerArn')
echo "Listener created with ARN: $LISTENER_ARN"

# Create Auto Scaling group
echo "Creating Auto Scaling group..."
ASG_NAME="AppAutoScalingGroup-$RANDOM_ID"
aws autoscaling create-auto-scaling-group \
  --auto-scaling-group-name "$ASG_NAME" \
  --launch-template "LaunchTemplateName=$LAUNCH_TEMPLATE_NAME,Version=\$Latest" \
  --min-size 2 \
  --max-size 4 \
  --desired-capacity 2 \
  --vpc-zone-identifier "$PRIVATE_SUBNET1_ID,$PRIVATE_SUBNET2_ID" \
  --target-group-arns "$TARGET_GROUP_ARN" \
  --health-check-type ELB \
  --health-check-grace-period 300 \
  --tags "Key=Name,Value=AppServer-$RANDOM_ID,PropagateAtLaunch=true"
check_command "Failed to create Auto Scaling group"
echo "Auto Scaling group created with name: $ASG_NAME"

# Get load balancer DNS name
LB_DNS_NAME=$(aws elbv2 describe-load-balancers --load-balancer-arns "$LB_ARN" --
query 'LoadBalancers[0].DNSName' --output text)
check_command "Failed to get load balancer DNS name"

echo ""
echo "========================================="
echo "DEPLOYMENT COMPLETE"
echo "========================================="
echo "VPC ID: $VPC_ID"
echo "Public Subnet 1: $PUBLIC_SUBNET1_ID (AZ: $AZ1)"
```

```
echo "Private Subnet 1: $PRIVATE_SUBNET1_ID (AZ: $AZ1)"
echo "Public Subnet 2: $PUBLIC_SUBNET2_ID (AZ: $AZ2)"
echo "Private Subnet 2: $PRIVATE_SUBNET2_ID (AZ: $AZ2)"
echo "NAT Gateway 1: $NAT_GW1_ID"
echo "NAT Gateway 2: $NAT_GW2_ID"
echo "Load Balancer: $LB_NAME"
echo "Auto Scaling Group: $ASG_NAME"
echo ""
echo "Your application will be available at: http://$LB_DNS_NAME"
echo "It may take a few minutes for the instances to launch and pass health checks."
echo ""

# Add health check monitoring
echo "=========================================="
echo "MONITORING INSTANCE HEALTH AND LOAD BALANCER"
echo "=========================================="
echo "Waiting for instances to launch and pass health checks..."
echo "This may take 3-5 minutes. Checking every 30 seconds..."

# Monitor instance health and load balancer accessibility
MAX_ATTEMPTS=10
ATTEMPT=1
HEALTHY_INSTANCES=0

while [ $ATTEMPT -le $MAX_ATTEMPTS ] && [ $HEALTHY_INSTANCES -lt 2 ]; do
  echo "Check attempt $ATTEMPT of $MAX_ATTEMPTS..."

  # Check Auto Scaling group instances
  echo "Checking Auto Scaling group instances..."
  ASG_INSTANCES=$(aws autoscaling describe-auto-scaling-groups --auto-
scaling-group-names "$ASG_NAME" --query 'AutoScalingGroups[0].Instances[*].
[InstanceId,HealthStatus]' --output json)
  echo "ASG Instances status:"
  echo "$ASG_INSTANCES" | jq -r '.[] | "Instance: \(.[0]), Health: \(.[1])"'

  # Check target group health
  echo "Checking target group health..."
  TARGET_HEALTH=$(aws elbv2 describe-target-health --target-group-arn
 "$TARGET_GROUP_ARN" --output json)
  echo "Target health status:"
  echo "$TARGET_HEALTH" | jq -r '.TargetHealthDescriptions[] | "Instance:
 \(.Target.Id), State: \(.TargetHealth.State), Reason: \(.TargetHealth.Reason // "N/
A"), Description: \(.TargetHealth.Description // "N/A")"'
```

```
 # Count healthy instances
 HEALTHY_INSTANCES=$(echo "$TARGET_HEALTH" | jq -r '[.TargetHealthDescriptions[] |
select(.TargetHealth.State=="healthy")] | length')
 echo "Number of healthy instances: $HEALTHY_INSTANCES of 2 expected"

 # Check if we have healthy instances
 if [ $HEALTHY_INSTANCES -ge 2 ]; then
   echo "All instances are healthy!"

   # Test load balancer accessibility
   echo "Testing load balancer accessibility..."
   HTTP_STATUS=$(curl -s -o /dev/null -w "%{http_code}" "http://$LB_DNS_NAME")

   if [ "$HTTP_STATUS" = "200" ]; then
     echo "Load balancer is accessible! HTTP Status: $HTTP_STATUS"
     echo "You can access your application at: http://$LB_DNS_NAME"

     # Try to get the content to verify IMDSv2 is working
     echo "Fetching content to verify IMDSv2 functionality..."
     CONTENT=$(curl -s "http://$LB_DNS_NAME")
     echo "Response from server:"
     echo "$CONTENT"

     # Check if the content contains the expected pattern
     if [[ "$CONTENT" == *"Hello from"* && "$CONTENT" == *"in"* ]]; then
       echo "IMDSv2 is working correctly! The instance was able to access metadata
using the token-based approach."
     else
       echo "Warning: Content doesn't match expected pattern. IMDSv2 functionality
could not be verified."
     fi

     break
   else
     echo "Load balancer returned HTTP status: $HTTP_STATUS"
     echo "Will try again in 30 seconds..."
   fi
 else
   echo "Waiting for instances to become healthy..."
   echo "Will check again in 30 seconds..."
 fi

 ATTEMPT=$((ATTEMPT+1))
```

```
  if [ $ATTEMPT -le $MAX_ATTEMPTS ]; then
    sleep 30
  fi
done

if [ $HEALTHY_INSTANCES -lt 2 ]; then
  echo "Warning: Not all instances are healthy after maximum attempts."
  echo "You may need to wait longer or check for configuration issues."
fi

echo "To test your application, run:"
echo "curl http://$LB_DNS_NAME"
echo ""
echo "========================================="
echo "CLEANUP CONFIRMATION"
echo "========================================="
echo "Do you want to clean up all created resources? (y/n): "
read -r CLEANUP_CHOICE

if [[ "$CLEANUP_CHOICE" =~ ^[Yy]$ ]]; then
  cleanup_resources
  echo "All resources have been deleted."
else
  echo "Resources will not be deleted. You can manually delete them later."
  echo "To delete resources, run this script again and choose to clean up."
fi
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - AllocateAddress
  - AssociateRouteTable
  - AttachInternetGateway
  - AuthorizeSecurityGroupIngress
  - CreateInternetGateway
  - CreateLaunchTemplate
  - CreateNatGateway
  - CreateRoute
  - CreateRouteTable

- CreateSecurityGroup
- CreateSubnet
- CreateVpc
- CreateVpcEndpoint
- DeleteAutoScalingGroup
- DeleteInternetGateway
- DeleteLaunchTemplate
- DeleteLoadBalancer
- DeleteNatGateway
- DeleteRouteTable
- DeleteSecurityGroup
- DeleteSubnet
- DeleteTargetGroup
- DeleteVpc
- DeleteVpcEndpoints
- DescribeAvailabilityZones
- DescribeImages
- DescribePrefixLists
- DetachInternetGateway
- ReleaseAddress

Introducción a Amazon VPC

En el siguiente ejemplo de código, se muestra cómo:

- Configure su cuenta
- Crear y configurar una VPC
- Configurar la red
- Configuración de la seguridad
- Implementación de recursos
- Prueba y verificación
- Eliminar recursos

- Consideración de las implicaciones de producción
- Consideración de las implicaciones de seguridad

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Encuentre el ejemplo completo y obtenga información sobre cómo configurarlo y ejecutarlo en el repositorio de Tutoriales para desarrolladores de ejemplo.

```
#!/bin/bash

# VPC Creation Script
# This script creates a VPC with public and private subnets, internet gateway, NAT
 gateway, and security groups

# Set up logging
LOG_FILE="vpc_creation.log"
exec > >(tee -a "$LOG_FILE") 2>&1

# Function to handle errors
handle_error() {
  echo "ERROR: $1"
  echo "Resources created before error:"
  for resource in "${CREATED_RESOURCES[@]}"
  do
    echo "- $resource"
  done

  echo "Attempting to clean up resources..."
  cleanup_resources
  exit 1
}

# Function to clean up resources
cleanup_resources() {
  echo "Cleaning up resources in reverse order..."

  # Reverse the array to delete in reverse order of creation
```

```
 for ((i=${#CREATED_RESOURCES[@]}-1; i>=0; i--))
 do
   resource="${CREATED_RESOURCES[$i]}"
   resource_type=$(echo "$resource" | cut -d':' -f1)
   resource_id=$(echo "$resource" | cut -d':' -f2)

   case "$resource_type" in
     "INSTANCE")
       echo "Terminating EC2 instance: $resource_id"
       aws ec2 terminate-instances --instance-ids "$resource_id" || echo "Failed to
terminate instance: $resource_id"
       # Wait for instance to terminate
       echo "Waiting for instance to terminate..."
       aws ec2 wait instance-terminated --instance-ids "$resource_id" || echo
"Failed to wait for instance termination: $resource_id"
       ;;
     "KEY_PAIR")
       echo "Deleting key pair: $resource_id"
       aws ec2 delete-key-pair --key-name "$resource_id" || echo "Failed to delete
key pair: $resource_id"
       # Remove the .pem file if it exists
       if [ -f "${resource_id}.pem" ]; then
         rm -f "${resource_id}.pem"
       fi
       ;;
     "NAT_GATEWAY")
       echo "Deleting NAT Gateway: $resource_id"
       aws ec2 delete-nat-gateway --nat-gateway-id "$resource_id" || echo "Failed
to delete NAT Gateway: $resource_id"
       # NAT Gateway deletion takes time, wait for it to complete
       echo "Waiting for NAT Gateway to be deleted..."
       aws ec2 wait nat-gateway-deleted --nat-gateway-ids "$resource_id" || echo
"Failed to wait for NAT Gateway deletion: $resource_id"
       ;;
     "EIP")
       echo "Releasing Elastic IP: $resource_id"
       aws ec2 release-address --allocation-id "$resource_id" || echo "Failed to
release Elastic IP: $resource_id"
       ;;
     "ROUTE_TABLE_ASSOCIATION")
       echo "Disassociating Route Table: $resource_id"
       aws ec2 disassociate-route-table --association-id "$resource_id" || echo
"Failed to disassociate Route Table: $resource_id"
       ;;
```

```
      "ROUTE_TABLE")
        echo "Deleting Route Table: $resource_id"
        aws ec2 delete-route-table --route-table-id "$resource_id" || echo "Failed
 to delete Route Table: $resource_id"
        ;;
      "INTERNET_GATEWAY")
        echo "Detaching Internet Gateway: $resource_id from VPC: $VPC_ID"
        aws ec2 detach-internet-gateway --internet-gateway-id "$resource_id" --vpc-
id "$VPC_ID" || echo "Failed to detach Internet Gateway: $resource_id"
        echo "Deleting Internet Gateway: $resource_id"
        aws ec2 delete-internet-gateway --internet-gateway-id "$resource_id" || echo
 "Failed to delete Internet Gateway: $resource_id"
        ;;
      "SECURITY_GROUP")
        echo "Deleting Security Group: $resource_id"
        aws ec2 delete-security-group --group-id "$resource_id" || echo "Failed to
 delete Security Group: $resource_id"
        ;;
      "SUBNET")
        echo "Deleting Subnet: $resource_id"
        aws ec2 delete-subnet --subnet-id "$resource_id" || echo "Failed to delete
 Subnet: $resource_id"
        ;;
      "VPC")
        echo "Deleting VPC: $resource_id"
        aws ec2 delete-vpc --vpc-id "$resource_id" || echo "Failed to delete VPC:
 $resource_id"
        ;;
    esac
  done
}

# Initialize array to track created resources
CREATED_RESOURCES=()

echo "Starting VPC creation script at $(date)"

# Verify AWS CLI configuration
echo "Verifying AWS CLI configuration..."
aws configure list || handle_error "AWS CLI is not properly configured"

# Verify identity and permissions
echo "Verifying identity and permissions..."
if ! aws sts get-caller-identity; then
```

```
  echo "ERROR: Unable to verify AWS identity. This could be due to:"
  echo "  - Expired credentials"
  echo "  - Missing or invalid AWS credentials"
  echo "  - Insufficient permissions"
  echo ""
  echo "Please run 'aws configure' to update your credentials or check your IAM
 permissions."
  exit 1
fi

# Create VPC
echo "Creating VPC with CIDR block 10.0.0.0/16..."
VPC_ID=$(aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications
 'ResourceType=vpc,Tags=[{Key=Name,Value=MyVPC}]' --query 'Vpc.VpcId' --output text)

if [ -z "$VPC_ID" ]; then
  handle_error "Failed to create VPC"
fi

CREATED_RESOURCES+=("VPC:$VPC_ID")
echo "VPC created with ID: $VPC_ID"

# Enable DNS support and hostnames
echo "Enabling DNS support and hostnames for VPC..."
aws ec2 modify-vpc-attribute --vpc-id "$VPC_ID" --enable-dns-support || handle_error
 "Failed to enable DNS support"
aws ec2 modify-vpc-attribute --vpc-id "$VPC_ID" --enable-dns-hostnames ||
 handle_error "Failed to enable DNS hostnames"

# Get available Availability Zones
echo "Getting available Availability Zones..."
AZ1=$(aws ec2 describe-availability-zones --query 'AvailabilityZones[0].ZoneName' --
output text)
AZ2=$(aws ec2 describe-availability-zones --query 'AvailabilityZones[1].ZoneName' --
output text)

if [ -z "$AZ1" ] || [ -z "$AZ2" ]; then
  handle_error "Failed to get Availability Zones"
fi

echo "Using Availability Zones: $AZ1 and $AZ2"

# Create public subnets
echo "Creating public subnet in $AZ1..."
```

```
PUBLIC_SUBNET_AZ1=$(aws ec2 create-subnet \
  --vpc-id "$VPC_ID" \
  --cidr-block 10.0.0.0/24 \
  --availability-zone "$AZ1" \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Public-Subnet-
AZ1}]' \
  --query 'Subnet.SubnetId' \
  --output text)

if [ -z "$PUBLIC_SUBNET_AZ1" ]; then
  handle_error "Failed to create public subnet in AZ1"
fi

CREATED_RESOURCES+=("SUBNET:$PUBLIC_SUBNET_AZ1")
echo "Public subnet created in $AZ1 with ID: $PUBLIC_SUBNET_AZ1"

echo "Creating public subnet in $AZ2..."
PUBLIC_SUBNET_AZ2=$(aws ec2 create-subnet \
  --vpc-id "$VPC_ID" \
  --cidr-block 10.0.1.0/24 \
  --availability-zone "$AZ2" \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Public-Subnet-
AZ2}]' \
  --query 'Subnet.SubnetId' \
  --output text)

if [ -z "$PUBLIC_SUBNET_AZ2" ]; then
  handle_error "Failed to create public subnet in AZ2"
fi

CREATED_RESOURCES+=("SUBNET:$PUBLIC_SUBNET_AZ2")
echo "Public subnet created in $AZ2 with ID: $PUBLIC_SUBNET_AZ2"

# Create private subnets
echo "Creating private subnet in $AZ1..."
PRIVATE_SUBNET_AZ1=$(aws ec2 create-subnet \
  --vpc-id "$VPC_ID" \
  --cidr-block 10.0.2.0/24 \
  --availability-zone "$AZ1" \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Private-Subnet-
AZ1}]' \
  --query 'Subnet.SubnetId' \
  --output text)
```

```
if [ -z "$PRIVATE_SUBNET_AZ1" ]; then
  handle_error "Failed to create private subnet in AZ1"
fi

CREATED_RESOURCES+=("SUBNET:$PRIVATE_SUBNET_AZ1")
echo "Private subnet created in $AZ1 with ID: $PRIVATE_SUBNET_AZ1"

echo "Creating private subnet in $AZ2..."
PRIVATE_SUBNET_AZ2=$(aws ec2 create-subnet \
  --vpc-id "$VPC_ID" \
  --cidr-block 10.0.3.0/24 \
  --availability-zone "$AZ2" \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Private-Subnet-
AZ2}]' \
  --query 'Subnet.SubnetId' \
  --output text)

if [ -z "$PRIVATE_SUBNET_AZ2" ]; then
  handle_error "Failed to create private subnet in AZ2"
fi

CREATED_RESOURCES+=("SUBNET:$PRIVATE_SUBNET_AZ2")
echo "Private subnet created in $AZ2 with ID: $PRIVATE_SUBNET_AZ2"

# Create Internet Gateway
echo "Creating Internet Gateway..."
IGW_ID=$(aws ec2 create-internet-gateway \
  --tag-specifications 'ResourceType=internet-gateway,Tags=[{Key=Name,Value=MyIGW}]'
 \
  --query 'InternetGateway.InternetGatewayId' \
  --output text)

if [ -z "$IGW_ID" ]; then
  handle_error "Failed to create Internet Gateway"
fi

CREATED_RESOURCES+=("INTERNET_GATEWAY:$IGW_ID")
echo "Internet Gateway created with ID: $IGW_ID"

# Attach Internet Gateway to VPC
echo "Attaching Internet Gateway to VPC..."
aws ec2 attach-internet-gateway --internet-gateway-id "$IGW_ID" --vpc-id "$VPC_ID"
 || handle_error "Failed to attach Internet Gateway to VPC"
```

```
# Create public route table
echo "Creating public route table..."
PUBLIC_RT=$(aws ec2 create-route-table \
  --vpc-id "$VPC_ID" \
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Public-RT}]'
 \
  --query 'RouteTable.RouteTableId' \
  --output text)

if [ -z "$PUBLIC_RT" ]; then
  handle_error "Failed to create public route table"
fi

CREATED_RESOURCES+=("ROUTE_TABLE:$PUBLIC_RT")
echo "Public route table created with ID: $PUBLIC_RT"

# Add route to Internet Gateway
echo "Adding route to Internet Gateway in public route table..."
aws ec2 create-route --route-table-id "$PUBLIC_RT" --destination-cidr-block
 0.0.0.0/0 --gateway-id "$IGW_ID" || handle_error "Failed to add route to Internet
 Gateway"

# Associate public subnets with public route table
echo "Associating public subnet in $AZ1 with public route table..."
PUBLIC_RT_ASSOC_1=$(aws ec2 associate-route-table --route-table-id "$PUBLIC_RT" --
subnet-id "$PUBLIC_SUBNET_AZ1" --query 'AssociationId' --output text)

if [ -z "$PUBLIC_RT_ASSOC_1" ]; then
  handle_error "Failed to associate public subnet in AZ1 with public route table"
fi

CREATED_RESOURCES+=("ROUTE_TABLE_ASSOCIATION:$PUBLIC_RT_ASSOC_1")

echo "Associating public subnet in $AZ2 with public route table..."
PUBLIC_RT_ASSOC_2=$(aws ec2 associate-route-table --route-table-id "$PUBLIC_RT" --
subnet-id "$PUBLIC_SUBNET_AZ2" --query 'AssociationId' --output text)

if [ -z "$PUBLIC_RT_ASSOC_2" ]; then
  handle_error "Failed to associate public subnet in AZ2 with public route table"
fi

CREATED_RESOURCES+=("ROUTE_TABLE_ASSOCIATION:$PUBLIC_RT_ASSOC_2")

# Create private route table
```

```
echo "Creating private route table..."
PRIVATE_RT=$(aws ec2 create-route-table \
  --vpc-id "$VPC_ID" \
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Private-RT}]'
 \
  --query 'RouteTable.RouteTableId' \
  --output text)

if [ -z "$PRIVATE_RT" ]; then
  handle_error "Failed to create private route table"
fi

CREATED_RESOURCES+=("ROUTE_TABLE:$PRIVATE_RT")
echo "Private route table created with ID: $PRIVATE_RT"

# Associate private subnets with private route table
echo "Associating private subnet in $AZ1 with private route table..."
PRIVATE_RT_ASSOC_1=$(aws ec2 associate-route-table --route-table-id "$PRIVATE_RT" --
subnet-id "$PRIVATE_SUBNET_AZ1" --query 'AssociationId' --output text)

if [ -z "$PRIVATE_RT_ASSOC_1" ]; then
  handle_error "Failed to associate private subnet in AZ1 with private route table"
fi

CREATED_RESOURCES+=("ROUTE_TABLE_ASSOCIATION:$PRIVATE_RT_ASSOC_1")

echo "Associating private subnet in $AZ2 with private route table..."
PRIVATE_RT_ASSOC_2=$(aws ec2 associate-route-table --route-table-id "$PRIVATE_RT" --
subnet-id "$PRIVATE_SUBNET_AZ2" --query 'AssociationId' --output text)

if [ -z "$PRIVATE_RT_ASSOC_2" ]; then
  handle_error "Failed to associate private subnet in AZ2 with private route table"
fi

CREATED_RESOURCES+=("ROUTE_TABLE_ASSOCIATION:$PRIVATE_RT_ASSOC_2")

# Allocate Elastic IP for NAT Gateway
echo "Allocating Elastic IP for NAT Gateway..."
EIP_ALLOC=$(aws ec2 allocate-address --domain vpc --query 'AllocationId' --output
 text)

if [ -z "$EIP_ALLOC" ]; then
  handle_error "Failed to allocate Elastic IP"
fi
```

```
CREATED_RESOURCES+=("EIP:$EIP_ALLOC")
echo "Elastic IP allocated with ID: $EIP_ALLOC"

# Create NAT Gateway
echo "Creating NAT Gateway in public subnet in $AZ1..."
NAT_GW=$(aws ec2 create-nat-gateway \
  --subnet-id "$PUBLIC_SUBNET_AZ1" \
  --allocation-id "$EIP_ALLOC" \
  --tag-specifications
 'ResourceType=natgateway,Tags=[{Key=Name,Value=MyNATGateway}]' \
  --query 'NatGateway.NatGatewayId' \
  --output text)

if [ -z "$NAT_GW" ]; then
  handle_error "Failed to create NAT Gateway"
fi

CREATED_RESOURCES+=("NAT_GATEWAY:$NAT_GW")
echo "NAT Gateway created with ID: $NAT_GW"

# Wait for NAT Gateway to be available
echo "Waiting for NAT Gateway to be available..."
aws ec2 wait nat-gateway-available --nat-gateway-ids "$NAT_GW" || handle_error "NAT
 Gateway did not become available"

# Add route to NAT Gateway in private route table
echo "Adding route to NAT Gateway in private route table..."
aws ec2 create-route --route-table-id "$PRIVATE_RT" --destination-cidr-block
 0.0.0.0/0 --nat-gateway-id "$NAT_GW" || handle_error "Failed to add route to NAT
 Gateway"

# Enable auto-assign public IP for instances in public subnets
echo "Enabling auto-assign public IP for instances in public subnet in $AZ1..."
aws ec2 modify-subnet-attribute --subnet-id "$PUBLIC_SUBNET_AZ1" --map-public-ip-on-
launch || handle_error "Failed to enable auto-assign public IP for public subnet in
 AZ1"

echo "Enabling auto-assign public IP for instances in public subnet in $AZ2..."
aws ec2 modify-subnet-attribute --subnet-id "$PUBLIC_SUBNET_AZ2" --map-public-ip-on-
launch || handle_error "Failed to enable auto-assign public IP for public subnet in
 AZ2"

# Create security group for web servers
```

```
echo "Creating security group for web servers..."
WEB_SG=$(aws ec2 create-security-group \
  --group-name "WebServerSG-$(date +%s)" \
  --description "Security group for web servers" \
  --vpc-id "$VPC_ID" \
  --query 'GroupId' \
  --output text)

if [ -z "$WEB_SG" ]; then
  handle_error "Failed to create security group for web servers"
fi

CREATED_RESOURCES+=("SECURITY_GROUP:$WEB_SG")
echo "Security group for web servers created with ID: $WEB_SG"

# Allow HTTP and HTTPS traffic
echo "Allowing HTTP traffic to web servers security group..."
aws ec2 authorize-security-group-ingress --group-id "$WEB_SG" --protocol tcp --port
 80 --cidr 0.0.0.0/0 || handle_error "Failed to allow HTTP traffic"

echo "Allowing HTTPS traffic to web servers security group..."
aws ec2 authorize-security-group-ingress --group-id "$WEB_SG" --protocol tcp --port
 443 --cidr 0.0.0.0/0 || handle_error "Failed to allow HTTPS traffic"

# Note: In a production environment, you should restrict the source IP ranges for
 security
echo "NOTE: In a production environment, you should restrict the source IP ranges
 for HTTP and HTTPS traffic"

# Create security group for database servers
echo "Creating security group for database servers..."
DB_SG=$(aws ec2 create-security-group \
  --group-name "DBServerSG-$(date +%s)" \
  --description "Security group for database servers" \
  --vpc-id "$VPC_ID" \
  --query 'GroupId' \
  --output text)

if [ -z "$DB_SG" ]; then
  handle_error "Failed to create security group for database servers"
fi

CREATED_RESOURCES+=("SECURITY_GROUP:$DB_SG")
echo "Security group for database servers created with ID: $DB_SG"
```

```
# Allow MySQL/Aurora traffic from web servers only
echo "Allowing MySQL/Aurora traffic from web servers to database servers..."
aws ec2 authorize-security-group-ingress --group-id "$DB_SG" --protocol tcp --
port 3306 --source-group "$WEB_SG" || handle_error "Failed to allow MySQL/Aurora
 traffic"

# Verify VPC configuration
echo "Verifying VPC configuration..."
echo "VPC:"
aws ec2 describe-vpcs --vpc-id "$VPC_ID" || handle_error "Failed to describe VPC"

echo "Subnets:"
aws ec2 describe-subnets --filters "Name=vpc-id,Values=$VPC_ID" || handle_error
 "Failed to describe subnets"

echo "Route tables:"
aws ec2 describe-route-tables --filters "Name=vpc-id,Values=$VPC_ID" || handle_error
 "Failed to describe route tables"

echo "Internet gateway:"
aws ec2 describe-internet-gateways --filters "Name=attachment.vpc-id,Values=$VPC_ID"
 || handle_error "Failed to describe Internet Gateway"

echo "NAT gateway:"
aws ec2 describe-nat-gateways --filter "Name=vpc-id,Values=$VPC_ID" || handle_error
 "Failed to describe NAT Gateway"

echo "Security groups:"
aws ec2 describe-security-groups --filters "Name=vpc-id,Values=$VPC_ID" ||
 handle_error "Failed to describe security groups"

echo ""
# Summary of created resources
echo "VPC creation completed successfully!"
echo "Summary of created resources:"
echo "- VPC: $VPC_ID"
echo "- Public Subnet in $AZ1: $PUBLIC_SUBNET_AZ1"
echo "- Public Subnet in $AZ2: $PUBLIC_SUBNET_AZ2"
echo "- Private Subnet in $AZ1: $PRIVATE_SUBNET_AZ1"
echo "- Private Subnet in $AZ2: $PRIVATE_SUBNET_AZ2"
echo "- Internet Gateway: $IGW_ID"
echo "- Public Route Table: $PUBLIC_RT"
echo "- Private Route Table: $PRIVATE_RT"
```

```
echo "- Elastic IP: $EIP_ALLOC"
echo "- NAT Gateway: $NAT_GW"
echo "- Web Servers Security Group: $WEB_SG"
echo "- Database Servers Security Group: $DB_SG"

# Deploy EC2 instances
echo ""
echo "Deploying EC2 instances..."

# Create key pair for SSH access
KEY_NAME="vpc-tutorial-key-$(date +%s)"
echo "Creating key pair $KEY_NAME..."
aws ec2 create-key-pair --key-name "$KEY_NAME" --query 'KeyMaterial' --output text >
 "${KEY_NAME}.pem" || handle_error "Failed to create key pair"
chmod 400 "${KEY_NAME}.pem"
echo "Key pair saved to ${KEY_NAME}.pem"
CREATED_RESOURCES+=("KEY_PAIR:$KEY_NAME")

# Get latest Amazon Linux 2 AMI
echo "Getting latest Amazon Linux 2 AMI..."
AMI_ID=$(aws ec2 describe-images --owners amazon \
  --filters "Name=name,Values=amzn2-ami-hvm-*-x86_64-gp2"
 "Name=state,Values=available" \
  --query "sort_by(Images, &CreationDate)[-1].ImageId" --output text) ||
 handle_error "Failed to get AMI"
echo "Using AMI: $AMI_ID"

# Launch web server in public subnet
echo "Launching web server in public subnet..."
WEB_INSTANCE=$(aws ec2 run-instances \
  --image-id "$AMI_ID" \
  --count 1 \
  --instance-type t2.micro \
  --key-name "$KEY_NAME" \
  --security-group-ids "$WEB_SG" \
  --subnet-id "$PUBLIC_SUBNET_AZ1" \
  --associate-public-ip-address \
  --user-data '#!/bin/bash
    yum update -y
    yum install -y httpd
    systemctl start httpd
    systemctl enable httpd
    echo "<h1>Hello from $(hostname -f) in the public subnet</h1>" > /var/www/html/
index.html' \
```

```
  --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=WebServer}]' \
  --query 'Instances[0].InstanceId' \
  --output text) || handle_error "Failed to launch web server"
echo "Web server instance created with ID: $WEB_INSTANCE"
CREATED_RESOURCES+=("INSTANCE:$WEB_INSTANCE")

# Wait for web server to be running
echo "Waiting for web server to be running..."
aws ec2 wait instance-running --instance-ids "$WEB_INSTANCE"

# Get web server public IP
WEB_PUBLIC_IP=$(aws ec2 describe-instances --instance-ids "$WEB_INSTANCE" \
  --query 'Reservations[0].Instances[0].PublicIpAddress' --output text)
echo "Web server public IP: $WEB_PUBLIC_IP"
echo "You can access the web server at: http://$WEB_PUBLIC_IP"

# Launch database server in private subnet
echo "Launching database server in private subnet..."
DB_INSTANCE=$(aws ec2 run-instances \
  --image-id "$AMI_ID" \
  --count 1 \
  --instance-type t2.micro \
  --key-name "$KEY_NAME" \
  --security-group-ids "$DB_SG" \
  --subnet-id "$PRIVATE_SUBNET_AZ1" \
  --user-data '#!/bin/bash
    yum update -y
    yum install -y mariadb-server
    systemctl start mariadb
    systemctl enable mariadb' \
  --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=DBServer}]' \
  --query 'Instances[0].InstanceId' \
  --output text) || handle_error "Failed to launch database server"
echo "Database server instance created with ID: $DB_INSTANCE"
CREATED_RESOURCES+=("INSTANCE:$DB_INSTANCE")

# Wait for database server to be running
echo "Waiting for database server to be running..."
aws ec2 wait instance-running --instance-ids "$DB_INSTANCE"

# Get database server private IP
DB_PRIVATE_IP=$(aws ec2 describe-instances --instance-ids "$DB_INSTANCE" \
  --query 'Reservations[0].Instances[0].PrivateIpAddress' --output text)
echo "Database server private IP: $DB_PRIVATE_IP"
```

```
echo "EC2 instances deployed successfully!"
echo "- Web Server (Public): $WEB_INSTANCE ($WEB_PUBLIC_IP)"
echo "- Database Server (Private): $DB_INSTANCE ($DB_PRIVATE_IP)"
echo ""
echo "Note: To connect to the web server: ssh -i ${KEY_NAME}.pem ec2-user@
$WEB_PUBLIC_IP"
echo "To connect to the database server, you must first connect to the web server,
 then use it as a bastion host."
echo "=========================================="
echo "CLEANUP CONFIRMATION"
echo "=========================================="
echo "Do you want to clean up all created resources? (y/n): "
read -r CLEANUP_CHOICE
if [[ "$CLEANUP_CHOICE" =~ ^[Yy]$ ]]; then
  echo "Cleaning up resources..."
  cleanup_resources
  echo "All resources have been cleaned up."
else
  echo "Resources will not be cleaned up. You can manually clean them up later."
fi

echo "Script completed at $(date)"
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - AllocateAddress
  - AssociateRouteTable
  - AttachInternetGateway
  - AuthorizeSecurityGroupIngress
  - CreateInternetGateway
  - CreateKeyPair
  - CreateNatGateway
  - CreateRoute
  - CreateRouteTable
  - CreateSecurityGroup
  - CreateSubnet

- CreateVpc
- DeleteInternetGateway
- DeleteKeyPair
- DeleteNatGateway
- DeleteRouteTable
- DeleteSecurityGroup
- DeleteSubnet
- DeleteVpc
- DescribeAvailabilityZones
- DescribeImages
- DescribeInstances
- DescribeInternetGateways
- DescribeNatGateways
- DescribeRouteTables
- DescribeSecurityGroups
- DescribeSubnets
- DescribeVpcs
- DetachInternetGateway
- DisassociateRouteTable
- ModifySubnetAttribute
- ModifyVpcAttribute
- ReleaseAddress
- RunInstances
- TerminateInstances

Introducción a la puerta de enlace de tránsito

En el siguiente ejemplo de código, se muestra cómo:

- Creación de una puerta de enlace de tránsito compatible con DNS y con la configuración predeterminada de la tabla de enrutamiento
- Espera para que la puerta de enlace de tránsito esté disponible

- Asociación de dos VPC a la puerta de enlace de tránsito mediante subredes
- Espera para que las conexiones de la VPC estén disponibles
- Agregación de rutas entre las VPC a través de la puerta de enlace de tránsito
- Prueba de la conectividad entre los recursos de la VPC
- Eliminación de los recursos, incluidas las rutas, los enlaces y la puerta de enlace de tránsito

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Encuentre el ejemplo completo y obtenga información sobre cómo configurarlo y ejecutarlo en el repositorio de Tutoriales para desarrolladores de ejemplo.

```
#!/bin/bash

# Amazon VPC Transit Gateway CLI Script
# This script demonstrates how to create a transit gateway and connect two VPCs
# Modified to work with older AWS CLI versions that don't support transit gateway
 wait commands

# Error handling
set -e
LOG_FILE="transit-gateway-tutorial.log"
exec > >(tee -a "$LOG_FILE") 2>&1

# Function to wait for transit gateway to be available
wait_for_tgw() {
  local tgw_id=$1
  echo "Waiting for Transit Gateway $tgw_id to become available..."

  while true; do
    status=$(aws ec2 describe-transit-gateways --transit-gateway-ids "$tgw_id" --
query "TransitGateways[0].State" --output text)
    echo "Current status: $status"

    if [ "$status" = "available" ]; then
      echo "Transit Gateway is now available"
      break
    fi
```

```
    echo "Waiting for transit gateway to become available. Current state: $status"
    sleep 10
  done
}

# Function to wait for transit gateway attachment to be available
wait_for_tgw_attachment() {
  local attachment_id=$1
  echo "Waiting for Transit Gateway Attachment $attachment_id to become
 available..."

  while true; do
    status=$(aws ec2 describe-transit-gateway-vpc-attachments --transit-gateway-
attachment-ids "$attachment_id" --query "TransitGatewayVpcAttachments[0].State" --
output text)
    echo "Current status: $status"

    if [ "$status" = "available" ]; then
      echo "Transit Gateway Attachment is now available"
      break
    fi

    echo "Waiting for transit gateway attachment to become available. Current state:
 $status"
    sleep 10
  done
}

# Function to wait for transit gateway attachment to be deleted
wait_for_tgw_attachment_deleted() {
  local attachment_id=$1
  echo "Waiting for Transit Gateway Attachment $attachment_id to be deleted..."

  while true; do
    # Check if the attachment still exists
    count=$(aws ec2 describe-transit-gateway-vpc-attachments --filters
 "Name=transit-gateway-attachment-id,Values=$attachment_id" --query
 "length(TransitGatewayVpcAttachments)" --output text)

    if [ "$count" = "0" ]; then
      echo "Transit Gateway Attachment has been deleted"
      break
    fi
```

```
    status=$(aws ec2 describe-transit-gateway-vpc-attachments --transit-gateway-
attachment-ids "$attachment_id" --query "TransitGatewayVpcAttachments[0].State" --
output text 2>/dev/null || echo "deleted")

    if [ "$status" = "deleted" ]; then
      echo "Transit Gateway Attachment has been deleted"
      break
    fi

    echo "Waiting for transit gateway attachment to be deleted. Current state:
 $status"
    sleep 10
  done
}

# Function to clean up resources
cleanup() {
  echo "Error occurred. Cleaning up resources..."

  # Delete resources in reverse order
  if [ ! -z "$TGW_ATTACHMENT_1_ID" ]; then
    echo "Deleting Transit Gateway VPC Attachment 1: $TGW_ATTACHMENT_1_ID"
    aws ec2 delete-transit-gateway-vpc-attachment --transit-gateway-attachment-id
 "$TGW_ATTACHMENT_1_ID" || true
    wait_for_tgw_attachment_deleted "$TGW_ATTACHMENT_1_ID" || true
  fi

  if [ ! -z "$TGW_ATTACHMENT_2_ID" ]; then
    echo "Deleting Transit Gateway VPC Attachment 2: $TGW_ATTACHMENT_2_ID"
    aws ec2 delete-transit-gateway-vpc-attachment --transit-gateway-attachment-id
 "$TGW_ATTACHMENT_2_ID" || true
    wait_for_tgw_attachment_deleted "$TGW_ATTACHMENT_2_ID" || true
  fi

  if [ ! -z "$TGW_ID" ]; then
    echo "Deleting Transit Gateway: $TGW_ID"
    aws ec2 delete-transit-gateway --transit-gateway-id "$TGW_ID" || true
  fi

  exit 1
}

# Set up trap for error handling
```

```
trap cleanup ERR

echo "=== Amazon VPC Transit Gateway Tutorial ==="
echo "This script will create a transit gateway and connect two VPCs"
echo ""

# Get a valid availability zone dynamically
echo "Getting available AZ in current region..."
AZ=$(aws ec2 describe-availability-zones --query "AvailabilityZones[0].ZoneName" --
output text)
echo "Using availability zone: $AZ"

# Check if VPCs exist
echo "Checking for existing VPCs..."
VPC1_ID=$(aws ec2 describe-vpcs --filters "Name=tag:Name,Values=VPC1" --query
 "Vpcs[0].VpcId" --output text)
VPC2_ID=$(aws ec2 describe-vpcs --filters "Name=tag:Name,Values=VPC2" --query
 "Vpcs[0].VpcId" --output text)

if [ "$VPC1_ID" == "None" ] || [ -z "$VPC1_ID" ]; then
  echo "Creating VPC1..."
  VPC1_ID=$(aws ec2 create-vpc --cidr-block 10.1.0.0/16 --tag-specifications
 'ResourceType=vpc,Tags=[{Key=Name,Value=VPC1}]' --query Vpc.VpcId --output text)
  echo "Created VPC1: $VPC1_ID"

  # Create a subnet in VPC1
  echo "Creating subnet in VPC1..."
  SUBNET1_ID=$(aws ec2 create-subnet --vpc-id "$VPC1_ID" --cidr-
block 10.1.0.0/24 --availability-zone "$AZ" --tag-specifications
 'ResourceType=subnet,Tags=[{Key=Name,Value=VPC1-Subnet}]' --query Subnet.SubnetId
 --output text)
  echo "Created subnet in VPC1: $SUBNET1_ID"
else
  echo "Using existing VPC1: $VPC1_ID"
  SUBNET1_ID=$(aws ec2 describe-subnets --filters "Name=vpc-id,Values=$VPC1_ID" --
query "Subnets[0].SubnetId" --output text)
  if [ "$SUBNET1_ID" == "None" ] || [ -z "$SUBNET1_ID" ]; then
    echo "Creating subnet in VPC1..."
    SUBNET1_ID=$(aws ec2 create-subnet --vpc-id "$VPC1_ID" --cidr-
block 10.1.0.0/24 --availability-zone "$AZ" --tag-specifications
 'ResourceType=subnet,Tags=[{Key=Name,Value=VPC1-Subnet}]' --query Subnet.SubnetId
 --output text)
    echo "Created subnet in VPC1: $SUBNET1_ID"
  else
```

```
    echo "Using existing subnet in VPC1: $SUBNET1_ID"
  fi
fi

if [ "$VPC2_ID" == "None" ] || [ -z "$VPC2_ID" ]; then
  echo "Creating VPC2..."
  VPC2_ID=$(aws ec2 create-vpc --cidr-block 10.2.0.0/16 --tag-specifications
 'ResourceType=vpc,Tags=[{Key=Name,Value=VPC2}]' --query Vpc.VpcId --output text)
  echo "Created VPC2: $VPC2_ID"

  # Create a subnet in VPC2
  echo "Creating subnet in VPC2..."
  SUBNET2_ID=$(aws ec2 create-subnet --vpc-id "$VPC2_ID" --cidr-
block 10.2.0.0/24 --availability-zone "$AZ" --tag-specifications
 'ResourceType=subnet,Tags=[{Key=Name,Value=VPC2-Subnet}]' --query Subnet.SubnetId
 --output text)
  echo "Created subnet in VPC2: $SUBNET2_ID"
else
  echo "Using existing VPC2: $VPC2_ID"
  SUBNET2_ID=$(aws ec2 describe-subnets --filters "Name=vpc-id,Values=$VPC2_ID" --
query "Subnets[0].SubnetId" --output text)
  if [ "$SUBNET2_ID" == "None" ] || [ -z "$SUBNET2_ID" ]; then
    echo "Creating subnet in VPC2..."
    SUBNET2_ID=$(aws ec2 create-subnet --vpc-id "$VPC2_ID" --cidr-
block 10.2.0.0/24 --availability-zone "$AZ" --tag-specifications
 'ResourceType=subnet,Tags=[{Key=Name,Value=VPC2-Subnet}]' --query Subnet.SubnetId
 --output text)
    echo "Created subnet in VPC2: $SUBNET2_ID"
  else
    echo "Using existing subnet in VPC2: $SUBNET2_ID"
  fi
fi

# Get route tables for each VPC
RTB1_ID=$(aws ec2 describe-route-tables --filters "Name=vpc-id,Values=$VPC1_ID" --
query "RouteTables[0].RouteTableId" --output text)
RTB2_ID=$(aws ec2 describe-route-tables --filters "Name=vpc-id,Values=$VPC2_ID" --
query "RouteTables[0].RouteTableId" --output text)

echo "Route table for VPC1: $RTB1_ID"
echo "Route table for VPC2: $RTB2_ID"

# Step 1: Create the transit gateway
echo "Creating Transit Gateway..."
```

```
TGW_ID=$(aws ec2 create-transit-gateway \
  --description "My Transit Gateway" \
  --options
 AmazonSideAsn=64512,AutoAcceptSharedAttachments=disable,DefaultRouteTableAssociation=enable
 \
  --tag-specifications 'ResourceType=transit-
gateway,Tags=[{Key=Name,Value=MyTransitGateway}]' \
  --query TransitGateway.TransitGatewayId \
  --output text)

echo "Created Transit Gateway: $TGW_ID"

# Wait for the transit gateway to become available
wait_for_tgw "$TGW_ID"

# Step 2: Attach VPCs to the transit gateway
echo "Attaching VPC1 to Transit Gateway..."
TGW_ATTACHMENT_1_ID=$(aws ec2 create-transit-gateway-vpc-attachment \
  --transit-gateway-id "$TGW_ID" \
  --vpc-id "$VPC1_ID" \
  --subnet-ids "$SUBNET1_ID" \
  --tag-specifications 'ResourceType=transit-gateway-
attachment,Tags=[{Key=Name,Value=VPC1-Attachment}]' \
  --query TransitGatewayVpcAttachment.TransitGatewayAttachmentId \
  --output text)

echo "Created Transit Gateway VPC Attachment for VPC1: $TGW_ATTACHMENT_1_ID"

echo "Attaching VPC2 to Transit Gateway..."
TGW_ATTACHMENT_2_ID=$(aws ec2 create-transit-gateway-vpc-attachment \
  --transit-gateway-id "$TGW_ID" \
  --vpc-id "$VPC2_ID" \
  --subnet-ids "$SUBNET2_ID" \
  --tag-specifications 'ResourceType=transit-gateway-
attachment,Tags=[{Key=Name,Value=VPC2-Attachment}]' \
  --query TransitGatewayVpcAttachment.TransitGatewayAttachmentId \
  --output text)

echo "Created Transit Gateway VPC Attachment for VPC2: $TGW_ATTACHMENT_2_ID"

# Wait for the attachments to become available
wait_for_tgw_attachment "$TGW_ATTACHMENT_1_ID"
wait_for_tgw_attachment "$TGW_ATTACHMENT_2_ID"
```

```
# Step 3: Add routes between the transit gateway and VPCs
echo "Adding route from VPC1 to VPC2 via Transit Gateway..."
aws ec2 create-route \
  --route-table-id "$RTB1_ID" \
  --destination-cidr-block 10.2.0.0/16 \
  --transit-gateway-id "$TGW_ID"

echo "Adding route from VPC2 to VPC1 via Transit Gateway..."
aws ec2 create-route \
  --route-table-id "$RTB2_ID" \
  --destination-cidr-block 10.1.0.0/16 \
  --transit-gateway-id "$TGW_ID"

echo "Routes added successfully"

# Step 4: Display information for testing
echo ""
echo "=== Transit Gateway Setup Complete ==="
echo "Transit Gateway ID: $TGW_ID"
echo "VPC1 ID: $VPC1_ID"
echo "VPC2 ID: $VPC2_ID"
echo ""
echo "To test connectivity:"
echo "1. Launch an EC2 instance in each VPC"
echo "2. Configure security groups to allow ICMP traffic"
echo "3. Connect to one instance and ping the other instance's private IP"
echo ""

# Prompt user before cleanup
read -p "Press Enter to view created resources, or Ctrl+C to exit without
 cleanup..."

echo ""
echo "=== Resources Created ==="
echo "Transit Gateway: $TGW_ID"
echo "VPC1: $VPC1_ID"
echo "VPC2: $VPC2_ID"
echo "Subnet in VPC1: $SUBNET1_ID"
echo "Subnet in VPC2: $SUBNET2_ID"
echo "Transit Gateway Attachment for VPC1: $TGW_ATTACHMENT_1_ID"
echo "Transit Gateway Attachment for VPC2: $TGW_ATTACHMENT_2_ID"
echo ""

read -p "Do you want to clean up these resources? (y/n): " CLEANUP_CONFIRM
```

```
if [[ $CLEANUP_CONFIRM == "y" || $CLEANUP_CONFIRM == "Y" ]]; then
  echo "Starting cleanup..."

  # Delete routes
  echo "Deleting routes..."
  aws ec2 delete-route --route-table-id "$RTB1_ID" --destination-cidr-block
 10.2.0.0/16
  aws ec2 delete-route --route-table-id "$RTB2_ID" --destination-cidr-block
 10.1.0.0/16

  # Delete transit gateway attachments
  echo "Deleting Transit Gateway VPC Attachment for VPC1: $TGW_ATTACHMENT_1_ID"
  aws ec2 delete-transit-gateway-vpc-attachment --transit-gateway-attachment-id
 "$TGW_ATTACHMENT_1_ID"

  echo "Deleting Transit Gateway VPC Attachment for VPC2: $TGW_ATTACHMENT_2_ID"
  aws ec2 delete-transit-gateway-vpc-attachment --transit-gateway-attachment-id
 "$TGW_ATTACHMENT_2_ID"

  # Wait for attachments to be deleted
  wait_for_tgw_attachment_deleted "$TGW_ATTACHMENT_1_ID"
  wait_for_tgw_attachment_deleted "$TGW_ATTACHMENT_2_ID"

  # Delete transit gateway
  echo "Deleting Transit Gateway: $TGW_ID"
  aws ec2 delete-transit-gateway --transit-gateway-id "$TGW_ID"

  echo "Cleanup completed successfully"
else
  echo "Skipping cleanup. Resources will continue to incur charges until manually
 deleted."
fi

echo "Tutorial completed. See $LOG_FILE for detailed logs."
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreateRoute
  - CreateSubnet
  - CreateTransitGateway
  - CreateTransitGatewayVpcAttachment

- CreateVpc
- DeleteRoute
- DeleteTransitGateway
- DeleteTransitGatewayVpcAttachment
- DescribeAvailabilityZones
- DescribeRouteTables
- DescribeSubnets
- DescribeTransitGatewayAttachments
- DescribeTransitGatewayVpcAttachments
- DescribeTransitGateways
- DescribeVpcs

Introducción a IPAM de VPC

En el siguiente ejemplo de código, se muestra cómo:

- Instale y configure el Administrador de direcciones IP (IPAM) de Amazon VPC mediante la CLI.
- Cree un IPAM con regiones operativas (por ejemplo, us-east-1, us-west-2).
- Recupere el ID del ámbito privado para el IPAM.
- Cree una estructura jerárquica de grupos de IPv4 (grupos de nivel superior, regionales y de desarrollo).
- Aprovisione bloques de CIDR para cada grupo (por ejemplo, 10.0.0.0/8, 10.0.0.0/16, 10.0.0.0/24).
- Cree una VPC con un CIDR asignado desde un grupo de IPAM.
- Compruebe las asignaciones de grupos de IPAM y la creación de VPC.
- Solucione problemas comunes como los errores de permisos, los errores de asignación de CIDR y las infracciones de dependencia.
- Elimine los recursos de IPAM (VPC, grupos, CIDR e IPAM) para evitar cargos innecesarios.
- Explore los siguientes pasos para conocer las características de IPAM avanzadas.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Encuentre el ejemplo completo y obtenga información sobre cómo configurarlo y ejecutarlo en el repositorio de Tutoriales para desarrolladores de ejemplo.

```
#!/bin/bash

# IPAM Getting Started CLI Script - Version 7
# This script creates an IPAM, creates a hierarchy of IP address pools, and
 allocates a CIDR to a VPC
# Fixed to correctly identify the private scope ID, wait for resources to be
 available, add locale to development pool,
# use the correct parameter names for VPC creation, and wait for CIDR provisioning
 to complete

# Set up logging
LOG_FILE="ipam_script.log"
exec > >(tee -a "$LOG_FILE") 2>&1

echo "Starting IPAM setup script at $(date)"
echo "All commands and outputs will be logged to $LOG_FILE"

# Function to handle errors
handle_error() {
    echo "ERROR: $1"
    echo "Attempting to clean up resources..."
    cleanup_resources
    exit 1
}

# Function to clean up resources
cleanup_resources() {
    echo ""
    echo "========================================="
    echo "RESOURCES CREATED:"
    echo "========================================="

    if [ -n "$VPC_ID" ]; then
```

```
        echo "VPC: $VPC_ID"
    fi

    if [ -n "$DEV_POOL_ID" ]; then
        echo "Development Pool: $DEV_POOL_ID"
    fi

    if [ -n "$REGIONAL_POOL_ID" ]; then
        echo "Regional Pool: $REGIONAL_POOL_ID"
    fi

    if [ -n "$TOP_POOL_ID" ]; then
        echo "Top-level Pool: $TOP_POOL_ID"
    fi

    if [ -n "$IPAM_ID" ]; then
        echo "IPAM: $IPAM_ID"
    fi

    echo ""
    echo "========================================="
    echo "CLEANUP CONFIRMATION"
    echo "========================================="
    echo "Do you want to clean up all created resources? (y/n): "
    read -r CLEANUP_CHOICE

    if [[ "$CLEANUP_CHOICE" =~ ^[Yy]$ ]]; then
        echo "Starting cleanup..."

        # Delete resources in reverse order of creation to handle dependencies

        if [ -n "$VPC_ID" ]; then
            echo "Deleting VPC: $VPC_ID"
            aws ec2 delete-vpc --vpc-id "$VPC_ID" || echo "Failed to delete VPC"
            echo "Waiting for VPC to be deleted..."
            sleep 10
        fi

        if [ -n "$DEV_POOL_ID" ]; then
            echo "Deleting Development Pool: $DEV_POOL_ID"
            # First deprovision any CIDRs from the pool
            CIDRS=$(aws ec2 get-ipam-pool-cidrs --ipam-pool-id "$DEV_POOL_ID" --
query 'IpamPoolCidrs[].Cidr' --output text)
            for CIDR in $CIDRS; do
```

```
                echo "Deprovisioning CIDR $CIDR from Development Pool"
                aws ec2 deprovision-ipam-pool-cidr --ipam-pool-id "$DEV_POOL_ID" --
cidr "$CIDR" || echo "Failed to deprovision CIDR $CIDR"
                sleep 5
            done
            aws ec2 delete-ipam-pool --ipam-pool-id "$DEV_POOL_ID" || echo "Failed
 to delete Development Pool"
            echo "Waiting for Development Pool to be deleted..."
            sleep 10
        fi

        if [ -n "$REGIONAL_POOL_ID" ]; then
            echo "Deleting Regional Pool: $REGIONAL_POOL_ID"
            # First deprovision any CIDRs from the pool
            CIDRS=$(aws ec2 get-ipam-pool-cidrs --ipam-pool-id "$REGIONAL_POOL_ID"
 --query 'IpamPoolCidrs[].Cidr' --output text)
            for CIDR in $CIDRS; do
                echo "Deprovisioning CIDR $CIDR from Regional Pool"
                aws ec2 deprovision-ipam-pool-cidr --ipam-pool-id
 "$REGIONAL_POOL_ID" --cidr "$CIDR" || echo "Failed to deprovision CIDR $CIDR"
                sleep 5
            done
            aws ec2 delete-ipam-pool --ipam-pool-id "$REGIONAL_POOL_ID" || echo
 "Failed to delete Regional Pool"
            echo "Waiting for Regional Pool to be deleted..."
            sleep 10
        fi

        if [ -n "$TOP_POOL_ID" ]; then
            echo "Deleting Top-level Pool: $TOP_POOL_ID"
            # First deprovision any CIDRs from the pool
            CIDRS=$(aws ec2 get-ipam-pool-cidrs --ipam-pool-id "$TOP_POOL_ID" --
query 'IpamPoolCidrs[].Cidr' --output text)
            for CIDR in $CIDRS; do
                echo "Deprovisioning CIDR $CIDR from Top-level Pool"
                aws ec2 deprovision-ipam-pool-cidr --ipam-pool-id "$TOP_POOL_ID" --
cidr "$CIDR" || echo "Failed to deprovision CIDR $CIDR"
                sleep 5
            done
            aws ec2 delete-ipam-pool --ipam-pool-id "$TOP_POOL_ID" || echo "Failed
 to delete Top-level Pool"
            echo "Waiting for Top-level Pool to be deleted..."
            sleep 10
        fi
```

```
        if [ -n "$IPAM_ID" ]; then
            echo "Deleting IPAM: $IPAM_ID"
            aws ec2 delete-ipam --ipam-id "$IPAM_ID" || echo "Failed to delete IPAM"
        fi

        echo "Cleanup completed."
    else
        echo "Cleanup skipped. Resources will remain in your account."
    fi
}

# Function to wait for a pool to be in the 'create-complete' state
wait_for_pool() {
    local pool_id=$1
    local max_attempts=30
    local attempt=1
    local state=""

    echo "Waiting for pool $pool_id to be available..."

    while [ $attempt -le $max_attempts ]; do
        state=$(aws ec2 describe-ipam-pools --ipam-pool-ids "$pool_id" --query
 'IpamPools[0].State' --output text)

        if [ "$state" = "create-complete" ]; then
            echo "Pool $pool_id is now available (state: $state)"
            return 0
        fi

        echo "Attempt $attempt/$max_attempts: Pool $pool_id is in state: $state.
 Waiting..."
        sleep 10
        ((attempt++))
    done

    echo "Timed out waiting for pool $pool_id to be available"
    return 1
}

# Function to wait for a CIDR to be fully provisioned
wait_for_cidr_provisioning() {
    local pool_id=$1
    local cidr=$2
```

```
    local max_attempts=30
    local attempt=1
    local state=""

    echo "Waiting for CIDR $cidr to be fully provisioned in pool $pool_id..."

    while [ $attempt -le $max_attempts ]; do
        state=$(aws ec2 get-ipam-pool-cidrs --ipam-pool-id "$pool_id" --query
 "IpamPoolCidrs[?Cidr=='$cidr'].State" --output text)

        if [ "$state" = "provisioned" ]; then
            echo "CIDR $cidr is now fully provisioned (state: $state)"
            return 0
        fi

        echo "Attempt $attempt/$max_attempts: CIDR $cidr is in state: $state.
 Waiting..."
        sleep 10
        ((attempt++))
    done

    echo "Timed out waiting for CIDR $cidr to be provisioned"
    return 1
}

# Step 1: Create an IPAM
echo "Creating IPAM..."
IPAM_RESULT=$(aws ec2 create-ipam \
    --description "My IPAM" \
    --operating-regions RegionName=us-east-1 RegionName=us-west-2)

if [ $? -ne 0 ]; then
    handle_error "Failed to create IPAM"
fi

IPAM_ID=$(echo "$IPAM_RESULT" | grep -o '"IpamId": "[^"]*' | cut -d'"' -f4)
echo "IPAM created with ID: $IPAM_ID"

# Wait for IPAM to be created and available
echo "Waiting for IPAM to be available..."
sleep 20

# Step 2: Get the IPAM Scope ID - FIXED to correctly identify the private scope
echo "Getting IPAM Scope ID..."
```

```
SCOPE_RESULT=$(aws ec2 describe-ipams --ipam-id "$IPAM_ID")

if [ $? -ne 0 ]; then
    handle_error "Failed to get IPAM details"
fi

# Extract the private scope ID directly from the IPAM details
PRIVATE_SCOPE_ID=$(echo "$SCOPE_RESULT" | grep -o '"PrivateDefaultScopeId": "[^"]*'
 | cut -d'"' -f4)
echo "Private Scope ID: $PRIVATE_SCOPE_ID"

if [ -z "$PRIVATE_SCOPE_ID" ]; then
    handle_error "Failed to get Private Scope ID"
fi

# Step 3: Create a Top-Level IPv4 Pool
echo "Creating Top-level IPv4 Pool..."
TOP_POOL_RESULT=$(aws ec2 create-ipam-pool \
    --ipam-scope-id "$PRIVATE_SCOPE_ID" \
    --address-family ipv4 \
    --description "Top-level pool")

if [ $? -ne 0 ]; then
    handle_error "Failed to create Top-level Pool"
fi

TOP_POOL_ID=$(echo "$TOP_POOL_RESULT" | grep -o '"IpamPoolId": "[^"]*' | cut -d'"' -
f4)
echo "Top-level Pool created with ID: $TOP_POOL_ID"

# Wait for the top-level pool to be available
if ! wait_for_pool "$TOP_POOL_ID"; then
    handle_error "Top-level Pool did not become available in time"
fi

# Provision CIDR to the top-level pool
echo "Provisioning CIDR to Top-level Pool..."
TOP_POOL_CIDR="10.0.0.0/8"
PROVISION_RESULT=$(aws ec2 provision-ipam-pool-cidr \
    --ipam-pool-id "$TOP_POOL_ID" \
    --cidr "$TOP_POOL_CIDR")

if [ $? -ne 0 ]; then
    handle_error "Failed to provision CIDR to Top-level Pool"
```

```
fi

echo "$PROVISION_RESULT"

# Wait for the CIDR to be fully provisioned
if ! wait_for_cidr_provisioning "$TOP_POOL_ID" "$TOP_POOL_CIDR"; then
    handle_error "CIDR provisioning to Top-level Pool did not complete in time"
fi

# Step 4: Create a Regional IPv4 Pool
echo "Creating Regional IPv4 Pool..."
REGIONAL_POOL_RESULT=$(aws ec2 create-ipam-pool \
    --ipam-scope-id "$PRIVATE_SCOPE_ID" \
    --source-ipam-pool-id "$TOP_POOL_ID" \
    --locale us-east-1 \
    --address-family ipv4 \
    --description "Regional pool in us-east-1")

if [ $? -ne 0 ]; then
    handle_error "Failed to create Regional Pool"
fi

REGIONAL_POOL_ID=$(echo "$REGIONAL_POOL_RESULT" | grep -o '"IpamPoolId": "[^"]*' |
 cut -d'"' -f4)
echo "Regional Pool created with ID: $REGIONAL_POOL_ID"

# Wait for the regional pool to be available
if ! wait_for_pool "$REGIONAL_POOL_ID"; then
    handle_error "Regional Pool did not become available in time"
fi

# Provision CIDR to the regional pool
echo "Provisioning CIDR to Regional Pool..."
REGIONAL_POOL_CIDR="10.0.0.0/16"
PROVISION_RESULT=$(aws ec2 provision-ipam-pool-cidr \
    --ipam-pool-id "$REGIONAL_POOL_ID" \
    --cidr "$REGIONAL_POOL_CIDR")

if [ $? -ne 0 ]; then
    handle_error "Failed to provision CIDR to Regional Pool"
fi

echo "$PROVISION_RESULT"
```

```
# Wait for the CIDR to be fully provisioned
if ! wait_for_cidr_provisioning "$REGIONAL_POOL_ID" "$REGIONAL_POOL_CIDR"; then
    handle_error "CIDR provisioning to Regional Pool did not complete in time"
fi

# Step 5: Create a Development IPv4 Pool - FIXED to include locale
echo "Creating Development IPv4 Pool..."
DEV_POOL_RESULT=$(aws ec2 create-ipam-pool \
    --ipam-scope-id "$PRIVATE_SCOPE_ID" \
    --source-ipam-pool-id "$REGIONAL_POOL_ID" \
    --locale us-east-1 \
    --address-family ipv4 \
    --description "Development pool")

if [ $? -ne 0 ]; then
    handle_error "Failed to create Development Pool"
fi

DEV_POOL_ID=$(echo "$DEV_POOL_RESULT" | grep -o '"IpamPoolId": "[^"]*' | cut -d'"' -
f4)
echo "Development Pool created with ID: $DEV_POOL_ID"

# Wait for the development pool to be available
if ! wait_for_pool "$DEV_POOL_ID"; then
    handle_error "Development Pool did not become available in time"
fi

# Provision CIDR to the development pool
echo "Provisioning CIDR to Development Pool..."
DEV_POOL_CIDR="10.0.0.0/24"
PROVISION_RESULT=$(aws ec2 provision-ipam-pool-cidr \
    --ipam-pool-id "$DEV_POOL_ID" \
    --cidr "$DEV_POOL_CIDR")

if [ $? -ne 0 ]; then
    handle_error "Failed to provision CIDR to Development Pool"
fi

echo "$PROVISION_RESULT"

# Wait for the CIDR to be fully provisioned
if ! wait_for_cidr_provisioning "$DEV_POOL_ID" "$DEV_POOL_CIDR"; then
    handle_error "CIDR provisioning to Development Pool did not complete in time"
fi
```

```
# Step 6: Create a VPC Using an IPAM Pool CIDR - FIXED to use the correct parameter
 names and a smaller netmask length
echo "Creating VPC using IPAM Pool CIDR..."
VPC_RESULT=$(aws ec2 create-vpc \
    --ipv4-ipam-pool-id "$DEV_POOL_ID" \
    --ipv4-netmask-length 26 \
    --tag-specifications 'ResourceType=vpc,Tags=[{Key=Name,Value=IPAM-VPC}]')

if [ $? -ne 0 ]; then
    handle_error "Failed to create VPC"
fi

VPC_ID=$(echo "$VPC_RESULT" | grep -o '"VpcId": "[^"]*' | cut -d'"' -f4)
echo "VPC created with ID: $VPC_ID"

# Step 7: Verify the IPAM Pool Allocation
echo "Verifying IPAM Pool Allocation..."
ALLOCATION_RESULT=$(aws ec2 get-ipam-pool-allocations \
    --ipam-pool-id "$DEV_POOL_ID")

if [ $? -ne 0 ]; then
    handle_error "Failed to verify IPAM Pool Allocation"
fi

echo "IPAM Pool Allocation verified:"
echo "$ALLOCATION_RESULT" | grep -A 5 "Allocations"

echo ""
echo "IPAM setup completed successfully!"
echo ""

# Prompt for cleanup
cleanup_resources

echo "Script completed at $(date)"
exit 0
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreateIpam

- CreateIpamPool
- CreateVpc
- DeleteIpam
- DeleteIpamPool
- DeleteVpc
- DeprovisionIpamPoolCidr
- DescribeIpamPools
- DescribeIpams
- DescribeVpcs
- GetIpamPoolAllocations
- GetIpamPoolCidrs
- ProvisionIpamPoolCidr

Ejemplos de HealthImaging que utilizan la AWS CLI con el script Bash

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes que usan AWS Command Line Interface con el script Bash con HealthImaging.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`CreateDatastore`

En el siguiente ejemplo de código, se muestra cómo utilizar `CreateDatastore`.

AWS CLI con Bash script

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function imaging_create_datastore
#
# This function creates an AWS HealthImaging data store for importing DICOM P10
 files.
#
# Parameters:
#       -n data_store_name - The name of the data store.
#
# Returns:
#       The datastore ID.
#    And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function imaging_create_datastore() {
  local datastore_name response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function imaging_create_datastore"
    echo "Creates an AWS HealthImaging data store for importing DICOM P10 files."
    echo "  -n data_store_name - The name of the data store."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:h" option; do
    case "${option}" in
      n) datastore_name="${OPTARG}" ;;
      h)
        usage
```

```
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$datastore_name" ]]; then
    errecho "ERROR: You must provide a data store name with the -n parameter."
    usage
    return 1
  fi

  response=$(aws medical-imaging create-datastore \
    --datastore-name "$datastore_name" \
    --output text \
    --query 'datastoreId')

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports medical-imaging create-datastore operation failed.
$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- Para obtener información sobre la API, consulte CreateDatastore en la Referencia de comandos de la AWS CLI.

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

`DeleteDatastore`

En el siguiente ejemplo de código, se muestra cómo utilizar `DeleteDatastore`.

AWS CLI con Bash script

```
##############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
##############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

##############################################################################
# function imaging_delete_datastore
#
# This function deletes an AWS HealthImaging data store.
#
# Parameters:
#       -i datastore_id - The ID of the data store.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
##############################################################################
function imaging_delete_datastore() {
  local datastore_id response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function imaging_delete_datastore"
    echo "Deletes an AWS HealthImaging data store."
    echo "  -i datastore_id - The ID of the data store."
    echo ""
```

```
  }

  # Retrieve the calling parameters.
  while getopts "i:h" option; do
    case "${option}" in
      i) datastore_id="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$datastore_id" ]]; then
    errecho "ERROR: You must provide a data store ID with the -i parameter."
    usage
    return 1
  fi

  response=$(aws medical-imaging delete-datastore \
    --datastore-id "$datastore_id")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports medical-imaging delete-datastore operation failed.
$response"
    return 1
  fi

  return 0
}
```

- Para obtener información sobre la API, consulte DeleteDatastore en la Referencia de comandos de la AWS CLI.

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

`GetDatastore`

En el siguiente ejemplo de código, se muestra cómo utilizar `GetDatastore`.

AWS CLI con Bash script

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function imaging_get_datastore
#
# Get a data store's properties.
#
# Parameters:
#       -i data_store_id - The ID of the data store.
#
# Returns:
#       [datastore_name, datastore_id, datastore_status, datastore_arn,  created_at,
 updated_at]
#    And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function imaging_get_datastore() {
  local datastore_id option OPTARG # Required to use getopts command in a function.
  local error_code
  # bashsupport disable=BP5008
  function usage() {
    echo "function imaging_get_datastore"
    echo "Gets a data store's properties."
```

```
    echo "  -i datastore_id - The ID of the data store."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "i:h" option; do
    case "${option}" in
      i) datastore_id="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$datastore_id" ]]; then
    errecho "ERROR: You must provide a data store ID with the -i parameter."
    usage
    return 1
  fi

  local response

  response=$(
    aws medical-imaging get-datastore \
      --datastore-id "$datastore_id" \
      --output text \
      --query "[ datastoreProperties.datastoreName,
datastoreProperties.datastoreId, datastoreProperties.datastoreStatus,
datastoreProperties.datastoreArn,  datastoreProperties.createdAt,
datastoreProperties.updatedAt]"
  )
  error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports list-datastores operation failed.$response"
    return 1
```

```
  fi

  echo "$response"

  return 0
}
```

- Para obtener información sobre la API, consulte GetDatastore en la Referencia de comandos de la AWS CLI.

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

`ListDatastores`

En el siguiente ejemplo de código, se muestra cómo utilizar `ListDatastores`.

AWS CLI con Bash script

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function imaging_list_datastores
#
# List the HealthImaging data stores in the account.
#
# Returns:
#       [[datastore_name, datastore_id, datastore_status]]
#    And:
#       0 - If successful.
#       1 - If it fails.
```

```
###############################################################################
function imaging_list_datastores() {
  local option OPTARG # Required to use getopts command in a function.
  local error_code
  # bashsupport disable=BP5008
  function usage() {
    echo "function imaging_list_datastores"
    echo "Lists the AWS HealthImaging data stores in the account."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "h" option; do
    case "${option}" in
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  local response
  response=$(aws medical-imaging list-datastores \
    --output text \
    --query "datastoreSummaries[*][datastoreName, datastoreId, datastoreStatus]")
  error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports list-datastores operation failed.$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- Para obtener información sobre la API, consulte ListDatastores en la Referencia de comandos de la AWS CLI.

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Ejemplos de IAM que utilizan la AWS CLI con el script Bash

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante AWS Command Line Interface con el script Bash con IAM.

Los conceptos básicos son ejemplos de código que muestran cómo realizar las operaciones esenciales dentro de un servicio.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica a través de llamadas a varias funciones dentro del servicio o combinado con otros Servicios de AWS.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Conceptos básicos
- Acciones
- Escenarios

Conceptos básicos

Conceptos básicos

En el siguiente ejemplo de código, se muestra cómo crear un usuario y asumir un rol.

> **Warning**
>
> Para evitar riesgos de seguridad, no utilice a los usuarios de IAM para la autenticación cuando desarrolle software especialmente diseñado o trabaje con datos reales. En cambio, utilice la federación con un proveedor de identidades como AWS IAM Identity Center.

- Crear un usuario que no tenga permisos.
- Crear un rol que conceda permiso para enumerar los buckets de Amazon S3 para la cuenta.
- Agregar una política para que el usuario asuma el rol.
- Asumir el rol y enumerar los buckets de S3 con credenciales temporales, y después limpiar los recursos.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function iam_create_user_assume_role
#
# Scenario to create an IAM user, create an IAM role, and apply the role to the
 user.
#
#     "IAM access" permissions are needed to run this code.
#     "STS assume role" permissions are needed to run this code. (Note: It might be
 necessary to
#           create a custom policy).
#
# Returns:
#       0 - If successful.
#       1 - If an error occurred.
###############################################################################
function iam_create_user_assume_role() {
  {
    if [ "$IAM_OPERATIONS_SOURCED" != "True" ]; then
```

```
    source ./iam_operations.sh
  fi
}

echo_repeat "*" 88
echo "Welcome to the IAM create user and assume role demo."
echo
echo "This demo will create an IAM user, create an IAM role, and apply the role to
the user."
echo_repeat "*" 88
echo

echo -n "Enter a name for a new IAM user: "
get_input
user_name=$get_input_result

local user_arn
user_arn=$(iam_create_user -u "$user_name")

# shellcheck disable=SC2181
if [[ ${?} == 0 ]]; then
  echo "Created demo IAM user named $user_name"
else
  errecho "$user_arn"
  errecho "The user failed to create. This demo will exit."
  return 1
fi

local access_key_response
access_key_response=$(iam_create_user_access_key -u "$user_name")
# shellcheck disable=SC2181
if [[ ${?} != 0 ]]; then
  errecho "The access key failed to create. This demo will exit."
  clean_up "$user_name"
  return 1
fi

IFS=$'\t ' read -r -a access_key_values <<<"$access_key_response"
local key_name=${access_key_values[0]}
local key_secret=${access_key_values[1]}

echo "Created access key named $key_name"
```

```
  echo "Wait 10 seconds for the user to be ready."
  sleep 10
  echo_repeat "*" 88
  echo

  local iam_role_name
  iam_role_name=$(generate_random_name "test-role")
  echo "Creating a role named $iam_role_name with user $user_name as the principal."

  local assume_role_policy_document="{
    \"Version\": \"2012-10-17\",
    \"Statement\": [{
        \"Effect\": \"Allow\",
        \"Principal\": {\"AWS\": \"$user_arn\"},
        \"Action\": \"sts:AssumeRole\"
        }]
    }"

  local role_arn
  role_arn=$(iam_create_role -n "$iam_role_name" -p "$assume_role_policy_document")

  # shellcheck disable=SC2181
  if [ ${?} == 0 ]; then
    echo "Created IAM role named $iam_role_name"
  else
    errecho "The role failed to create. This demo will exit."
    clean_up "$user_name" "$key_name"
    return 1
  fi

  local policy_name
  policy_name=$(generate_random_name "test-policy")
  local policy_document="{
                \"Version\": \"2012-10-17\",
                \"Statement\": [{
                    \"Effect\": \"Allow\",
                    \"Action\": \"s3:ListAllMyBuckets\",
                    \"Resource\": \"arn:aws:s3:::*\"}]}"

  local policy_arn
  policy_arn=$(iam_create_policy -n "$policy_name" -p "$policy_document")
  # shellcheck disable=SC2181
  if [[ ${?} == 0 ]]; then
    echo "Created  IAM policy named $policy_name"
```

```
  else
    errecho "The policy failed to create."
    clean_up "$user_name" "$key_name" "$iam_role_name"
    return 1
  fi

  if (iam_attach_role_policy -n "$iam_role_name" -p "$policy_arn"); then
    echo "Attached policy $policy_arn to role $iam_role_name"
  else
    errecho "The policy failed to attach."
    clean_up "$user_name" "$key_name" "$iam_role_name" "$policy_arn"
    return 1
  fi

  local assume_role_policy_document="{
                \"Version\": \"2012-10-17\",
                \"Statement\": [{
                    \"Effect\": \"Allow\",
                    \"Action\": \"sts:AssumeRole\",
                    \"Resource\": \"$role_arn\"}]}"

  local assume_role_policy_name
  assume_role_policy_name=$(generate_random_name "test-assume-role-")

  # shellcheck disable=SC2181
  local assume_role_policy_arn
  assume_role_policy_arn=$(iam_create_policy -n "$assume_role_policy_name" -p
"$assume_role_policy_document")
  # shellcheck disable=SC2181
  if [ ${?} == 0 ]; then
    echo "Created  IAM policy named $assume_role_policy_name for sts assume role"
  else
    errecho "The policy failed to create."
    clean_up "$user_name" "$key_name" "$iam_role_name" "$policy_arn" "$policy_arn"
    return 1
  fi

  echo "Wait 10 seconds to give AWS time to propagate these new resources and
connections."
  sleep 10
  echo_repeat "*" 88
  echo

  echo "Try to list buckets without the new user assuming the role."
```

```
 echo_repeat "*" 88
 echo

 # Set the environment variables for the created user.
 # bashsupport disable=BP2001
 export AWS_ACCESS_KEY_ID=$key_name
 # bashsupport disable=BP2001
 export AWS_SECRET_ACCESS_KEY=$key_secret

 local buckets
 buckets=$(s3_list_buckets)

 # shellcheck disable=SC2181
 if [ ${?} == 0 ]; then
   local bucket_count
   bucket_count=$(echo "$buckets" | wc -w | xargs)
   echo "There are $bucket_count buckets in the account. This should not have
happened."
 else
   errecho "Because the role with permissions has not been assumed, listing buckets
failed."
 fi

 echo
 echo_repeat "*" 88
 echo "Now assume the role $iam_role_name and list the buckets."
 echo_repeat "*" 88
 echo

 local credentials

 credentials=$(sts_assume_role -r "$role_arn" -n "AssumeRoleDemoSession")
 # shellcheck disable=SC2181
 if [ ${?} == 0 ]; then
   echo "Assumed role $iam_role_name"
 else
   errecho "Failed to assume role."
   export AWS_ACCESS_KEY_ID=""
   export AWS_SECRET_ACCESS_KEY=""
   clean_up "$user_name" "$key_name" "$iam_role_name" "$policy_arn" "$policy_arn"
"$assume_role_policy_arn"
   return 1
 fi
```

```
 IFS=$'\t ' read -r -a credentials <<<"$credentials"

 export AWS_ACCESS_KEY_ID=${credentials[0]}
 export AWS_SECRET_ACCESS_KEY=${credentials[1]}
 # bashsupport disable=BP2001
 export AWS_SESSION_TOKEN=${credentials[2]}

 buckets=$(s3_list_buckets)

 # shellcheck disable=SC2181
 if [ ${?} == 0 ]; then
   local bucket_count
   bucket_count=$(echo "$buckets" | wc -w | xargs)
   echo "There are $bucket_count buckets in the account. Listing buckets succeeded
because of "
   echo "the assumed role."
 else
   errecho "Failed to list buckets. This should not happen."
   export AWS_ACCESS_KEY_ID=""
   export AWS_SECRET_ACCESS_KEY=""
   export AWS_SESSION_TOKEN=""
   clean_up "$user_name" "$key_name" "$iam_role_name" "$policy_arn" "$policy_arn"
"$assume_role_policy_arn"
   return 1
 fi

 local result=0
 export AWS_ACCESS_KEY_ID=""
 export AWS_SECRET_ACCESS_KEY=""

 echo
 echo_repeat "*" 88
 echo "The created resources will now be deleted."
 echo_repeat "*" 88
 echo

 clean_up "$user_name" "$key_name" "$iam_role_name" "$policy_arn" "$policy_arn"
"$assume_role_policy_arn"

 # shellcheck disable=SC2181
 if [[ ${?} -ne 0 ]]; then
   result=1
 fi
```

```
  return $result
}
```

Las funciones de IAM que se usan en este escenario.

```
#############################################################################
# function iam_user_exists
#
# This function checks to see if the specified AWS Identity and Access Management
 (IAM) user already exists.
#
# Parameters:
#       $1 - The name of the IAM user to check.
#
# Returns:
#       0 - If the user already exists.
#       1 - If the user doesn't exist.
#############################################################################
function iam_user_exists() {
  local user_name
  user_name=$1

  # Check whether the IAM user already exists.
  # We suppress all output - we're interested only in the return code.

  local errors
  errors=$(aws iam get-user \
    --user-name "$user_name" 2>&1 >/dev/null)

  local error_code=${?}

  if [[ $error_code -eq 0 ]]; then
    return 0 # 0 in Bash script means true.
  else
    if [[ $errors != *"error"*"(NoSuchEntity)"* ]]; then
      aws_cli_error_log $error_code
      errecho "Error calling iam get-user $errors"
    fi

    return 1 # 1 in Bash script means false.
  fi
}
```

```
###############################################################################
# function iam_create_user
#
# This function creates the specified IAM user, unless
# it already exists.
#
# Parameters:
#       -u user_name  -- The name of the user to create.
#
# Returns:
#       The ARN of the user.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_user() {
  local user_name response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_user"
    echo "Creates an AWS Identity and Access Management (IAM) user. You must supply
 a username:"
    echo "  -u user_name    The name of the user. It must be unique within the
 account."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "u:h" option; do
    case "${option}" in
      u) user_name="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
```

```
  done
  export OPTIND=1

  if [[ -z "$user_name" ]]; then
    errecho "ERROR: You must provide a username with the -u parameter."
    usage
    return 1
  fi

  iecho "Parameters:\n"
  iecho "    User name:   $user_name"
  iecho ""

  # If the user already exists, we don't want to try to create it.
  if (iam_user_exists "$user_name"); then
    errecho "ERROR: A user with that name already exists in the account."
    return 1
  fi

  response=$(aws iam create-user --user-name "$user_name" \
    --output text \
    --query 'User.Arn')

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-user operation failed.$response"
    return 1
  fi

  echo "$response"

  return 0
}

###############################################################################
# function iam_create_user_access_key
#
# This function creates an IAM access key for the specified user.
#
# Parameters:
#       -u user_name -- The name of the IAM user.
#       [-f file_name] -- The optional file name for the access key output.
```

```
#
# Returns:
#       [access_key_id access_key_secret]
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_user_access_key() {
  local user_name file_name response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_user_access_key"
    echo "Creates an AWS Identity and Access Management (IAM) key pair."
    echo "  -u user_name   The name of the IAM user."
    echo "  [-f file_name]   Optional file name for the access key output."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "u:f:h" option; do
    case "${option}" in
      u) user_name="${OPTARG}" ;;
      f) file_name="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$user_name" ]]; then
    errecho "ERROR: You must provide a username with the -u parameter."
    usage
    return 1
  fi
```

```
  response=$(aws iam create-access-key \
    --user-name "$user_name" \
    --output text)

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-access-key operation failed.$response"
    return 1
  fi

  if [[ -n "$file_name" ]]; then
    echo "$response" >"$file_name"
  fi

  local key_id key_secret
  # shellcheck disable=SC2086
  key_id=$(echo $response | cut -f 2 -d ' ')
  # shellcheck disable=SC2086
  key_secret=$(echo $response | cut -f 4 -d ' ')

  echo "$key_id $key_secret"

  return 0
}

###############################################################################
# function iam_create_role
#
# This function creates an IAM role.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_json -- The assume role policy document.
#
# Returns:
#       The ARN of the role.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_role() {
  local role_name policy_document response
```

```
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_user_access_key"
    echo "Creates an AWS Identity and Access Management (IAM) role."
    echo "  -n role_name   The name of the IAM role."
    echo "  -p policy_json -- The assume role policy document."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:p:h" option; do
    case "${option}" in
      n) role_name="${OPTARG}" ;;
      p) policy_document="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$role_name" ]]; then
    errecho "ERROR: You must provide a role name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$policy_document" ]]; then
    errecho "ERROR: You must provide a policy document with the -p parameter."
    usage
    return 1
  fi

  response=$(aws iam create-role \
    --role-name "$role_name" \
    --assume-role-policy-document "$policy_document" \
```

```
    --output text \
    --query Role.Arn)

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-role operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}

###############################################################################
# function iam_create_policy
#
# This function creates an IAM policy.
#
# Parameters:
#       -n policy_name -- The name of the IAM policy.
#       -p policy_json -- The policy document.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_policy() {
  local policy_name policy_document response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_policy"
    echo "Creates an AWS Identity and Access Management (IAM) policy."
    echo "  -n policy_name   The name of the IAM policy."
    echo "  -p policy_json -- The policy document."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:p:h" option; do
```

```
    case "${option}" in
      n) policy_name="${OPTARG}" ;;
      p) policy_document="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$policy_name" ]]; then
    errecho "ERROR: You must provide a policy name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$policy_document" ]]; then
    errecho "ERROR: You must provide a policy document with the -p parameter."
    usage
    return 1
  fi

  response=$(aws iam create-policy \
    --policy-name "$policy_name" \
    --policy-document "$policy_document" \
    --output text \
    --query Policy.Arn)

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-policy operation failed.\n$response"
    return 1
  fi

  echo "$response"
}
```

```
###############################################################################
# function iam_attach_role_policy
#
# This function attaches an IAM policy to a tole.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_ARN -- The IAM policy document ARN..
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_attach_role_policy() {
  local role_name policy_arn response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_attach_role_policy"
    echo "Attaches an AWS Identity and Access Management (IAM) policy to an IAM
 role."
    echo "  -n role_name   The name of the IAM role."
    echo "  -p policy_ARN -- The IAM policy document ARN."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:p:h" option; do
    case "${option}" in
      n) role_name="${OPTARG}" ;;
      p) policy_arn="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
```

```
  export OPTIND=1

  if [[ -z "$role_name" ]]; then
    errecho "ERROR: You must provide a role name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$policy_arn" ]]; then
    errecho "ERROR: You must provide a policy ARN with the -p parameter."
    usage
    return 1
  fi

  response=$(aws iam attach-role-policy \
    --role-name "$role_name" \
    --policy-arn "$policy_arn")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports attach-role-policy operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}

###############################################################################
# function iam_detach_role_policy
#
# This function detaches an IAM policy to a tole.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_ARN -- The IAM policy document ARN..
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
```

```
function iam_detach_role_policy() {
  local role_name policy_arn response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_detach_role_policy"
    echo "Detaches an AWS Identity and Access Management (IAM) policy to an IAM
 role."
    echo "  -n role_name   The name of the IAM role."
    echo "  -p policy_ARN -- The IAM policy document ARN."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:p:h" option; do
    case "${option}" in
      n) role_name="${OPTARG}" ;;
      p) policy_arn="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$role_name" ]]; then
    errecho "ERROR: You must provide a role name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$policy_arn" ]]; then
    errecho "ERROR: You must provide a policy ARN with the -p parameter."
    usage
    return 1
  fi
```

```
  response=$(aws iam detach-role-policy \
    --role-name "$role_name" \
    --policy-arn "$policy_arn")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports detach-role-policy operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}

###############################################################################
# function iam_delete_policy
#
# This function deletes an IAM policy.
#
# Parameters:
#       -n policy_arn -- The name of the IAM policy arn.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_delete_policy() {
  local policy_arn response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_delete_policy"
    echo "Deletes an AWS Identity and Access Management (IAM) policy"
    echo "  -n policy_arn -- The name of the IAM policy arn."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:h" option; do
    case "${option}" in
```

```
      n) policy_arn="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$policy_arn" ]]; then
    errecho "ERROR: You must provide a policy arn with the -n parameter."
    usage
    return 1
  fi

  iecho "Parameters:\n"
  iecho "    Policy arn:  $policy_arn"
  iecho ""

  response=$(aws iam delete-policy \
    --policy-arn "$policy_arn")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports delete-policy operation failed.\n$response"
    return 1
  fi

  iecho "delete-policy response:$response"
  iecho

  return 0
}

###############################################################################
# function iam_delete_role
#
```

```
# This function deletes an IAM role.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_delete_role() {
  local role_name response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_delete_role"
    echo "Deletes an AWS Identity and Access Management (IAM) role"
    echo "  -n role_name -- The name of the IAM role."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:h" option; do
    case "${option}" in
      n) role_name="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  echo "role_name:$role_name"
  if [[ -z "$role_name" ]]; then
    errecho "ERROR: You must provide a role name with the -n parameter."
    usage
    return 1
  fi
```

```
  iecho "Parameters:\n"
  iecho "    Role name:  $role_name"
  iecho ""

  response=$(aws iam delete-role \
    --role-name "$role_name")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports delete-role operation failed.\n$response"
    return 1
  fi

  iecho "delete-role response:$response"
  iecho

  return 0
}

###############################################################################
# function iam_delete_access_key
#
# This function deletes an IAM access key for the specified IAM user.
#
# Parameters:
#       -u user_name  -- The name of the user.
#       -k access_key -- The access key to delete.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_delete_access_key() {
  local user_name access_key response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_delete_access_key"
    echo "Deletes an AWS Identity and Access Management (IAM) access key for the
 specified IAM user"
```

```
  echo "  -u user_name    The name of the user."
  echo "  -k access_key   The access key to delete."
  echo ""
}

# Retrieve the calling parameters.
while getopts "u:k:h" option; do
  case "${option}" in
    u) user_name="${OPTARG}" ;;
    k) access_key="${OPTARG}" ;;
    h)
      usage
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$user_name" ]]; then
  errecho "ERROR: You must provide a username with the -u parameter."
  usage
  return 1
fi

if [[ -z "$access_key" ]]; then
  errecho "ERROR: You must provide an access key with the -k parameter."
  usage
  return 1
fi

iecho "Parameters:\n"
iecho "    Username:   $user_name"
iecho "    Access key:   $access_key"
iecho ""

response=$(aws iam delete-access-key \
  --user-name "$user_name" \
  --access-key-id "$access_key")
```

```
  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports delete-access-key operation failed.\n$response"
    return 1
  fi

  iecho "delete-access-key response:$response"
  iecho

  return 0
}

###############################################################################
# function iam_delete_user
#
# This function deletes the specified IAM user.
#
# Parameters:
#       -u user_name  -- The name of the user to create.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_delete_user() {
  local user_name response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_delete_user"
    echo "Deletes an AWS Identity and Access Management (IAM) user. You must supply
 a username:"
    echo "  -u user_name    The name of the user."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "u:h" option; do
    case "${option}" in
      u) user_name="${OPTARG}" ;;
      h)
```

```
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$user_name" ]]; then
    errecho "ERROR: You must provide a username with the -u parameter."
    usage
    return 1
  fi

  iecho "Parameters:\n"
  iecho "    User name:   $user_name"
  iecho ""

  # If the user does not exist, we don't want to try to delete it.
  if (! iam_user_exists "$user_name"); then
    errecho "ERROR: A user with that name does not exist in the account."
    return 1
  fi

  response=$(aws iam delete-user \
    --user-name "$user_name")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports delete-user operation failed.$response"
    return 1
  fi

  iecho "delete-user response:$response"
  iecho

  return 0
}
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - AttachRolePolicy
  - CreateAccessKey
  - CreatePolicy
  - CreateRole
  - CreateUser
  - DeleteAccessKey
  - DeletePolicy
  - DeleteRole
  - DeleteUser
  - DeleteUserPolicy
  - DetachRolePolicy
  - PutUserPolicy

Acciones

`AttachRolePolicy`

En el siguiente ejemplo de código, se muestra cómo utilizar `AttachRolePolicy`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
```

```
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_attach_role_policy
#
# This function attaches an IAM policy to a tole.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_ARN -- The IAM policy document ARN..
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_attach_role_policy() {
  local role_name policy_arn response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_attach_role_policy"
    echo "Attaches an AWS Identity and Access Management (IAM) policy to an IAM
 role."
    echo "  -n role_name   The name of the IAM role."
    echo "  -p policy_ARN -- The IAM policy document ARN."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:p:h" option; do
    case "${option}" in
      n) role_name="${OPTARG}" ;;
      p) policy_arn="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
```

```
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$role_name" ]]; then
    errecho "ERROR: You must provide a role name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$policy_arn" ]]; then
    errecho "ERROR: You must provide a policy ARN with the -p parameter."
    usage
    return 1
  fi

  response=$(aws iam attach-role-policy \
    --role-name "$role_name" \
    --policy-arn "$policy_arn")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports attach-role-policy operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- Para obtener información sobre la API, consulte AttachRolePolicy en la Referencia de comandos de la AWS CLI.

`CreateAccessKey`

En el siguiente ejemplo de código, se muestra cómo utilizar `CreateAccessKey`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
##############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

##############################################################################
# function iam_create_user_access_key
#
# This function creates an IAM access key for the specified user.
#
# Parameters:
#       -u user_name -- The name of the IAM user.
#       [-f file_name] -- The optional file name for the access key output.
#
# Returns:
#       [access_key_id access_key_secret]
#     And:
#       0 - If successful.
#       1 - If it fails.
##############################################################################
function iam_create_user_access_key() {
  local user_name file_name response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_user_access_key"
    echo "Creates an AWS Identity and Access Management (IAM) key pair."
    echo "  -u user_name   The name of the IAM user."
    echo "  [-f file_name]   Optional file name for the access key output."
```

```
  echo ""
}

# Retrieve the calling parameters.
while getopts "u:f:h" option; do
  case "${option}" in
    u) user_name="${OPTARG}" ;;
    f) file_name="${OPTARG}" ;;
    h)
      usage
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$user_name" ]]; then
  errecho "ERROR: You must provide a username with the -u parameter."
  usage
  return 1
fi

response=$(aws iam create-access-key \
  --user-name "$user_name" \
  --output text)

local error_code=${?}

if [[ $error_code -ne 0 ]]; then
  aws_cli_error_log $error_code
  errecho "ERROR: AWS reports create-access-key operation failed.$response"
  return 1
fi

if [[ -n "$file_name" ]]; then
  echo "$response" >"$file_name"
fi

local key_id key_secret
```

```
  # shellcheck disable=SC2086
  key_id=$(echo $response | cut -f 2 -d ' ')
  # shellcheck disable=SC2086
  key_secret=$(echo $response | cut -f 4 -d ' ')

  echo "$key_id $key_secret"

  return 0
}
```

- Para obtener información sobre la API, consulte CreateAccessKey en la Referencia de comandos de la AWS CLI.

`CreatePolicy`

En el siguiente ejemplo de código, se muestra cómo utilizar `CreatePolicy`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_create_policy
#
# This function creates an IAM policy.
#
# Parameters:
```

```
#       -n policy_name -- The name of the IAM policy.
#       -p policy_json -- The policy document.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_policy() {
  local policy_name policy_document response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_policy"
    echo "Creates an AWS Identity and Access Management (IAM) policy."
    echo "  -n policy_name   The name of the IAM policy."
    echo "  -p policy_json -- The policy document."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:p:h" option; do
    case "${option}" in
      n) policy_name="${OPTARG}" ;;
      p) policy_document="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$policy_name" ]]; then
    errecho "ERROR: You must provide a policy name with the -n parameter."
    usage
    return 1
  fi
```

```
  if [[ -z "$policy_document" ]]; then
    errecho "ERROR: You must provide a policy document with the -p parameter."
    usage
    return 1
  fi

  response=$(aws iam create-policy \
    --policy-name "$policy_name" \
    --policy-document "$policy_document" \
    --output text \
    --query Policy.Arn)

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-policy operation failed.\n$response"
    return 1
  fi

  echo "$response"
}
```

- Para obtener información sobre la API, consulte CreatePolicy en la Referencia de comandos de la AWS CLI.

`CreateRole`

En el siguiente ejemplo de código, se muestra cómo utilizar `CreateRole`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function errecho
```

```
#
# This function outputs everything sent to it to STDERR (standard error output).
#############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

#############################################################################
# function iam_create_role
#
# This function creates an IAM role.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_json -- The assume role policy document.
#
# Returns:
#       The ARN of the role.
#     And:
#       0 - If successful.
#       1 - If it fails.
#############################################################################
function iam_create_role() {
  local role_name policy_document response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_user_access_key"
    echo "Creates an AWS Identity and Access Management (IAM) role."
    echo "  -n role_name   The name of the IAM role."
    echo "  -p policy_json -- The assume role policy document."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:p:h" option; do
    case "${option}" in
      n) role_name="${OPTARG}" ;;
      p) policy_document="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
```

```
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$role_name" ]]; then
    errecho "ERROR: You must provide a role name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$policy_document" ]]; then
    errecho "ERROR: You must provide a policy document with the -p parameter."
    usage
    return 1
  fi

  response=$(aws iam create-role \
    --role-name "$role_name" \
    --assume-role-policy-document "$policy_document" \
    --output text \
    --query Role.Arn)

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-role operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- Para obtener información sobre la API, consulte CreateRole en la Referencia de comandos de la AWS CLI.

`CreateUser`

En el siguiente ejemplo de código, se muestra cómo utilizar `CreateUser`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_create_user
#
# This function creates the specified IAM user, unless
# it already exists.
#
# Parameters:
#       -u user_name  -- The name of the user to create.
#
# Returns:
```

```
#       The ARN of the user.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_user() {
  local user_name response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_user"
    echo "Creates an AWS Identity and Access Management (IAM) user. You must supply
 a username:"
    echo "  -u user_name    The name of the user. It must be unique within the
 account."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "u:h" option; do
    case "${option}" in
      u) user_name="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$user_name" ]]; then
    errecho "ERROR: You must provide a username with the -u parameter."
    usage
    return 1
  fi

  iecho "Parameters:\n"
  iecho "    User name:   $user_name"
```

```
  iecho ""

  # If the user already exists, we don't want to try to create it.
  if (iam_user_exists "$user_name"); then
    errecho "ERROR: A user with that name already exists in the account."
    return 1
  fi

  response=$(aws iam create-user --user-name "$user_name" \
    --output text \
    --query 'User.Arn')

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-user operation failed.$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- Para obtener información sobre la API, consulte CreateUser en la Referencia de comandos de la AWS CLI.

`DeleteAccessKey`

En el siguiente ejemplo de código, se muestra cómo utilizar `DeleteAccessKey`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_delete_access_key
#
# This function deletes an IAM access key for the specified IAM user.
#
# Parameters:
#       -u user_name  -- The name of the user.
#       -k access_key -- The access key to delete.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_delete_access_key() {
  local user_name access_key response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_delete_access_key"
    echo "Deletes an AWS Identity and Access Management (IAM) access key for the
 specified IAM user"
    echo "  -u user_name    The name of the user."
    echo "  -k access_key   The access key to delete."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "u:k:h" option; do
    case "${option}" in
      u) user_name="${OPTARG}" ;;
      k) access_key="${OPTARG}" ;;
      h)
        usage
```

```
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$user_name" ]]; then
  errecho "ERROR: You must provide a username with the -u parameter."
  usage
  return 1
fi

if [[ -z "$access_key" ]]; then
  errecho "ERROR: You must provide an access key with the -k parameter."
  usage
  return 1
fi

iecho "Parameters:\n"
iecho "    Username:   $user_name"
iecho "    Access key:   $access_key"
iecho ""

response=$(aws iam delete-access-key \
  --user-name "$user_name" \
  --access-key-id "$access_key")

local error_code=${?}

if [[ $error_code -ne 0 ]]; then
  aws_cli_error_log $error_code
  errecho "ERROR: AWS reports delete-access-key operation failed.\n$response"
  return 1
fi

iecho "delete-access-key response:$response"
iecho

return 0
```

```
}
```

- Para obtener información sobre la API, consulte DeleteAccessKey en la Referencia de comandos de la AWS CLI.

`DeletePolicy`

En el siguiente ejemplo de código, se muestra cómo utilizar `DeletePolicy`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_delete_policy
```

```
#
# This function deletes an IAM policy.
#
# Parameters:
#       -n policy_arn -- The name of the IAM policy arn.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_delete_policy() {
  local policy_arn response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_delete_policy"
    echo "Deletes an AWS Identity and Access Management (IAM) policy"
    echo "  -n policy_arn -- The name of the IAM policy arn."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:h" option; do
    case "${option}" in
      n) policy_arn="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$policy_arn" ]]; then
    errecho "ERROR: You must provide a policy arn with the -n parameter."
    usage
    return 1
  fi
```

```
  iecho "Parameters:\n"
  iecho "    Policy arn:  $policy_arn"
  iecho ""

  response=$(aws iam delete-policy \
    --policy-arn "$policy_arn")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports delete-policy operation failed.\n$response"
    return 1
  fi

  iecho "delete-policy response:$response"
  iecho

  return 0
}
```

- Para obtener información sobre la API, consulte DeletePolicy en la Referencia de comandos de la AWS CLI.

`DeleteRole`

En el siguiente ejemplo de código, se muestra cómo utilizar `DeleteRole`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
# function iecho
#
```

```
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_delete_role
#
# This function deletes an IAM role.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_delete_role() {
  local role_name response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_delete_role"
    echo "Deletes an AWS Identity and Access Management (IAM) role"
    echo "  -n role_name -- The name of the IAM role."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:h" option; do
```

```
    case "${option}" in
      n) role_name="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  echo "role_name:$role_name"
  if [[ -z "$role_name" ]]; then
    errecho "ERROR: You must provide a role name with the -n parameter."
    usage
    return 1
  fi

  iecho "Parameters:\n"
  iecho "    Role name:  $role_name"
  iecho ""

  response=$(aws iam delete-role \
    --role-name "$role_name")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports delete-role operation failed.\n$response"
    return 1
  fi

  iecho "delete-role response:$response"
  iecho

  return 0
}
```

- Para obtener información sobre la API, consulte DeleteRole en la Referencia de comandos de la AWS CLI.

`DeleteUser`

En el siguiente ejemplo de código, se muestra cómo utilizar `DeleteUser`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_delete_user
#
# This function deletes the specified IAM user.
#
# Parameters:
```

```
#       -u user_name  -- The name of the user to create.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_delete_user() {
  local user_name response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_delete_user"
    echo "Deletes an AWS Identity and Access Management (IAM) user. You must supply
 a username:"
    echo "  -u user_name    The name of the user."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "u:h" option; do
    case "${option}" in
      u) user_name="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$user_name" ]]; then
    errecho "ERROR: You must provide a username with the -u parameter."
    usage
    return 1
  fi

  iecho "Parameters:\n"
  iecho "    User name:   $user_name"
```

```
  iecho ""

  # If the user does not exist, we don't want to try to delete it.
  if (! iam_user_exists "$user_name"); then
    errecho "ERROR: A user with that name does not exist in the account."
    return 1
  fi

  response=$(aws iam delete-user \
    --user-name "$user_name")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports delete-user operation failed.$response"
    return 1
  fi

  iecho "delete-user response:$response"
  iecho

  return 0
}
```

- Para obtener información sobre la API, consulte DeleteUser en la Referencia de comandos de la AWS CLI.

`DetachRolePolicy`

En el siguiente ejemplo de código, se muestra cómo utilizar `DetachRolePolicy`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_detach_role_policy
#
# This function detaches an IAM policy to a tole.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_ARN -- The IAM policy document ARN..
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_detach_role_policy() {
  local role_name policy_arn response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_detach_role_policy"
    echo "Detaches an AWS Identity and Access Management (IAM) policy to an IAM
 role."
    echo "  -n role_name   The name of the IAM role."
    echo "  -p policy_ARN -- The IAM policy document ARN."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:p:h" option; do
    case "${option}" in
      n) role_name="${OPTARG}" ;;
      p) policy_arn="${OPTARG}" ;;
      h)
        usage
```

```
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$role_name" ]]; then
    errecho "ERROR: You must provide a role name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$policy_arn" ]]; then
    errecho "ERROR: You must provide a policy ARN with the -p parameter."
    usage
    return 1
  fi

  response=$(aws iam detach-role-policy \
    --role-name "$role_name" \
    --policy-arn "$policy_arn")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports detach-role-policy operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- Para obtener información sobre la API, consulte DetachRolePolicy en la Referencia de comandos de la AWS CLI.

`GetUser`

En el siguiente ejemplo de código, se muestra cómo utilizar `GetUser`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
##############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

##############################################################################
# function iam_user_exists
#
# This function checks to see if the specified AWS Identity and Access Management
 (IAM) user already exists.
#
# Parameters:
#       $1 - The name of the IAM user to check.
#
# Returns:
#       0 - If the user already exists.
#       1 - If the user doesn't exist.
##############################################################################
function iam_user_exists() {
  local user_name
  user_name=$1

  # Check whether the IAM user already exists.
  # We suppress all output - we're interested only in the return code.

  local errors
  errors=$(aws iam get-user \
```

```
    --user-name "$user_name" 2>&1 >/dev/null)

  local error_code=${?}

  if [[ $error_code -eq 0 ]]; then
    return 0 # 0 in Bash script means true.
  else
    if [[ $errors != *"error"*"(NoSuchEntity)"* ]]; then
      aws_cli_error_log $error_code
      errecho "Error calling iam get-user $errors"
    fi

    return 1 # 1 in Bash script means false.
  fi
}
```

- Para obtener información sobre la API, consulte GetUser en la Referencia de comandos de la AWS CLI.

`ListAccessKeys`

En el siguiente ejemplo de código, se muestra cómo utilizar `ListAccessKeys`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}
```

```
###############################################################################
# function iam_list_access_keys
#
# This function lists the access keys for the specified user.
#
# Parameters:
#       -u user_name -- The name of the IAM user.
#
# Returns:
#       access_key_ids
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_list_access_keys() {

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_list_access_keys"
    echo "Lists the AWS Identity and Access Management (IAM) access key IDs for the
 specified user."
    echo "  -u user_name   The name of the IAM user."
    echo ""
  }

  local user_name response
  local option OPTARG # Required to use getopts command in a function.
  # Retrieve the calling parameters.
  while getopts "u:h" option; do
    case "${option}" in
      u) user_name="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1
```

```
  if [[ -z "$user_name" ]]; then
    errecho "ERROR: You must provide a username with the -u parameter."
    usage
    return 1
  fi

  response=$(aws iam list-access-keys \
    --user-name "$user_name" \
    --output text \
    --query 'AccessKeyMetadata[].AccessKeyId')

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports list-access-keys operation failed.$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- Para obtener información sobre la API, consulte ListAccessKeys en la Referencia de comandos de la AWS CLI.

`ListUsers`

En el siguiente ejemplo de código, se muestra cómo utilizar `ListUsers`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
```

```
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_list_users
#
# List the IAM users in the account.
#
# Returns:
#       The list of users names
#    And:
#       0 - If the user already exists.
#       1 - If the user doesn't exist.
###############################################################################
function iam_list_users() {
  local option OPTARG # Required to use getopts command in a function.
  local error_code
  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_list_users"
    echo "Lists the AWS Identity and Access Management (IAM) user in the account."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "h" option; do
    case "${option}" in
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1
```

```
  local response

  response=$(aws iam list-users \
    --output text \
    --query "Users[].UserName")
  error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports list-users operation failed.$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- Para obtener información sobre la API, consulte ListUsers en la Referencia de comandos de la AWS CLI.

`UpdateAccessKey`

En el siguiente ejemplo de código, se muestra cómo utilizar `UpdateAccessKey`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function iam_update_access_key
#
# This function can activate or deactivate an IAM access key for the specified IAM
 user.
#
```

```
# Parameters:
#       -u user_name  -- The name of the user.
#       -k access_key -- The access key to update.
#       -a            -- Activate the selected access key.
#       -d            -- Deactivate the selected access key.
#
# Example:
#       # To deactivate the selected access key for IAM user Bob
#       iam_update_access_key -u Bob -k AKIAIOSFODNN7EXAMPLE -d
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_update_access_key() {
  local user_name access_key status response
  local option OPTARG # Required to use getopts command in a function.
  local activate_flag=false deactivate_flag=false

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_update_access_key"
    echo "Updates the status of an AWS Identity and Access Management (IAM) access
 key for the specified IAM user"
    echo "  -u user_name    The name of the user."
    echo "  -k access_key   The access key to update."
    echo "  -a              Activate the access key."
    echo "  -d              Deactivate the access key."
    echo ""
  }

  # Retrieve the calling parameters.
    while getopts "u:k:adh" option; do
      case "${option}" in
        u) user_name="${OPTARG}" ;;
        k) access_key="${OPTARG}" ;;
        a) activate_flag=true ;;
        d) deactivate_flag=true ;;
        h)
          usage
          return 0
          ;;
        \?)
          echo "Invalid parameter"
```

```
          usage
          return 1
          ;;
      esac
    done
    export OPTIND=1

  # Validate input parameters
    if [[ -z "$user_name" ]]; then
      errecho "ERROR: You must provide a username with the -u parameter."
      usage
      return 1
    fi

    if [[ -z "$access_key" ]]; then
      errecho "ERROR: You must provide an access key with the -k parameter."
      usage
      return 1
    fi

    # Ensure that only -a or -d is specified
    if [[ "$activate_flag" == true && "$deactivate_flag" == true ]]; then
      errecho "ERROR: You cannot specify both -a (activate) and -d (deactivate) at
the same time."
      usage
      return 1
    fi

    # If neither -a nor -d is provided, return an error
    if [[ "$activate_flag" == false && "$deactivate_flag" == false ]]; then
      errecho "ERROR: You must specify either -a (activate) or -d (deactivate)."
      usage
      return 1
    fi

    # Determine the status based on the flag
    if [[ "$activate_flag" == true ]]; then
      status="Active"
    elif [[ "$deactivate_flag" == true ]]; then
      status="Inactive"
    fi

    iecho "Parameters:\n"
    iecho "    Username:   $user_name"
```

```
    iecho "    Access key: $access_key"
    iecho "    New status: $status"
    iecho ""

    # Update the access key status
    response=$(aws iam update-access-key \
      --user-name "$user_name" \
      --access-key-id "$access_key" \
      --status "$status" 2>&1)

    local error_code=${?}

    if [[ $error_code -ne 0 ]]; then
      aws_cli_error_log $error_code
      errecho "ERROR: AWS reports update-access-key operation failed.\n$response"
      return 1
    fi

    iecho "update-access-key response: $response"
    iecho

    return 0
}
```

- Para obtener información sobre la API, consulte UpdateAccessKey en la Referencia de la API de la AWS CLI.

Escenarios

Configuración del control de acceso basado en atributos

El siguiente ejemplo de código muestra cómo implementar el control de acceso basado en atributos (ABAC) para DynamoDB.

- Cree una política de IAM para ABAC.
- Cree tablas con etiquetas para diferentes departamentos.
- Enumere y filtre las tablas en función de las etiquetas.

AWS CLI con Bash script

Cree una política de IAM para ABAC.

```
# Step 1: Create a policy document for ABAC
cat > abac-policy.json << 'EOF'
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:GetItem",
        "dynamodb:BatchGetItem",
        "dynamodb:Query",
        "dynamodb:Scan"
      ],
      "Resource": "arn:aws:dynamodb:*:*:table/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "${aws:PrincipalTag/Department}"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:PutItem",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteItem",
        "dynamodb:BatchWriteItem"
      ],
      "Resource": "arn:aws:dynamodb:*:*:table/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "${aws:PrincipalTag/Department}",
          "aws:ResourceTag/Environment": "Development"
        }
      }
    }
  ]
}
EOF
```

```
# Step 2: Create the IAM policy
aws iam create-policy \
    --policy-name DynamoDBDepartmentBasedAccess \
    --policy-document file://abac-policy.json
```

Cree tablas con etiquetas para diferentes departamentos.

```
# Create a DynamoDB table with tags for ABAC
aws dynamodb create-table \
    --table-name FinanceData \
    --attribute-definitions \
        AttributeName=RecordID,AttributeType=S \
    --key-schema \
        AttributeName=RecordID,KeyType=HASH \
    --billing-mode PAY_PER_REQUEST \
    --tags \
        Key=Department,Value=Finance \
        Key=Environment,Value=Development

# Create another table with different tags
aws dynamodb create-table \
    --table-name MarketingData \
    --attribute-definitions \
        AttributeName=RecordID,AttributeType=S \
    --key-schema \
        AttributeName=RecordID,KeyType=HASH \
    --billing-mode PAY_PER_REQUEST \
    --tags \
        Key=Department,Value=Marketing \
        Key=Environment,Value=Production
```

Enumere y filtre las tablas en función de las etiquetas.

```
# List all DynamoDB tables
echo "Listing all tables:"
aws dynamodb list-tables

# Get ARNs for all tables
echo -e "\nGetting ARNs for all tables:"
```

```
TABLE_ARNS=$(aws dynamodb list-tables --query "TableNames[*]" --output text | xargs
 -I {} aws dynamodb describe-table --table-name {} --query "Table.TableArn" --output
 text)

# For each table ARN, list its tags
echo -e "\nListing tags for each table:"
for ARN in $TABLE_ARNS; do
    TABLE_NAME=$(echo $ARN | awk -F/ '{print $2}')
    echo -e "\nTags for table: $TABLE_NAME"
    aws dynamodb list-tags-of-resource --resource-arn $ARN
done

# Example: Find tables with a specific tag
echo -e "\nFinding tables with Environment=Production tag:"
for ARN in $TABLE_ARNS; do
    TABLE_NAME=$(echo $ARN | awk -F/ '{print $2}')
    TAGS=$(aws dynamodb list-tags-of-resource --resource-arn $ARN --query "Tags[?
Key=='Environment' && Value=='Production']" --output text)
    if [ ! -z "$TAGS" ]; then
        echo "Table with Production tag: $TABLE_NAME"
    fi
done
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreatePolicy
  - CreateTable
  - ListTables

Trabajo con Streams y tiempo de vida

El siguiente ejemplo de código muestra cómo administrar las características de DynamoDB Streams y tiempo de vida.

- Cree una tabla con Streams habilitado.
- Describa Streams.
- Cree una función de Lambda para procesar Streams.
- Habilite TTL en una tabla.

- Agregue elementos con atributos TTL.
- Describa la configuración de TTL.

AWS CLI con Bash script

Cree una tabla con Streams habilitado.

```
# Create a table with DynamoDB Streams enabled
aws dynamodb create-table \
    --table-name StreamsDemo \
    --attribute-definitions \
        AttributeName=ID,AttributeType=S \
    --key-schema \
        AttributeName=ID,KeyType=HASH \
    --billing-mode PAY_PER_REQUEST \
    --stream-specification StreamEnabled=true,StreamViewType=NEW_AND_OLD_IMAGES
```

Describa Streams.

```
# Get information about the stream
aws dynamodb describe-table \
    --table-name StreamsDemo \
    --query "Table.StreamSpecification"

# Get the stream ARN
STREAM_ARN=$(aws dynamodb describe-table \
    --table-name StreamsDemo \
    --query "Table.LatestStreamArn" \
    --output text)

echo "Stream ARN: $STREAM_ARN"

# Describe the stream
aws dynamodbstreams describe-stream \
    --stream-arn $STREAM_ARN
```

Cree una función de Lambda para Streams.

```
# Step 1: Create an IAM role for the Lambda function
```

```
cat > trust-policy.json << 'EOF'
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF

aws iam create-role \
    --role-name DynamoDBStreamsLambdaRole \
    --assume-role-policy-document file://trust-policy.json

# Step 2: Attach permissions to the role
aws iam attach-role-policy \
    --role-name DynamoDBStreamsLambdaRole \
    --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole

# Step 3: Create a Lambda function (code would be in a separate file)
echo "Lambda function creation would be done separately with appropriate code"

# Step 4: Create an event source mapping
echo "Example command to create event source mapping:"
echo "aws lambda create-event-source-mapping \\"
echo "    --function-name ProcessDynamoDBRecords \\"
echo "    --event-source $STREAM_ARN \\"
echo "    --batch-size 100 \\"
echo "    --starting-position LATEST"
```

Habilite TTL en una tabla.

```
# Create a table for TTL demonstration
aws dynamodb create-table \
    --table-name TTLDemo \
    --attribute-definitions \
        AttributeName=ID,AttributeType=S \
```

```
    --key-schema \
        AttributeName=ID,KeyType=HASH \
    --billing-mode PAY_PER_REQUEST

# Wait for table to become active
aws dynamodb wait table-exists --table-name TTLDemo

# Enable TTL on the table
aws dynamodb update-time-to-live \
    --table-name TTLDemo \
    --time-to-live-specification "Enabled=true, AttributeName=ExpirationTime"
```

Agregue elementos con atributos TTL.

```
# Calculate expiration time (current time + 1 day in seconds)
EXPIRATION_TIME=$(date -d "+1 day" +%s)

# Add an item with TTL attribute
aws dynamodb put-item \
    --table-name TTLDemo \
    --item '{
        "ID": {"S": "item1"},
        "Data": {"S": "This item will expire in 1 day"},
        "ExpirationTime": {"N": "'$EXPIRATION_TIME'"}
    }'

# Add an item that expires in 1 hour
EXPIRATION_TIME_HOUR=$(date -d "+1 hour" +%s)
aws dynamodb put-item \
    --table-name TTLDemo \
    --item '{
        "ID": {"S": "item2"},
        "Data": {"S": "This item will expire in 1 hour"},
        "ExpirationTime": {"N": "'$EXPIRATION_TIME_HOUR'"}
    }'
```

Describa la configuración de TTL.

```
# Describe TTL settings for a table
aws dynamodb describe-time-to-live \
    --table-name TTLDemo
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - AttachRolePolicy
  - CreateRole
  - CreateTable
  - DescribeTable
  - DescribeTimeToLive
  - PutItem
  - UpdateTimeToLive

Ejemplos de AWS KMS que utilizan la AWS CLI con el script Bash

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante AWS Command Line Interface con el script Bash con AWS KMS.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica a través de llamadas a varias funciones dentro del servicio o combinado con otros Servicios de AWS.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Escenarios

Escenarios

Trabajo con el cifrado de tablas

En el siguiente ejemplo de código se muestra cómo administrar las opciones de cifrado de las tablas de DynamoDB.

- Cree una tabla con un cifrado predeterminado.
- Cree una tabla con una CMK administrada por el cliente.
- Actualice la configuración de cifrado de la tabla.

- Describa el cifrado de la tabla.

AWS CLI con Bash script

Cree una tabla con un cifrado predeterminado.

```
# Create a table with default encryption (AWS owned key)
aws dynamodb create-table \
    --table-name CustomerData \
    --attribute-definitions \
        AttributeName=CustomerID,AttributeType=S \
    --key-schema \
        AttributeName=CustomerID,KeyType=HASH \
    --billing-mode PAY_PER_REQUEST \
    --sse-specification Enabled=true,SSEType=KMS
```

Cree una tabla con una CMK administrada por el cliente.

```
# Step 1: Create a customer managed key in KMS
aws kms create-key \
    --description "Key for DynamoDB table encryption" \
    --key-usage ENCRYPT_DECRYPT \
    --customer-master-key-spec SYMMETRIC_DEFAULT

# Store the key ID for later use
KEY_ID=$(aws kms list-keys --query "Keys[?contains(KeyArn, 'Key for
 DynamoDB')].KeyId" --output text)

# Step 2: Create a table with the customer managed key
aws dynamodb create-table \
    --table-name SensitiveData \
    --attribute-definitions \
        AttributeName=RecordID,AttributeType=S \
    --key-schema \
        AttributeName=RecordID,KeyType=HASH \
    --billing-mode PAY_PER_REQUEST \
    --sse-specification Enabled=true,SSEType=KMS,KMSMasterKeyId=$KEY_ID
```

Actualice el cifrado de la tabla.

```
# Update a table to use a different KMS key
aws dynamodb update-table \
    --table-name CustomerData \
    --sse-specification Enabled=true,SSEType=KMS,KMSMasterKeyId=$KEY_ID
```

Describa el cifrado de la tabla.

```
# Describe the table to see encryption settings
aws dynamodb describe-table \
    --table-name CustomerData \
    --query "Table.SSEDescription"
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreateKey
  - CreateTable
  - DescribeTable
  - UpdateTable

Ejemplos de Lightsail que utilizan la AWS CLI con el script Bash

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante AWS Command Line Interface con el script Bash con Lightsail.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica a través de llamadas a varias funciones dentro del servicio o combinado con otros Servicios de AWS.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Escenarios

Escenarios

Empiece a utilizar Lightsail

En el siguiente ejemplo de código, se muestra cómo:

- Exploración de los esquemas y las agrupaciones disponibles para la creación de instancias
- Creación de una instancia de Lightsail con Amazon Linux 2023
- Supervisión del estado de la instancia hasta que esté en ejecución
- Descarga del par de claves predeterminado para el acceso de SSH
- Creación y asociación de un disco de almacenamiento de bloques adicional
- Creación de una instantánea de instancia para copia de seguridad
- Eliminación de los recursos para evitar cargos continuos

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Encuentre el ejemplo completo y obtenga información sobre cómo configurarlo y ejecutarlo en el repositorio de Tutoriales para desarrolladores de ejemplo.

```
#!/bin/bash

# Amazon Lightsail Getting Started CLI Script
# This script demonstrates how to create and manage Lightsail resources using the
 AWS CLI

# FIXES APPLIED:
# 1. Added polling mechanism to check disk state before attaching
# 2. Added polling mechanism to check snapshot state before proceeding with cleanup
# 3. Set AWS_REGION variable to us-west-2 for consistent region usage

# Set AWS region
export AWS_REGION="us-west-2"
echo "Using AWS region: $AWS_REGION"

# Set up logging
LOG_FILE="lightsail-script.log"
```

```
exec > >(tee -a "$LOG_FILE") 2>&1

echo "Starting Lightsail Getting Started script at $(date)"

# Error handling function
handle_error() {
  echo "ERROR: $1"
  echo "Attempting to clean up resources..."
  cleanup_resources
  exit 1
}

# Function to check if a command succeeded
check_status() {
  if [ $? -ne 0 ]; then
    handle_error "$1"
  fi
}

# Generate a random identifier for resource names
RANDOM_ID=$(openssl rand -hex 4)
INSTANCE_NAME="LightsailInstance-${RANDOM_ID}"
DISK_NAME="LightsailDisk-${RANDOM_ID}"
SNAPSHOT_NAME="LightsailSnapshot-${RANDOM_ID}"

# Array to track created resources
declare -a CREATED_RESOURCES

# Function to add a resource to the tracking array
track_resource() {
  CREATED_RESOURCES+=("$1:$2")
  echo "Created $1: $2"
}

# Function to clean up resources
cleanup_resources() {
  echo "Resources created by this script:"
  for resource in "${CREATED_RESOURCES[@]}"; do
    echo "  $resource"
  done

  # Reverse the array to delete resources in reverse order
  for (( idx=${#CREATED_RESOURCES[@]}-1 ; idx>=0 ; idx-- )); do
    IFS=':' read -r type name <<< "${CREATED_RESOURCES[idx]}"
```

```
    case "$type" in
      "instance_snapshot")
        echo "Deleting instance snapshot: $name"
        aws lightsail delete-instance-snapshot --instance-snapshot-name "$name" --
region $AWS_REGION
        ;;
      "disk_snapshot")
        echo "Deleting disk snapshot: $name"
        aws lightsail delete-disk-snapshot --disk-snapshot-name "$name" --region
 $AWS_REGION
        ;;
      "disk")
        echo "Detaching disk: $name"
        aws lightsail detach-disk --disk-name "$name" --region $AWS_REGION
        sleep 10 # Wait for detach to complete
        echo "Deleting disk: $name"
        aws lightsail delete-disk --disk-name "$name" --region $AWS_REGION
        ;;
      "instance")
        echo "Deleting instance: $name"
        # Check instance state before attempting to delete
        INSTANCE_STATE=$(aws lightsail get-instance-state --instance-name "$name" --
region $AWS_REGION --query 'state.name' --output text 2>/dev/null)
        if [ "$INSTANCE_STATE" == "pending" ]; then
          echo "Instance is in pending state. Waiting for it to be ready before
 deleting..."
          MAX_WAIT=30
          WAITED=0
          while [ "$INSTANCE_STATE" == "pending" ] && [ $WAITED -lt $MAX_WAIT ]; do
            sleep 10
            WAITED=$((WAITED+1))
            INSTANCE_STATE=$(aws lightsail get-instance-state --instance-name
 "$name" --region $AWS_REGION --query 'state.name' --output text 2>/dev/null)
            echo "Instance state: $INSTANCE_STATE"
          done
        fi
        aws lightsail delete-instance --instance-name "$name" --region $AWS_REGION
        ;;
    esac
  done

  echo "Cleanup completed"
}
```

```
# Step 1: Verify AWS CLI configuration
echo "Step 1: Verifying AWS CLI configuration"
aws configure list
check_status "Failed to verify AWS CLI configuration"

# Step 2: Get available blueprints and bundles
echo "Step 2: Getting available blueprints and bundles"
echo "Available blueprints (showing first 5):"
aws lightsail get-blueprints --region $AWS_REGION --query 'blueprints[0:5].
[blueprintId,name]' --output table
check_status "Failed to get blueprints"

echo "Available bundles (showing first 5):"
aws lightsail get-bundles --region $AWS_REGION --query 'bundles[0:5].
[bundleId,name,price]' --output table
check_status "Failed to get bundles"

# Get available regions and availability zones
echo "Getting available regions and availability zones"
# Use a specific availability zone in us-west-2 region
AVAILABILITY_ZONE="us-west-2a"
echo "Using availability zone: $AVAILABILITY_ZONE"

# Step 3: Create a Lightsail instance
echo "Step 3: Creating Lightsail instance: $INSTANCE_NAME"
aws lightsail create-instances \
  --instance-names "$INSTANCE_NAME" \
  --availability-zone "$AVAILABILITY_ZONE" \
  --blueprint-id amazon_linux_2023 \
  --bundle-id nano_3_0 \
  --region $AWS_REGION
check_status "Failed to create Lightsail instance"
track_resource "instance" "$INSTANCE_NAME"

# Wait for the instance to be in a running state
echo "Waiting for instance to be in running state..."
# Wait for the instance to be ready (polling approach)
MAX_ATTEMPTS=30
ATTEMPTS=0
while [ $ATTEMPTS -lt $MAX_ATTEMPTS ]; do
  STATUS=$(aws lightsail get-instance-state --instance-name "$INSTANCE_NAME" --
region $AWS_REGION --query 'state.name' --output text)
  if [ "$STATUS" == "running" ]; then
```

```
    echo "Instance is now running"
    break
  fi
  echo "Instance status: $STATUS. Waiting..."
  ATTEMPTS=$((ATTEMPTS+1))
  sleep 10
done

if [ $ATTEMPTS -eq $MAX_ATTEMPTS ]; then
  handle_error "Instance failed to reach running state after 5 minutes"
fi

# Get instance details
echo "Getting instance details"
INSTANCE_IP=$(aws lightsail get-instance --instance-name "$INSTANCE_NAME" --region
 $AWS_REGION --query 'instance.publicIpAddress' --output text)
check_status "Failed to get instance IP address"
echo "Instance IP address: $INSTANCE_IP"

# Step 4: Download the default key pair
echo "Step 4: Downloading default key pair"
KEY_FILE="lightsail_key_${RANDOM_ID}.pem"
aws lightsail download-default-key-pair --region $AWS_REGION --output text >
 "$KEY_FILE"
check_status "Failed to download key pair"
chmod 400 "$KEY_FILE"
check_status "Failed to set permissions on key pair"
echo "Key pair downloaded to $KEY_FILE"

echo "To connect to your instance, use:"
echo "ssh -i $KEY_FILE ec2-user@$INSTANCE_IP"

# Step 5: Create a block storage disk
echo "Step 5: Creating block storage disk: $DISK_NAME"
aws lightsail create-disk \
  --disk-name "$DISK_NAME" \
  --availability-zone "$AVAILABILITY_ZONE" \
  --size-in-gb 8 \
  --region $AWS_REGION
check_status "Failed to create disk"
track_resource "disk" "$DISK_NAME"

# FIX: Wait for the disk to be available using polling instead of fixed sleep
echo "Waiting for disk to be available..."
```

```
MAX_ATTEMPTS=30
ATTEMPTS=0
while [ $ATTEMPTS -lt $MAX_ATTEMPTS ]; do
  DISK_STATE=$(aws lightsail get-disk --disk-name "$DISK_NAME" --region $AWS_REGION
 --query 'disk.state' --output text 2>/dev/null)
  if [ "$DISK_STATE" == "available" ]; then
    echo "Disk is now available"
    break
  fi
  echo "Disk status: $DISK_STATE. Waiting..."
  ATTEMPTS=$((ATTEMPTS+1))
  sleep 10
done

if [ $ATTEMPTS -eq $MAX_ATTEMPTS ]; then
  handle_error "Disk failed to become available after 5 minutes"
fi

# Attach the disk to the instance
echo "Attaching disk to instance"
aws lightsail attach-disk \
  --disk-name "$DISK_NAME" \
  --instance-name "$INSTANCE_NAME" \
  --disk-path /dev/xvdf \
  --region $AWS_REGION
check_status "Failed to attach disk to instance"

echo "Disk attached. To format and mount the disk, connect to your instance and
 run:"
echo "sudo mkfs -t ext4 /dev/xvdf"
echo "sudo mkdir -p /mnt/my-data"
echo "sudo mount /dev/xvdf /mnt/my-data"
echo "sudo chown ec2-user:ec2-user /mnt/my-data"

# Step 6: Create a snapshot of the instance
echo "Step 6: Creating snapshot of the instance: $SNAPSHOT_NAME"
aws lightsail create-instance-snapshot \
  --instance-name "$INSTANCE_NAME" \
  --instance-snapshot-name "$SNAPSHOT_NAME" \
  --region $AWS_REGION
check_status "Failed to create instance snapshot"
track_resource "instance_snapshot" "$SNAPSHOT_NAME"

# FIX: Wait for the snapshot to complete using polling instead of fixed sleep
```

```
echo "Waiting for snapshot to complete... (this may take several minutes)"
MAX_ATTEMPTS=60  # Increased timeout for snapshot creation
ATTEMPTS=0
while [ $ATTEMPTS -lt $MAX_ATTEMPTS ]; do
  SNAPSHOT_STATE=$(aws lightsail get-instance-snapshot --instance-snapshot-name
 "$SNAPSHOT_NAME" --region $AWS_REGION --query 'instanceSnapshot.state' --output
 text 2>/dev/null)
  if [ "$SNAPSHOT_STATE" == "completed" ]; then
    echo "Snapshot creation completed"
    break
  fi
  echo "Snapshot status: $SNAPSHOT_STATE. Waiting... ($ATTEMPTS/$MAX_ATTEMPTS)"
  ATTEMPTS=$((ATTEMPTS+1))
  sleep 10
done

if [ $ATTEMPTS -eq $MAX_ATTEMPTS ]; then
  echo "Warning: Snapshot creation is taking longer than expected but will continue
 in the background."
  echo "You can check its status later with: aws lightsail get-instance-snapshot --
instance-snapshot-name $SNAPSHOT_NAME --region $AWS_REGION"
fi

# Step 7: Clean up resources
echo "Step 7: Clean up resources"
echo "The script has created the following resources:"
for resource in "${CREATED_RESOURCES[@]}"; do
  echo "  $resource"
done

read -p "Do you want to clean up these resources? (y/n): " CLEANUP_CONFIRM
if [[ "$CLEANUP_CONFIRM" == "y" || "$CLEANUP_CONFIRM" == "Y" ]]; then
  cleanup_resources
else
  echo "Resources will not be cleaned up. You can manually delete them later."
  echo "To clean up manually, use the following commands:"
  echo "aws lightsail delete-instance-snapshot --instance-snapshot-name
 $SNAPSHOT_NAME --region $AWS_REGION"
  echo "aws lightsail detach-disk --disk-name $DISK_NAME --region $AWS_REGION"
  echo "aws lightsail delete-disk --disk-name $DISK_NAME --region $AWS_REGION"
  echo "aws lightsail delete-instance --instance-name $INSTANCE_NAME --region
 $AWS_REGION"
fi
```

```
echo "Script completed at $(date)"
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - AttachDisk
  - CreateDisk
  - CreateInstanceSnapshot
  - CreateInstances
  - DeleteDisk
  - DeleteInstance
  - DeleteInstanceSnapshot
  - DetachDisk
  - DownloadDefaultKeyPair
  - GetBlueprints
  - GetBundles
  - GetDisk
  - GetInstance
  - GetInstanceSnapshot
  - GetInstanceState

Ejemplos de Amazon S3 que utilizan la AWS CLI con el script Bash

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante AWS Command Line Interface con el script Bash con Amazon S3.

Los conceptos básicos son ejemplos de código que muestran cómo realizar las operaciones esenciales dentro de un servicio.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica a través de llamadas a varias funciones dentro del servicio o combinado con otros Servicios de AWS.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Conceptos básicos
- Acciones
- Escenarios

Conceptos básicos

Conceptos básicos

En el siguiente ejemplo de código, se muestra cómo:

- Creación de un bucket y cargar un archivo en el bucket.
- Descargar un objeto desde un bucket.
- Copiar un objeto en una subcarpeta de un bucket.
- Obtención de una lista de los objetos de un bucket.
- Eliminación del bucket y todos los objetos que incluye.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function s3_getting_started
#
# This function creates, copies, and deletes S3 buckets and objects.
#
# Returns:
#       0 - If successful.
#       1 - If an error occurred.
###############################################################################
function s3_getting_started() {
```

```
{
  if [ "$BUCKET_OPERATIONS_SOURCED" != "True" ]; then
    cd bucket-lifecycle-operations || exit

    source ./bucket_operations.sh
    cd ..
  fi
}

echo_repeat "*" 88
echo "Welcome to the Amazon S3 getting started demo."
echo_repeat "*" 88
  echo "A unique bucket will be created by appending a Universally Unique
Identifier to a bucket name prefix."
  echo -n "Enter a prefix for the S3 bucket that will be used in this demo: "
  get_input
  bucket_name_prefix=$get_input_result
local bucket_name
bucket_name=$(generate_random_name "$bucket_name_prefix")

local region_code
region_code=$(aws configure get region)

if create_bucket -b "$bucket_name" -r "$region_code"; then
  echo "Created demo bucket named $bucket_name"
else
  errecho "The bucket failed to create. This demo will exit."
  return 1
fi

local file_name
while [ -z "$file_name" ]; do
  echo -n "Enter a file you want to upload to your bucket: "
  get_input
  file_name=$get_input_result

  if [ ! -f "$file_name" ]; then
    echo "Could not find file $file_name. Are you sure it exists?"
    file_name=""
  fi
done

local key
key="$(basename "$file_name")"
```

```
  local result=0
  if copy_file_to_bucket "$bucket_name" "$file_name" "$key"; then
    echo "Uploaded file $file_name into bucket $bucket_name with key $key."
  else
    result=1
  fi

  local destination_file
  destination_file="$file_name.download"
  if yes_no_input "Would you like to download $key to the file $destination_file?
 (y/n) "; then
    if download_object_from_bucket "$bucket_name" "$destination_file" "$key"; then
      echo "Downloaded $key in the bucket $bucket_name to the file
 $destination_file."
    else
      result=1
    fi
  fi

  if yes_no_input "Would you like to copy $key a new object key in your bucket? (y/
n) "; then
    local to_key
    to_key="demo/$key"
    if copy_item_in_bucket "$bucket_name" "$key" "$to_key"; then
      echo "Copied $key in the bucket $bucket_name to the  $to_key."
    else
      result=1
    fi
  fi

  local bucket_items
  bucket_items=$(list_items_in_bucket "$bucket_name")

  # shellcheck disable=SC2181
  if [[ $? -ne 0 ]]; then
    result=1
  fi

  echo "Your bucket contains the following items."
  echo -e "Name\t\tSize"
  echo "$bucket_items"
```

```
  if yes_no_input "Delete the bucket, $bucket_name, as well as the objects in it?
 (y/n) "; then
    bucket_items=$(echo "$bucket_items" | cut -f 1)

    if delete_items_in_bucket "$bucket_name" "$bucket_items"; then
      echo "The following items were deleted from the bucket $bucket_name"
      echo "$bucket_items"
    else
      result=1
    fi

    if delete_bucket "$bucket_name"; then
      echo "Deleted the bucket $bucket_name"
    else
      result=1
    fi
  fi

  return $result
}
```

Las funciones de Amazon S3 utilizadas en este escenario.

```
##############################################################################
# function create-bucket
#
# This function creates the specified bucket in the specified AWS Region, unless
# it already exists.
#
# Parameters:
#       -b bucket_name  -- The name of the bucket to create.
#       -r region_code  -- The code for an AWS Region in which to
#                          create the bucket.
#
# Returns:
#       The URL of the bucket that was created.
#     And:
#       0 - If successful.
#       1 - If it fails.
##############################################################################
function create_bucket() {
  local bucket_name region_code response
```

```
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function create_bucket"
    echo "Creates an Amazon S3 bucket. You must supply a bucket name:"
    echo "  -b bucket_name    The name of the bucket. It must be globally unique."
    echo "  [-r region_code]    The code for an AWS Region in which the bucket is
 created."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "b:r:h" option; do
    case "${option}" in
      b) bucket_name="${OPTARG}" ;;
      r) region_code="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done

  if [[ -z "$bucket_name" ]]; then
    errecho "ERROR: You must provide a bucket name with the -b parameter."
    usage
    return 1
  fi

  local bucket_config_arg
  # A location constraint for "us-east-1" returns an error.
  if [[ -n "$region_code" ]] && [[ "$region_code" != "us-east-1" ]]; then
    bucket_config_arg="--create-bucket-configuration LocationConstraint=
$region_code"
  fi

  iecho "Parameters:\n"
  iecho "    Bucket name:   $bucket_name"
```

```
  iecho "    Region code:   $region_code"
  iecho ""

  # If the bucket already exists, we don't want to try to create it.
  if (bucket_exists "$bucket_name"); then
    errecho "ERROR: A bucket with that name already exists. Try again."
    return 1
  fi

  # shellcheck disable=SC2086
  response=$(aws s3api create-bucket \
    --bucket "$bucket_name" \
    $bucket_config_arg)

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports create-bucket operation failed.\n$response"
    return 1
  fi
}

################################################################################
# function copy_file_to_bucket
#
# This function creates a file in the specified bucket.
#
# Parameters:
#       $1 - The name of the bucket to copy the file to.
#       $2 - The path and file name of the local file to copy to the bucket.
#       $3 - The key (name) to call the copy of the file in the bucket.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
################################################################################
function copy_file_to_bucket() {
  local response bucket_name source_file destination_file_name
  bucket_name=$1
  source_file=$2
  destination_file_name=$3

  response=$(aws s3api put-object \
    --bucket "$bucket_name" \
    --body "$source_file" \
```

```
    --key "$destination_file_name")

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports put-object operation failed.\n$response"
    return 1
  fi
}

################################################################################
# function download_object_from_bucket
#
# This function downloads an object in a bucket to a file.
#
# Parameters:
#       $1 - The name of the bucket to download the object from.
#       $2 - The path and file name to store the downloaded bucket.
#       $3 - The key (name) of the object in the bucket.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
################################################################################
function download_object_from_bucket() {
  local bucket_name=$1
  local destination_file_name=$2
  local object_name=$3
  local response

  response=$(aws s3api get-object \
    --bucket "$bucket_name" \
    --key "$object_name" \
    "$destination_file_name")

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports put-object operation failed.\n$response"
    return 1
  fi
}

################################################################################
# function copy_item_in_bucket
#
```

```
# This function creates a copy of the specified file in the same bucket.
#
# Parameters:
#       $1 - The name of the bucket to copy the file from and to.
#       $2 - The key of the source file to copy.
#       $3 - The key of the destination file.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function copy_item_in_bucket() {
  local bucket_name=$1
  local source_key=$2
  local destination_key=$3
  local response

  response=$(aws s3api copy-object \
    --bucket "$bucket_name" \
    --copy-source "$bucket_name/$source_key" \
    --key "$destination_key")

  # shellcheck disable=SC2181
  if [[ $? -ne 0 ]]; then
    errecho "ERROR:  AWS reports s3api copy-object operation failed.\n$response"
    return 1
  fi
}

###############################################################################
# function list_items_in_bucket
#
# This function displays a list of the files in the bucket with each file's
# size. The function uses the --query parameter to retrieve only the key and
# size fields from the Contents collection.
#
# Parameters:
#       $1 - The name of the bucket.
#
# Returns:
#       The list of files in text format.
#     And:
#       0 - If successful.
#       1 - If it fails.
```

```
################################################################################
function list_items_in_bucket() {
  local bucket_name=$1
  local response

  response=$(aws s3api list-objects \
    --bucket "$bucket_name" \
    --output text \
    --query 'Contents[].{Key: Key, Size: Size}')

  # shellcheck disable=SC2181
  if [[ ${?} -eq 0 ]]; then
    echo "$response"
  else
    errecho "ERROR: AWS reports s3api list-objects operation failed.\n$response"
    return 1
  fi
}

################################################################################
# function delete_items_in_bucket
#
# This function deletes the specified list of keys from the specified bucket.
#
# Parameters:
#       $1 - The name of the bucket.
#       $2 - A list of keys in the bucket to delete.

# Returns:
#       0 - If successful.
#       1 - If it fails.
################################################################################
function delete_items_in_bucket() {
  local bucket_name=$1
  local keys=$2
  local response

  # Create the JSON for the items to delete.
  local delete_items
  delete_items="{\"Objects\":["
  for key in $keys; do
    delete_items="$delete_items{\"Key\": \"$key\"},"
  done
  delete_items=${delete_items%?} # Remove the final comma.
```

```
  delete_items="$delete_items]}"

  response=$(aws s3api delete-objects \
    --bucket "$bucket_name" \
    --delete "$delete_items")

  # shellcheck disable=SC2181
  if [[ $? -ne 0 ]]; then
    errecho "ERROR:  AWS reports s3api delete-object operation failed.\n$response"
    return 1
  fi
}

################################################################################
# function delete_bucket
#
# This function deletes the specified bucket.
#
# Parameters:
#       $1 - The name of the bucket.

# Returns:
#       0 - If successful.
#       1 - If it fails.
################################################################################
function delete_bucket() {
  local bucket_name=$1
  local response

  response=$(aws s3api delete-bucket \
    --bucket "$bucket_name")

  # shellcheck disable=SC2181
  if [[ $? -ne 0 ]]; then
    errecho "ERROR: AWS reports s3api delete-bucket failed.\n$response"
    return 1
  fi
}
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CopyObject

- CreateBucket
- DeleteBucket
- DeleteObjects
- GetObject
- ListObjectsV2
- PutObject

Acciones

`CopyObject`

En el siguiente ejemplo de código, se muestra cómo utilizar `CopyObject`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
##############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

##############################################################################
# function copy_item_in_bucket
#
# This function creates a copy of the specified file in the same bucket.
#
# Parameters:
#       $1 - The name of the bucket to copy the file from and to.
#       $2 - The key of the source file to copy.
#       $3 - The key of the destination file.
```

```
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function copy_item_in_bucket() {
  local bucket_name=$1
  local source_key=$2
  local destination_key=$3
  local response

  response=$(aws s3api copy-object \
    --bucket "$bucket_name" \
    --copy-source "$bucket_name/$source_key" \
    --key "$destination_key")

  # shellcheck disable=SC2181
  if [[ $? -ne 0 ]]; then
    errecho "ERROR:  AWS reports s3api copy-object operation failed.\n$response"
    return 1
  fi
}
```

- Para obtener información sobre la API, consulte CopyObject en la Referencia de comandos de AWS CLI.

`CreateBucket`

En el siguiente ejemplo de código, se muestra cómo utilizar `CreateBucket`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function iecho
```

```
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function create-bucket
#
# This function creates the specified bucket in the specified AWS Region, unless
# it already exists.
#
# Parameters:
#       -b bucket_name  -- The name of the bucket to create.
#       -r region_code  -- The code for an AWS Region in which to
#                          create the bucket.
#
# Returns:
#       The URL of the bucket that was created.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function create_bucket() {
  local bucket_name region_code response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function create_bucket"
    echo "Creates an Amazon S3 bucket. You must supply a bucket name:"
```

```
    echo "  -b bucket_name    The name of the bucket. It must be globally unique."
    echo "  [-r region_code]    The code for an AWS Region in which the bucket is
 created."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "b:r:h" option; do
    case "${option}" in
      b) bucket_name="${OPTARG}" ;;
      r) region_code="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done

  if [[ -z "$bucket_name" ]]; then
    errecho "ERROR: You must provide a bucket name with the -b parameter."
    usage
    return 1
  fi

  local bucket_config_arg
  # A location constraint for "us-east-1" returns an error.
  if [[ -n "$region_code" ]] && [[ "$region_code" != "us-east-1" ]]; then
    bucket_config_arg="--create-bucket-configuration LocationConstraint=
$region_code"
  fi

  iecho "Parameters:\n"
  iecho "    Bucket name:   $bucket_name"
  iecho "    Region code:   $region_code"
  iecho ""

  # If the bucket already exists, we don't want to try to create it.
  if (bucket_exists "$bucket_name"); then
    errecho "ERROR: A bucket with that name already exists. Try again."
```

```
    return 1
  fi

  # shellcheck disable=SC2086
  response=$(aws s3api create-bucket \
    --bucket "$bucket_name" \
    $bucket_config_arg)

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports create-bucket operation failed.\n$response"
    return 1
  fi
}
```

- Para obtener información sobre la API, consulte CreateBucket en la Referencia de comandos de AWS CLI.

`DeleteBucket`

En el siguiente ejemplo de código, se muestra cómo utilizar `DeleteBucket`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
```

```
# function delete_bucket
#
# This function deletes the specified bucket.
#
# Parameters:
#       $1 - The name of the bucket.

# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function delete_bucket() {
  local bucket_name=$1
  local response

  response=$(aws s3api delete-bucket \
    --bucket "$bucket_name")

  # shellcheck disable=SC2181
  if [[ $? -ne 0 ]]; then
    errecho "ERROR: AWS reports s3api delete-bucket failed.\n$response"
    return 1
  fi
}
```

- Para obtener información sobre la API, consulte DeleteBucket en la Referencia de comandos de AWS CLI.

`DeleteObject`

En el siguiente ejemplo de código, se muestra cómo utilizar `DeleteObject`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
##############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

##############################################################################
# function delete_item_in_bucket
#
# This function deletes the specified file from the specified bucket.
#
# Parameters:
#       $1 - The name of the bucket.
#       $2 - The key (file name) in the bucket to delete.

# Returns:
#       0 - If successful.
#       1 - If it fails.
##############################################################################
function delete_item_in_bucket() {
  local bucket_name=$1
  local key=$2
  local response

  response=$(aws s3api delete-object \
    --bucket "$bucket_name" \
    --key "$key")

  # shellcheck disable=SC2181
  if [[ $? -ne 0 ]]; then
    errecho "ERROR:  AWS reports s3api delete-object operation failed.\n$response"
    return 1
  fi
}
```

- Para obtener información sobre la API, consulte DeleteObject en la Referencia de comandos de AWS CLI.

`DeleteObjects`

En el siguiente ejemplo de código, se muestra cómo utilizar `DeleteObjects`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function delete_items_in_bucket
#
# This function deletes the specified list of keys from the specified bucket.
#
# Parameters:
#       $1 - The name of the bucket.
#       $2 - A list of keys in the bucket to delete.

# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function delete_items_in_bucket() {
  local bucket_name=$1
  local keys=$2
  local response

  # Create the JSON for the items to delete.
  local delete_items
  delete_items="{\"Objects\":["
  for key in $keys; do
```

```
    delete_items="$delete_items{\"Key\": \"$key\"},"
  done
  delete_items=${delete_items%?} # Remove the final comma.
  delete_items="$delete_items]}"

  response=$(aws s3api delete-objects \
    --bucket "$bucket_name" \
    --delete "$delete_items")

  # shellcheck disable=SC2181
  if [[ $? -ne 0 ]]; then
    errecho "ERROR:  AWS reports s3api delete-object operation failed.\n$response"
    return 1
  fi
}
```

- Para obtener información sobre la API, consulte DeleteObjects en la Referencia de comandos de AWS CLI.

`GetObject`

En el siguiente ejemplo de código, se muestra cómo utilizar `GetObject`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
##############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}
```

```
##############################################################################
# function download_object_from_bucket
#
# This function downloads an object in a bucket to a file.
#
# Parameters:
#       $1 - The name of the bucket to download the object from.
#       $2 - The path and file name to store the downloaded bucket.
#       $3 - The key (name) of the object in the bucket.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
##############################################################################
function download_object_from_bucket() {
  local bucket_name=$1
  local destination_file_name=$2
  local object_name=$3
  local response

  response=$(aws s3api get-object \
    --bucket "$bucket_name" \
    --key "$object_name" \
    "$destination_file_name")

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports put-object operation failed.\n$response"
    return 1
  fi
}
```

- Para obtener información sobre la API, consulte GetObject en la Referencia de comandos de AWS CLI.

`HeadBucket`

En el siguiente ejemplo de código, se muestra cómo utilizar `HeadBucket`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
# function bucket_exists
#
# This function checks to see if the specified bucket already exists.
#
# Parameters:
#       $1 - The name of the bucket to check.
#
# Returns:
#       0 - If the bucket already exists.
#       1 - If the bucket doesn't exist.
##############################################################################
function bucket_exists() {
  local bucket_name
  bucket_name=$1

  # Check whether the bucket already exists.
  # We suppress all output - we're interested only in the return code.

  if aws s3api head-bucket \
    --bucket "$bucket_name" \
    >/dev/null 2>&1; then
    return 0 # 0 in Bash script means true.
  else
    return 1 # 1 in Bash script means false.
  fi
}
```

- Para obtener información sobre la API, consulte HeadBucket en la Referencia de comandos de AWS CLI.

`ListObjectsV2`

En el siguiente ejemplo de código, se muestra cómo utilizar `ListObjectsV2`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
##############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

##############################################################################
# function list_items_in_bucket
#
# This function displays a list of the files in the bucket with each file's
# size. The function uses the --query parameter to retrieve only the key and
# size fields from the Contents collection.
#
# Parameters:
#       $1 - The name of the bucket.
#
# Returns:
#       The list of files in text format.
#     And:
#       0 - If successful.
#       1 - If it fails.
##############################################################################
function list_items_in_bucket() {
  local bucket_name=$1
  local response

  response=$(aws s3api list-objects \
    --bucket "$bucket_name" \
```

```
    --output text \
    --query 'Contents[].{Key: Key, Size: Size}')

  # shellcheck disable=SC2181
  if [[ ${?} -eq 0 ]]; then
    echo "$response"
  else
    errecho "ERROR: AWS reports s3api list-objects operation failed.\n$response"
    return 1
  fi
}
```

- Para obtener información sobre la API, consulte ListObjectsV2 en la Referencia de comandos de AWS CLI.

`PutObject`

En el siguiente ejemplo de código, se muestra cómo utilizar `PutObject`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
##############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
##############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

##############################################################################
# function copy_file_to_bucket
#
# This function creates a file in the specified bucket.
```

```
#
# Parameters:
#       $1 - The name of the bucket to copy the file to.
#       $2 - The path and file name of the local file to copy to the bucket.
#       $3 - The key (name) to call the copy of the file in the bucket.
#
# Returns:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function copy_file_to_bucket() {
  local response bucket_name source_file destination_file_name
  bucket_name=$1
  source_file=$2
  destination_file_name=$3

  response=$(aws s3api put-object \
    --bucket "$bucket_name" \
    --body "$source_file" \
    --key "$destination_file_name")

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports put-object operation failed.\n$response"
    return 1
  fi
}
```

- Para obtener información sobre la API, consulte PutObject en la Referencia de comandos de AWS CLI.

Escenarios

Introducción a S3

En el siguiente ejemplo de código, se muestra cómo:

- Creación de un bucket de S3 con un nombre y una configuración regional únicos
- Configuración de los ajustes de seguridad del bucket, incluido el bloqueo del acceso público
- Habilitación del control de versiones y el cifrado predeterminado para la protección de datos

- Carga de objetos con y sin metadatos personalizados
- Descarga de objetos del bucket al almacenamiento local
- Copia de objetos dentro del bucket para organizar los datos en carpetas
- Muestra del contenido y los objetos del bucket con prefijos específicos
- Agregación de etiquetas a los buckets para la administración de los recursos
- Eliminación de todos los recursos, incluidos los objetos versionados

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Encuentre el ejemplo completo y obtenga información sobre cómo configurarlo y ejecutarlo en el repositorio de Tutoriales para desarrolladores de ejemplo.

```
#!/bin/bash

# Amazon S3 Getting Started Tutorial Script
# This script demonstrates basic S3 operations including:
# - Creating a bucket
# - Configuring bucket settings
# - Uploading, downloading, and copying objects
# - Deleting objects and buckets

# Latest fixes:
# 1. Fixed folder creation using temporary file
# 2. Corrected versioned object deletion in cleanup
# 3. Improved error handling for cleanup operations

# Set up error handling
set -e
trap 'cleanup_handler $?' EXIT

# Log file setup
LOG_FILE="s3-tutorial-$(date +%Y%m%d-%H%M%S).log"
exec > >(tee -a "$LOG_FILE") 2>&1

# Function to log messages
log() {
```

```
    echo "[$(date +"%Y-%m-%d %H:%M:%S")] $1"
}

# Function to handle errors
handle_error() {
    log "ERROR: $1"
    exit 1
}

# Function to check if a bucket exists
bucket_exists() {
    if aws s3api head-bucket --bucket "$1" 2>/dev/null; then
        return 0
    else
        return 1
    fi
}

# Function to delete all versions of objects in a bucket
delete_all_versions() {
    local bucket=$1
    log "Deleting all object versions from bucket $bucket..."

    # Get and delete all versions
    versions=$(aws s3api list-object-versions --bucket "$bucket" --query
 'Versions[].{Key:Key,VersionId:VersionId}' --output json 2>/dev/null)
    if [ -n "$versions" ] && [ "$versions" != "null" ]; then
        echo "{\"Objects\": $versions}" | aws s3api delete-objects --bucket
 "$bucket" --delete file:///dev/stdin >/dev/null 2>&1 || log "Warning: Some versions
 could not be deleted"
    fi

    # Get and delete all delete markers
    markers=$(aws s3api list-object-versions --bucket "$bucket" --query
 'DeleteMarkers[].{Key:Key,VersionId:VersionId}' --output json 2>/dev/null)
    if [ -n "$markers" ] && [ "$markers" != "null" ]; then
        echo "{\"Objects\": $markers}" | aws s3api delete-objects --bucket "$bucket"
 --delete file:///dev/stdin >/dev/null 2>&1 || log "Warning: Some delete markers
 could not be deleted"
    fi
}

# Function to handle cleanup on exit
cleanup_handler() {
```

```
    local exit_code=$1

    # Only run cleanup if it hasn't been run already
    if [ -z "$CLEANUP_DONE" ]; then
        cleanup
    fi

    exit $exit_code
}

# Function to clean up resources
cleanup() {
    log "Starting cleanup process..."
    CLEANUP_DONE=1

    # List all resources created for confirmation
    log "Resources created:"
    if [ -n "$BUCKET_NAME" ]; then
        log "- S3 Bucket: $BUCKET_NAME"

        # Only try to list objects if the bucket exists
        if bucket_exists "$BUCKET_NAME"; then
            # Check if any objects were created
            OBJECTS=$(aws s3api list-objects-v2 --bucket "$BUCKET_NAME" --query
 'Contents[].Key' --output text 2>/dev/null || echo "")
            if [ -n "$OBJECTS" ]; then
                log "- Objects in bucket:"
                echo "$OBJECTS" | tr '\t' '\n' | while read -r obj; do
                    log "  - $obj"
                done
            fi

            # Ask for confirmation before cleanup
            read -p "Do you want to proceed with cleanup and delete all resources?
 (y/n): " confirm
            if [[ $confirm != [yY] && $confirm != [yY][eE][sS] ]]; then
                log "Cleanup aborted by user."
                return
            fi

            # Delete all versions of objects
            delete_all_versions "$BUCKET_NAME"

            # Delete the bucket
```

```
            log "Deleting bucket $BUCKET_NAME..."
            aws s3api delete-bucket --bucket "$BUCKET_NAME" || log "Warning: Failed
 to delete bucket"
        else
            log "Bucket $BUCKET_NAME does not exist, skipping cleanup"
        fi
    fi

    # Clean up local files
    log "Removing local files..."
    rm -f sample-file.txt sample-document.txt downloaded-sample-file.txt empty-
file.tmp

    log "Cleanup completed."
}

# Generate a random bucket name
generate_bucket_name() {
    local hex_id
    hex_id=$(openssl rand -hex 6)
    echo "demo-s3-bucket-$hex_id"
}

# Main script execution
main() {
    log "Starting Amazon S3 Getting Started Tutorial"

    # Generate a unique bucket name
    BUCKET_NAME=$(generate_bucket_name)
    log "Generated bucket name: $BUCKET_NAME"

    # Step 1: Create a bucket
    log "Step 1: Creating S3 bucket..."

    # Get the current region or default to us-east-1
    REGION=$(aws configure get region)
    REGION=${REGION:-us-east-1}
    log "Using region: $REGION"

    if [ "$REGION" = "us-east-1" ]; then
        aws s3api create-bucket --bucket "$BUCKET_NAME" || handle_error "Failed to
 create bucket"
    else
        aws s3api create-bucket \
```

```
            --bucket "$BUCKET_NAME" \
            --region "$REGION" \
            --create-bucket-configuration LocationConstraint="$REGION" ||
handle_error "Failed to create bucket"
    fi
    log "Bucket created successfully"

    # Configure bucket settings
    log "Configuring bucket settings..."

    # Block public access (security best practice)
    log "Blocking public access..."
    aws s3api put-public-access-block \
        --bucket "$BUCKET_NAME" \
        --public-access-block-configuration
"BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=tr
|| handle_error "Failed to configure public access block"

    # Enable versioning
    log "Enabling versioning..."
    aws s3api put-bucket-versioning \
        --bucket "$BUCKET_NAME" \
        --versioning-configuration Status=Enabled || handle_error "Failed to enable
versioning"

    # Set default encryption
    log "Setting default encryption..."
    aws s3api put-bucket-encryption \
        --bucket "$BUCKET_NAME" \
        --server-side-encryption-configuration '{"Rules":
[{"ApplyServerSideEncryptionByDefault": {"SSEAlgorithm": "AES256"}}]}' ||
handle_error "Failed to set encryption"

    # Step 2: Upload an object
    log "Step 2: Uploading objects to bucket..."

    # Create a sample file
    echo "This is a sample file for the S3 tutorial." > sample-file.txt

    # Upload the file
    aws s3api put-object \
        --bucket "$BUCKET_NAME" \
        --key "sample-file.txt" \
        --body "sample-file.txt" || handle_error "Failed to upload object"
```

```
    log "Object uploaded successfully"

    # Upload with metadata
    echo "This is a document with metadata." > sample-document.txt
    aws s3api put-object \
        --bucket "$BUCKET_NAME" \
        --key "documents/sample-document.txt" \
        --body "sample-document.txt" \
        --content-type "text/plain" \
        --metadata "author=AWSDocumentation,purpose=tutorial" || handle_error
"Failed to upload object with metadata"
    log "Object with metadata uploaded successfully"

    # Step 3: Download an object
    log "Step 3: Downloading object from bucket..."
    aws s3api get-object \
        --bucket "$BUCKET_NAME" \
        --key "sample-file.txt" \
        "downloaded-sample-file.txt" || handle_error "Failed to download object"
    log "Object downloaded successfully"

    # Check if an object exists
    log "Checking if object exists..."
    aws s3api head-object \
        --bucket "$BUCKET_NAME" \
        --key "sample-file.txt" || handle_error "Object does not exist"
    log "Object exists"

    # Step 4: Copy object to a folder
    log "Step 4: Copying object to a folder..."

    # Create a folder structure using a temporary empty file
    log "Creating folder structure..."
    touch empty-file.tmp
    aws s3api put-object \
        --bucket "$BUCKET_NAME" \
        --key "favorite-files/" \
        --body empty-file.tmp || handle_error "Failed to create folder"

    # Copy the object
    log "Copying object..."
    aws s3api copy-object \
        --bucket "$BUCKET_NAME" \
        --copy-source "$BUCKET_NAME/sample-file.txt" \
```

```
        --key "favorite-files/sample-file.txt" || handle_error "Failed to copy
 object"
    log "Object copied successfully"

    # List objects in the bucket
    log "Listing all objects in the bucket..."
    aws s3api list-objects-v2 \
        --bucket "$BUCKET_NAME" \
        --query 'Contents[].Key' \
        --output table || handle_error "Failed to list objects"

    # List objects with a specific prefix
    log "Listing objects in the favorite-files folder..."
    aws s3api list-objects-v2 \
        --bucket "$BUCKET_NAME" \
        --prefix "favorite-files/" \
        --query 'Contents[].Key' \
        --output table || handle_error "Failed to list objects with prefix"

    # Add tags to the bucket
    log "Adding tags to the bucket..."
    aws s3api put-bucket-tagging \
        --bucket "$BUCKET_NAME" \
        --tagging 'TagSet=[{Key=Project,Value=S3Tutorial},
{Key=Environment,Value=Demo}]' || handle_error "Failed to add tags"
    log "Tags added successfully"

    log "Tutorial completed successfully!"
}

# Execute the main function
main
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CopyObject
  - CreateBucket
  - DeleteBucket
  - DeleteObjects
  - GetObject

- HeadObject
- ListObjectVersions
- ListObjectsV2
- PutBucketEncryption
- PutBucketTagging
- PutBucketVersioning
- PutObject
- PutPublicAccessBlock

Ejemplos de AWS STS que utilizan la AWS CLI con el script Bash

En los siguientes ejemplos de código, se muestra cómo realizar acciones e implementar escenarios comunes mediante AWS Command Line Interface con el script Bash con AWS STS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

En cada ejemplo se incluye un enlace al código de origen completo, con instrucciones de configuración y ejecución del código en el contexto.

Temas

- Acciones

Acciones

`AssumeRole`

En el siguiente ejemplo de código, se muestra cómo utilizar `AssumeRole`.

AWS CLI con Bash script

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function sts_assume_role
#
# This function assumes a role in the AWS account and returns the temporary
#  credentials.
#
# Parameters:
#       -n role_session_name -- The name of the session.
#       -r role_arn -- The ARN of the role to assume.
#
# Returns:
#       [access_key_id, secret_access_key, session_token]
#     And:
#       0 - If successful.
#       1 - If an error occurred.
###############################################################################
function sts_assume_role() {
  local role_session_name role_arn response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
```

```
    echo "function sts_assume_role"
    echo "Assumes a role in the AWS account and returns the temporary credentials:"
    echo "  -n role_session_name -- The name of the session."
    echo "  -r role_arn -- The ARN of the role to assume."
    echo ""
  }

  while getopts n:r:h option; do
    case "${option}" in
      n) role_session_name=${OPTARG} ;;
      r) role_arn=${OPTARG} ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done

  response=$(aws sts assume-role \
    --role-session-name "$role_session_name" \
    --role-arn "$role_arn" \
    --output text \
    --query "Credentials.[AccessKeyId, SecretAccessKey, SessionToken]")

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-role operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- Para obtener información sobre la API, consulte AssumeRole en la Referencia de comandos de la AWS CLI.

Seguridad en AWS CLI

La seguridad en la nube de AWS es la máxima prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida describe esto como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWSes responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWSProgramas de conformidad de . Para obtener información sobre los programas de conformidad que se aplican a AWS Command Line Interface, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad se determina según el servicio de AWSque utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo puede aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Command Line Interface (AWS CLI). En los siguientes temas, aprenderá a configurar AWS CLI conforme a sus objetivos de seguridad y conformidad. También aprenderá a usar la AWS CLI para que le ayude a monitorizar y proteger los recursos de AWS.

Temas

- Protección de datos en la AWS CLI
- Gestión de identidad y acceso
- Validación de la conformidad de este producto o servicio de AWS
- Resiliencia de este producto o servicio de AWS
- Seguridad de la infraestructura de este producto o servicio de AWS
- Aplicación de una versión de TLS mínima para la AWS CLI

Protección de datos en la AWS CLI

El modelo de responsabilidad compartida, y de AWS se aplica a la protección de datos de AWS Command Line Interface. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure los registros de API y de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre cómo utilizar registros de seguimiento de CloudTrail para capturar actividades de AWS, consulte Working with CloudTrail trails en la Guía del usuario de AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-3 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no ingresar nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye las situaciones en las que debe trabajar con la AWS CLI u

otros Servicios de AWS a través de la consola, la API, la AWS CLI o los SDK de AWS. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos

Una característica clave de cualquier servicio seguro es que la información se cifre cuando no se está utilizando activamente.

Cifrado en reposo

La AWS CLI no guarda ningún otro datos de los clientes salvo las credenciales necesarias para interactuar con los servicios de AWS en nombre del usuario.

Si utiliza la AWS CLI para invocar un servicio de AWS que transmita datos del cliente al equipo local para su almacenamiento, consulte el capítulo «Seguridad y conformidad» de la Guía del usuario de ese servicio para obtener información sobre cómo se almacenan, protegen y cifran esos datos.

Cifrado en tránsito

De forma predeterminada, todos los datos transmitidos desde el equipo cliente en el que se ejecuta la AWS CLI y los puntos de enlace de servicio de AWS están cifrados, ya que todo se envía a través de una conexión HTTPS/TLS.

No es necesario hacer nada para habilitar el uso de HTTPS/TLS. Siempre está habilitado, a menos que se deshabilite explícitamente para un determinado comando con la opción de línea de comandos `--no-verify-ssl`.

Gestión de identidad y acceso

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de AWS. IAM es un Servicio de AWS que se puede utilizar sin cargo adicional.

Temas

- Público

- Autenticación con identidades
- Administración del acceso con políticas
- Cómo funcionan los Servicios de AWS con IAM
- Solución de problemas de identidades y accesos en AWS

Público

La forma en que utilice AWS Identity and Access Management (IAM) difiere en función del trabajo que realice en AWS.

Usuario de servicio: si utiliza Servicios de AWS para realizar el trabajo, el administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de AWS para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en AWS, consulte Solución de problemas de identidades y accesos en AWS o la Guía del usuario del Servicio de AWS que esté usando.

Administrador de servicio: si está a cargo de los recursos de AWS en su empresa, probablemente tenga acceso completo a AWS. Su trabajo consiste en determinar a qué características y recursos de AWS deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de sus servicios. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo la empresa puede utilizar IAM con AWS, consulte la Guía del usuario del Servicio de AWS que esté usando.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a AWS. Para consultar ejemplos de políticas basadas en la identidad de AWS que puede utilizar en IAM, consulte la Guía del usuario del Servicio de AWS que esté usando.

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe autenticarse como el Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Se puede iniciar sesión como una identidad federada con las credenciales de un origen de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las

credenciales de Google/Facebook. Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en la Cuenta de AWS en la Guía del usuario de AWS Sign-In.

Para el acceso mediante programación, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Usuario raíz de la Cuenta de AWS

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario raíz de la Cuenta de AWS que tiene acceso completo a todos los Servicios de AWS y recursos. Se recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder a Servicios de AWS con credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, proveedor de identidad web o Directory Service que accede a los Servicios de AWS mediante credenciales de un origen de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte Exigir que los usuarios humanos utilicen la federación con un proveedor de identidades para acceder a AWS con credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un Rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Se puede asumir un rol cambiando de un usuario a un rol de IAM (consola) o llamando a una operación de la API de la AWS CLI o AWS. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política define los permisos cuando se asocia a una identidad o un recurso. AWS evalúa estas políticas cuando una entidad principal realiza una solicitud. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de política de permisos JSON que asocia a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden ser políticas insertadas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte Selección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se puede utilizar políticas de IAM administradas de AWS en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulta Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer el máximo de permisos concedidos por los tipos de políticas más frecuentes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations.
- Políticas de control de recursos (RCP): definen los permisos máximos disponibles para los recursos de las cuentas. Para obtener más información, consulte Políticas de control de recursos (RCP) en la Guía del usuario de AWS Organizations.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información acerca de cómo AWS decide si permitir o no una solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funcionan los Servicios de AWS con IAM

Para obtener una perspectiva general sobre cómo funcionan los Servicios de AWS con la mayoría de las características de IAM, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Para obtener información sobre cómo usar un Servicio de AWS específico con IAM, consulte la sección de seguridad de la Guía del usuario del servicio correspondiente.

Solución de problemas de identidades y accesos en AWS

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con AWS e IAM.

Temas

- No tengo autorización para realizar una acción en AWS
- No tengo autorización para realizar la operación iam:PassRole
- Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de AWS

No tengo autorización para realizar una acción en AWS

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `awes:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 awes:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `awes:`*`GetWidget`*.

Si necesita ayuda, contacte con su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No tengo autorización para realizar la operación iam:PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a AWS.

Algunos Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de AWS

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información acerca de si AWS admite estas características, consulte Cómo funcionan los Servicios de AWS con IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuenta de AWS de su propiedad, consulte Proporcionar acceso a un usuario de IAM a otra Cuentas de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a sus recursos a Cuentas de AWS de terceros, consulte Proporcionar acceso a Cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Validación de la conformidad de este producto o servicio de AWS

Para saber si un Servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte Servicios de AWS incluidos por programa de conformidad y escoja el programa de conformidad que le interese. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad de conformidad al utilizar Servicios de AWS se determina en función de la confidencialidad de los datos, los objetivos de conformidad de la empresa, así como de la legislación y los reglamentos aplicables. Para obtener más información sobre su responsabilidad en cuanto a la conformidad al utilizar los Servicios de AWS, consulte Documentación de seguridad de AWS.

Este producto o servicio de AWS sigue el modelo de responsabilidad compartida a través de los servicios específicos de Amazon Web Services (AWS) que admite. Para obtener información sobre la seguridad de los servicios de AWS, consulte la página de documentación sobre la seguridad de los servicios de AWS y los servicios de AWS sujetos a las medidas de conformidad de AWS de cada programa de conformidad.

Resiliencia de este producto o servicio de AWS

La infraestructura global de AWS está conformada por Regiones de AWS y zonas de disponibilidad.

Las Regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia.

Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las regiones y zonas de disponibilidad de AWS, consulte Infraestructura global de AWS.

Este producto o servicio de AWS sigue el modelo de responsabilidad compartida a través de los servicios específicos de Amazon Web Services (AWS) que admite. Para obtener información sobre la seguridad de los servicios de AWS, consulte la página de documentación sobre la seguridad de los servicios de AWS y los servicios de AWS sujetos a las medidas de conformidad de AWS de cada programa de conformidad.

Seguridad de la infraestructura de este producto o servicio de AWS

Este producto o servicio de AWS utiliza servicios administrados y, por lo tanto, está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de la infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas en AWS para acceder a este producto o servicio de AWS a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Este producto o servicio de AWS sigue el modelo de responsabilidad compartida a través de los servicios específicos de Amazon Web Services (AWS) que admite. Para obtener información sobre la seguridad de los servicios de AWS, consulte la página de documentación sobre la seguridad de los servicios de AWS y los servicios de AWS sujetos a las medidas de conformidad de AWS de cada programa de conformidad.

Aplicación de una versión de TLS mínima para la AWS CLI

Cuando se utiliza la AWS Command Line Interface (AWS CLI), el protocolo de seguridad de la capa de transporte (TLS) desempeña un papel crucial a la hora de proteger la comunicación entre la AWS CLI y los Servicios de AWS. Para aumentar la seguridad al comunicarse con los servicios de AWS, debe usar TLS 1.2 o una versión posterior.

La versión 2 de la AWS CLI usa un script interno de Python que se compila con el fin de usar la versión mínima de TLS 1.2 cuando el servicio con el que se comunica lo admite. Siempre que utilice la versión 2 de AWS CLI, no se necesitan más pasos para aplicar este mínimo. Para garantizar una mayor seguridad, asegúrese de actualizar a una versión reciente de la AWS CLI.

La AWS CLI y el Servicio de AWS pueden intercambiar datos de forma segura con el protocolo TLS que proporciona cifrado, autenticación e integridad de los datos. Al utilizar el protocolo TLS, la AWS CLI garantiza que sus interacciones con los Servicios de AWS estén protegidas frente el acceso no autorizado y las filtraciones de datos, lo que mejora la seguridad general de su ecosistema AWS.

El modelo de responsabilidad compartida, y de AWS se aplica a la protección de datos de AWS Command Line Interface. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Servicios de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la protección de datos, consulte the section called “Protección de los datos”.

Guía de migración para la versión 2 de la AWS CLI

Esta sección contiene instrucciones para actualizar la AWS CLI versión 1 a la AWS CLI versión 2. La versión 2 de la AWS CLI se basa en la versión 1 de la AWS CLI e incluye características y mejoras basadas en los comentarios de la comunidad. La versión 2 de la AWS CLI es la versión principal y más reciente de la AWS CLI y es compatible con todas las características más recientes. Algunas características ingresadas en la versión 2 no son compatibles con la versión 1 y debe realizar una actualización para acceder a esas características.

Para evitar problemas inesperados, antes de migrar a la versión 2, consulte las diferencias entre las versiones. La versión 2 de la AWS CLI incluye nuevas características y cambios que podrían requerir la actualización de los scripts o los comandos para obtener compatibilidad con versiones anteriores.

Las versiones 1 y 2 de la AWS CLI utilizan el mismo nombre de comando de `aws`. Si tiene ambas versiones instaladas, el equipo utiliza la primera que encuentra en la ruta de búsqueda. Esto puede provocar que el nombre de comando `aws` ejecute la versión anterior de AWS CLI, incluso si tiene instalada la versión nueva.

Para actualizar a la versión 2 de AWS CLI, siga una de las siguientes instrucciones:

- Si ha instalado previamente la versión 1 de la AWS CLI, siga las instrucciones que se indican en the section called “Instrucciones de migración”.
- Si no ha instalado previamente la versión 1 de la AWS CLI, siga las instrucciones que se indican en Introducción.

Temas

- Nuevas características y cambios en la versión 2 de la AWS CLI
- Instalación de la versión 2 de la AWS CLI a partir de la versión 1 de la AWS CLI
- Uso del modo de depuración de actualizaciones para actualizar la versión 1 de AWS CLI a la versión 2 de AWS CLI

Nuevas características y cambios en la versión 2 de la AWS CLI

En este tema se describen las nuevas características y los cambios en el comportamiento entre la versión 1 de la AWS CLI y la versión 2 de la AWS CLI. Estos cambios pueden requerir que actualice los scripts o comandos para obtener el mismo comportamiento en la versión 2 que en la versión 1.

Temas

- Nuevas características de AWS CLI versión 2
- Cambios importantes entre la AWS CLI versión 1 y la AWS CLI versión 2

Nuevas características de AWS CLI versión 2

La versión 2 de la AWS CLI es la versión principal y más reciente de la AWS CLI y es compatible con todas las características más recientes. Algunas características introducidas en la versión 2 no son compatibles con la versión 1 y debe realizar una actualización para acceder a esas características. Estas son algunas de ellas:

No se necesita intérprete de Python

La AWS CLI versión 2 no necesita una instalación por separado de Python. Incluye una versión insertada.

Asistentes

Puede utilizar un asistente con la AWS CLI versión 2. El asistente le guía por la creación de determinados comandos.

Autenticación del Centro de identidades de IAM

Si la organización utiliza AWS IAM Identity Center (IAM Identity Center), los usuarios pueden iniciar sesión en Active Directory, en un directorio de IAM Identity Center integrado o en otra IdP conectada a IAM Identity Center. A continuación, se asignan a un rol de AWS Identity and Access Management (IAM) que le permite ejecutar comandos de la AWS CLI.

Mensaje automático

Cuando se activa, la AWS CLI versión 2 le puede pedir comandos, parámetros y recursos cuando ejecute un comando de `aws`.

Ejecución de las imágenes oficiales de Amazon ECR Public o Docker para la AWS CLI

Las imágenes de Docker oficiales para la AWS CLI proporcionan aislamiento, portabilidad y seguridad que AWS apoya y mantiene directamente. De este modo, puede utilizar la AWS CLI versión 2 en un entorno basado en contenedores sin tener que administrar la instalación por su cuenta.

Paginación del lado del cliente

La AWS CLI versión 2 proporciona el uso de un programa de paginación en el cliente para la salida. De forma predeterminada, esta característica está activada y devuelve todas las salidas a través del programa de paginación predeterminado del sistema operativo.

`aws configure import`

Importe las credenciales de `.csv` generadas desde la Consola de administración de AWS. Se importa un archivo `.csv` con el nombre de perfil que coincide con el nombre de usuario de IAM.

`aws configure list-profiles`

Muestra los nombres de todos los perfiles que ha configurado.

the section called “Formato de salida de transmisión YAML ”

Los formatos `yaml` y `yaml-stream` aprovechan el formato YAML a la vez que proporcionan una visualización más receptiva de los conjuntos de datos grandes mediante el streaming de datos a usted. Puede comenzar a ver y usar datos YAML antes de que se descargue toda la consulta.

Nuevos comandos **ddb** de alto nivel para DynamoDB

La AWS CLI versión 2 tiene los comandos de alto nivel de Amazon DynamoDB `ddb put` y `ddb select`. Estos comandos proporcionan una interfaz simplificada para colocar elementos en las tablas de DynamoDB y buscar en una tabla o índice de DynamoDB.

`aws logs tail`

La AWS CLI versión 2 dispone de un comando `aws logs tail` personalizado que pone a la cola los registros de un grupo de Registros de Amazon CloudWatch. De forma predeterminada, el comando devuelve los registros de todos los flujos asociados de CloudWatch Logs durante los últimos diez minutos.

Se ha agregado compatibilidad con los metadatos para los comandos **s3** de alto nivel

La AWS CLI versión 2 agrega el parámetro `--copy-props` a los comandos `s3` de alto nivel. Con este parámetro, puede configurar metadatos y etiquetas adicionales para Amazon Simple Storage Service (Amazon S3).

`AWS_REGION`

La AWS CLI versión 2 tiene una variable de entorno compatible con SDK de AWS llamada `AWS_REGION`. Esta variable especifica a la que Región de AWS envía solicitudes. Anula la variable de entorno `AWS_DEFAULT_REGION`, que solo es aplicable en la AWS CLI.

Cambios importantes entre la AWS CLI versión 1 y la AWS CLI versión 2

En estas secciones se describen los cambios en el comportamiento entre la AWS CLI versión 1 y la AWS CLI versión 2. Estos cambios pueden requerir que actualice los scripts o comandos para obtener el mismo comportamiento en la versión 2 que en la versión 1.

Temas

- Se ha agregado una variable de entorno para establecer la codificación de los archivos de texto
- Los parámetros binarios se pasan como cadenas codificadas en base64 de forma predeterminada
- Mejora de la gestión de Amazon S3 de las propiedades y etiquetas de los archivos para las copias multiparte
- No hay recuperación automática de las URL http:// o https:// para los parámetros
- Paginador usado para toda la salida de forma predeterminada
- Los valores de salida de la marca de tiempo están estandarizados según el formato ISO 8601
- Control mejorado de las implementaciones de CloudFormation que no producen cambios
- Se ha cambiado el comportamiento predeterminado del punto de conexión regional de Amazon S3 para la región us-east-1
- Se ha cambiado el comportamiento predeterminado de los puntos de conexión de AWS STS regionales
- Se ha eliminado ecr get-login y se ha reemplazado por ecr get-login-password
- AWS CLIEl soporte de la versión 2 de la para complementos está cambiando
- Se ha eliminado la compatibilidad con los alias ocultos
- No se admite la opción api_versions del archivo de configuración
- La AWS CLI versión 2 solo usa Signature v4 para autenticar las solicitudes de Amazon S3
- La AWS CLI versión 2 es más coherente con los parámetros de paginación
- La AWS CLI versión 2 proporciona códigos de retorno más coherentes en todos los comandos

Se ha agregado una variable de entorno para establecer la codificación de los archivos de texto

De forma predeterminada, los archivos de texto de the section called “Blob” utilizan la misma codificación que la configuración regional instalada. Debido a que la AWS CLI versión 2 utiliza una versión incrustada de Python, las variables de entorno `PYTHONUTF8` y `PYTHONIOENCODING` no se

admiten. Para establecer que la codificación de los archivos de texto sea distinta de la configuración regional, utilice la variable de entorno `AWS_CLI_FILE_ENCODING`. El siguiente ejemplo establece la AWS CLI para abrir archivos de texto con `UTF-8` en Windows.

```
AWS_CLI_FILE_ENCODING=UTF-8
```

Para obtener más información, consulte Configuración de variables de entorno para la AWS CLI .

Los parámetros binarios se pasan como cadenas codificadas en base64 de forma predeterminada

En la AWS CLI, algunos comandos requerían cadenas codificadas en base64, mientras que otros requerían cadenas de bytes codificadas en UTF-8. En la AWS CLI versión 1, el paso de datos entre dos tipos de cadenas codificadas requería a menudo algún procesamiento intermedio. La AWS CLI versión 2 aumenta la coherencia de la gestión de los parámetros binarios, lo que ayuda a pasar los valores de un comando a otro de forma más fiable.

De forma predeterminada, la AWS CLI versión 2 pasa todos los parámetros binarios de entrada y salida como `blobs` (objeto grande binario) de cadena codificada en base64. Para obtener más información, consulte the section called “Blob”.

Para volver al comportamiento de la AWS CLI versión 1, utilice el archivo de configuración `cli_binary_format` o el parámetro `--cli-binary-format`.

Mejora de la gestión de Amazon S3 de las propiedades y etiquetas de los archivos para las copias multiparte

Cuando se utilizan los comandos de la AWS CLI versión 1 del espacio de nombres `aws s3` para copiar un archivo de una ubicación de bucket de S3 a otra, y esa operación utiliza la copia multiparte, no se copian las propiedades del archivo del objeto de origen en el de destino.

De forma predeterminada, los comandos correspondientes de la AWS CLI versión 2 transfieren todas las etiquetas y algunas de las propiedades de la copia de origen a la de destino. En comparación con la AWS CLI versión 1, esto puede generar más llamadas a la API de AWS en el punto de conexión de Amazon S3. Para cambiar el comportamiento predeterminado de los comandos `s3` en la AWS CLI versión 2, utilice el parámetro `--copy-props`.

Para obtener más información, consulte the section called “Propiedades de archivo y etiquetas en copias multiparte”.

No hay recuperación automática de las URL **`http://`** o **`https://`** para los parámetros

La AWS CLI versión 2 no realiza una operación `GET` cuando el valor de un parámetro empieza por `http://` o `https://`, ni utiliza el contenido devuelto como valor del parámetro. Como resultado, la opción de línea de comandos asociada `cli_follow_urlparam` se elimina de la AWS CLI versión 2.

Si necesita recuperar una URL y pasar el contenido de la URL en un valor de parámetro, le recomendamos que utilice `curl` o una herramienta similar para descargar el contenido de la URL en un archivo local. Después, use la sintaxis `file://` para leer el contenido de ese archivo y utilizarlo como valor del parámetro.

Por ejemplo, el siguiente comando ya no intenta recuperar el contenido de la página encontrada en `http://www.example.com` y pasar ese contenido como parámetro. En cambio, pasa la cadena de texto literal `https://example.com` como parámetro.

```
$ aws ssm put-parameter \
    --value http://www.example.com \
    --name prod.microservice1.db.secret \
    --type String 2
```

Si necesita recuperar y usar el contenido de la URL de una web como parámetro, puede hacer lo siguiente en la versión 2.

```
$ curl https://my.example.com/mypolicyfile.json -o mypolicyfile.json
$ aws iam put-role-policy \
    --policy-document file://./mypolicyfile.json \
    --role-name MyRole \
    --policy-name MyReadOnlyPolicy
```

En el ejemplo anterior, el parámetro `-o` indica a `curl` que guarde el archivo en la carpeta actual con el mismo nombre que el archivo de origen. El segundo comando recupera el contenido de ese archivo descargado y lo pasa como valor de `--policy-document`.

Paginador usado para toda la salida de forma predeterminada

De forma predeterminada, la AWS CLI versión 2 devuelve todas las salidas a través del paginador predeterminado de su sistema operativo. Este programa es el programa `less` en Linux o macOS, y

el programa `more` en Windows. Esto puede ayudarle a navegar por gran cantidad de resultados de un servicio al mostrar las páginas de salida de una en una.

Puede configurar la AWS CLI versión 2 para usar un programa de paginación diferente o ninguno en absoluto. Para obtener más información, consulte the section called “Paginación del lado del cliente”.

Los valores de salida de la marca de tiempo están estandarizados según el formato ISO 8601

De forma predeterminada, la AWS CLI versión 2 devuelve todos los valores de respuesta de marca temporal en formato ISO 8601. En la versión 1 de la AWS CLI, los comandos devolvían valores de marca temporal en el formato en el que estuviera la respuesta de la API HTTP, que podía ser diferente en cada servicio.

Para ver las marcas temporales en el formato devuelto por la respuesta de la API HTTP, utilice el valor `wire` en su archivo `config`. Para obtener más información, consulte `cli_timestamp_format`.

Control mejorado de las implementaciones de CloudFormation que no producen cambios

De forma predeterminada, en la AWS CLI versión 1, si implementa una plantilla de CloudFormation que no produce cambios, la AWS CLI devuelve un código de error. Esto causa problemas si no lo considera un error y quiere que su script continúe. Puede solucionar esto en la AWS CLI versión 1 si agrega la marca `--no-fail-on-empty-changeset`, que devuelve `0`.

Dado que este es un caso de uso común, la AWS CLI versión 2 devuelve de forma predeterminada un código de salida correcto `0` cuando no hay ningún cambio provocado por una implementación y la operación devuelve un conjunto de cambios vacío.

Para volver al comportamiento original, debe agregar la marca `--fail-on-empty-changeset`.

Se ha cambiado el comportamiento predeterminado del punto de conexión regional de Amazon S3 para la región **`us-east-1`**

Cuando configura la AWS CLI versión 1 para utilizar la región `us-east-1`, la AWS CLI utiliza el punto de conexión global `s3.amazonaws.com` que está alojado físicamente en la región `us-east-1`. La AWS CLI versión 2 utiliza el punto de conexión regional verdadero cuando `s3.us-east-1.amazonaws.com` se especifica esa región. Para obligar a la versión 2 de la AWS CLI a que use el punto de enlace global, puede establecer la región de un comando en `aws-global`.

Se ha cambiado el comportamiento predeterminado de los puntos de conexión de AWS STS regionales

De forma predeterminada, la AWS CLI versión 2 envía todas las solicitudes de la API AWS Security Token Service (AWS STS) al punto de conexión regional para la Región de AWS configurada actualmente.

De forma predeterminada, la versión antes de `1.42.0` para la versión 1 de AWS CLI envía las solicitudes de AWS STS al punto de conexión de AWS STS global. Puede controlar este comportamiento predeterminado en la versión 1 con la configuración `sts_regional_endpoints`.

Todas las versiones posteriores a `1.42.0` utilizan el punto de conexión regional como predeterminado. Si se migra a la versión 2 de AWS CLI desde estas versiones más recientes, este comportamiento permanece inalterado.

Se ha eliminado **`ecr get-login`** y se ha reemplazado por **`ecr get-login-password`**

La AWS CLI versión 2 reemplaza el comando `aws ecr get-login` por el comando `aws ecr get-login-password` que mejora la integración automatizada con la autenticación de contenedores.

El comando `aws ecr get-login-password` reduce el riesgo de exponer sus credenciales en la lista de procesos, historial de shell u otros archivos de registro. También mejora la compatibilidad con el comando `docker login`, lo que mejora la automatización.

El comando `aws ecr get-login-password` está disponible en la versión 1.17.10 y posterior de la AWS CLI, y versión 2 de la AWS CLI. El anterior comando `aws ecr get-login` todavía está disponible en la AWS CLI versión 1 por compatibilidad con versiones anteriores.

Con el comando `aws ecr get-login-password`, puede reemplazar el siguiente código que recupera una contraseña.

```
$ (aws ecr get-login --no-include-email)
```

Para reducir el riesgo de exponer la contraseña al historial de shell o a los registros, utilice el siguiente comando de ejemplo. En este ejemplo, la contraseña se canaliza directamente al comando `docker login`, donde se asigna al parámetro password mediante la opción `--password-stdin`.

```
$ aws ecr get-login-password | docker login --username AWS --password-stdin MY-REGISTRY-URL
```

Para obtener más información, consulte `aws ecr get-login-password` en la Guía de referencia de la AWS CLI versión 2.

AWS CLIEl soporte de la versión 2 de la para complementos está cambiando

La compatibilidad con complementos en la AWS CLI versión 2 es completamente provisional y está destinada a ayudar a los usuarios a migrar desde la AWS CLI versión 1 hasta que se lance una interfaz estable y actualizada. No hay garantías de que un complemento en particular o incluso la interfaz de complementos de la AWS CLI sean compatibles en futuras versiones de la AWS CLI versión 2. Si se basa en complementos, asegúrese de bloquear una versión concreta de la AWS CLI y probar la funcionalidad de su complemento cuando realice la actualización.

Para habilitar el soporte de complementos, cree una sección `[plugins]` en su `~/.aws/config`.

```
[plugins]
cli_legacy_plugin_path = <path-to-plugins>/python3.7/site-packages
<plugin-name> = <plugin-module>
```

En la sección `[plugins]`, defina la variable `cli_legacy_plugin_path` y establezca su valor en la ruta de paquetes del sitio de Python en la que se encuentra su módulo de complemento. Después, puede configurar un complemento si proporciona un nombre para el complemento (`plugin-name`) y el nombre de archivo del módulo Python (`plugin-module`) que contiene el código fuente de su complemento. La AWS CLI carga cada complemento mediante la importación de su `plugin-module` y la llamada a su función `awscli_initialize`.

Se ha eliminado la compatibilidad con los alias ocultos

AWS CLILa versión 2 de la ya no admite los siguientes alias ocultos que se admitían en la versión 1.

En la tabla siguiente, la primera columna muestra el servicio, el comando y el parámetro que funcionan en todas las versiones, incluida la AWS CLI versión 2. La segunda columna muestra el alias que ya no funciona en la AWS CLI versión 2.

Servicio, comando y parámetro que funcionan	Alias obsoleto
cognito-identity create-identity-pool open-id-connect-provider-arns	open-id-connect-provider-ar-ns
storagegateway describe-tapes tape-arns	tape-ar-ns
storagegateway.describe-tape-archives.tape-arns	tape-ar-ns
storagegateway.describe-vtl-devices.vtl-device-arns	vtl-device-ar-ns
storagegateway.describe-cached-iscsi-volumes.volume-arns	volume-ar-ns
storagegateway.describe-stored-iscsi-volumes.volume-arns	volume-ar-ns
route53domains.view-billing.start-time	iniciar
deploy.create-deployment-group.ec2-tag-set	ec-2-tag-set
deploy.list-application-revisions.s3-bucket	s-3-bucket
deploy.list-application-revisions.s3-key-prefix	s-3-key-prefix
deploy.update-deployment-group.ec2-tag-set	ec-2-tag-set
iam.enable-mfa-device.authentication-code1	authentication-code-1
iam.enable-mfa-device.authentication-code2	authentication-code-2
iam.resync-mfa-device.authentication-code1	authentication-code-1
iam.resync-mfa-device.authentication-code2	authentication-code-2
importexport.get-shipping-label.street1	street-1
importexport.get-shipping-label.street2	street-2
importexport.get-shipping-label.street3	street-3
lambda.publish-version.code-sha256	code-sha-256
lightsail.import-key-pair.public-key-base64	public-key-base-64

Servicio, comando y parámetro que funcionan	Alias obsoleto
opsworks.register-volume.ec2-volume-id	ec-2-volume-id

No se admite la opción **`api_versions`** del archivo de configuración

La AWS CLI versión 2 ya no es compatible con la llamada a versiones anteriores de las API de servicio de AWS mediante la opción del archivo de configuración `api_versions`. Todos los comandos de la AWS CLI ahora llaman a la versión más reciente de las API de servicio que son compatibles actualmente con el punto de enlace.

La AWS CLI versión 2 solo usa Signature v4 para autenticar las solicitudes de Amazon S3

La AWS CLI versión 2 no admite algoritmos de firma anteriores para autenticar criptográficamente las solicitudes de servicio enviadas a los puntos de conexión de Amazon S3. Esta firma se produce automáticamente con cada solicitud de Amazon S3 y solo se admite el proceso de firma de Signature versión 4. No puede configurar la versión de la firma. Todas las URL firmadas previamente de los buckets de Amazon S3 ahora solo utilizan SigV4 y tienen una duración máxima de caducidad de una semana.

La AWS CLI versión 2 es más coherente con los parámetros de paginación

En la AWS CLI versión 1, si se especifican los parámetros de paginación en la línea de comandos, la paginación automática se desactiva del modo previsto. No obstante, al especificar los parámetros de paginación mediante un archivo con el parámetro `--cli-input-json`, no se desactivaba la paginación automática, lo que podía dar lugar a una salida inesperada. La AWS CLI versión 2 desactiva la paginación automática independientemente de cómo se proporcionen los parámetros.

La AWS CLI versión 2 proporciona códigos de retorno más coherentes en todos los comandos

La AWS CLI versión 2 es más coherente en todos los comandos y devuelve correctamente un código de salida adecuado en comparación con la AWS CLI versión 1. También hemos añadido los códigos de salida 252, 253 y 254. Para obtener más información sobre los códigos de salida, consulte the section called “Códigos de devolución”.

Si tiene una dependencia de cómo la AWS CLI versión 1 utiliza valores de código de devolución, le recomendamos que consulte los códigos de salida para asegurarse de que obtiene los valores que espera.

Instalación de la versión 2 de la AWS CLI a partir de la versión 1 de la AWS CLI

En este tema se ofrecen instrucciones para migrar desde la AWS CLI versión 1 a la AWS CLI versión 2.

Las versiones 1 y 2 de la AWS CLI utilizan el mismo nombre de comando de `aws`. Si tiene ambas versiones instaladas, el equipo utiliza la primera que encuentra en la ruta de búsqueda. Si ha instalado la versión 1 de la AWS CLI anteriormente, le recomendamos que realice una de las siguientes acciones para usar la versión 2 de la AWS CLI:

- Recomendado: desinstale la AWS CLI versión 1 y use solo la AWS CLI versión 2.
- Para tener ambas versiones instaladas, utilice la capacidad de su sistema operativo para crear un enlace simbólico (symlink) o un alias con otro nombre para uno de los dos comandos `aws`.

Para obtener información sobre los cambios notorios entre la versión 1 y la versión 2, consulte the section called “Nuevas características y cambios”.

Reemplazo de la versión 1 por la versión 2

Siga estos pasos para reemplazar la AWS CLI versión 1 por la AWS CLI versión 2.

Para reemplazar la AWS CLI versión 1 por la AWS CLI versión 2

1. Prepare los scripts existentes que tenga para la migración mediante la confirmación de confirmando los cambios importantes entre la versión 1 y la versión 2 en the section called “Nuevas características y cambios”.
2. Desinstale la AWS CLI versión 1 siguiendo las instrucciones de desinstalación correspondientes a su sistema operativo en Instalación, actualización y desinstalación de la AWS CLI versión 1.
3. Confirme que la AWS CLI se ha desinstalado completamente mediante el siguiente comando.

```
$ aws --version
```

Complete uno de los siguientes procesos en función del resultado:

- No se ha devuelto ninguna versión: ha desinstalado correctamente la AWS CLI versión 1 y continúe con el siguiente paso.
- Se ha devuelto una versión: aún tiene una instalación de la AWS CLI versión 1. Para ver los pasos de solución de problemas, consulte the section called “El comando "`aws --version`" devuelve una versión después de desinstalar la AWS CLI”. Realice los pasos de resolución de problemas hasta que no se reciba ninguna salida de versión.

4. Instale la AWS CLI versión 2 siguiendo las instrucciones de instalación adecuadas para su sistema operativo en Instalación o actualización de la versión más reciente de AWS CLI.

Instalación en paralelo

Para tener ambas versiones instaladas, utilice la capacidad de su sistema operativo para crear un enlace simbólico (symlink) o un alias con otro nombre para uno de los dos comandos `aws`.

1. Instale la AWS CLI versión 2 siguiendo las instrucciones de instalación adecuadas para su sistema operativo en Instalación o actualización de la versión más reciente de AWS CLI.
2. Utilice la capacidad de su sistema operativo para crear un enlace simbólico (symlink) o un alias con otro nombre para uno de los dos comandos `aws`, por ejemplo, use *`aws2`* para la AWS CLI versión 2. A continuación, se muestran ejemplos de enlaces simbólicos para la AWS CLI versión 2. Reemplace el valor de *PATH* por su ubicación de instalación.

   Linux and macOS

   Puede usar un enlace simbólico o un alias en Linux y macOS.

   ```
   $ alias aws2='PATH'
   ```

   Windows command prompt

   `DOSKEY` en Windows.

   ```
   C:\> doskey aws2=PATH
   ```

Uso del modo de depuración de actualizaciones para actualizar la versión 1 de AWS CLI a la versión 2 de AWS CLI

Recomendamos a los usuarios de la versión 1 de AWS CLI que actualicen a la versión 2 de AWS CLI para acceder a las nuevas características y al rendimiento mejorado. Hay cambios de comportamiento entre la versión 1 de AWS CLI y la versión 2 de AWS CLI que pueden requerir que actualice los scripts o comandos para conseguir el mismo comportamiento. El modo de depuración de actualizaciones de la versión 1 de AWS CLI genera advertencias cuando se utilizan características que tienen un comportamiento diferente en la versión 2 de AWS CLI. Esta característica mejora la experiencia de actualización al detectar automáticamente cuáles de los comandos de la versión 1 de AWS CLI deben modificarse antes de actualizar a la versión 2 de AWS CLI para evitar problemas inesperados.

Para obtener más información, consulta Cambios importantes entre la AWS CLI versión 1 y la AWS CLI versión 2.

Al actualizar de la versión 1 a la versión 2 de AWS CLI, es posible que Cambios importantes entre la AWS CLI versión 1 y la AWS CLI versión 2 afecte a los scripts y flujos de trabajo existentes. El modo de depuración de actualizaciones lo ayuda a identificar estos problemas antes de completar la migración.

El modo de depuración de actualizaciones detecta cuándo se utilizan características que tienen cambios importantes en la versión 2 de AWS CLI. Cuando ejecuta un comando que se interrumpe tras la actualización, el modo muestra una advertencia con los pasos específicos para solucionar el problema. Esto ahorra tiempo al encontrar automáticamente los posibles problemas en lugar de buscar manualmente en el código.

Funcionamiento

Si está habilitado, el modo de depuración de actualizaciones detecta el uso de características que se actualizaron con cambios importantes en la versión 2 de AWS CLI. Si utiliza uno de los comandos o características mostrados en nuestro Cambios importantes entre la AWS CLI versión 1 y la AWS CLI versión 2 después de actualizar a la versión 2 de AWS CLI, aparecerá una advertencia en el resultado. La detección de cambios importantes se basa en el comando utilizado, los argumentos proporcionados, el entorno de ejecución (por ejemplo, las variables de entorno, los ajustes de configuración, etc.) y, en algunos casos, el contenido o la configuración de los recursos de la cuenta de AWS que se está utilizando.

En el siguiente ejemplo, se muestra el aspecto de estas advertencias. Este comando muestra un ejemplo de advertencia. Todo el texto de advertencia comienza con “AWS CLI V2 UPGRADE WARNING”, seguido del mensaje de advertencia específico. En este caso, se muestra una advertencia porque el comando se basa en la AWS CLI para recuperar el contenido de la URL y usarlo como valor del parámetro `--template-body`, una característica eliminada en la versión 2 de la AWS CLI.

En el siguiente ejemplo se muestra el aspecto de una advertencia:

```
$ aws cloudformation create-stack \
  --stack-name "stack012345" \
  --template-body "https://s3.amazonaws.com/amzn-s3-demo-bucket/template.json"

AWS CLI v2 UPGRADE WARNING: For input parameters that have a prefix of http:// or
https://, AWS CLI v2 will not automatically request the content of the URL for
the parameter, and the `cli_follow_urlparam` option has been removed. See
https://docs.aws.amazon.com/cli/latest/userguide/cliv2-migration-changes.html#cliv2-
migration-paramfile.
```

La siguiente tabla muestra todos los cambios importantes y cómo evitar enfrentarse a un cambio importante en la versión 2 de AWS CLI. Las acciones correctivas que resuelven las advertencias en el modo de depuración aparecen en negrita.

Cambios importantes	En la versión 1, migre al comportamiento de la versión 2	En la versión 2, retenga el comportamiento de la versión 1
Se ha agregado una variable de entorno para establecer la codificación de los archivos de texto	Desactive las variables de entorno **`PYTHONUTF8`** y **`PYTHONIOENCODING`** .	Establezca la variable de entorno **`AWS_CLI_FILE_ENCODING`** con la codificación especificada en la versión 1.
Los parámetros binarios se pasan como cadenas codificadas en base64 de forma predeterminada	Codifique el valor del parámetro con base64. Si el parámetro se carga desde un archivo, codifique el contenido del archivo con base64.	Ajuste la configuración **`cli_binary_format`** en **`raw-in-base64-out`** .

Cambios importantes	En la versión 1, migre al comportamiento de la versión 2	En la versión 2, retenga el comportamiento de la versión 1
Mejora de la gestión de Amazon S3 de las propiedades y etiquetas de los archivos para las copias multiparte	N/A. No se puede migrar al comportamiento de la versión 2 en la versión 1.	Utilice el parámetro `--copy-props none` .
No hay recuperación automática de las URL `http://` o `https://` para los parámetros	Utilice curl (o herramientas alternativas) para descargar el contenido de las direcciones URL a un archivo local. A continuación, cargue el contenido del archivo en el parámetro con file://. Como opción alternativa, configure **`cli_follow_urlparam`** en falso para especificar la URL sin procesar como valor del parámetro.	N/A. Imposible retener el comportamiento de la versión 1 en la versión 2.
Paginador usado para toda la salida de forma predeterminada	N/A. No se puede migrar al comportamiento de la versión 2 en la versión 1.	Establezca la configuración **`cli_pager`** o la variable **`AWS_PAGER`** en una cadena vacía.
Los valores de salida de la marca de tiempo están estandarizados según el formato ISO 8601	Establezca la configuración de **`cli_timestamp`** _format en **`iso8601`**.	Establezca la configuración de **`cli_timestamp_format`** para conectar.
Control mejorado de las implementaciones de CloudFormation que no producen cambios	Use el parámetro **`--no-fail-on-empty-changeset`** .	Utilice el parámetro `--fail-on-empty-changeset` .

Cambios importantes	En la versión 1, migre al comportamiento de la versión 2	En la versión 2, retenga el comportamiento de la versión 1
Se ha cambiado el comportamiento predeterminado del punto de conexión regional de Amazon S3 para la región `us-east-1`	Defina la variable de entorno **`AWS_ENDPOINT_URL_S3`** o la opción de línea de comandos **`--endpoint-url`** en la URL regional us-east-1.	Use la opción de línea de comandos **`--region aws-global`** .
Se ha eliminado `ecr get-login` y se ha reemplazado por `ecr get-login-password`	(1.17.10 o posterior) Use Se ha eliminado **`ecr get-login`** y se ha reemplazado por **`ecr get-login-password`** y canalice el resultado a un comando de docker.	N/A. Imposible retener el comportamiento de la versión 1 en la versión 2.
AWS CLIEl soporte de la versión 2 de la para complementos está cambiando	N/A. No se puede migrar al comportamiento de la versión 2 en la versión 1.	Configure cli_legacy_plugin_path en la sección del archivo de configuración `[plugins]` . Pruebe los complementos en la versión 2, bloquee la versión 2 y pruebe los complementos cada vez que actualice.
Se ha eliminado la compatibilidad con los alias ocultos	Pase de usar el alias oculto obsoleto a Se ha eliminado la compatibilidad con los alias ocultos que funciona en todas las versiones.	N/A. Imposible retener el comportamiento de la versión 1 en la versión 2.

Cambios importantes	En la versión 1, migre al comportamiento de la versión 2	En la versión 2, retenga el comportamiento de la versión 1
No se admite la opción `api_versions` del archivo de configuración	Migre y pruebe el uso de las versiones anteriores de la API a la última versión de la API y elimine api_versions de los ajustes de configuración.	N/A. Imposible retener el comportamiento de la versión 1 en la versión 2.
La AWS CLI versión 2 solo usa Signature v4 para autenticar las solicitudes de Amazon S3	Especifique Signature Version en la versión 4 (consulte Especificación de Signature Version al solicitar la autenticación).	N/A. Imposible retener el comportamiento de la versión 1 en la versión 2.
La AWS CLI versión 2 es más coherente con los parámetros de paginación	Mueva los parámetros de paginación del parámetro JSON de entrada al propio comando.	Elimine los parámetros de paginación del parámetro JSON de entrada.
La AWS CLI versión 2 proporciona códigos de retorno más coherentes en todos los comandos	N/A. No se puede migrar al comportamiento de la versión 2 en la versión 1.	N/A. Imposible retener el comportamiento de la versión 1 en la versión 2.

Limitaciones

Recomendamos encarecidamente a los clientes que revisen nuestro Cambios importantes entre la AWS CLI versión 1 y la AWS CLI versión 2.

Detección de cambios importantes no compatible

La característica del modo de depuración de actualizaciones admite todos los cambios importantes excepto ese La AWS CLI versión 2 proporciona códigos de retorno más coherentes en todos los comandos. Este modo no puede explicar cómo se utilizan los códigos de error devueltos por la AWS CLI posterior.

Detección condicional de cambios importantes

La detección de Los valores de salida de la marca de tiempo están estandarizados según el formato ISO 8601 es el único caso en el que la detección depende del estado de la cuenta de AWS y puede estar sujeta a cambios importantes si los recursos de la cuenta se actualizan más adelante. Si no se incluye ninguna marca temporal en la respuesta de la API del servicio, no se detectará este cambio importante.

Si confía en el formato de marca temporal devuelto por los comandos de la AWS CLI y aún no ha configurado la AWS CLI para que utilice la norma ISO 8601, tome precauciones adicionales para asegurarse de que el procesamiento de la marca temporal no se interrumpa después de actualizar a la versión 2.

Detección de cambios importantes irresolubles

Algunas advertencias generadas por el modo de depuración de actualizaciones no se pueden resolver modificando el comando o el entorno. En los siguientes casos, siempre se emitirán advertencias del modo de depuración de actualizaciones, siempre que se utilice la característica correspondiente:

- AWS CLIEl soporte de la versión 2 de la para complementos está cambiando: si confía en complementos en el archivo de configuración, el modo de depuración de la actualización siempre generará una advertencia que no se podrá resolver. Este modo no puede garantizar que alguno de los complementos funcione en la versión 2 de AWS CLI.
- Mejora de la gestión de Amazon S3 de las propiedades y etiquetas de los archivos para las copias multiparte : si `aws s3` se utiliza para realizar una copia de Amazon S3 de bucket a bucket, el modo de depuración de actualizaciones siempre generará una advertencia que no se puede resolver.

Detecciones falsas

Las advertencias emitidas por el modo de depuración de la actualización no garantizan que se produzcan cambios importantes tras la actualización a AWS CLI v2. A continuación, se muestran los casos en los que se generarían advertencias al actualizar el modo de depuración, a pesar de que no se haya ingresado ningún cambio importante en la AWS CLI v2:

- Se ha agregado una variable de entorno para establecer la codificación de los archivos de texto: si se especifican las variables de entorno `PYTHONUTF8` y `PYTHONIOENCODING` para configurar

la codificación del archivo de texto y la codificación especificada ya coincide con la configuración local instalada, la advertencia podría ser una detección falsa, ya que el modo de depuración no comprueba si la codificación coincide con la configuración local instalada.

- Mejora de la gestión de Amazon S3 de las propiedades y etiquetas de los archivos para las copias multiparte : si `aws s3` se utiliza para realizar una copia de Amazon S3 de bucket a bucket y la copia no es multiparte debido a que el objeto de origen está por debajo del tamaño del umbral multiparte, se generará una falsa detección.
- Los valores de salida de la marca de tiempo están estandarizados según el formato ISO 8601: si el ajuste de configuración cli_timestamp_format está establecido en conectar (predeterminado) y el servicio devuelve una marca temporal en formato ISO 8601.
- Control mejorado de las implementaciones de CloudFormation que no producen cambios: si el indicador `--fail-on-empty-changeset` se utiliza con el comando `aws cloudformation deploy` y el conjunto de cambios resultante está vacío, se mostrará una detección falsa. Además, si el conjunto de cambios no está vacío y no se utiliza `--no-fail-on-empty-changeset`, se mostrará una detección falsa.
- Se ha cambiado el comportamiento predeterminado del punto de conexión regional de Amazon S3 para la región `us-east-1`: si se utiliza `aws s3` o `aws s3api` para realizar una operación de Amazon S3, y la región está configurada en `us-east-1`, la configuración de `s3.us_east_1_regional_endpoint` no está configurada como regional y el punto de conexión global de Amazon S3 se utiliza para la solicitud debido a los ajustes de configuración de punto de conexión, la advertencia podría ser una detección falsa, ya que el modo de depuración no comprueba los ajustes de punto de conexión configurados.

Configuración del modo de depuración de actualizaciones

Puede habilitar o desactivar el modo de depuración de actualizaciones mediante los siguientes métodos, mostrados según el orden de prioridad:

- Las opciones de línea de comandos habilitan o desactivan el modo de depuración de actualizaciones para un solo comando. Utilice --v2-debug para utilizar el modo de depuración de actualizaciones.
- Las variables de entorno usan la variable AWS_CLI_UPGRADE_DEBUG_MODE.

Desinstalación de la versión 2 de AWS CLI

En este tema, se describe cómo desinstalar la versión 2 de AWS Command Line Interface (versión 2 de AWS CLI).

Instrucciones de desinstalación de la versión 2 de AWS CLI:

Linux

Para desinstalarla, siga el mismo método que ha utilizado para instalar la AWS CLI.

Command line installer

Para desinstalar la versión 2 de la AWS CLI, ejecute los siguientes comandos.

1. Busque el enlace simbólico y las rutas de instalación.

   - Utilice el comando `which` para encontrar el enlace simbólico. Se muestra la ruta que utilizó con el parámetro `--bin-dir`.

     ```
     $ which aws
     /usr/local/bin/aws
     ```

   - Utilice el comando `ls` para buscar el directorio al que apunta el enlace simbólico. Esto le da la ruta que utilizó con el parámetro `--install-dir`.

     ```
     $ ls -l /usr/local/bin/aws
     lrwxrwxrwx 1 ec2-user ec2-user 49 Oct 22 09:49 /usr/local/bin/aws -> /usr/local/aws-cli/v2/current/bin/aws
     ```

2. Elimine los dos enlaces simbólicos del directorio `--bin-dir`. Si su usuario tiene permiso de escritura en estos directorios, no es necesario que utilice `sudo`.

   ```
   $ sudo rm /usr/local/bin/aws
   $ sudo rm /usr/local/bin/aws_completer
   ```

3. Elimine directorio `--install-dir`. Si su usuario tiene permiso de escritura en este directorio, no es necesario que utilice `sudo`.

   ```
   $ sudo rm -rf /usr/local/aws-cli
   ```

4. (Opcional) Elimine el SDK de AWS compartido e información de configuración de AWS CLI en la carpeta `.aws`.

   > **Warning**
   >
   > Estos ajustes de configuración y credenciales se comparten en todos los SDK de AWS y AWS CLI. Si elimina esta carpeta, ningún SDK de AWS que todavía sigue en el sistema podrá acceder a ella.

   La ubicación predeterminada de la carpeta `.aws` difiere entre plataformas, de forma predeterminada la carpeta se encuentra en *`~/.aws/`*. Si su usuario tiene permiso de escritura en este directorio, no es necesario que utilice `sudo`.

   ```
   $ sudo rm -rf ~/.aws/
   ```

Snap

Proporcionamos una versión oficial de AWS compatible de la AWS CLI en `snap`. Si ha usado `snap` para instalar la AWS CLI, siga estos pasos:

1. Ejecute el siguiente comando `snap remove` para la AWS CLI.

   ```
   $ snap remove aws-cli --classic
   ```

   Si ha usado `sudo` para instalar la AWS CLI, tendrá que añadirlo al comando.

   ```
   $ sudo snap remove aws-cli --classic
   ```

2. Es posible que deba reiniciar la ventana del símbolo del sistema o el equipo para eliminar todos los archivos.
3. (Opcional) Elimine el SDK de AWS compartido e información de configuración de AWS CLI en la carpeta `.aws`.

> **Warning**
>
> Estos ajustes de configuración y credenciales se comparten en todos los SDK de AWS y AWS CLI. Si elimina esta carpeta, ningún SDK de AWS que todavía sigue en el sistema podrá acceder a ella.

La ubicación predeterminada de la carpeta `.aws` difiere entre plataformas, de forma predeterminada la carpeta se encuentra en *~/.aws/*. Si su usuario tiene permisos de escritura en este directorio, no es necesario que utilice `sudo`.

```
$ sudo rm -r ~/.aws/
```

macOS

Para desinstalar la versión 2 de la AWS CLI, ejecute los siguientes comandos sustituyendo las rutas que utilizó en la instalación. Los comandos de ejemplo utilizan las rutas de instalación predeterminadas.

1. Busque la carpeta que contiene los enlaces simbólicos al programa principal y al completer.

   ```
   $ which aws
   /usr/local/bin/aws
   ```

2. Con esa información, ejecute el siguiente comando para buscar la carpeta de instalación a la que apuntan los enlaces simbólicos.

   ```
   $ ls -l /usr/local/bin/aws
   lrwxrwxrwx 1 ec2-user ec2-user 49 Oct 22 09:49 /usr/local/bin/aws -> /usr/local/
   aws-cli/aws
   ```

3. Elimine los dos enlaces simbólicos de la primera carpeta. Si su usuario ya tiene permisos de escritura en estas carpetas, no es necesario que utilice `sudo`.

   ```
   $ sudo rm /usr/local/bin/aws
   $ sudo rm /usr/local/bin/aws_completer
   ```

4. Elimine la carpeta de instalación principal. Use `sudo` para obtener acceso de escritura a la carpeta `/usr/local`.

```
$ sudo rm -rf /usr/local/aws-cli
```

5. (Opcional) Elimine el SDK de AWS compartido e información de configuración de AWS CLI en la carpeta `.aws`.

> **Warning**
>
> Estos ajustes de configuración y credenciales se comparten en todos los SDK de AWS y AWS CLI. Si elimina esta carpeta, ningún SDK de AWS que todavía sigue en el sistema podrá acceder a ella.

La ubicación predeterminada de la carpeta `.aws` difiere entre plataformas, de forma predeterminada la carpeta se encuentra en *~/.aws/*. Si su usuario tiene permiso de escritura en este directorio, no es necesario que utilice `sudo`.

```
$ sudo rm -rf ~/.aws/
```

Windows

1. Abra Programas y características mediante una de las siguientes acciones:
   - Abra el Panel de control y elija Programas y características.
   - Abra un símbolo del sistema y, a continuación, escriba el comando siguiente:

```
C:\> appwiz.cpl
```

2. Seleccione la entrada denominada AWS Command Line Interface y elija Desinstalar para iniciar el desinstalador.
3. Confirme que desea desinstalar la AWS CLI.
4. (Opcional) Elimine el SDK de AWS compartido e información de configuración de AWS CLI en la carpeta `.aws`.

> **Warning**
>
> Estos ajustes de configuración y credenciales se comparten en todos los SDK de AWS y AWS CLI. Si elimina esta carpeta, ningún SDK de AWS que todavía sigue en el sistema podrá acceder a ella.

La ubicación predeterminada de la carpeta `.aws` difiere entre plataformas, de forma predeterminada la carpeta se encuentra en *`%UserProfile%\.aws`*.

```
$ rmdir %UserProfile%\.aws
```

Solución de errores de instalación y desinstalación de AWS CLI

Si se encuentra con problemas después de instalar o desinstalar la AWS CLI, consulte en the section called “Errores de solución de problemas” los pasos para la solución de problemas. Para conocer los pasos más relevantes de la solución de problemas, consulte the section called “Errores de comando no encontrado”, the section called “El comando "`aws --version`" devuelve una versión diferente a la instalada” y the section called “El comando "`aws --version`" devuelve una versión después de desinstalar la AWS CLI”.

Historial de la documentación de la guía del usuario de AWS CLI

En la siguiente tabla se describen los cambios importantes de la Guía del usuario de AWS Command Line Interface, a partir de enero de 2019. Para obtener notificaciones sobre las actualizaciones de esta documentación, puede suscribirse a la fuente RSS.

Cambio	Descripción	Fecha
Se ha agregado compatibilidad con puntos de conexión basados en cuentas a la versión 2 de la AWS CLI	Los puntos de conexión basados en cuentas que utilizan el ID de cuenta de AWS ahora son compatibles con la versión 2 de la AWS CLI.	20 de marzo de 2025
Se ha agregado compatibilidad con puntos de conexión basados en cuentas a la versión 1 de la AWS CLI	Los puntos de conexión basados en cuentas que utilizan el ID de cuenta de AWS ahora son compatibles con la versión 2 de la AWS CLI.	24 de febrero de 2025
Información de credenciales y autenticación actualizada.	Instrucciones y ejemplos de credenciales y métodos de autenticación actualizados. Esto incluye la actualización de las páginas de introducción y de configuración pertinentes. Para dar cabida a este aumento de la documentación, los temas relevantes de las credenciales se trasladaron a la nueva sección Autenticación y credenciales de acceso.	31 de marzo de 2023

Configuración del proveedor de tokens con actualización automática de autenticación para AWS IAM Identity Center agregado	El nuevo proceso para configurar la AWS CLI para autenticar a los usuarios con AWS IAM Identity Center (Centro de identidades de IAM) con la configuración del proveedor de tokens de SSO, que puede recuperar automáticamente los tokens de autenticación actualizados.	7 de diciembre de 2022
Se lanzó la imagen Amazon ECR Public oficial para la AWS CLI versión 2	Se lanzó la imagen Amazon ECR Public con asistenci a oficial para la AWS CLI versión 2 para Linux, macOS y Windows.	18 de noviembre de 2022
Se actualizó la guía para migrar desde AWS CLI V1 a V2	Se amplió la guía de cambios de última hora para incluir instrucciones de migración a fin de pasar de la versión 1 de AWS CLI a la versión 2 de AWS CLI. Incluye actualiza ciones a la página de Solución de problemas para ayudar con los problemas de instalación.	13 de mayo de 2022
Nuevo proceso para crear un instalador de la AWS CLI desde el código fuente.	Nuevo proceso para instalar o actualizar desde el origen la última versión de la AWS CLI en sistemas operativos compatibles.	17 de febrero de 2022

El contenido de la V1 y V2 de AWS CLI ahora están separados en sus respectivas guías	Para mayor claridad y facilidad , la versión 1 de AWS CLI y la versión 2 de AWS CLI ahora están separadas en sus propias guías. Para la versión 1 de AWS CLI, consulte la Guía del usuario de la versión 1 de AWS CLI. más reciente	2 de noviembre de 2021
Se ha agregado información de alias de AWS CLI	Se añadió información de alias de la AWS CLI. Los alias son accesos directos que se pueden crear en la AWS Command Line Interface (AWS CLI) para acortar los comandos o los scripts que utiliza con frecuencia.	11 de marzo de 2021
Se actualizó la información de salida del filtro	Se actualizó la información de los filtros y se trasladó a su propia página.	1 de febrero de 2021
Se ha agregado información para asistentes	Se añadió información sobre el asistente de la versión 2 de la AWS CLI.	20 de noviembre de 2020
Se ha actualizado el mensaje automático	Se actualizó la información del mensaje automático de la versión 2 de la AWS CLI con las características actuales.	10 de noviembre de 2020
Se ha agregado un ejemplo de scripting de Amazon S3	Se agregó un ejemplo de scripting del ciclo de vida de Amazon S3.	15 de octubre de 2020
Se ha agregado un ejemplo de scripting de Amazon EC2	Se agregó un ejemplo de scripting de tipo de instancia de Amazon EC2.	15 de octubre de 2020

Se ha agregado información de reintentos	Se agregó una página de reintentos para las caracterí sticas y el comportamiento de los reintentos en la AWS CLI.	17 de septiembre de 2020
Página de paginación en el cliente y en el servidor	Se actualizó la información de paginación y se centralizó en una sola página.	17 de agosto de 2020
Se actualizó la página de comandos de S3	Se actualizó la página de comandos s3 de alto nivel con nuevos ejemplos y recursos.	30 de julio de 2020
Información de instalación actualizada	Se ha actualizado la informaci ón de instalación, actualiza ción y desinstalación de Linux, macOS y Windows.	19 de mayo de 2020
Se ha agregado informaci ón para la codificación de archivos de texto en la versión 2 de AWS CLI	De forma predeterminada, la versión 2 de la AWS CLI utiliza la misma codificación de archivo de texto que la configuración local. Ahora puede usar variables de entorno para establecer la codificación de archivos de texto.	14 de mayo de 2020
Se ha lanzado la imagen oficial de Docker para la versión 2 de AWS CLI	Se lanzó la imagen de Docker con soporte oficial para la versión 2 de la AWS CLI para Linux, macOS y Windows.	31 de marzo de 2020
Se ha agregado información sobre los buscapersonas del lado del cliente para la versión 2 de AWS CLI	De forma predeterminada, la versión 2 de la AWS CLI utiliza el programa de paginador `less` para todos los resultado s del lado del cliente.	19 de febrero de 2020

AWS Command Line Interface (AWS CLI) versión 2 se ha lanzado oficialmente	La versión 2 de la AWS CLI está disponible en general y es la versión de instalación recomendada para los clientes.	10 de febrero de 2020
Ahora el instalador de macOS para la versión 2 de AWS CLI es un archivo `.pkg` para el instalador de Apple Package.	Se ha actualizado el instalador de macOS de la versión 2 de la AWS CLI, pasando de un archivo `.zip` con script de shell a un paquete de instalador de macOS completo. Esto simplifica la instalación y la hace compatible con las versiones más recientes de macOS.	3 de febrero de 2020
Se ha agregado contenido para el control predeterminado mejorado de los puntos de conexión regionales de S3 y STS por parte de AWS CLI versión 2	De forma predeterminada, AWS CLI versión 2 ahora dirige las solicitudes de los servicios de Amazon S3 y AWS STS al punto de conexión regional configurado actualmente en lugar de al punto de conexión global.	13 de enero de 2020
Lanzamiento de la vista previa del desarrollador para la versión 2 de AWS CLI	Anuncio de la vista previa de la versión 2 de la AWS CLI. Se han agregado instrucciones sobre la instalación de la versión 2. Se ha agregado el tema sobre migración para analizar las diferencias entre las versiones 1 y 2.	7 de noviembre de 2019

Se ha agregado compatibilidad para perfiles con nombre de AWS IAM Identity Center a AWS CLI	La versión 2 de la AWS CLI agrega compatibilidad para crear un perfil con nombre que puede iniciar sesión directamente en IAM Identity Center y obtener credenciales temporales de AWS para su uso posterior en comandos de la AWS CLI.	7 de noviembre de 2019
Nueva sección de MFA	Se ha añadido una nueva sección que describe cómo obtener acceso a la CLI mediante la autenticación multifactor y los roles.	3 de mayo de 2019
Se ha actualizado la sección "Uso de la CLI"	Se han mejorado y añadido instrucciones y procedimientos de uso.	7 de marzo de 2019
Se ha actualizado la sección "Instalación de la CLI"	Se han mejorado y agregado instrucciones y procedimientos de instalación de la AWS CLI.	7 de marzo de 2019
Se ha actualizado la sección "Configuración de la CLI"	Se han mejorado y agregado instrucciones y procedimientos de configuración de la AWS CLI.	7 de marzo de 2019